CENTRO UNIVERSITÁRIO DE BRASÍLIA -UniCEUB

CURSO DE ENGENHARIA DE COMPUTAÇÃO

LEONARDO CONDE DOS SANTOS

CONVERGÊNCIA ENTRE IPv4 E IPv6

Brasília

Junho, 2013

LEONARDO CONDE DOS SANTOS

CONVERGÊNCIA ENTRE IPv4 E IPv6

Projeto final apresentado ao Centro Universitário de Brasília (UniCEUB) como pré-requisito para a obtenção de Certificado de Conclusão de Curso de Engenharia de Computação.

Orientador: Prof. MsC Francisco Javier de Obaldía Díaz.

Brasília

Junho, 2013

LEONARDO CONDE DOS SANTOS

CONVERGÊNCIA ENTRE IPv4 E IPv6

Projeto final apresentado ao Centro Universitário de Brasília (UniCEUB) como pré-requisito para a obtenção do Certificado de Conclusão de Curso de Engenharia de Computação.

Este trabalho foi julgado adequado para a obtenção do título de Engenheiro de Computação e aprovado em sua forma final pela Faculdade de Tecnologia e Ciências Sociais Aplicadas - FATECS.

_____

Prof. Abiezer Amarilia Fernandes

Coordenador do Curso

Banca Examinadora:

_____

MsC Eliomar Araújo de Lima.

UniCEUB

_____

MsC Luís Cláudio Lopes de Araújo

UniCEUB.

_____

MsC Francisco Javier de Obaldía Díaz.

Orientador

_____

MsC Marco Antônio Araújo.

UniCEUB

AGRADECIMENTOS

À minha família por incentivar meu crescimento profissional.

Aos meus amigos e esposa, pelo incentivo, apoio e pelas conversas estimulantes sobre o presente e o futuro. À minha inspiração Ana Clara, amada filha.

Ao professor Francisco Javier, pela atenção e bom humor em todos os momentos de orientação.

Aos professores especiais, como Luiz Cláudio e Gil Renato, que me fizeram acreditar nesta formação.

Meus agradecimentos também ao instrutor da CISCO Elvio de Sousa que, com paciência e amizade, me ensinou muito sobre a profissão.

RESUMO

Com o esgotamento do protocolo de rede IPv4, surge a necessidade de se substituir esse protocolo pelo IPv6. Para tanto, este trabalho abordará a substituição destes protocolos apresentando as características de cada um deles, juntamente com as técnicas de tradução, tunelamento e pilha dupla. A partir de um cenário, com melhor entendimento das principais técnicas de transição, serão apresentadas as características e as diferenças entre os endereçamentos IPv4 e IPv6. Após verificação das suas diferenças e incompatibilidade, serão implementadas técnicas de transição visando à total convergência entre as duas versões do protocolo IP.

Palavras Chave: IPv4, IPv6, migração, internet.

ABSTRACT

With the depletion of the IPv4 network protocol arises the need to replace the IPv6. Therefore, this paper will address the replacement of these protocols presenting the features of each, along with the techniques of translation, tunneling and dual stack. From a scenario, with better understanding of the major technical transition, will be presented the characteristics and differences between IPv4 and IPv6 addresses. After verification of their differences and incompatibility will be implemented techniques transition toward full convergence between the two versions of IP protocol.

Keywords: IPv4, IPv6, migration, internet.

LISTA DE FIGURAS

LISTA DE ABREVIATURAS

ACL	Access Control List
DARPA	Defense Advanced Research Projects Agency (Agência de Pesquisa de Projetos Avançados de Defesa)
DCE	Data Communications Equipment, Data Circuit-terminating Equipment,
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System (Sistema de Nomes de Domínio)
EUI	Extended Unique Interface
IANA	Internet Assigned Numbers Authority
IEEE	Institute of Electrical and Electronic Engineers (Instituto de Engenheiros Eletricistas e Eletrônicos)
IP	Internet Protocol
IPng	IP next generation
IPv4	Internet Protocol Version 4
IPv6	Internet Protocol Version 6
ISATAP	Intra-Site Automatic Tunnel Addressing Protocol
ISP	Internet Service Provider (Provedor de Acesso Internet)
MAC	Medium Access Control
MTU	Maximum Transmission Unit
NA	NeighBor Advertisement
NAT-PT	Network Address Translation - Protocol Translation
ND	NeighBor Discovery
NS	NeighBor Solicitation
QoS	Quality of Service (Qualidade de Serviço)
RA	Router Advertisement
RS	Router Solicitation
TCP	Transmission Control Protocol
TCP/IP	Transmission Control Protocol/Internet Protocol
TOS	Type Of Service (Tipo de Serviço)
TTL	Time To Live (Tempo de Vida)
UDP	User Datagram Protocol

VLAN	Virtual Local Area Network

SUMÁRIO

1 INTRODUÇÃO

1.1. MOTIVAÇÃO

O Protocolo IPv6, conhecido também como IPng (*Internet Protocol next generation),* já é uma realidade, assim como a necessidade de seu conhecimento e sua implementação. Com os novos recursos apresentados pela evolução do protocolo IPv4, o IPv6 apresenta melhorias em segurança, qualidade de serviço, dentre outros. Atualmente, o IPv4 é utilizado pela maioria das empresas em sua estrutura lógica. Mas o que acontecerá quando essas ou novas empresas começarem a utilizar plenamente o IPv6?

Novos serviços sobre IP estão surgindo e se tornando cada vez mais essenciais. E o esgotamento de endereços IPv4 já é fato devido ao crescimento computacional, de serviços e de usuários.

A implementação do IPv6 não excluirá de imediato o IPv4, havendo assim a necessidade de convergência entre os dois protocolos. Ao mesmo tempo, com o esgotamento do IPv4, a versão 6 será, por enquanto, a única solução para novas empresas.

A motivação deste trabalho é demonstrar e aplicar técnicas de convergência entre os dois protocolos IPv4 e IPv6. O desafio é atestar que os dois protocolos podem coexistir. Muitas pessoas não têm o conhecimento de como funciona essa transição. Para tanto, serão demonstradas e esclarecidas algumas das principais técnicas.

1.2. OBJETIVOS DO TRABALHO

O conhecimento e aplicação dessas técnicas de transição já se fazem necessários. Este trabalho visa analisar duas empresas fictícias, uma com rede IPv4 e outra com rede IPv6, sendo que a primeira trocará informações com a segunda empresa. A proposta é evidenciar a total convergência entre os dois protocolos, tendo como objetivo demonstrar de maneira

prática a possibilidade de se migrar e utilizar uma rede sobre IPv6, garantindo total conexão com outras redes independentemente da versão do protocolo IP utilizado.

Através de técnicas de transição será mostrado como funciona a tradução, tunelamento e pilha dupla. A implementação das três técnicas é devido à necessidade de convergência entre os dois protocolos.

Com a solução apresentada será possível trafegar de uma rede para outra livremente, atendendo assim o requisito de interoperabilidade necessária para as empresas.

1.3. JUSTIFICATIVA E IMPORTÂNCIA DO TRABALHO

Através da solução apresentada, o trabalho demonstrará que os dois protocolos – IPv4 e IPv6 – podem coexistir através de técnicas de transição. Apesar de conhecidas, essas técnicas não são aplicadas e difundidas na maioria das empresas, pois estas ainda não se preocupam com a real necessidade de comunicação e convergência com estabelecimentos que utilizam o protocolo IPv6.

Entretanto, as empresas podem e devem aplicar essas técnicas na atualidade. Aliás, é possível aplicá-las de forma gradual sem que haja necessidade de parar o serviço em operação. O presente trabalho salienta que essa mudança deve ser imediata, não podendo ser mais postergada.

O conhecimento desta solução é de suma importância não só para os profissionais de redes e infraestrutura, como também para estudantes e pesquisadores. Alcançar todos os objetivos servirá como alicerce para a implementação da solução mediante o problema apresentado.

1.4. ESCOPO DO TRABALHO

O escopo do projeto consiste em disponibilizar uma solução para convergência entre os protocolos IP utilizando a plataforma da CISCO. O trabalho simulará o funcionamento de duas empresas: uma com IPv4 e outra em IPv6. A primeira será segmentada em VLANs diferentes, endereçada em redes distintas e aplicada uma técnica de NAT, simulando o funcionamento básico da maioria das empresas. A segunda também será segmentada em duas VLANs, sendo a VLAN 6 destinada para o modo STATELESS e a VLAN 60 para o STATEFULL. Todas as interfaces dos roteadores deverão estar com diferentes endereços de redes.

O trabalho também mostrará a aplicação de roteamento dinâmico - tanto em IPv4 quanto em IPv6 - e técnicas de transição de pilha dupla, de tradução (NAT-PT) e de tunelamento (ISATAP).

O escopo do projeto não demonstrará todas as técnicas de tradução e tunelamento devido a sua variedade de soluções. O foco é demonstrar que, com um conjunto de técnicas de transição, é possível haver interoperabilidade entre as duas redes. A solução apresentada utilizará um simulador de redes da CISCO. A aplicação também não abordará todos os serviços existentes em um ambiente de rede como *firewall*, antivírus, dentre outros.

1.5. RESULTADOS ESPERADOS

Com o resultado do projeto desenvolvido, as duas empresas que utilizam protocolos IP diferentes terão total convergência entre elas. Essa troca de informações realizada entre as empresas citadas é extremamente importante porque a solução desenvolvida é voltada para aquelas que só utilizam o protocolo IPv4.

De maneira complementar, as configurações aplicadas permitirão a troca de pacotes e acesso a serviços independentes do protocolo utilizado pela empresa. A solução apresentada está de acordo com as normas de infraestrutura e rede para permitir total harmonia entre as duas versões do protocolo IP.

A convergência entre os protocolos IP só será possível se as configurações forem bem executadas e precisas. Somente desta forma promoverá solução para o bom funcionamento dos seus serviços independentemente do protocolo.

1.6. ESTRUTURA DO TRABALHO

O trabalho desenvolvido ao longo deste projeto encontra-se dividido em seis capítulos dispostos da seguinte forma:

a) **Introdução:** trata do tema abordado, bem como sua relevância. O texto ainda apresenta a justificativa para o desenvolvimento do projeto;
b) **Capítulo 2:** apresenta a contextualização do problema mediante ao cenário atual das tecnologias existentes e aponta problemas enfrentados no mercado;
c) **Capítulo 3:** abrange todo o referencial teórico necessário para a compreensão do que foi desenvolvido;
d) **Capítulo 4**: refere-se à solução projetada, juntamente com a sua explicação e funcionamento;
e) **Capítulo 5:** aborda a implementação juntamente com os testes realizados para o total funcionamento do projeto;
f) **Considerações finais:** conclui o trabalho, avaliando as soluções propostas e o seu cumprimento.

CAPÍTULO 2 - APRESENTAÇÃO DO PROBLEMA

Atualmente o tipo de endereçamento lógico utilizado na Internet está na versão 4 do padrão IP e este por sua vez possuiu um número total de quatro bilhões de endereços. Com o aumento de usuários utilizando computadores, *smartphones* e *tablet* para acessar a Internet, houve um aumento considerável na utilização de endereçamentos IP e, com isso, está ocorrendo um esgotamento gradativo da quantidade de endereços disponíveis para distribuição aos usuários (IPV6.BR, 2012).

A Internet surgiu originalmente para um projeto militar conhecido como *ARPANET*, durante a Guerra Fria (1945-1991), com o objetivo de criar uma rede mundial de comunicação, como uma malha, teia de aranha, onde cada nó iria comunicar-se com o outro nó por caminhos diferentes (IPV6.BR, 2012).

Em 1983 o protocolo TCP/IP de 32 bits (IPv4) foi oficialmente implementado pelos sistemas operacionais. Nessa época não se imaginava que se esgotaria o número de endereços. Contudo, na segunda metade da década de 90, se não fosse por uma série de soluções paliativas, como a separação de endereços públicos e privados (RFC 1918) com as técnicas de DHCP (limitando o período, tempo de vida, do IP), separação de endereços público dos privados combinados com o uso de NAT (poupando endereços internos), os endereços IPv4 já teriam esgotados há muito tempo (TANENBAUM, 2003).

Uma das possíveis causas desse esgotamento foi a divisão desigual de blocos de endereço IP. Antes das regras se tornarem mais rígidas e controladas pela Internet *Assigned Numbers Authority* (IANA), algumas empresas adquiriram bloco /8, ou seja, 16.777.216 endereços. Entretanto, mesmo que houvesse redistribuição mais igualitá, o problema de escassez não seria resolvido, pois: “vivemos um momento de *Internet das coisas*, que permite integrar casas, computadores, eletrodomésticos, enfim todos os eletrônicos que nos cercam e necessitam de um endereço IP para que se estabeleça uma comunicação” (IPV6. BR, 2012).

Desde a sua criação, a Internet foi aprimorada nas universidades com a utilização de *backbone* para a conversa entre professores e com objetivos acadêmicos, ou seja, sem muito tráfego. Nessa época, no entanto, não se imaginava a proporção que iria ter sobre o seu crescimento e popularidade (OLIFER, 2008).

A última estimativa quanto à população mundial foi divulgada em outubro de 2011 e, segundo a Organização das Nações Unidas (ONU), o mundo já ultrapassava sete bilhões de

pessoas. Já o Censo 2010 brasileiro compreendeu um levantamento minucioso de todos os domicílios do Brasil em novembro de 2010, onde apontou que o país tem 190.755.799 habitantes (BUARQUE, 2011).

Nos tempos atuais com o uso comercial da Internet, houve um crescimento inesperado de conexões, o que exigiu a implementação de um novo protocolo (IPv6). Também em 2010, outra pesquisa apontou que, das 2,8 milhões de empresas brasileiras com uma ou mais pessoas ocupadas, cerca de 2,2 milhões (80,8%) utilizaram computador e 2,1 milhões (76,9%) fizeram uso da Internet (RIBEIRO, 2012).

Dados do IBGE também destacaram que, entre 2005 e 2011, a população de 10 anos ou mais de idade cresceu 9,7%, enquanto que o contingente de pessoas nessa faixa etária que utilizaram a Internet aumentou 143,8%.

Para atender essa nova demanda de uso da Internet e a necessidade de se manter conectado através de uma conexão fim-a-fim surge o IPv6, conhecido também como Ipng, que utiliza um espaço de endereçamento maior, permitindo maiores níveis de hierarquia de endereçamento, suporte a undecilhões de *hosts*, maior segurança, maior controle de tráfego entre outras melhorias.

O protocolo IP versão seis foi amplamente modificado para se adaptar ao crescimento acelerado da Internet. O formato e o comprimento dos endereços IP foram alterados, assim como o formato do pacote. Protocolos relacionados, como o ICMP, também foram modificados. Outros protocolos da camada de rede, como ARP, RARP E IGMP, foram excluídos ou incluídos no protocolo ICMPv6. Protocolos de roteamento dinâmico foram ligeiramente modificados, dentre outras melhorias (FOROUZAN, 2010).

Desta forma a migração do IPv4 para o IPv6 torna-se eminente devido à rápida expansão da Internet juntamente com novos serviços, como IP móvel, telefonia IP e outras vantagens em relação ao IPv4 (FOROUZAN, 2010):

a) **Espaço de endereçamentos maior:** O endereço IPv6 tem 128 bits (2^{128}) de comprimento contra 32 bits (2^{32}) do IPv4;

b) **Formato de cabeçalho melhor:** Informações adicionais são inseridas no cabeçalho de base, caso seja necessário utiliza-se cabeçalhos de extensão onde são inseridas informações adicionais nas camadas superiores (aplicação), aumentando a desempenho dos roteadores;

c) **Novas opções:** Funcionalidades adicionais, como *flow control* e QOS;

d) **Margem para ampliação:** O IPv6 é projetado para ser ampliado caso seja necessário ou exigido por novas tecnologias e aplicações;

e) **Suporte para a alocação de recursos:** O campo tipo de serviço foi removido, mas foi adicionado o rótulo de fluxo onde permite que a origem solicite tratamento especial do pacote, permitindo tráfego de vídeo e áudio em tempo real;

f) **Suporte para mais segurança:** As opções de criptografia e autenticação proporcionam maior segurança, confidencialidade e integridade do pacote.

Há tempos ouvimos sobre o fim de IPv4 e a necessidade de migração e implementação do IPv6. Sabe-se que, se não fosse o uso de NAT e a segmentação de IPv4 público de privado, os endereçamentos de IPv4 já estariam esgotados.

Na época em que o protocolo TCP/IP nasceu, um endereço de 32 bits, ou seja, mais de 4 bilhões de endereços, parecia quase impossível utilizar todos os endereços disponíveis, porém não foi o que aconteceu na metade dos anos 90. Nessa época começaram-se estudos sobre o seu esgotamento.

Para solucionar o problema de falta de endereçamento surge o IPv6, uma versão aprimorada do antigo IPv4. A diferença de quantidade de endereços entre as versões do protocolo IP pode ser observada ao compará-los. O IPv4 tem 32 bits e o IPv6 128 bits, ou seja:

a) IPv4 versão de 32 bits, (2^{32}) = 4.294.967.296 endereços (cerca de 4 bilhões);

b) IPv6 versão de 128 bits, (2^{128})= 340.282.366.920.938.463.463.374.607.431.768.211.456 endereços (cerca de 340 undecilhões).

De acordo com a Equipe IPv6.br - acessado em 17 de abril de 2013 - se fosse possível medir o endereçamento IPv6, ele seria capaz de cobrir cada centímetro quadrado da Terra, mas não só isso, cobriria sete camadas de cada centímetro quadrado do nosso planeta.

A infraestrutura da grande maioria das empresas ainda usa a tecnologia sob IPv4 e demorará em trabalhar totalmente sob o protocolo IPv6. Atualmente teremos duas redes em paralelo. Neste ponto surge a preocupação: como fazer com que as duas redes tenham uma convergência entre elas? Se a rede do usuário é IPv4, como fará para se comunicar com a rede em IPv6, ou vice-versa?

Diante do exposto, será abordado neste trabalho a substituição do IPv4 pelo IPv6 e apresentadas as características de cada protocolo e análise final de um projeto baseado em IPv4 que será migrado para IPv6. Será utilizado um cenário com roteadores e switchs.

CAPÍTULO 3 - REFERENCIAL TEÓRICO

O desenvolvimento do projeto utiliza vários conceitos de rede, protocolos, infraestrutura, roteadores, *switchs* e servidores. Para que haja convergência das versões do protocolos IP é necessário o entendimento destes conceitos e aplicá-los corretamente para o completo funcionamento entre as duas redes, IPv4 e IPv6.

3.1 HISTÓRICO DO PROTOCOLO TCP/IP

O surgimento do protocolo TCP/IP (Transmission Control Protocol / Internet Protocol) deveu-se à necessidade de comunicação do exército americano com outros setores do governo, durante a Guerra Fria, com os trabalhos realizado pelo DARPA (*Defense Advanced Research Projects Agency*) dos Estados Unidos que constituiu a ARPAnet, posteriormente se desmembrou em ARPAnet, destinado para pesquisas e MILNET para instituições militares. O protocolo TCP/IP permitiu que pequenas redes do exército Americano fossem interligadas. Com o tempo, o número de redes interligadas foi crescendo, gerando o que atualmente é conhecida como Internet (BURGESS, 2006).

O TCP/IP é uma pilha de protocolos: o IP é responsável pelo endereçamento e o TCP da transmissão de dados e correção de erros. Ele segmenta a rede em pequenas redes independentes e são interligadas por roteadores, de modo que caso uma das conexões seja perdida a rede permanece intacta (CISCO, 2013).

Após o aumento de número de conexões devido à sua popularidade e número de usuários da Internet, o TCP/IP tornou-se a arquitetura padrão de uso. Desta forma computadores que utilizavam protocolos diferentes não podiam se comunicar entre si e nem trocar informações. Antes da sua padronização e utilização, os protocolos mais utilizados nas redes das empresas eram: TCP/IP NETBEUI e o IPX/SPX Apple Talk (OLIFER, 2008).

O sistema operacional UNIX sempre utilizou o protocolo TCP/IP como padrão, devido à implementação de baixo custo feita pelo DARPA no sistema, como forma de encorajar os pesquisadores universitários a adotar o protocolo. O *Windows* sempre deu suporte ao TCP/IP

desde as suas primeiras versões, mas o protocolo somente tornou-se padrão a partir do Windows 2000. (TANENBAUM, 2003)

Atualmente o protocolo utilizado nas empresas é o IPv4, sendo que as novas versões de sistemas operacionais já dão suporte ao IPv6.

3.2 ARQUITETURA TCP/IP

O modelo TCP/IP é composto por quatro camadas e embora o seu conjunto de protocolos tenha sido desenvolvido antes da definição do modelo OSI, a funcionalidade dos protocolos da camada de aplicação TCP/IP se ajusta à estrutura das três camadas superiores do modelo OSI: camadas de Aplicação, Apresentação e Sessão. (CISCO, 2013). A figura 3.1 mostra a comparação em termos das camadas.

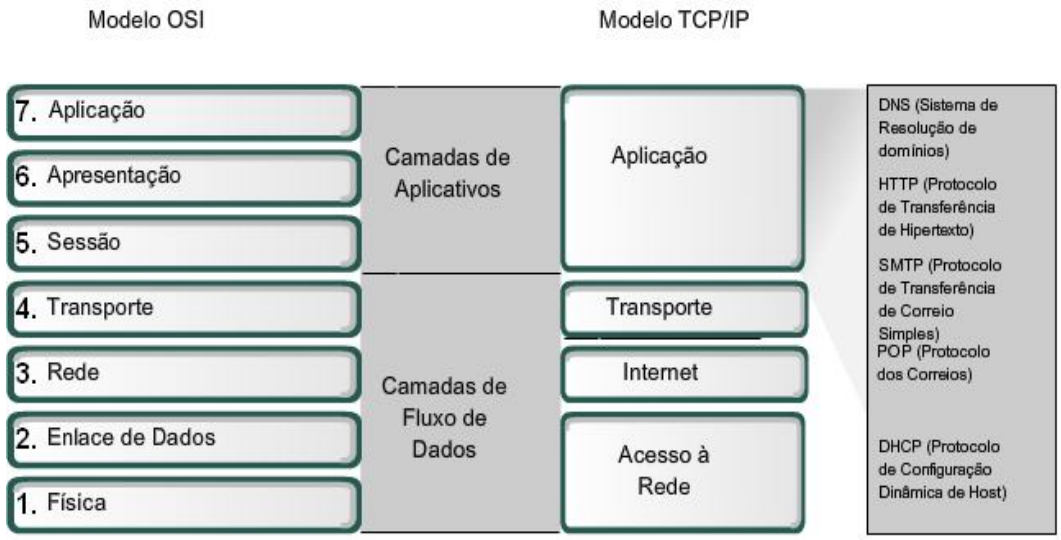

Figura 3.1 - Descrição do protocolo TCP/IP.
Fonte: CISCO, 2013

As camadas do modelo TCP/IP são:

a) **Aplicação:** fornece a interface entre as aplicações que utilizamos para comunicação e a rede subjacente pelas quais nossas mensagens são transmitidas. Os protocolos da camada de aplicação são utilizados para troca de dados entre programas executados nos *hosts* de origem e de destino (CISCO, 2013);

b) **Transporte:** prepara os dados de aplicativos para o transporte através da rede e processa os dados da rede para o uso pelos aplicativos. Proporciona a segmentação de dados e o controle necessário para reagrupar esses segmentos em fluxos de comunicação. Realiza esse processo através do rastreamento da comunicação individual entre as aplicações nos *hosts* de origem e destino, segmentando os dados e gerenciando cada segmento, reagrupando os segmentos em fluxos de dados de aplicação e Identificando as diferentes aplicações. São dois os protocolos dessa camada: o TCP (*Transmission Control Protocol*), que é orientado a conexão e garante a entrega dos dados, na ordem correta; e UDP (*User Datagram Protocol*), que opera no modo sem conexão e fornece um serviço datagrama não-confiável (SOARES , 1995);

c) **Rede:** Fornece serviços para realizar trocas de fragmentos individuais de dados na rede entre dispositivos finais identificados. Para realizar o transporte de uma ponta à outra utiliza os processos de endereçamento, encapsulamento, roteamento e desencapsulamento. Os protocolos implementados nessa camada são: Internet Protocol version 4 (IPv4), Internet Protocol version 6 (IPv6), Novell Internetwork Packet Exchange (IPX), AppleTalk e Connectionless Network Service (CLNS/DECNet) (CISCO, 2013);

d) **Acesso à Rede:** Consiste de rotinas de acesso à rede física. A camada de Interface de Rede interage com o *hardware*, permitindo que as demais camadas sejam independentes do hardware utilizado (COMER, 2003; SOARES, 1995). Define como o cabo está conectado à placa de rede, como por exemplo o tipo de conector e quais pinos serão utilizados. Ela também define qual técnica de transmissão será utilizada para enviar os dados para o cabo da rede. Essa camada corresponde às camadas 1 e 2 do modelo OSI.

3.3 IPv4

Os serviços da camada de rede implementados pelo conjunto dos protocolos TCP/IP constituem o Internet Protocol (IP). Atualmente, a versão 4 do IP (IPv4) é a mais utilizada.

Este é o único protocolo da camada 3 usado para levar dados de usuários através da Internet. As características básicas do IPv4 são (CISCO, 2013):

a) Sem conexão – A conexão não é estabelecida antes do envio dos pacotes de dados. Os pacotes IP são enviados sem notificar que estão chegando para o host final. A entrega de pacotes sem conexão pode resultar na chegada fora de sequência aos pacotes de destino. Se a entrega de pacotes foi feita fora de ordem ou ocorreu a falta de pacotes, isso criará problemas para a aplicação que usará os dados, os serviços das camadas superiores terão que resolver estas questões;

b) Melhor Esforço (não confiável) - Nenhum cabeçalho é usado para garantir a entrega dos pacotes. O IP não possui a capacidade de gerenciar e recuperar pacotes não entregues ou corrompidos, uma vez que a missão da camada 3 é transportar os pacotes entre os *hosts*, e ao mesmo tempo sobrecarregar a rede o menos possível. Se um cabeçalho de confiabilidade for incluído no da camada 3, as comunicações que não requerem conexões ou confiabilidade seriam sobrecarregadas com o consumo de largura de banda e o atraso produzido por este cabeçalho. No conjunto TCP/IP, a camada de transporte pode escolher entre TCP ou UDP, com base nas necessidades de comunicação. Assim como com todo o isolamento de camadas proporcionado pelos modelos de rede, deixar a decisão sobre confiabilidade para a camada de transporte torna o IP mais adaptável e fácil de se acomodar com diferentes tipos de comunicação;

c) Independente de Meios Físicos - Opera independentemente do meio que transporta os dados nas camadas inferiores da pilha de protocolo. Somente considera o tamanho máximo do pacote que cada meio físico consegue transportar.

3.4 CABEÇALHO DE PACOTE IPV4

Um datagrama IP consiste em uma parte de cabeçalho e uma parte de texto. O formato do cabeçalho tem uma parte fixa de 20 bytes e outra opcional de tamanho variável até 40 bytes, conforme demonstra a figura abaixo (TANENBAUM, 2003). A figura 3.2 mostra os cabeçalhos do protocolo IPv4.

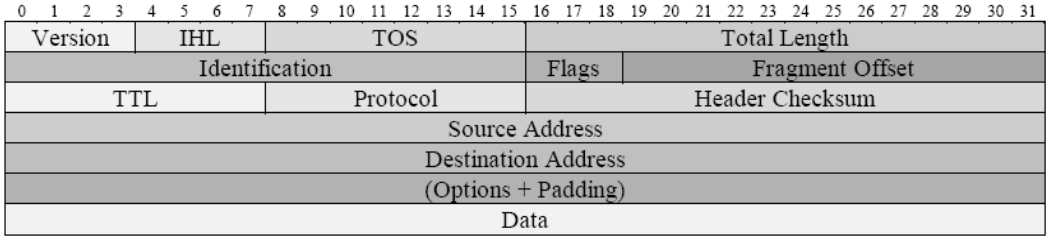

Figura 3.2 - Ilustração do cabeçalho IPv4
Fonte: CISCO, 2013

Campos chaves do cabeçalho:

a) **Version:** a versão atual é a 4, motivo pelo qual chamamos de IPv4 o protocolo IP. O campo versão tem o tamanho de quatro bits (RFC 0791, 1981);

b) **IHL (Internet Header Lengh):** tamanho do cabeçalho do pacote. Informa seu tamanho em palavras de 32 bits. O valor mínimo é 5, quando não há nenhuma opção presente. O valor máximo desse campo de 4 bits é 15, o que limita o cabeçalho a 60 bytes e o campo *Options* a 40 bytes (RFC 0791,1981);

c) **TOS (Type of service):** possui 8 bits e é utilizado para indicar o QoS (Quality of Service) (SOUZA, 2005) desejado. Seus bits caracterizam os serviços escolhidos ara serem considerados pelos *gateway*s para processar o pacote. Originalmente o campo de 6 bits continha (da esquerda para a direita) um campo *Precedence* de três bits e três *flags*, D, T e R. O campo Precedence tinha uma prioridade que variava de 0 (normal) a 7 (pacote de controle de rede). Os três bits de *flags* permitiam que o host especificasse o que era mais importante no conjunto {Retardo, Throughp ut, Confiabilidade} (RFC 0791,1981);

d) **Total Length:** campo de 16 bits que fornece o tamanho total do pacote em bytes, incluindo o cabeçalho e os dados. O tamanho mínimo do pacote é de 20 bytes e o máximo de 65.535 (RFC 0791, 1981);

e) **Identificacion:** identifica unicamente os fragmentos de um pacote IP original, permitindo que o host de destino determine a qual datagrama pertence um fragmento recém-chegado. Todos os fragmentos de um datagrama contêm o mesmo valor de identificação (RFC 0791, 1981);

f) **Flags:** bits que identificam a transmissão de sinais de controle;

g) **Fragmento Offset:** informa a que ponto do datagrama atual o fragmento pertence. Todos os fragmentos de um datagrama, com exceção do último, devem ser múltiplos de 8 bytes, a unidade elementar de fragmento. Como são fornecidos 13 bits,

existem no máximo 8192 fragmentos por datagrama, resultando em um tamanho máximo de datagrama igual a 65.536 bytes, um a mais que o campo *Total Length* (CISCO, 2013);

h) **TTL (Time to live):** contador usado para limitar a vida útil dos pacotes. Esse campo conta o tempo em segundos, permitindo uma vida útil máxima de 255s. Ele é decrementado a cada hop e supõe-se que seja decrementado diversas vezes quando estiverem enfileirados durante um longo tempo em um roteador. Na prática, ele simplesmente conta os hops. Quando o contador chega a zero, o pacote é descartado e enviado uma advertência para o host de origem. Com isso evita-se que os datagramas fiquem vagando indefinidamente, algo que aconteceria se as tabelas de roteamento fossem danificadas (CISCO, 2013);

i) **Protocol**: este campo informa a que processo de transporte o datagrama deve ser entregue quando o mesmo estiver montado por completo. O número do TCP, por exemplo, é seis, UDP é 17 e ICMP igual a um. O campo protocolo tem o tamanho de oito bits (RFC 0791, 1981);

j) **Header Checksun:** utilizado somente para verificação de erros no cabeçalho do pacote. Em cada salto o *checksum* do cabeçalho é comparado com o valor deste campo. Se o valor não corresponder ao *checksum* calculado, o pacote é descartado. Em cada salto, o campo TTL é reduzido e o *checksum* é recalculado em cada salto (CISCO, 2013);

k) **Source Address:** segundo a CISCO este campo informa o endereço de origem do host que está enviando o pacote;

l) **Destination Address:** este campo de endereço é destinado ao host que receberá o pacote (CISCO, 2013);

m) **Options:** este campo foi projetado para permitir que versões posteriores do protocolo incluam informações inexistentes no projeto original, possibilitando a experimentação de novas ideias e evitando a alocação de bits de cabeçalho para informações raramente necessárias (CISCO, 2013);

n) **Padding:** tamanho variável, entre 0 e 31 bits. Serve apenas para que o cabeçalho IP tenha um tamanho múltiplo de 32 bits e é feito seu preenchimento (obrigatoriamente com 0), somente se o tamanho do campo *Options* não for múltiplo de 32 bits (CISCO, 2013).

3.5 ENDEREÇAMENTO NO IPv4

O endereçamento dos protocolos da camada de rede permite a comunicação de dados entre *hosts* na mesma ou em redes diferentes. O IPv4 permite o endereçamento hierárquico para pacotes que transportam dados.

No IPv4 cada pacote no cabeçalho da camada 3 possuí 32 bits tanto no endereço de origem quanto no de destino. Na rede esses endereços são utilizados em padrões binários e representados em formato decimal pontuada para os usuários, conforme demonstrado na figura abaixo (CISCO, 2013).

Figura 3.3 - Formato do endereço IP
Fonte: CISCO, 2013

Os 32 bits são separados em grupos de oito números que formam assim um octeto. O conjunto dos primeiros 24 octetos representam a parte de Rede e os oito últimos a parte de host do endereço. O número de bits usados nessa porção de host vai determinar o número de host possíveis a serem utilizado na rede.

3.6 TIPOS DE ENDEREÇOS

Dentro do intervalo de endereço de cada rede IPv4, temos três tipos de endereço de acordo com *Networking Academy* da CISCO:

a) **Endereço de rede:** dentro do intervalo de endereços IPv4 de uma rede, o primeiro endereço é reservado para o endereço de rede. Esse endereço possui o valor 0 para cada bit de host do endereço;

b) **Endereço de broadcast:** endereço especial usado para enviar dados a todos os *hosts* da rede. O envio de dados para todos os *hosts* em uma rede pode ser feito por um

host que envia um único pacote que é endereçado para o endereço de broadcast da rede;

c) **Endereços de host:** os endereços designados aos dispositivos finais da rede.

Existem três tipos de endereços de *hosts* que não podem ser usados para uma comunicação com outro host individual. São eles (CISCO, 2013):

a) **Endereços Experimentais:** um intervalo principal de endereços reservados para propósitos especiais IPv4 que vão de 240.0.0.0 a 255.255.255.254. Atualmente, esses endereços são registrados como reservados para uso futuro (RFC 3330, 2002). Atualmente, não podem ser usados em redes IPv4, mas podem ser usados para pesquisa ou testes;

b) **Endereços Multicast:** os endereços *multicast* IPv4 de 224.0.0.0 a 224.0.0.255 são endereços locais de link reservados. Esses endereços são usados para grupos *multicast* em uma rede local. Os pacotes para esses destinos sempre são transmitidos com um valor TTL igual a 1. Portanto, um roteador conectado à rede local nunca deve encaminhá-los. Uma utilização típica é o de endereços locais de link reservados para protocolos de roteamento usando transmissão *multicast* para trocar informações de roteamento. Os endereços globalmente restritos são de 224.0.1.0 a 238.255.255.255. Eles podem ser usados para dados *multicast* pela Internet;

c) **Endereços de Host:** depois de retirado os intervalos reservados para endereços experimentais e de *multicast* foi determinado o intervalo de 0.0.0.0 a 223.255.255.255 para utilização dos *hosts* IPv4. Contudo, dentro desse intervalo há muitos endereços reservados para fins especiais, denominados de endereços privados que são: de 10.0.0.0 a 10.255.255.255 (10.0.0.0 /8), de 172.16.0.0 a 172.31.255.255 (172.16.0.0 /12) e de 192.168.0.0 a 192.168.255.255 (192.168.0.0 /16) para utilização em redes privadas.

3.7 TIPOS DE CLASSES

Os endereços IPv4 foram divididos em classes: A, B, C, D e E. Cada classe possui um intervalo de endereço específico. As principais são (CISCO, 2013):

a) **Classe A:** um intervalo de endereços classe A de 0.0.0.0 a 127.255.255.255 foi projetado para suportar redes extremamente grandes, com mais de 16 milhões de endereços de host. Os endereços IPv4 classe A usavam um prefixo /8 com o primeiro octeto para indicar os endereços da rede. Os três octetos finais eram usados para endereços de host;

b) **Classe B:** o espaço de endereços Classe B de 128.0.0.0 a 191.255.255.255 foi projetado para suportar as necessidades de redes de tamanho moderado a muito grande com mais de 65.000 *hosts*. Um endereço IP classe B usava os dois primeiros octetos para indicar o endereço de rede. Os outros dois octetos especificavam os endereços de host. Como no caso da classe A, o espaço para endereços das classes de endereços restantes precisava ser reservado também. No caso de endereços classe B, os dois bits mais significativos do primeiro octeto eram 10 utilizando assim um prefixo /16. Por possuir uma alocação de endereços mais eficiente que os de classe A, ele tornou-se ligeiramente mais eficiente;

c) **Classe C:** o espaço de endereços classe C foi o mais comumente disponível das classes de endereços foi de 192.0.0.255 a 223.255.255.255. Esse espaço de endereço fornecia endereços para redes pequenas, com no máximo 254 *hosts*. Os intervalos de endereço classe C usavam um prefixo /24. Isso quer dizer que uma rede classe C usava apenas o último octeto como endereço de host, e os três primeiros octetos eram usados para indicar o endereço de rede.

3.8 SURGIMENTO DO IPV6

Com a expansão, inovação e utilização por um número cada vez maior de usuários da Internet, no início dos anos 90 a *Internet Engineering Task Force* (IETF) começou a se preocupar com o esgotamento de endereços IPv4 e buscou substituir esse protocolo. Iniciou

trabalho com uma nova versão do IP, capaz de impedir que os endereços fossem esgotados e de resolver uma série de outros problemas, além de ser mais flexível e eficiente. Esse trabalho deu origem ao que conhecemos hoje como IP versão 6 (IPv6) (FOROUZAN, 2010).

Os principais objetivos propostos que o IPv6 deveria atender eram (TANENBAUM, 2003):

a) Aceitar bilhões de *hosts*, mesmo com alocação de espaço de endereços ineficiente;

b) Reduzir o tamanho das tabelas de roteamento;

c) Simplificar o protocolo, de modo a permitir que os roteadores processem os pacotes com mais rapidez;

d) Oferecer mais segurança (autenticação e privacidade) do que o IP atual;

e) Dar mais importância ao tipo de serviço, particularmente no caso de dados em tempo real;

f) Permitir multidifusão, possibilitando a especificação de escopos;

g) Permitir que um host mude de lugar sem precisar mudar o endereço;

h) Permitir que o protocolo evolua no futuro;

i) Permitir a coexistência entre protocolos novos e antigos durante anos.

O IPv6 atende a todos os objetivos propostos, preservando os bons recursos do IP, descartando ou reduzindo a importância das características ruins e criando outras quando necessário. Genericamente, o IPv6 não é compatível com o IPv4, mas é compatível com todos os outros protocolos auxiliares da Internet, incluindo TCP, UDP, ICMP, IGMP, OSPF, BGP e DNS, apesar de, em certos momentos, serem necessárias pequenas modificações principalmente quando têm de lidar com endereços mais longos.

3.9 Características do IPv6

Ao ser comparado com o IPv4, o IPv6 possuí endereços mais longos que saíram dos 32 bits para 128 bits oferecendo assim um número ilimitado de endereços na Internet e resolvendo o problema de esgotamento dos mesmos enfrentado pelo IPv4.

Seu cabeçalho é mais simplificado contando apenas com 7 campos, permitindo que os roteadores processem os pacotes com mais rapidez, melhorando assim o *throughput* e o

retardo. Foram retirados os campos: *IHL*, *identification*, *flags*, *fragment offset*, *header checksum*, *options* e *Padding* que pertencem ao IPv4. A figura 3.4 mostra os campos que foram alterados no protocolo IPv6 em relação ao IPv4.

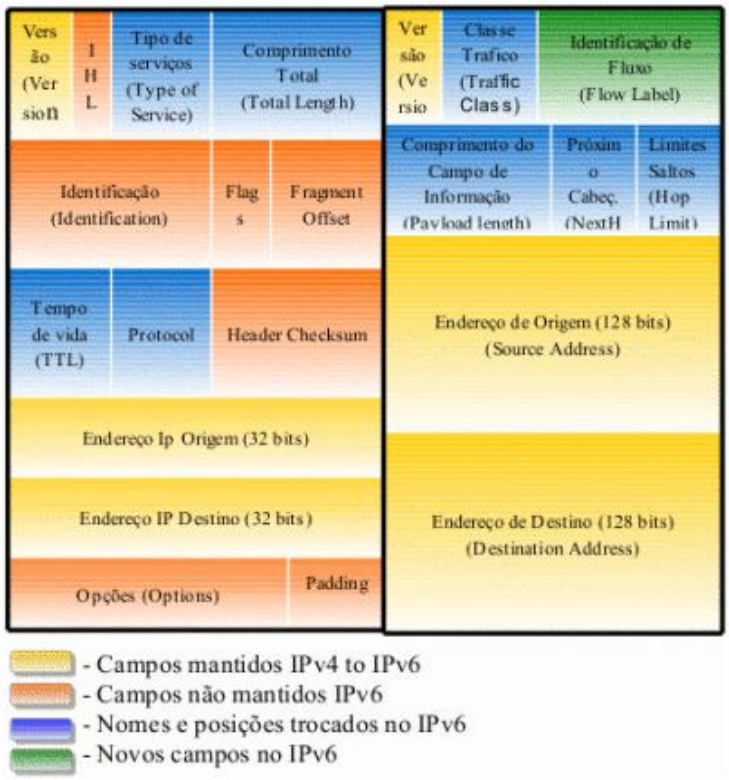

Figura 3.4 - Comparação e exposição do cabeçalho IPv6 x IPv4.
Fonte: IPV6.BR, 2012, Características do IPV6

Possuí também um número máximo de roteadores por onde passar (*Hop Limit*), além de possuir um melhoramento na segurança, onde a autenticação e a privacidade são recursos importantes do novo IP, permite uma maior atenção à qualidade de serviço.

3.10 CABEÇALHO DO IPV6

Desenhado para ser o sucessor do IPv4, o datagrama do IPv6, segundo COMER (2003), é composto por um cabeçalho (*header*) com menos campos, alguns cabeçalhos estendidos opcionais e o campo para dados. O datagrama mínimo tem o cabeçalho base seguido dos dados. A figura 3.5 mostra o cabeçalho IPv6, mais resumido e eficiente.

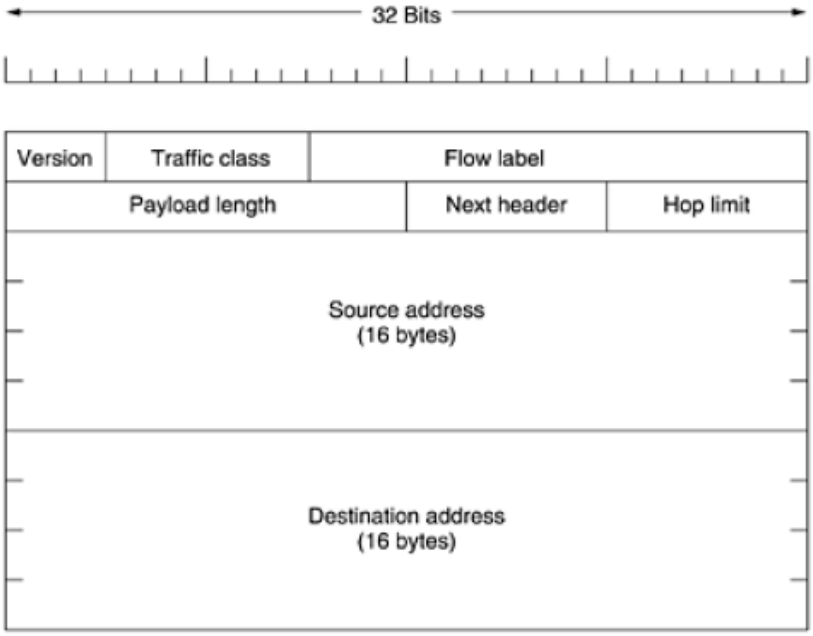

Figura 3.5 - Cabeçalho do IPv6. Imagem extraída do livro
Fonte: TANEBAUM, 2003.

3.10.1 Descrição dos campos do cabeçalho:

a) **Version:** esse campo sempre será 6;

b) **Traffic class:** faz distinção entre os pacotes com diferentes requisitos de entrega em tempo real;

c) **Flow label:** permite que uma origem e um destino configurem uma pseudoconexão com propriedades e necessidades específicas. Ainda está sendo usado em fase de experiência;

d) **Payload lenght:** determina o número de bytes que seguem o cabeçalho de 40 bytes que deixaram de ser contados como parte do tamanho, como acontece no IPv4 onde seu nome é consta como *Total Lenght;*

e) **Next header:** o cabeçalho pode ser simplificado, porque existe a possibilidade de haver outros cabeçalhos de extensão (opcionais). 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);

f) **Hop limit:** impede que os pacotes tenham duração eterna limitando o número máximo de saltos nos equipamentos e a cada salto decrementa de 1 a 1 cada nó que segue o pacote e quando esse valor chega a 0 o pacote é descartado;

g) **Source address:** endereço de origem do pacote – 128 bits (4 x 32 bits);

h) **Destination address:** informa o endereço de destino – 128 bits (4 x 32 bits). O endereço de destino pode não ser o do *host* final, porque pode ser um cabeçalho de roteamento.

3.11 ICMPv6

O protocolo ICMP que foi modificado para a versão 6 do conjunto de protocolos TCP/IP (ICMPv6) segue com a mesma estratégia e finalidades da antiga versão quatro. O ICMPv6 foi modificado para torná-lo compatível com o IPv6. Além disso, alguns protocolos que eram independentes na versão 4 agora fazem parte do ICMPv6. A Figura 3.6 apresenta uma comparação entre a camada de rede da versão 4 com a da versão 6. (FOROUZAN, 2010).

A RFC4443 definiu o protocolo ICMPv6 e no campo *Next Header* é identificado pelo valor 58. A figura 3.6 mostra a evolução do protocolo ICMP.

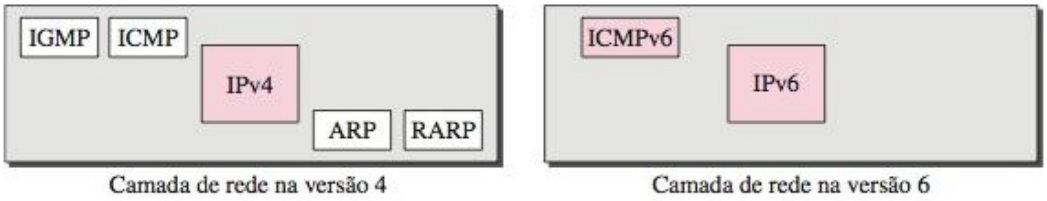

Figura 3.6: Comunicação de Dados e Redes de Computadores.
Fonte: FOROUZAN, 2010

De acordo com a página eletrônica www.IPv6.br, o ICMPv6 exerce funções antes desempenhadas pelo IGMP e RARP. Desta forma, caso o firewall esteja ativado para evitar ICMPv6 a rede simplesmente não funcionará.

O ICMPv6 tem cinco mensagens que são trocadas em um segmento de rede muito importante para a descoberta de vizinhança (www.IPv6.br acessado em 20 de março de 2013):

a) **RS** (Router Solicitation) – Enviada por uma estação que deseja aprender informações de um roteador dentro do segmento de rede local. Desta forma o host poderá ter conectividade com o mundo sem a necessidade de um servidor DHCPv6;

b) **RA** (Router Advertisement) – O RA pode ser utilizado para responder a uma solicitação **RS** e para configurar um roteador para enviar anúncios regulares em intervalos regulares. Nos equipamentos CISCO o RA é configurado para enviar anúncios periodicamente. Quando o anúncio é feito de forma automática, a origem será um endereço *Multicast All-Nodes* ff02::1;

c) **Gerenciamento de Grupos Multicast** – Para *switch* que tenha suporte a IPv6 ele utilizará um protocolo MLD (multicast listener Discovery), este protocolo substitui o IGMP, cuja função é controlar os membros de um grupo de multicast;

d) **NS –** Mensagem enviada de um host para encontrar o endereço MAC correspondente a um determinado endereço IPv6 ou para confirmar que aquele endereço é único;

e) **NA –** Estas são mensagens enviadas em resposta a solicitação NS.

De acordo com a RFC4861 uma interface IPv6 terá automaticamente 3 endereços configurados:

a) Link-Local: Começa sempre com FE80::

b) All Nodes: FF02::1

c) Solicited Node: FF002::1:FFxx:xxxx)

3.11.1 Packet too big

Este mensagem é nova e foi acrescentada à versão 6. Caso um roteador receba um datagrama que é maior que o tamanho do MTU (Maximmum Transmission Unit — Unidade Máxima de Transmissão) da rede pela qual o datagrama deve passar, acontecem duas coisas. Primeiro o roteador descarta e em seguida envia um pacote ICMP notificando o erro ocorrido a quem originou a mensagem.

3.11.2 Neighbor Discovery

The Neighbor Discovery Protocol ou NDP no IPv6 é uma melhoria sobre o Internet Control Message Protocol (ICMP). É um protocolo de mensagens que facilita a descoberta de dispositivos vizinhos através de uma rede. O NDP usa dois tipos de endereços: endereços *unicast e multicast* (DAS).

3.12 STATELESS

De acordo com Equipe IPv6.br o STATELESS é uma configuração automática, aonde ele descobrirá o *gateway* e atribuirá um IP para a sua conexão à interface. Com este prefixo ele atribuirá os 48 bits do Mac-address da interface acrescentando o FFFE, ou seja, os 16 bits que faltam para completar 64 bits restantes do endereçamento. Ex: Se o MAC-address da interface for 1111.2222.3333 com o prefixo 2010:1::/64 o endereço da interface será 2010:1::1**2**11.22ff.fe22.3333. Ele troca o segundo bit do Mac-addres sempre pelo número dois.

Configuração Automática Stateless é um recurso importante oferecido pelo protocolo IPv6. Ele permite que os vários dispositivos ligados a uma rede IPv6 para se conectar à Internet usando a configuração Auto Stateless, sem necessidade de qualquer apoio IP intermediário na forma de um servidor Dynamic Host Configuration Protocol (DHCP).

Um servidor DHCP mantém uma faixa de endereços IP atribuídos dinamicamente por um período de tempo.

De acordo com o site http://IPv6.com acessado em 08 de maio de 2013 a configuração Automática Stateless ajudará muito os administradores de rede, pois automatiza a configuração de IP dos dispositivos. Em uma rede muito grande que utilizam IPv4 necessitava configurar um servidor DHCP para facilitar a sua. No entanto, o IPv6 permite que os dispositivos de rede possam adquirir automaticamente endereços

A configuração automático e recursos de endereçamento automático de IPv6 (Internet Protocol version 6) são definido no RFC 2462.

3.13 STATEFULL

Statefull é um estado dado para a configuração que se baseia em um protocolo de configuração de endereço a fim de obter endereços e outras configurações

Um *host* usa a configuração de endereço com estado quando recebe mensagens de anúncio de roteador que não incluem prefixos de endereço e requerem que o host use um protocolo de configuração de endereço com estado. Um *host* também usará um protocolo de configuração de endereço com estado quando não houver roteadores na conexão local (MICROSOFT).

3.14 DHCPv6

O DHCPv6 permite não só a configuração STATEFULL informando o intervalo de endereços que será utilizado como se pode combinar coma a solução STATELESS EUI-64.

O DHCPv6 de acordo com o *site* www.IPv6.br acessado em 15 de maio de 2013 não atribui apenas o endereço, a máscara e o *gateway* para o host. De acordo com este site existe mais de 30 opções disponíveis no campo *Option* como nome de domínio, servidor DNS, servidor WINS, endereço de Proxy, configurações de VOIP dentre outras coisas.

O DHCP para a versão IPv6 usam as portas 546 e 547, diferentes da versão IPv4 que utilizavam as portas 67 e 68.

3.15 COMPARAÇÃO DO CABEÇALHO IPV4 COM O DO IPV6

Conforme descrito anteriormente neste trabalho, alguns campos pertencentes no IPv4 foram retirados do IPv6. Como o cabeçalho do IPv6 tem um tamanho fixo o campo IHL foi. O campo *Protocol* foi retirado já que o campo *Next header* faz a identificação do que vem após o último cabeçalho IP. Foram retirados também todos os campos relacionados com a

fragmentação, uma vez todos os *hosts* e roteadores que são compatíveis com o IPv6 devem determinar dinamicamente o tamanho do datagrama que será usado. Foi aumentado também o valor mínimo de 576 para 1280 (MTU) permitindo o uso dos 1024 bytes de dados e muitos cabeçalhos. Além disso, um host é obrigado a enviar pacotes com tamanhos exatos quando o mesmo envia pacotes IPv6 muito grandes e o roteador não consegue encaminhá-los que envia uma mensagem de erro de volta instruindo o host a dividir todos os novos pacotes enviados a esse destino.

O campo *Checksum* foi eliminado, porque esse cálculo reduz de forma significativa o desempenho. Com as redes confiáveis usadas atualmente, além do fato de a camada de enlace de dados e as camadas de transporte terem seus próprios totais de verificação, a importância de um novo total é insignificante, se comparada com a queda de desempenho que ela implica. Com a remoção de todos esses recursos, o protocolo da camada de rede ficou muito mais enxuto e prático. Assim, o objetivo do IPv6 — um protocolo a um só tempo rápido e flexível, capaz de oferecer um grande espaço de endereços — foi atendido por esse projeto (FOROUZAN, 2010).

3.16 FORMAS DE TRANSIÇÃO DO IPV4 PARA O IPV6

Conforme explicado anteriormente, a implantação do IPv6, além de necessária, se tornou inevitável, uma vez que o esgotamento dos endereços IPv4 na Internet ocasionará uma diminuição na taxa de crescimento da rede e impossibilitará o desenvolvimento de novas aplicações, tornando assim a utilização da Internet mais cara pela escassez de conexões.

O ambiente atual a implantação do IPv6 não ocorrerá de forma imediata, ou seja, a troca de protocolo ocorrerá de forma gradual e essa migração acontecerá com o IPv4 ainda em funcionamento, havendo assim um grande período de coexistência entre os dois protocolos.

A grande preocupação no momento é manter a compatibilidade entre as duas versões do protocolo IP e que as redes possam se comunicar entre si de IPv4 para IPv6 e vice e versa. Para facilitar essa comunicação foram desenvolvidos mecanismos que visam manter a compatibilidade de toda base das redes instaladas sobre IPv4 com o novo protocolo IPv6 são eles: tunelamento, tradução e pilha dupla (IPV6.BRhttp://www.ipv6.br/, 2012)

3.16.1 Tunelamento

Método mais utilizado na fase inicial de implantação do IPv6, que permite transmitir pacotes IPv6 em redes IPv4 existentes por meio da criação de túneis ou tunelamento, sem a necessidade de realizar mudanças nos mecanismos de roteamento, através do encapsulamento do conteúdo do pacote IPv6 em um pacote IPv4, onde o nó de entrada do túnel, cria um cabeçalho IPv4 com o pacote IPv6 encapsulado e o transmite através da rede IPv4. O nó de saída recebe o pacote encapsulado, retira o cabeçalho IPv4 e processa o pacote IPv6 recebido. Esse processo de encapsulamento é conhecido como 6in4 e tem como protocolo de identificação o tipo 41. Sua utilização é comum nas técnicas de tunelamento 6to4, ISATAP e Tunnel Broker. (IPV6.BRhttp://www.ipv6.br/, 2012). A figura 3.7 mostra o pacote IPv6 sendo encapsulado com a técnica 6in4:

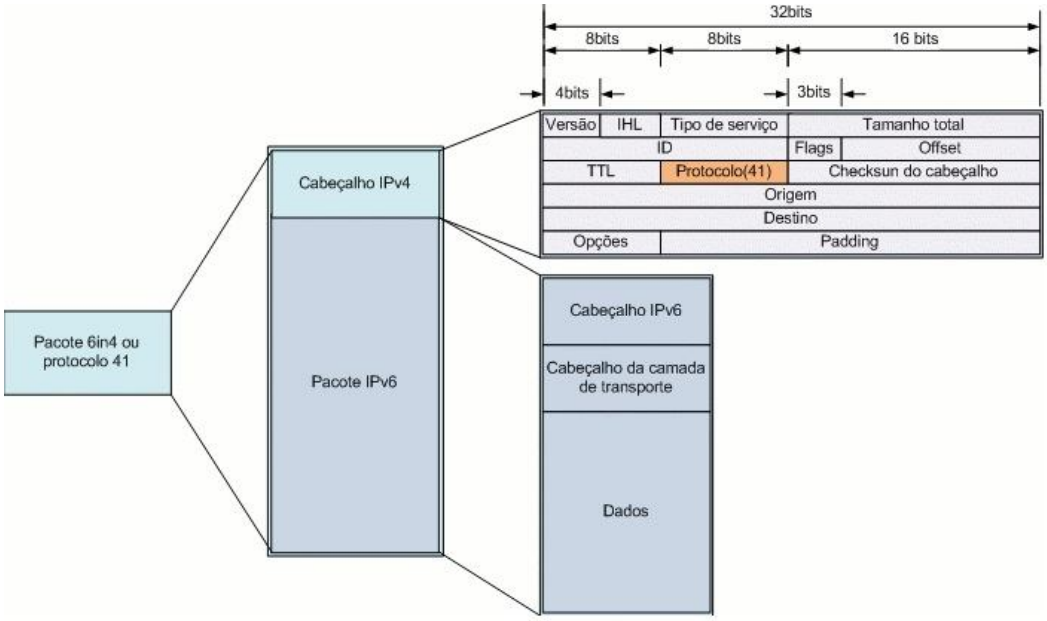

Figura 3.7 - Estrutura de pacote IPv6 encapsulado em IPv4
Fonte: IPV6.BR, 2012, Técnicas de transição.

3.16.1.1 Classificação dos Túneis:

a) **Roteador-a-Roteador** - roteadores IPv6/IPv4, conectados via rede IPv4, podem trocar pacotes IPv6 entre si, ligando um segmento no caminho entre dois *hosts*, mostrado na figura 3.8;

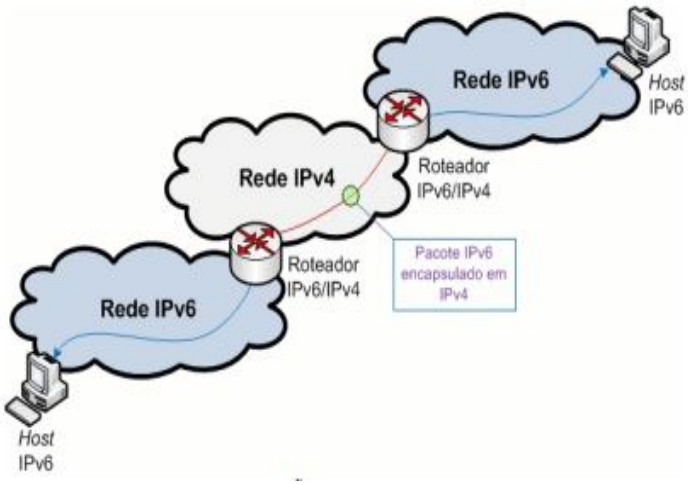

Figura 3.8 - Configuração Roteador-a-roteador
Fonte: IPV6.BR, 2012, Técnicas de transição.

b) **Host-a-Roteador** - *hosts* IPv6/IPv4 enviam pacotes IPv6 a um roteador IPv6/IPv4 intermediário via rede IPv4, ligando o primeiro segmento no caminho entre dois *hosts*;

c) **Roteador-a-Host** - roteadores IPv6/IPv4 enviam pacotes IPv6 ao destino final IPv6/IPv4, ligando o último segmento do caminho entre dois *hosts conforme a figura 3.9*;

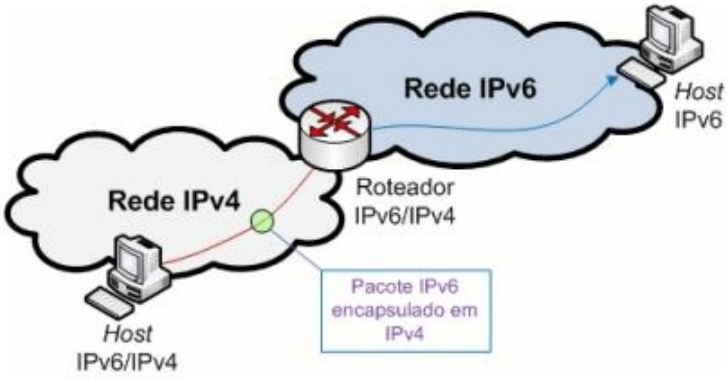

Figura 3.9 - Configuração Host-a-Roteador e Roteador-a-Host
Fonte: IPV6.BR, 2012, Técnicas de transição.

d) **Host-a-Host** - *hosts* IPv6/IPv4, conectados via rede IPv4, trocam pacotes IPv6 entre si, ligando todo o caminho entre os dois *hosts, mostrado na figura 3.10*.

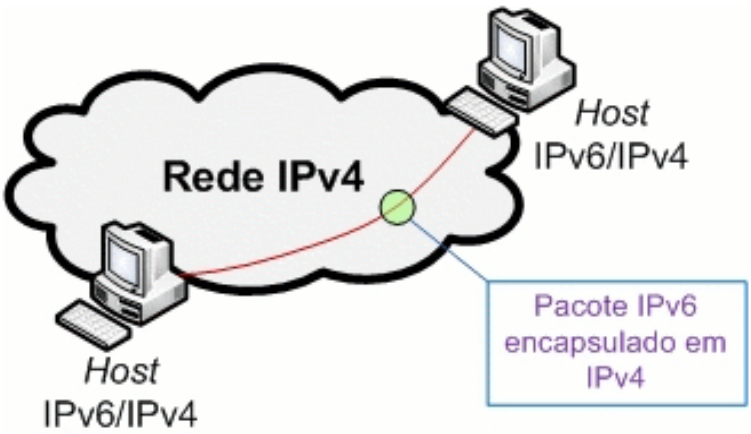

Figura 3.10 - Configuração Host-a-Host
Fonte: IPV6.BR, 2012, Técnicas de transição.

3.16.1.2 Tipos de Túneis:

a) **Tunnel Broker** - técnica que permite que *hosts* IPv6/IPv4 isolados em uma rede IPv4 acessem redes IPv6. Sua configuração é feita através do cadastramento em um provedor de acesso Tunnel Broker e efetuar o download do software ou script de configuração. A conexão será feita através de solicitação do serviço ao Servidor Web do provedor (IPV6.BR, 2012);

b) **6to4 -** técnica de tunelamento roteador-a-roteador, que permite a comunicação entre *hosts* IPv6 através de uma infraestrutura IPv4, onde é fornecido um endereço IPv6 único formado pelo prefixo de endereço global **2002:wwxx:yyzz::/48**, onde **wwxx:yyzz** é o endereço IPv4 público do *host* convertido para hexadecimal. O host IPv6 envia um pacote IPv6 ao roteador 6to4 que o encapsula em um pacote IPv4 utilizando o protocolo tipo 41 e o encaminha ao host de destino IPv6 através de uma rede IPv4 (IPV6.BR, 2012);

c) **ISATAP (*Intra-Site Automatic Tunnel Addressing Protocol)*** - técnica que permite a criação de túneis que ligam host a roteadores através de uma rede IPv4 onde o endereço IPv6 que é atribuído aos *hosts* e roteadores é baseado em um prefixo de 64 bits que pode ser *link-local*, um prefixo 6to4, ou um prefixo *global* atribuído por um provedor, seguido por **::0:5EFE:w.x.y.z** ou **::0:5EFE:w.x.y.z**, onde o **w.x.y.z** representa o endereço IPv4 do *host* ou do roteador, e os valores **0:5EFE** e **200:5EFE** indicam se esse endereço IPv4 é privado ou público, respectivamente. O ISATAP

também utiliza o protocolo tipo 41 para transmissão de pacotes IPv6 (CISCO ISATAP, 2013);

d) **Teredo** - técnica que permite o tráfego IPv6 através de NAT, do encapsulamento do pacote IPv6 em pacotes UDP. Um túnel Teredo é criado através da conexão de um cliente a um servidor Teredo, que irá definir o endereço IPv6 do cliente e em qual tipo de NAT ele se encontra. O servidor estabelecerá conexão inicial com o host IPv6 de destino e este host manterá a conexão com a origem através do Relay Teredo mais próximo dele. O túnel Teredo é uma das únicas opções para habilitar a comunicação IPv6 através de NAT e permite que os *hosts* de rede internos obtenham temporariamente um endereço de IP de Internet legítimo enquanto acessam os recursos da Internet (IPV6.BR, 2012, Técnicas de transição).

3.16.2 Tradução

As técnicas de tradução visam possibilitar um roteamento transparente na comunicação entre nós que apresentam suporte apenas para uma versão do protocolo IP, ou utilizem Pilha Dupla. Atuam em camadas distintas, traduzindo cabeçalhos IPv4 em cabeçalhos IPv6 e o contrário, realizando conversões de endereços, de APIs (*Aplication Program Interface*) de programação, ou atuando na troca de tráfego TCP ou UDP.

3.16.2.1 Tipos de Tradução:

a) SIIT (*Stateless IP/ICMP Translation Algorithm)* – mecanismo de tradução *stateless* de cabeçalhos IP/ICMP, permite a comunicação entre nós com suporte apenas ao IPv6 com nós que apresentam suporte apenas ao IPv4. Utiliza um tradutor que fica localizado na camada de rede da pilha, que converte campos específicos dos cabeçalhos de pacotes IPv6 em cabeçalhos de pacotes IPv4 e vice-versa. Para realizar este processo, o tradutor necessita de um endereço IPv4-mapeado em IPv6, no formato **0::FFFF:a.b.c.d**, que identifica o destino IPv4, e um endereço IPv4-traduzido, no formato **0::FFFF:0:a.b.c.d**, para identificar o nó IPv6. Quando o pacote chega ao

SIIT, o cabeçalho é traduzido, convertendo o endereço para IPv4 e encaminhado ao nó de destino. (IPV6.BR, 2012, Técnicas de transição)

b) **NAPT-PT** (*Network Address Port Translation and Packet Translation*) - mecanismo de tradução que possibilita a comunicação entre *hosts* IPv6 e IPv4 de forma transparente, utilizando apenas um único endereço IPv4. Seu funcionamento consiste em traduzir as portas TCP/UDP dos *hosts* IPv6 em porta TCP/UDP do endereço IPv4 registrado. Deste modo, enquanto no NAT-PT o número de sessões limita-se a quantidade de endereços IPv4 disponíveis para a tradução, no NAPT-PT é possível realizar 63.000 sessões TCP e 63.000 sessões UDP por endereço IPv4. .(IPV6.BR, 2012, Técnicas de transição)

c) **BIS** (*Bump in the Stack*) – mecanismo de tradução que possibilita a comunicação de aplicações IPv4 com nós IPv6. O BIS funciona entre a camada de aplicação e a de rede, adicionando à pilha IPv4 três módulos: **translator**, que traduz os cabeçalhos IPv4 enviados em cabeçalhos IPv6 e os cabeçalhos IPv6 recebidos em cabeçalhos IPv4; **extension name resolver**, que atua nas *DNS queries* realizadas pelo IPv4, de modo que, se o servidor DNS retorna um registro AAAA, o *resolver* pede ao *address mapper* para atribuir um endereço IPv4 correspondente ao endereço IPv6; e **address mapper**, que possui certa quantidade de endereços IPv4 para associar a endereços IPv6 quando o *translator* receber um pacote IPv6. Como os endereços IPv4 não são transmitidos na rede, eles podem ser endereços privados. Esse método permite apenas a comunicação de aplicações IPv4 com *hosts* IPv6, e não o contrário, além de não funcionar em comunicações *multicast* (IPV6.BR, 2012, Técnicas de transição).

d) **BIA** (*Bump in the API*) - similar ao BIS, esse mecanismo de tradução adiciona uma API de tradução entre o *socket* API e os módulos TPC/IP dos *hosts* de pilha dupla, permitindo a comunicação de aplicações IPv4 com *hosts* IPv6, traduzindo as funções do *socket* IPv4 em funções do *socket* IPv6 e vice-versa. São adicionados três módulos, **extension name resolver** e **address mapper**, que funcionam da mesma forma que no BIS, e o **function mapper**, que detecta as chamadas das funções do *socket* IPv4 e invoca as funções correspondentes do *socket* IPv6 e vice-versa. O BIA apresenta duas vantagens em relação ao BIS: não depender do *driver* da interface de rede e não introduzir *overhead* na tradução dos cabeçalhos dos pacotes. No entanto, ele também não suporta comunicações *multicast*. .(IPV6.BR, 2012, Técnicas de transição)

e) **TRT** (*Transport Relay Translator*) - Atua como um tradutor de camada de transporte, esse mecanismo possibilita a comunicação entre *hosts* apenas IPv6 e *hosts* apenas IPv4 através de trafego TCP/UDP. Sem a necessidade de se instalar qualquer tipo de software, o TRT roda em máquinas com pilha dupla que devem ser inseridas em um ponto intermediário dentro da rede. Na comunicação de um *host* IPv6 com um *host* IPv4, é adicionado um prefixo IPv6 falso ao endereço IPv4 do destino. Quando um pacote com esse prefixo falso passa pelo TRT, esse pacote é interceptado e enviado ao *host* IPv4 de destino em um pacote TCP ou UDP. Na tradução TCP e UDP o *checksum* deve ser recalculado e apenas no caso das conexões TCP, o estado do *socket* sobre o qual o *host* está conectado deve ser mantido, removendo-o quando a comunicação for finalizada. Para que o mecanismo funcione de forma bidirecional, é necessário a adição de um bloco de endereços IPv4 públicos e o uso de um servidor DNS-ALG para mapear os endereços IPv4 para IPv6. .(IPV6.BR, 2012, Técnicas de transição)

f) **SOCKS64** (*Socks-Based IPv6/IPv4 Gateway*) - baseado no *proxy* SOCKS convencional, esse mecanismo de tradução é composto por um *gateway* SOCKS implementado como um *host* com pilha dupla IPv4/IPv6 e um *host* cliente implementado com um software chamado SOCKS LIB entre as camadas de aplicação e transporte. Esse software intercepta as pesquisas DNS e as responde com endereços IPv4 falsos, de modo que, quando o cliente realiza uma chama a API de conexão, o SOCKS LIB substitui o endereço falso pelo original e envia o pacote, chamado de *socksified*, para o *proxy* que executa a pesquisa DNS real. Se o servidor DNS responder com um registro AAAA, o *proxy* abre um *socket* IPv6, caso contrário, será aberto um *socket* IPv4. O SOCKS64 é uma solução bidirecional, permitindo que tanto *hosts* IPv4 quanto *hosts* IPv6 iniciem sessões. Entretanto, é necessário que se utilize endereços IPv4 públicos (IPV6.BR, 2012, Técnicas de transição)

g) **ALG** (*Application Layer Gateway*) – mecanismo de tradução que trabalha como um *proxy* HTTP, onde o cliente primeiramente inicia a conexão com o ALG, que, então, estabelece uma conexão com o servidor, retransmitindo as requisições de saída e os dados de entrada. Em redes apenas IPv6, o ALG habilita a comunicação dos *hosts* com serviços em redes apenas IPv4, configurando o ALG em nós com pilha dupla. Este tipo de mecanismo e normalmente utilizado quando o *host* que deseja

acessar a aplicação no servidor IPv4, está atrás de NAT ou de um *firewall*. (IPV6.BR, 2012, Técnicas de transição).

3.16.3 Pilha Dupla

O método de transição denominado de Pilha Dupla permite que *hosts* e roteadores sejam equipados com pilhas para ambos o protocolos, tornando-os capazes de enviar e receber pacotes tanto para o IPv4 quanto para o IPv6. Um nó Pilha Dupla (IPv4/IPv6) na comunicação com um nó IPv4, se comportará como um nó IPv4 e na comunicação de um nó IPv6 como nó IPv6.

Para possibilitar essa comunicação cada nó IPv4/IPv6 é configurado com ambos os endereços, utilizando mecanismos IPv4 que podemos citar como exemplo o DHCP para adquirir seu endereço IPv4 e mecanismos do IPv6 como por exemplo auto-configuração e/ou DHCPv6 para adquirir seu endereço IPv6. A figura 3.11 mostra como funciona o sistema de pilha dupla.

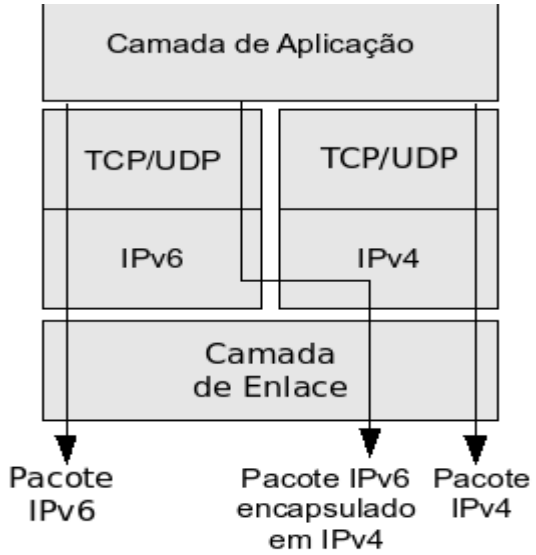

Figura 3.11 - Tráfego de pacotes utilizando pilha dupla
Fonte: IPV6.BR, 2012, Técnicas de transição

Esse método de transição visa facilitar o gerenciamento de implantação do IPv6, permitindo que este seja feito de forma gradual, uma vez que são configurados apenas

pequenas seções do ambiente de rede por vez e se futuramente o IPv4 deixe de ser utilizado basta apenas desabilitar a pilha IPv4 de cada nó.

Para a implantação desse método em uma rede, devem ser analisados alguns aspectos relacionados às mudanças na infraestrutura como: configuração dos servidores DNS, configuração dos protocolos de roteamento e configuração dos firewalls.

3.16.4 Análise dos aspectos de infraestrutura:

a) **Configuração servidor DNS –** devem ser habilitados para resolver nomes e endereços tanto de IPv4 quanto de IPv6. No caso do IPv6 deve responder a consultas de registros do tipo AAAA (quad-A), que armazenam endereços no formato IPv6, e para o domínio criado para a resolução de reverso, o IPv6.arpa (FOROUZAN, 2010);

b) **Configuração dos protocolos de roteamento –** numa rede IPv4/IPv6 a configuração de roteamento do IPv6 é independente da configuração de roteamento do IPv4, sendo assim uma rede onde foi implementado a Pilha Dupla utilize o protocolo de roteamento interno com suporte apenas ao IPv4 como por exemplo o OSPFv2, será necessário migrar para um protocolo que suporte os dois protocolos, como o IS-IS, ou forçar a execução de um IS-IS ou OSPFv3 paralelamente com o OSPFv2;

c) **Configuração dos firewalls –** a filtragem dos pacotes que trafegam na rede vai depender da plataforma a ser utilizada. Em alguns Sistemas Operacionais, os filtros de pacotes são totalmente independentes, as regras são aplicadas a ambos os protocolos, a não ser que o usuário restrinja explicitamente a qual família de protocolo as regras devem ser aplicadas.

3.17 PROTOCOLOS DE ROTEAMENTO UTILIZADOS

O projeto utiliza protocolo de roteamento dinâmico. Demonstrado o estudo realizado e o laboratório com protocolos de roteamentos dinâmicos EIGRP IPv6, RIPng e OSPFv3. Consultar apêndice B para verificar o funcionamento desses protocolos para redes na versão IPv6.

3.17.1 Routing Information Protocol RIP

O protocolo RIP é um dos primeiros de uma família de protocolos de roteamento dinâmico que calcula automaticamente as tabelas de roteamento, não sendo necessária assim a especificação de rotas para cada rede existente utilizando rotas estáticas. É baseado em um algoritmo conhecido como *distance-vetor* (distância vetorial), que baseia-se na distância entre dois vetores. A mesma é medida em termos do número de roteadores existentes no caminho entre dois roteadores (OLIFER, 2008).

O referido protocolo utiliza a troca de mensagens para se comunicar com outros roteadores que utilizam o mesmo protocolo. Cada mensagem enviada do RIP contém uma série de informações sobre as rotas que o roteador conhece - baseado na sua tabela de roteamento atual - e a distância do roteador para cada uma das rotas. O roteador que recebe as mensagens, com base na sua distância para o roteador que enviou a mensagem, calcula a distância para as demais redes e grava estas informações em sua tabela de roteamento (OLIFER, 2008).

As informações entre roteadores são trocadas quando o roteador é inicializado, quando o roteador recebe atualizações em sua tabela de roteamento e também em intervalos regulares. Mesmo que não exista nenhuma alteração nas rotas da rede, os roteadores baseados em RIP continuarão a trocar mensagens de atualização em intervalos regulares, por padrão a cada 30 segundos (OLIFER, 2008).

No RIP versão 2 foram acrescentados novos campos no pacote de atualização de rota e uma chave entre eles trazendo as informações de máscara de sub-rede em cada entrada de rota que não existiam no RIP versão 1 (CISCO, 2013).

De acordo com a RFC 2080 o protocolo RIP funciona em redes com IPv6, conhecido com o RIPng, nesta versão muda o sistema de descoberta, feita através das interfaces do roteador. O RIP não resolve todos os problemas de roteamento, seu principal uso é em redes moderadas e de pequeno porte devido algumas limitações:

a) Redes com mais de 15 saltos podem haver problemas no roteamento;

b) Em redes muito grandes pode haver demora no roteamento e largura de banda;

c) É um protocolo que utiliza de métrica, mas não quer dizer que o caminho mais curto será o melhor.

3.18 NETWORK ADDRESS TRANSLATION (NAT)

O roteamento na Internet é realizado com base em endereços de destino presentes nos cabeçalhos dos pacotes. Esses endereços normalmente permanecem imutáveis do momento em que são criados pelo remetente até o momento em que chegam ao nó de destino. Entretanto, essa regra tem algumas exceções. Por exemplo, na largamente usada tecnologia NAT (*Network Address Translation* — Tradução de Endereços de Rede) presume-se que o pacote seja encaminhado para a Internet externa com base nos endereços usados para o roteamento de pacotes na rede interna da empresa (OLIFER, 2008).

O NAT é utilizado principalmente pelas empresas para ocultar endereços de sua rede interna e aproveitar o número de endereços divulgados externamente. Desta forma economizam-se endereços “públicos”. Este recurso começou a ser utilizado devido a escassez de endereços IPv4. Com esta técnica permite que uma grande empresa consiga levar Internet, acesso, a vários computadores utilizando apenas um endereço.

Para fornecer aos *hosts* endereços privados para se comunicar usando a Internet ou se conectar aos *hosts* que têm endereços globais é necessário usar a tecnologia NAT (OLIFER, 2008).

Várias empresas utilizam o NAT como um recurso de segurança, evitando, assim, que os endereços de sua rede sejam divulgados.

Todos os conceitos apresentados servirão como fundamento para elaboração do projeto. Entende-los e compreende-los irão auxiliar na solução para o problema de incompatibilidade entre os protocolos IPv4 e IPv6. Assim como a importância de campos e diferenças entre os protocolos IPv4 e IPv6 que irão servir de base principal do projeto para a sua construção e desenvolvimento. Um dos principais protocolos que evoluiu e é de extrema importância o seu entendimento e compreensão foi o ICMPv6, pois a evolução do protocolo ICMP auxilia na atribuição de endereços IPv6; a descoberta de vizinhança deste protocolo auxiliam no endereçamento IP e os modos STATELESS e STATEFULL e as suas diferenças.

As técnicas de transição que foram implementadas são de suma importância para seu entendimento, para escolher qual utilizar e como utilizar, facilitando e auxiliando, desta forma, na convergência dos protocolos IP. Isso tudo não seria possível sem o completo entendimento do modelo OSI e as suas camadas, pois através dele será possível identificar aonde o problema está ocorrendo e prover a correta solução assim como a técnica de NAT utilizada para traduzir endereços públicos em privados e vice-versa. A implementação de roteamento dinâmico foi essencial para a troca de tabelas de roteamento, principalmente em redes IPv6, aonde seria inviável criar uma rota estática para cada rede utilizada. Todos os conceitos apresentados servirão como fundamento para elaboração do projeto. Entendê-los e compreendê-los irão auxiliar na solução para o problema de incompatibilidade entre os protocolos IPv4 e IPv6.

CAPÍTULO 4 - SOLUÇÃO DE CONVERGÊNCIA ENTRE IPv4 E IPv6

Foi realizado um estudo da Migração do IPv4 para IPv6 utilizando o método de transição denominado de Pilha Dupla em conjunto com o NAT-PT e o ISATAP, já explicados anteriormente neste trabalho.

Para demonstrar o comportamento na rede ao receber tanto pacotes IPv4 quanto pacotes IPv6, foi criado um ambiente virtual utilizando o Packet Tracer da CISCO.

O aplicativo Packet Tracer® permite simular o comportamento de roteadores, computadores, servidores dentre outros dispositivos da CISCO. A simulação dele é fidedigna a de um roteador do mesmo modelo. Como roteadores são caros e para demonstrar a solução aplicada seriam necessários muitos roteadores, optou-se por utilizar o emulador da CISCO para construir a topologia e analisar o seu comportamento.

Nesse cenário foi construída uma estrutura fictícia utilizando-se 2 empresas, uma com a estrutura IPv4 e a segunda empresa com a estrutura IPv6. Este cenário representa a realidade da maioria das empresas na atualidade que estão organizadas e endereçadas pela estrutura IPv4.

Com a escassez de endereços no modelo IPv4 novas empresas surgirão já utilizando IPv6. Desta forma, há a necessidade de soluções para integração entre as duas redes.

A simulação tem o intuito de fazer com que as duas empresas consigam conversar utilizando técnicas de NAT-PT, pilha dupla e ISATAP. Essas técnicas foram escolhidas devido à compatibilidade com o sistema IOS da CISCO. Serão utilizadas técnicas de acl, *loopback* e roteamento dinâmico, RIP e RIPng.

A pilha dupla é uma excelente solução, mas tem a inconveniência de duplicar toda a infraestrutura, levando a uma dupla gerência. Para sanar este problema, foi implementada uma técnica de tradução. Porém, a tradução exige que os *hosts* saibam qual a tradução do endereço desejado. Se um host da rede IPv6 desejar acessar um host da rede IPv4 ele necessitará saber qual é o endereço da rede IPv4 traduzido para o formato IPv6 e vice versa. Visando solucionar este problema foi implementado em conjunto com a técnica de PILHA DUPLA E NAT-PT uma técnica de tunelamento, conhecida como ISATAP. O ISATAP permite que uma rede IPv6 navegue sobre uma rede IPv4.

Este cenário visa mostrar a total integração entre elas utilizando o roteador como gateway da rede e responsável pela divulgação dos seus endereços entre eles, mesmo estando em redes diferentes e utilizando protocolos diferentes, como mostra a figura 4.1. A empresa da rede IPv4 e IPv6 se encontram todas em redes segmentadas e distintas:

4.1 DESCRIÇÃO DO CENÁRIO ELABORADO

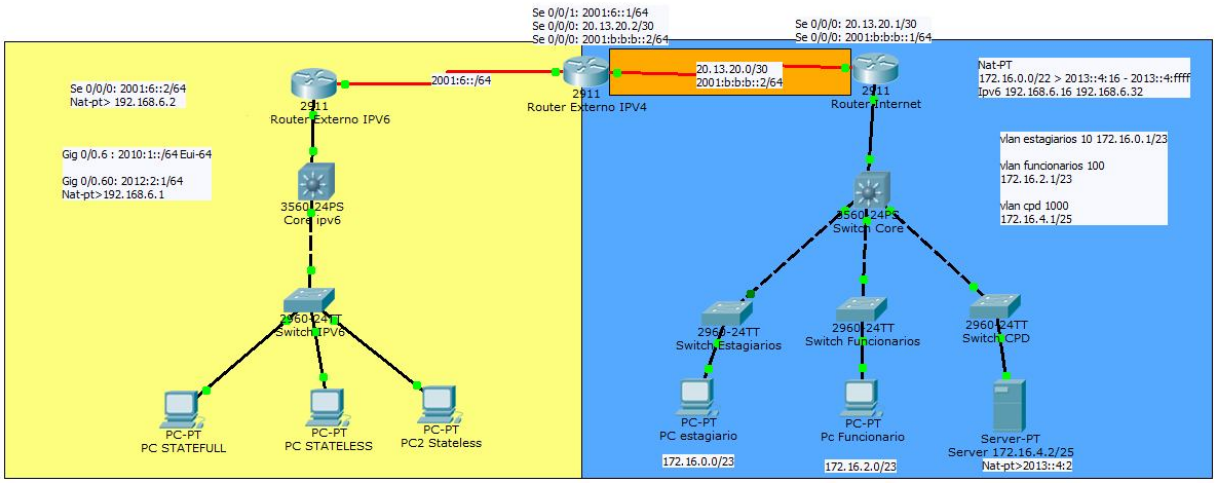

Figura 4.1 - Topologia da Rede Implementada

No cenário virtual elaborado (Figura 4.1), foram utilizados roteadores e SWITCHs da CISCO distribuídos da seguinte forma:

a) Empresa IPv4 (representado pela cor azul):

- 1 roteador CISCO 2911 – *Router Internet*;
  - Roteador da empresa sobre IPv4, responsável pelo controle de entrada,saída e roteamento da rede IPv4. Neste roteador será configurado Roteamento dinâmico para IPv4 e IPv6, Pilha dupla, Nat, Nat-Pt e ISATAP
  - IPs destinados a WAN na interface serial 0/0/0:
    - IPv4 – 20.13.20.1/30
    - IPv6 - 2001:b:b:b::1/64
  - IPs destinados a LAN na interface Giga 0/0
    - VLAN 10 – 172.16.0.1/23
    - VLAN 100 – 172.16.2.1/23

- VLAN 1000 – 172.16.4.1/25

- 1 switch CISCO CORE 3560 – *Switch Core*;
  - Switch de camada 3 utilizado não só como switch, mas também como roteador. Neste cenário ele será o switch de distribuição com os switchs de borda, sendo necessário configurar suas portas no modo TRUNK, marcar os pacotes e levar as VLANs necessárias para os outros switchs. Foram configuradas as VLANs 10, 100 e 1000 no modo trunk em suas interfaces
- 3 SWITCHs CISCO 2960 – *SWITCHs Estagiários, Funcionários e CPD.*
  - Switch de camada 2 utilizado para acesso, este switch será configurado nas suas interfaces de acesso com os *hosts* no modo acesso, pois não precisam marcar os pacotes, porém a conexão entre o seu switch de distribuição deverá estar no modo TRUNK para identificar e direcionar os pacotes marcados.
- Segmentação da rede
  - A rede foi segmentada em três: Rede para estagiários, funcionários e Servidores. Isso ocorre porque facilita a gerência e regras de segurança quando implementadas. Sua segmentação utilizou técnicas de CIDR e deverá ser da seguinte maneira:
    - REDE ESTAGIÁRIOS: 172.16.0.0/23
    - REDE FUNCIONÁRIOS: 172.16.2.0/23
    - REDE SERVIDORES: 172.16.4.0/25

b) Empresa IPv6 (representada pela cor amarela);

- 1 roteador CISCO 2911 – *Router Externo IPv6*;
  - Roteador responsável pelo roteamento de redes e controle da rede IPv6. Nele será configurado DHCPv6 e roteamento dinâmico para IPv6.
  - IPs destinados a WAN na interface serial 0/0/0:
    - IPv6 - 2001:6::2/64
  - IPs destinados a LAN na interface Giga 0/0

- VLAN 6 - 2010:1::/64 eui-64 (STATELESS)
  - No modo STATELESS será utilizado o prefixo 2010:1:: como endereço de rede mais o mac-addres de 48 bits convertido para 64 bits como endereço de host.
  - EX: 48-AA-BB-CC-DD-EE em 48 bits, altera os primeiros 8 bits, número 48 em binário 01001000 muda o sétimo bit para 01001010, VIRANDO 4A 4**A**-AA-BB-**FF**-**FE**-CC-DD-EE número em 64 bits ficando da seguinte maneira :2010:1::4**A**AA:BB**FF**:**FE**CC:DDEE
- VLAN 60 - 2012:2::1/64 (STATEFULL), configurado um DHCPv6 para a rede que ficará na VLAN 60 e será configurado no roteador da Rede IPv6

- 1 switch CISCO CORE 3560 – *Core IPv6*;
  - Switch de camada três do modelo OSI responsável pela distribuição. Este switch contém funções de roteamento além das funções de camada dois. Assim como na empresa IPv4 foram criadas as VLANs e configuradas as interfaces no modo TRUNK. Estas configurações serviram para demonstrar que o protocolo IPv6 funciona perfeitamente com equipamentos criados e destinados para IPv4. Criada a VLAN 6 destinada para o modo STATELESS e VLAN 60 para o modo STETEFULL.

- 1 SWITCH CISCO 2960 – *Switch IPv6* .
  - Switch de camada dois responsável pelo acesso dos equipamentos, assim como na empresa sobre a rede IPv4, sendo as portas dos equipamentos configuradas para o modo de acesso às VLANs necessárias e a porta com o switch CORE no modo TRUNK.

ISP

a. 1 roteador CISCO 2911 – *Router Externo IPv4*.

b. Os roteadores *Router Externo IPv4 e Router Internet* utilizados foram configurados utilizando o método de transição de Pilha Dupla, representados pela cor laranja da figura 11, para possibilitar o recebimento de pacotes tanto IPv4 quanto IPv6. Configurado Roteamento dinâmico para IPv4 e IPv6.
    i. .Interface para conexão com a rede IPv6 Serial 0/0/1 – Ipv6 2001:6::1/64
    ii. Interface para conexão com a rede IPv4 e Pilha dupla Serial 0/0/0 – Ipv6 2001:b:b:b::2/64 e IPv4 20.13.10.12/30

4.2 CISCO PACKET TRACER®

O Cisco Packet Tracer 6.0.1 é um programa simulador de Rede que permite aos usuários criar, praticar e solucionar problemas em uma Rede.

O software Packet Tracer está disponível gratuitamente somente para instrutores Networking Academy, alunos, ex-alunos, e administradores que estão registrados como usuários do Academy Connection da Cisco. O acesso a este material foi possível graças a um instrutor da CISCO que forneceu acesso para pesquisa e fins acadêmicos.

Inicialmente o projeto iria ser desenvolvido utilizando um roteador da CISCO, porém, com o progresso do desenvolvimento, foi verificado que apenas um roteador não seria possível apresentar e simular uma situação real da maioria das empresas, não sendo possível explorar o roteamento dinâmico sobre Ipv4 e Ipv6.

4.2.1 Por que CISCO?

A maioria das soluções voltadas para infraestrutura e *backbone* estão disponíveis pela CISCO. Várias empresas utilizam equipamentos da CISCO devido a sua estabilidade e vasta gama de soluções, documentações e testes. As técnicas aplicadas neste trabalho utilizadas pela CISCO em sua grande maioria podem ser utilizadas em qualquer equipamento de outras marcas, pois a ideia e o funcionamento é o mesmo. Assim como criação de vlan,

funcionamento de roteadores, subinterfaces, marcação de pacotes, utilização de acl e as técnicas de transição como PILHA DUPLA, TRADUÇÃO e TUNELAMENTO podem ser realizados em outros equipamentos.

Conhecimento nos equipamentos CISCO, adquiridos com o material da CISCO CCNA ajudarão na elaboração do projeto juntamente com a sua solução.

4.3 REQUISITOS DE HARDWARE E SOFTWARE

Para o desenvolvimento do cenário que será apresentado neste trabalho, utilizamos um computador básico com as seguintes configurações:

a) Processador Intel® Core™ 2 i5-2430M CPU 2.40 GHz;
b) 4GB de memória RAM;
c) Placa de vídeo NVIDIA GeForce GT 540M;
d) Hard Disk de 700 GB.

Utilizou-se também os seguintes softwares básicos:

a) Sistema Operacional Microsoft Windows 8 Pro 64 bits – Licenciado;
b) Microsoft Office 2007 – Licenciado;
c) Cisco Packet Tracer 6.0.1.

CAPÍTULO 5 - IMPLEMENTAÇÃO DA SOLUÇÃO, TESTES E RESULTADOS

Neste capítulo será demonstrado o desenvolvimento do trabalho e como foram utilizadas e aplicadas as técnicas de rede para a construção da topologia que representa cada uma das empresas. Será demonstrada a aplicação das técnicas de transição, atribuição de IPs e configurações necessárias para que as duas redes tenham total convergência através destas técnicas.

5.1 EMPRESA IPv4

Esta empresa tem conexão com o seu ISP *Router Externo IPv4* através de uma pilha dupla. Quando a rede tentar conectar a uma rede IPv4 externa ela irá trafegar pela pilha IPv4 e sem divulgar o endereço da sua rede interna através de um NAT. NAT é uma técnica de tradução de endereços visando ocultar os IPs privados de uma rede através de um IP público, e também de fornecer acesso a várias pessoas utilizando apenas um endereço. Graças a esta técnica foi possível prolongar a vida útil do protocolo IPv4.

Quando necessitar acessar uma rede IPv6 ela utilizará o NAT-PT para traduzir endereços IPv6 em IPv4 e vice versa, e trafegará através da pilha dupla para o seu ISP.

Todas as rotas são divulgadas dinamicamente através do RIP e RIPng.

A empresa IPv4 foi segmentada em VLANs, sendo a VLAN 10 destinada para estagiários, VLAN 100 para funcionários e VLAN 1000 para o CPD. A intenção de se criar as VLANs foi de segmentar a rede e de se utilizar endereçamentos de redes diferentes. Isolando-as e para uma futura e melhor gerência.

As redes foram segmentadas da seguinte forma:

- VLAN 10: 172.16.0.0/23 e *gateway* 172.16.0.1. *Gateway* configurado na interface do roteador *Router Internet* utilizando uma subinterface GigabitEthernet 0/0.10
    - Endereço de rede: 172.16.0.0
    - Endereço de broadcast: 172.16.1.255

- VLAN 100: 172.16.2.0/23 e *gateway* 172.16.2.1. *Gateway* configurado na interface do roteador *Router Internet* utilizando uma subinterface GigabitEthernet 0/0.100
    - Endereço de rede: 172.16.2.0
    - Endereço de broadcast: 172.16.3.255

- VLAN 1000: 172.16.4.0/25 e *gateway* 172.16.4.1. *Gateway* configurado na interface do roteador *Router Internet* utilizando uma subinterface GigabitEthernet 0/0.1000
    - Endereço de rede: 172.16.4.0
    - Endereço de broadcast: 172.16.4.127

A figura 5.1 mostra as redes endereçadas em redes diferentes e sendo roteadas pelo *Router Internet.*

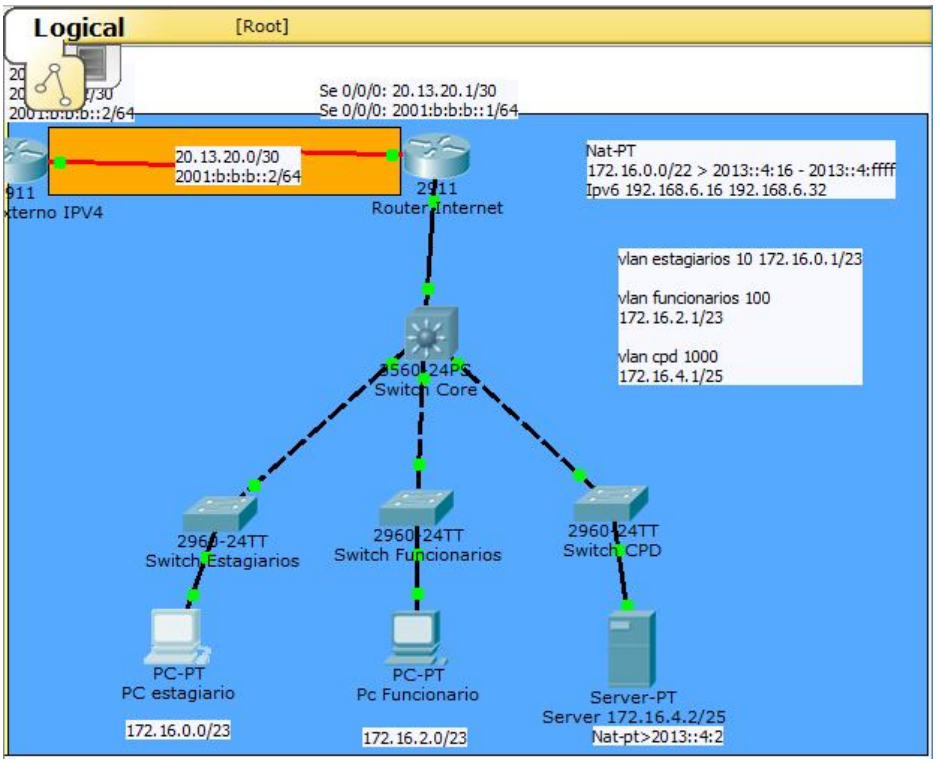

Figura 5.1 – Endereçamento de rede IPv4

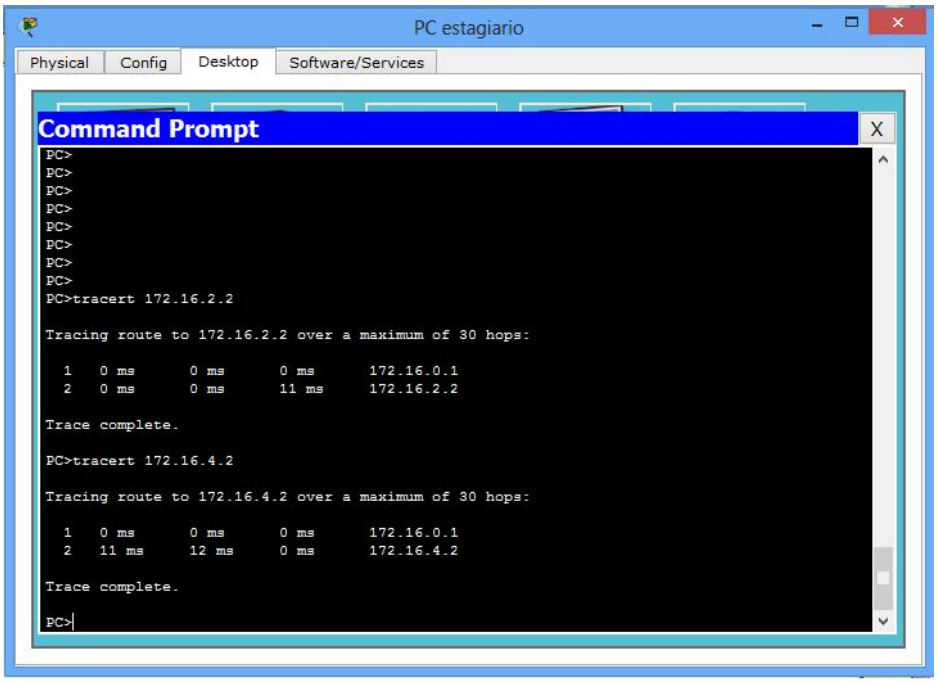

Figura 5.2 - *tracert* realizado do PC estagiário para o PC Funcionário e Server-pt

A figura 5.2 mostra um *tracert* realizado do PC estagiário 172.16.0.2/23 para o PC Funcionario com o IP 172.16.2.2/23 e para Server-PT com IP 172.16.4.2/25. O comando *tracert* mostra o caminho que o pacote utiliza para alcançar o destino, mostrando a quantidade de saltos utilizada até o destino. Neste caso o destino é o IP da rede distinta da origem, sendo necessário ir até o gateway da rede, o roteador, para alcançar o destino.

No *tracert* observa-se que para chegar ao seu destino o pacote teve que ir até o *Router Internet* de IP 172.16.0.1, *gateway* da rede 172.16.0.0/23, por se tratar de redes distintas o pacote é encaminhado sempre para o *gateway* da rede. Se fosse o mesmo segmento de rede ele não necessitaria de consultar o *gateway* para encaminhar os pacotes e a comunicação seria direta.

Este *tracert* foi realizado para demonstrar que há total comunicação entre as VLANs e redes distintas dentro da rede IPv4.

Para que haja esta total integração e comunicação foi necessário configurar os SWITCHs e o roteador. Abaixo segue a configuração utilizada em cada um dos equipamentos: Os comandos utilizados para configuração dos equipamentos estão disponíveis no IOS (*Internetwork Operating System*) da CISCO através da tecla “?”. Este tecla exibe os comandos disponíveis ajudando desta forma a configurar os equipamentos de acordo com a necessidade.

5.1.1 Switch estagiários

Ilustrado na figura 5.1, segue a configuração necessária para criação das VLANs do switch da sub-rede destinada para os estagiários.

```
Switch>
Switch>en
# Comando en habilita o modo privilegiado, administrativo do equipamento
Switch#config terminal
# Comando config terminal habilita o modo de configuração do equipamento
Criando as VLANs 10, 100 e 1000
Switch(config)#vlan 10
Switch(config-vlan)#name Estagiarios
Switch(config-vlan)#exit
Switch(config)#vlan 100
Switch(config-vlan)#name Funcionarios
Switch(config-vlan)#exit
Switch(config)#Vlan 1000
Switch(config-vlan)#name CPD
Switch(config-vlan)#exit
```

Aplicando as VLANs no modo **acesso** para as interfaces que serão conectados os equipamentos.

```
Switch(config)#interface range fastEthernet 0/2 - fastEthernet 0/24
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#switchport access vlan 10
#Vlan 10 destinada aos estagiários
Switch(config-if-range)#exit
```

 # swichport mode access serve para que equipamentos não tenham que marcar o pacote identificando a sua vlan, quem fará isso será o *switch.* Neste modo só é possível passar uma VLAN para a interface do switch.

Aplicando o **trunk** na interface de conexão entre os SWITCHs. O *trunk* nos equipamentos da CISCO utilizam o dot1q, o qual serve para passar e identificar várias VLANs.

```
Switch(config)#interface fastEthernet 0/1
Switch(config-if)#switchport mode trunk
Switch(config-if)#switchport trunk allowed vlan all
```

```
Switch(config-if)#exit
```

Identificando e aplicando um nome para o *Switch*

```
Switch(config)#hostname sw-estagiarios
sw-estagiarios(config)#
```

Após as configurações, elas já estão em execução, porém não estão salvas, se reiniciar o equipamento a configuração será perdida. Para salvar basta digitar o comando **wr** no modo privilegiado ou **do wr** no modo de configuração.

```
sw-estagiarios#wr
Building configuration...
[OK]
```

As configurações realizadas podem ser verificadas através do comando **show running-config** no modo privilegiado. Para verificar a configuração que é utilizada após iniciar, ligar o equipamento é show **startup-config.**

```
sw-estagiarios#show running-config
```

Consultar Apêndice A configuração do switch.

5.1.2 Switch funcionários

A configuração utilizada é a mesma do switch Estagiarios, o que muda é o hostname e a VLAN de acesso das interfaces que serão conectados os equipamentos. Na figura 5.1 pode-se verificar a posição desse switch.

```
Switch(config)#interface range fastEthernet 0/2 - fastEthernet 0/24
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#switchport access vlan 100
Switch(config-if-range)#exit
Switch(config)#hostname sw-funcionarios
sw-funcionarios#
```

Para verificar a configuração do switch

```
sw-funcionarios#show running-config
```

5.1.3 Switch CPD

A configuração utilizada é a mesma dos outros SWITCHs, o que muda é o hostname e a VLAN de acesso das interfaces que serão conectados os equipamentos.

```
Switch(config)#interface range fastEthernet 0/2 - fastEthernet 0/24
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#switchport access vlan 1000
Switch(config-if-range)#exit
Switch(config)#hostname sw-CPD
sw-CPD#
```

Para verificar a configuração do switch

```
sw-CPD#show running-config
```

5.1.4 Switch Core

Este switch demonstrado na Figura 5.1 é considerado um switch de distribuição da rede, de acordo com o conceito da CISCO. A rede deve ter acesso, distribuição e núcleo, representados respectivamente pelos switchs (estagiários, funcionários e CPD), switch core e o roteador.

Neste switch foi configurado trunk em todas as suas conexões, conexão destinada para outros switch’s e roteadores. No modo trunk é necessário habilitar o encapsulamento por dot1q para transportar todas as VLANs necessárias.

```
Switch(config)#interface range fastEthernet 0/1 - fastEthernet 0/24
Switch(config-if-range)# switchport trunk encapsulation dot1q
Switch(config-if-range)#switchport mode trunk
Switch(config-if-range)#exit
Switch(config)#hostname sw-core
```

Para verificar a configuração do switch

```
sw-core#show running-config
```

5.1.5 Router Internet

Este roteador será o grande responsável por permitir o acesso a uma rede IPv6 ao seu ISP e roteamento da sua rede interna. Permitir que a sua rede privada tenha acesso a uma rede pública através de soluções apresentadas neste trabalho.

Primeiramente para fácil identificação foi atribuído um nome para este roteador através do comando “hostname INTERNET” no modo de configuração.

Para que a rede interna funcione entre elas, que estão em segmento de rede e VLANs diferentes é necessário criar as subinterfaces as encapsulando com dot1q com a vlan desejada.

Estas subinterfaces serão o *gateway* das redes, ou seja, responsável pelo roteamento das redes, para redes conhecidas ou não.

Os seguintes comandos a partir do modo de configuração são para criar e atribuir ip para as subinterfaces:

Para se utilizar uma vlan no roteador é necessário criar uma subinterface com o mesmo número da vlan e encapsular utilizando o protocolo 802.1q, conhecido também como dot1q.

```
INTERNET(config)# interface GigabitEthernet0/0.10
INTERNET(config-subif)# description Estagiarios
INTERNET(config-subif)# encapsulation dot1Q 10
INTERNET(config-subif)# ip address 172.16.0.1 255.255.254.0
```

```
INTERNET(config)# interface GigabitEthernet0/0.100
INTERNET(config-subif)# description Funcionarios
INTERNET(config-subif)# encapsulation dot1Q 100
INTERNET(config-subif)# ip address 172.16.2.1 255.255.254.0
```

```
INTERNET(config)# interface GigabitEthernet0/0.1000
INTERNET(config-subif)# description CPD
INTERNET(config-subif)# encapsulation dot1Q 1000
INTERNET(config-subif)# ip address 172.16.4.1 255.255.255.128
```

Após as configurações acima é necessário ligar interface da rede interna.

```
INTERNET(config)#interface GigabitEthernet0/0
INTERNET(config-if)#no shutdown
```

Após criar as subinterfaces, as redes 172.16.0.0/23, 172.16.2.0/23 e 172.16.4.0/25 serão capazes de convergirem e se comunicarem.

Para comunicar com o ISP *Router Externo IPv4* será necessário configurar a interface de saída da rede, a serial 0/0/0.

```
INTERNET(config)#       interface Serial0/0/0
INTERNET(config-if)# ip address 20.13.20.1 255.255.255.252
INTERNET(config-if)# clock rate 64000
```

Nesta interface é necessário definir o *clock rate* para que haja comunicação com o outro roteador, por se tratar de uma interface DCE, de acordo com normas e o curso da CISCO.

Será necessário configurar o roteador *Router Externo IPv4* que representa o ISP para que haja uma comunicação, conforme figura 5.3:

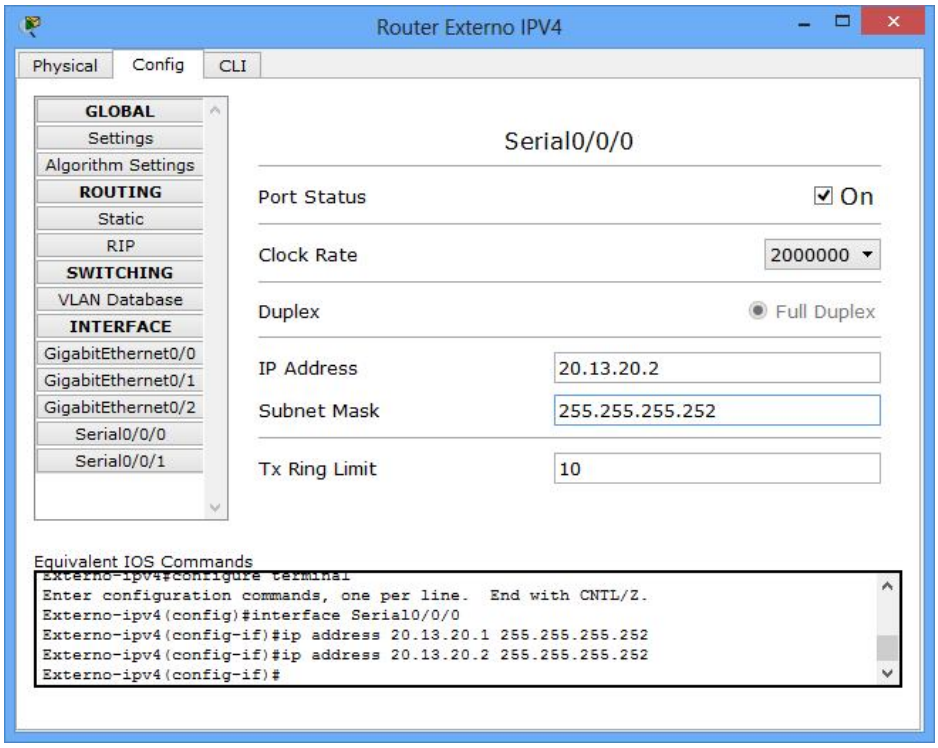

Figura 5.3 – Configuração do roteador Router Externo IPv4

Com estas configurações a rede interna ainda não conseguirá se comunicar com a rede externa, por que ao chegar no *Router Externo IPv4* o pacote não conseguirá voltar, pois o outro roteador não conhece as redes internas, ou seja, o pacote chegará ao destino mas não retornará.

Para que haja a comunicação é necessário divulgar a sua rede para o outro roteador, ou por roteamento estático ou por roteamento dinâmico. Como foi abordado no trabalho o RIP,

será utilizado este roteamento de vetor de distância para divulgar a sua rede interna. O problema é que desta forma estará sendo divulgada toda a rede interna para outros roteadores, para contornar este problema será utilizado a tradução de endereços, posteriormente.

```
INTERNET(config)#       router rip
INTERNET(config-router)#        version 2
INTERNET(config-router)#        network 20.0.0.0
INTERNET(config-router)#        network 172.16.0.0
```

A CISCO recomenda que sejam divulgadas e informadas, todas as redes diretamente conectada em seu protocolo de roteamento, para que roteadores mais distantes tenham acesso a esta rede. Se caso fosse divulgada apenas a rede 172.16.0.0 ela teria conexão com todas as outras redes, porém a rede 20.0.0.0 teria apenas conexão com o roteador diretamente conectado.

É necessário, então, configurar o *Router Externo IPv4* para receber e divulgar as rotas pelo RIP.

```
Externo-IPv4(config)# router rip
Externo-IPv4(config-router)# version 2
Externo-IPv4(config-router)# network 20.0.0.0
```

Após estas configurações a comunicação será possível com o roteador *Router Externo IPv4*, porém com as rotas internas, privadas, divulgadas. Para evitar isso será configurado o NAT no roteador INTERNET

```
INTERNET(config)#       ip nat inside source list 10 interface Serial0/0/0 overload
```

O *overload* habilitará o NAT dinâmico, para economizar IP a tradução utilizará o IP da interface serial 0/0/0 e a comunicação garantida através de portas distintas.

Com isso fará com que a tradução de endereços aceite uma ACL (*access list*) numerada 10 para traduzir através da interface serial 0/0/0, mas para isso deve-se criar a ACL numerada.

```
INTERNET(config)#access-list 10 permit 172.16.0.0 0.0.7.255
```

Esta ACL está permitindo todos os *hosts* da rede 172.16.0.0/21, ou seja, do *host* 172.16.0.1 ao 172.16.7.254.

Para o NAT funcionar tem que informar aonde ocorrerá o NAT e qual a direção da tradução. Para a rede privada será inserido NAT INSIDE e para rede pública, externa, NAT OUTSIDE.

```
INTERNET(config)#       interface GigabitEthernet0/0.10
INTERNET(config-subif)# ip nat inside
```

```
INTERNET(config)#       interface GigabitEthernet0/0.100
INTERNET(config-subif)# ip nat inside
INTERNET(config)#       interface GigabitEthernet0/0.1000
INTERNET(config-subif)# ip nat inside
```

```
INTERNET(config)#       interface Serial0/0/0
INTERNET(config-if)# ip nat outside
```

Depois de configurado o NAT, as traduções realizadas podem ser verificadas através do comando:

```
INTERNET#show ip nat translations
Pro  Inside global     Inside local       Outside local      Outside global
tcp 20.13.20.1:4000    172.16.0.2:4000    20.13.20.2:23      20.13.20.2:23
```

Esta tradução ocorrida anteriormente mostra o host 172.16.0.2 realizando um *telnet* para o *Router Externo IPv4* pela porta 4000 (aleatória) para a 23 (*telnet*).

Ao realizar a captura dos pacotes pode-se verificar a tradução ocorrendo no roteador *INTERNET* e a troca de IP de acordo com as figuras 5.4 e 5.5.

Abaixo seguem as imagens com o caminhos do pacote até o roteador *Router Externo* IPv4. A figura 5.4 mostra a PDU do pacote com o *telnet* realizado.

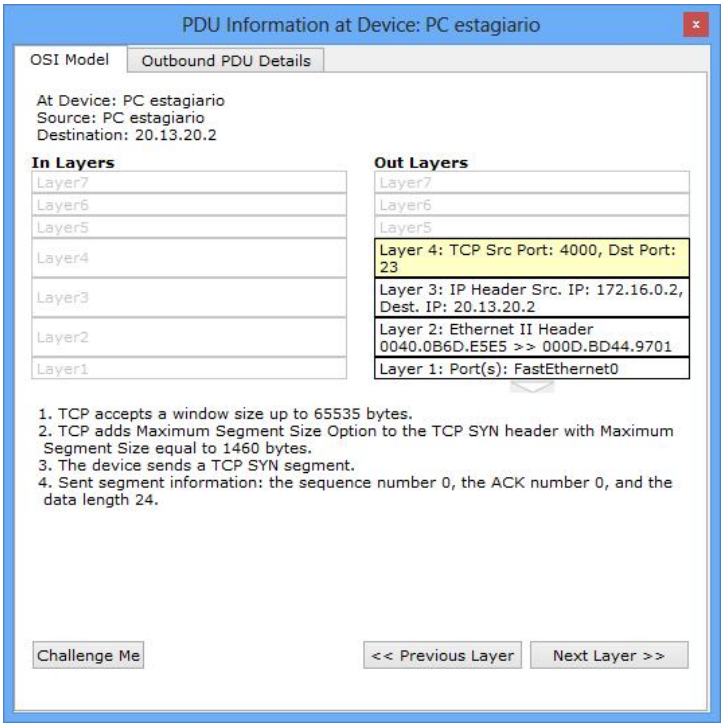

Figura 5.4 - Telnet originado do PC Estagiario pela porta 4000 para a porta 23

A figura 5.5 mostra a troca do IP de origem, alterando a origem coma técnica de NAT.

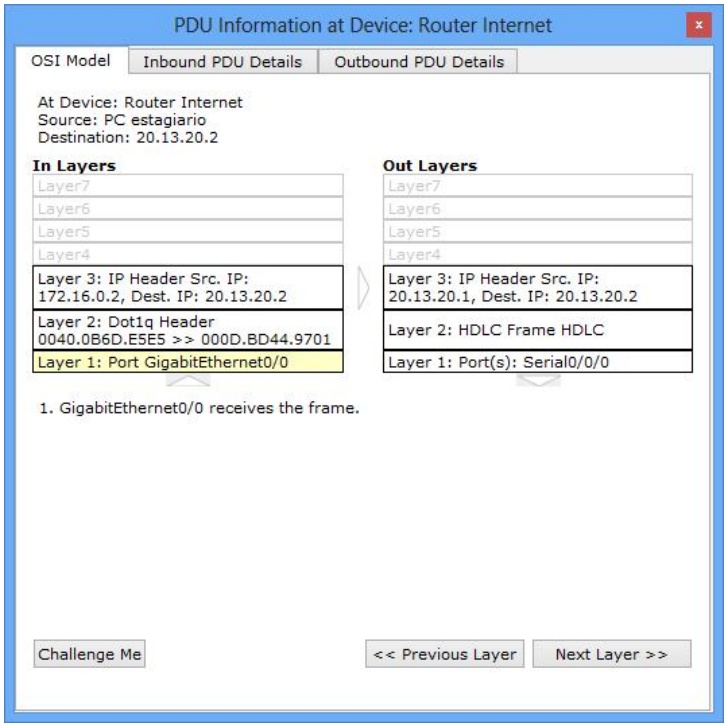

Figura 5.5 - O IP de origem sendo trocado no roteador Router Internet para 20.13.20.1

Figura 5.6 mostra o roteador Externo aceitando a conexão *telnet* do PC Estagiário com o seu ip traduzido, origem, 20.13.20.2.

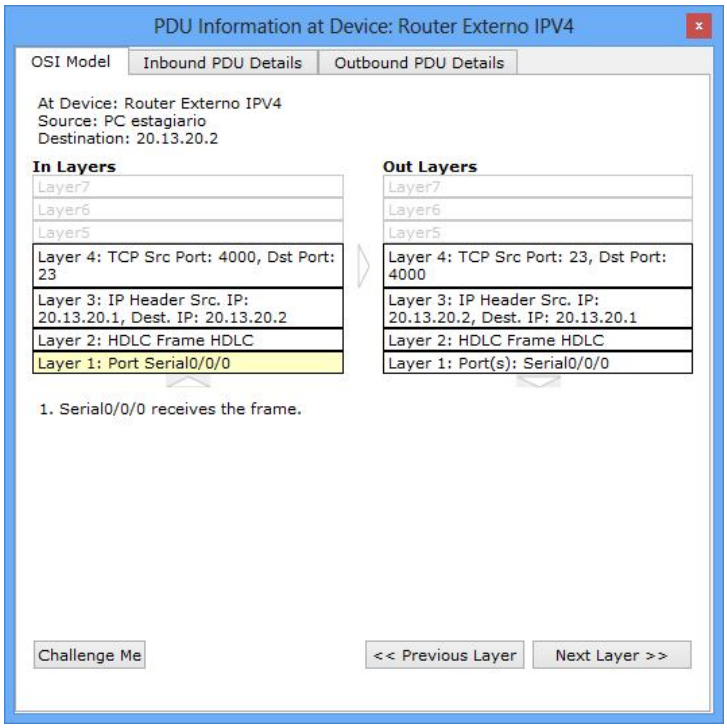

Figura 5.6 - Roteador Router Externo IPv4 recebendo o telnet com o ip de origem 20.13.20.1 e devolvendo a solicitação do telnet.

A figura 5.7 mostra o pacote voltando com a requisição e traduzindo novamente para o endereço de origem original do PC Estagiário.

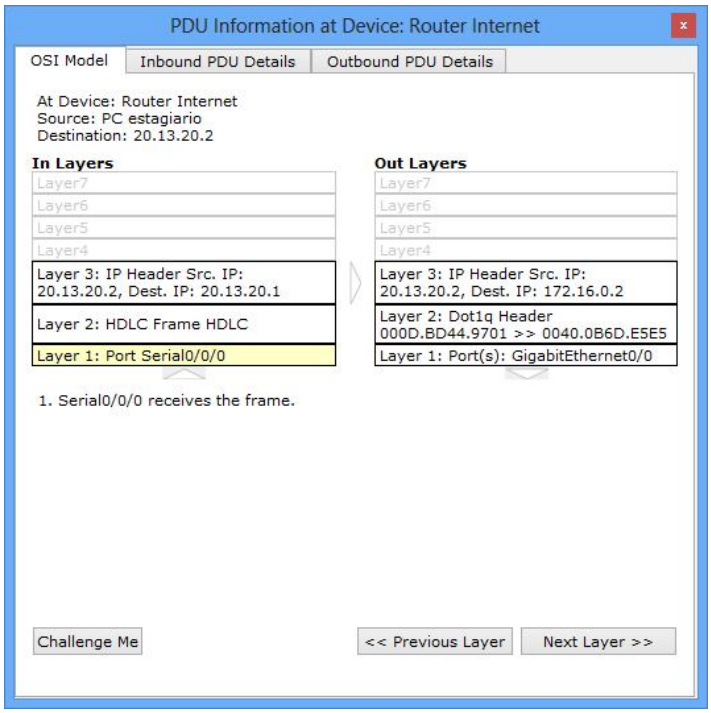

Figura 5.7 - Pacote voltando e traduzindo novamente no roteado Router Internet o ip de destino para o endereço correto 172.16.0.2

A figura 5.8 mostra a conexão *telnet* estabelecida entre o PC Estagiário e o Roteador Externo.

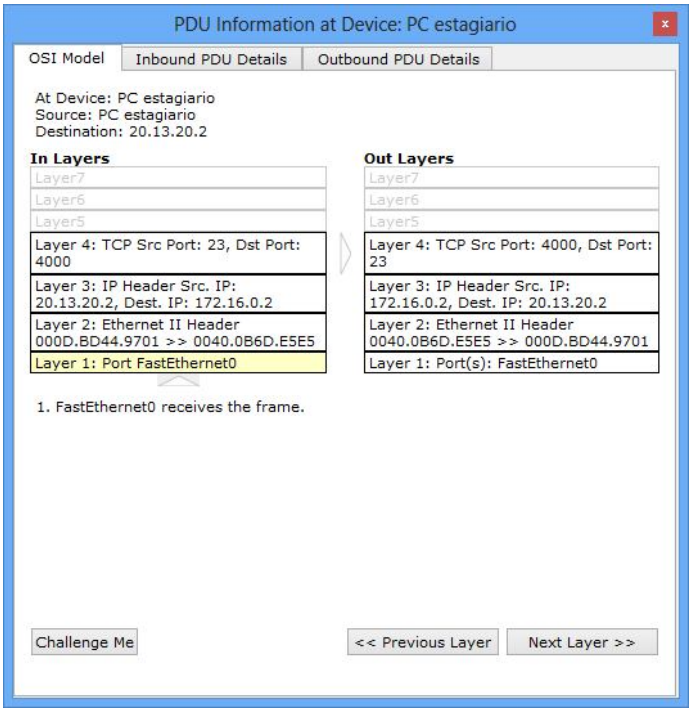

Figura 5.8 - Pacote recebido no PC Estagiário com o telnet bem sucedido.

A figura 5.9 mostra a tradução sendo feita e a alteração do cabeçalho do IPv4.

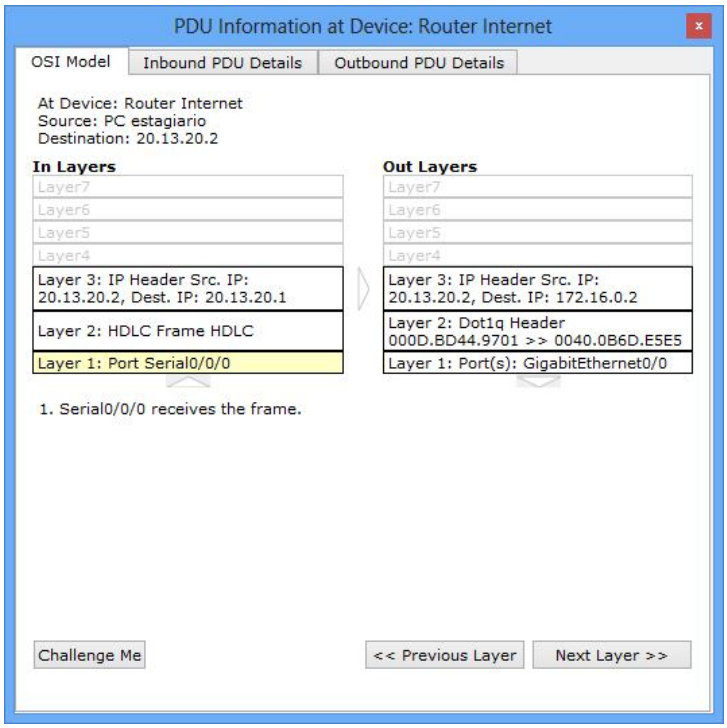

Figura 5.9 – Tradução NAT do IP 20.13.20.1 para o IP 172.16.0.2

5.2 EMPRESA IPv6

A empresa IPv6 é uma empresa fictícia que entrou no mercado recentemente. Todos os seus equipamentos são compatíveis com o protocolo IPv6. Neste cenário fictício será mostrada a configuração para que ela funcione com o protocolo IPv6 seguindo alguns padrões, segmentando-a com VLANs, subinterfaces, redes distintas, com o modo STATEFULL e STATELESS. Empresa é representada pela área amarela da figura 4.1.

Essa empresa tem conexão com o seu ISP *Router Externo IPv4* através de um endereço IPv6 único.

Nessa empresa não é necessária a configuração de NAT, pois os endereços IPv6 são únicos e de uma grandeza incontável. O NAT será necessário apenas para traduzir endereços IPv4 para IPv6 e vice versa. Para continuar a comunicação com futuros equipamentos legados. O NAT compatível com equipamentos CISCO é o NAT-PT, já explicado anteriormente.

Assim como a empresa IPv4 a empresa IPv6 foi segmentada em VLANs, esta segmentação serve para demonstrar total compatibilidade do protocolo IPv6 com a

infraestrutura já conhecida, e também, demonstrar separadamente o conceito STATEFULL e STATELESS do IPv6.

Foram criadas as VLANs 6 e 60, sendo que a VLAN 6 foi destinada aos equipamentos que adquirirão endereçamento IPv6 através do modo STATELESS e a VLAN 60 destinada aos equipamentos que funcionarão no modo STATEFULL.

A VLAN 6 será responsável para a demonstração do modo STATELESS se encontra na rede 2010:1::/64.

A VLAN 60 será responsável para a demonstração do modo STATEFULL se encontra na rede 2012:2::/64. Este modo será descrito através do DHCPv6.

A seguir apresenta-se as configurações dessa empresa.

5.2.1 Switch IPv6

Será criado as VLANs 6 e 60 neste switch e configurado o *trunk* para comunicação com o switch *CORE IPv6* e transportar as duas VLANs através de uma única conexão

```
Switch(config)#vlan 6
Switch(config-vlan)#name vlan-stateless
Switch(config-vlan)#exit
Switch(config)#vlan 60
Switch(config-vlan)# name vlan-statefull
Switch(config-vlan)# exit
```

```
Switch(config)#interface GigaEthernet 0/1
Switch(config-if)#switchport mode trunk
Switch(config-if)#switchport trunk allowed vlan all
Switch(config-if)#exit
```

Associando a VLAN 60 a um conjunto de portas no modo acesso.

```
Switch(config)#interface range fastEthernet 0/1 - fastEthernet 0/2
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#switchport access vlan 60
Switch(config-if-range)#exit
```

Associando a VLAN 6 a um conjunto de portas no modo acesso.

```
Switch(config)#interface range fastEthernet 0/3 - fastEthernet 0/4
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#switchport access vlan 6
Switch(config-if-range)#exit
```

Atribuindo um nome para identificação deste *switch*

```
Switch(config)#hostname sw-IPv6
sw-IPv6#
```

Para visualizar as configurações deste *switch*

```
sw-IPv6#show running-config
```

5.2.2 Core IPv6

Configurado todas as portas como *trunk* encapsulando dot1q.

```
Switch(config)#interface range fastEthernet 0/1 - fastEthernet 0/24
Switch(config-if-range)# switchport trunk encapsulation dot1q
Switch(config-if-range)#switchport mode trunk
Switch(config-if-range)#exit
Switch(config)#interface range gigaEthernet 0/1 - gigaEthernet 0/2
Switch(config-if-range)# switchport trunk encapsulation dot1q
Switch(config-if-range)#switchport mode trunk
Switch(config-if-range)#exit
```

Atribuindo um nome para identificação deste *core:*

```
Switch(config)#hostname core-IPv6
core-IPv6#
```

Para verificar as configurações deste *core:*

```
core-IPv6#show running-config
```

5.2.3 Router externo IPv6

Este roteador será responsável pela comunicação dos equipamentos internos, pela sua convergência e comunicação com a rede externa.

Para fácil identificação foi atribuído um nome para este roteador através do comando **hostname Externo-IPv6** no modo de configuração global (**router(config)#**).

Para o correto funcionamento e roteamento no modo IPv6 é necessário habilita-lo. Por default a opção de roteamento no modo IPv6 vem desabilitada nos equipamentos da CISCO.

```
Externo-IPv6 (config)# IPv6 unicast-routing
```

As subinterfaces serão o *gateway* de suas respectivas redes.

A configuração das subinterfaces necessárias para a comunicação e convergência da rede interna segue logo abaixo:

```
Externo-IPv6(config)#interface GigabitEthernet0/0.6
 Externo-IPv6(config-subif)#description IPv6 stateless
Externo-IPv6(config-subif)#encapsulation dot1Q 6
```

O comando a seguir servirá para retirar qualquer IPv4 desta subinterface, para evitar pilha dupla.

```
Externo-IPv6(config-subif)#no ip address
```

Habilitando o IPv6 para esta subinterface:

```
Externo-IPv6(config-subif)#IPv6 enable
```

Habilitando o modo STATELESS EUI-64:

```
Externo-IPv6(config-subif)#IPv6 address 2010:1::/64 eui-64
```

Antes de configurar a subinterface da VLAN 60, no modo *statefull* será configurado o DHCPv6 no roteador.

```
Externo-IPv6(config)# IPv6 dhcp pool dhcpv6
```

Habilitando o DHCPv6 local com o seu espaço de endereços:

```
Externo-IPv6(config)# IPv6 local pool dhcpv6 2012:2::/120 124
```

O comando a seguir define o tempo de vida para 3.600 segundos para o modo depreciado e em seguida o preferido.

```
Externo-IPv6(config-dhcp)# prefix-delegation pool dhcpv6 lifetime 3600 3600
```

Após configurar o DHCP com o nome DHCPv6 será necessária a configuração da interface que utilizará o modo STATEFULL.

```
Externo-IPv6(config)#interface GigabitEthernet0/0.60
```

```
Externo-IPv6(config-subif)# description statefull
Externo-IPv6(config-subif)# encapsulation dot1Q 60
Externo-IPv6(config-subif)#no ip address
Externo-IPv6(config-subif)# IPv6 enable
```

Atribuído um endereço IPv6 para esta subinterface:

```
Externo-IPv6(config-subif)#IPv6 address 2012:2::1/64
```

Este endereço é igual ao 2012:2:0:0:0:0:0:2/64, sendo que 2012:2:0:0 destinados para endereço de rede e 0:0:0:2 para endereço de *host*. Os números zeros não precisam ser informados, podendo serem resumidos da seguinte maneira 2012:2::2/64.

Habilitando o DHCPv6 na subinterface e colocando-a no modo servidor:

```
Externo-IPv6(config-subif)#IPv6 dhcp server dhcpv6
```

Lembrando que após as configurações das subinterfaces é necessário ligá-las através do seguinte comando:

```
Externo-IPv6(config)# interface giga 0/0
Externo-IPv6(config-if)#no shutdown
```

Após estas configurações todos os equipamentos que estiverem ligados a subinterface e configurados no modo DHCP receberão endereço de IP e como *gateway* o endereço da interface do roteador, conforme Figura 5.10:

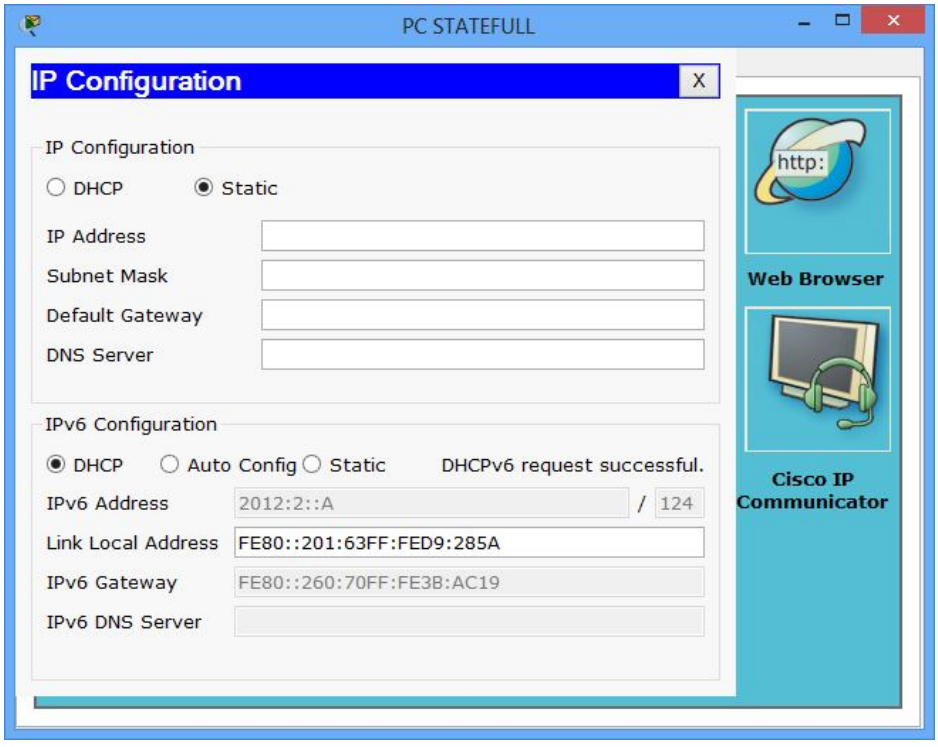

Figura 5.10 - Endereço de IP e gateway do PC STATEFULL.

Para configuração com o ISP *Router Externo IPv6* é necessária a configuração da interface serial, podendo ser atribuído o IP de modo STATELESS, mas para fácil gerência e dedução foi atribuído um endereço de IP estaticamente.

```
Externo-IPv6(config)# interface Serial0/0/0
Externo-IPv6(config-if)# no ip address
Externo-IPv6(config-if)# IPv6 address 2001:6::2/64
Externo-IPv6(config-if)# clock rate 64000
```

Como foi dito anteriormente é necessária a configuração *clock rate* por se tratar de uma conexão do tipo DCE. Conexões DCE são a fêmea do *plug* do cabo serial.

Após esta configuração é necessário configurar o ISP *Router externo IPv4* para a correta comunicação e convergência de rede.

```
Externo-IPv4(config)#interface serial 0/0/1
Externo-IPv4(config-if)# no ip address
Externo-IPv4(config-if)# IPv6 address 2001:6::1/64
Externo-IPv4(config-if)# IPv6 enable
```

Desta forma foi habilitada a conexão entre os roteadores *Router Externo IPv6* e o *Router Externo IPv4*. Mas a conexão só é possível entre eles. A rede IPv6 da empresa não conseguirá se comunicar com o ISP *Router Externo IPv4* se não for configurado uma rota padrão (rota estática) ou rota dinâmica.

De acordo com a CISCO rota padrão serve para quando um pacote não souber para aonde ser encaminhado ter uma rota de fuga, ou seja, o pacote chegará no roteador *Router Externo IPv4* com origem 2012:2::1/64, porém ele desconhece esta rede. Se tiver uma rota padrão , representada por ::/0, configurada ele encaminharia o pacote para esta rota.

No modo de configuração global o comando para a configuração de uma rota padrão é:

```
IPv6 route ::/0 [interface ou IP do próximo salto] podendo ser
IPv6 route ::/0 serial 0/0/1 ou IPv6 route ::/0 2001:6::2
```

Contudo, o objetivo é que os roteadores aprendam as rotas de maneira dinâmica. Será configurado o RIPng.

No RIP era necessário divulgar as redes que estavam diretamente conectadas, diferentemente no RIPng, RIP do IPv6. No RIPng basta configurar o RIP e atribuí-lo nas interfaces que gostaria que divulgasse a rede. A sua distância administrativa (120) continua a mesma e com as limitações do RIP para IPv4. De acordo com a CISCO a distância administrativa serve para dar prioridade ao roteamento dinâmico. Caso crie-se uma rota

estática sua distância administrativa será igual a um, desta forma tendo prioridade sobre o RIP. A distância administrativa pode ser alterada.

Abaixo segue as configurações necessárias para a divulgação das redes dinamicamente pelo RIPng:

```
Externo-IPv6(config)# IPv6 router rip rIPv6
Externo-IPv6(config-rtr)#exit
```

Após criar o *rip* com o nome rIPv6 é necessário ativa-lo nas interfaces desejadas:

```
Externo-IPv6(config)# interface GigabitEthernet0/0.6
Externo-IPv6(config-subif)# IPv6 rip rIPv6 enable
Externo-IPv6(config-subif)# exit
Externo-IPv6(config)# interface GigabitEthernet0/0.60
Externo-IPv6(config-subif)# IPv6 rip rIPv6 enable
Externo-IPv6(config-subif)# exit
Externo-IPv6(config)# interface Serial0/0/0
Externo-IPv6(config-if)#  IPv6 rip rIPv6 enable
```

Agora será necessário configurar o RIPng também no *Router Externo IPv4:*

```
Externo-IPv4(config)# interface Serial0/0/1
Externo-IPv4(config-if)#IPv6 rip rIPv6 enable
```

Lembrando que após todas as configurações é necessário salva-las através do comando **wr** no modo privilegiado:

```
Externo-IPv6# wr
```

Após as configurações pode ser verificada através do comando show running-config:

```
Externo-IPv6#show running-config
```

Após estas configurações realizadas será possível os *hosts* se comunicarem com o ISP *Router Externo IPv4.*

Como podemos verificar através do comando *tracert* realizado através do PC STATEFULL e PC STATELESS.

A figura 5.11 mostra a convergência entre redes distintas que estão no modo STATEFULL e STATELESS; ao realizar o comando *tracert no prompt* de comando do PC STATEFULL verifica-se que o destino foi alcançado passando pela interface do roteador de IP **2012:2**::1/64 para alcançar o destino **2001:6**::1/64

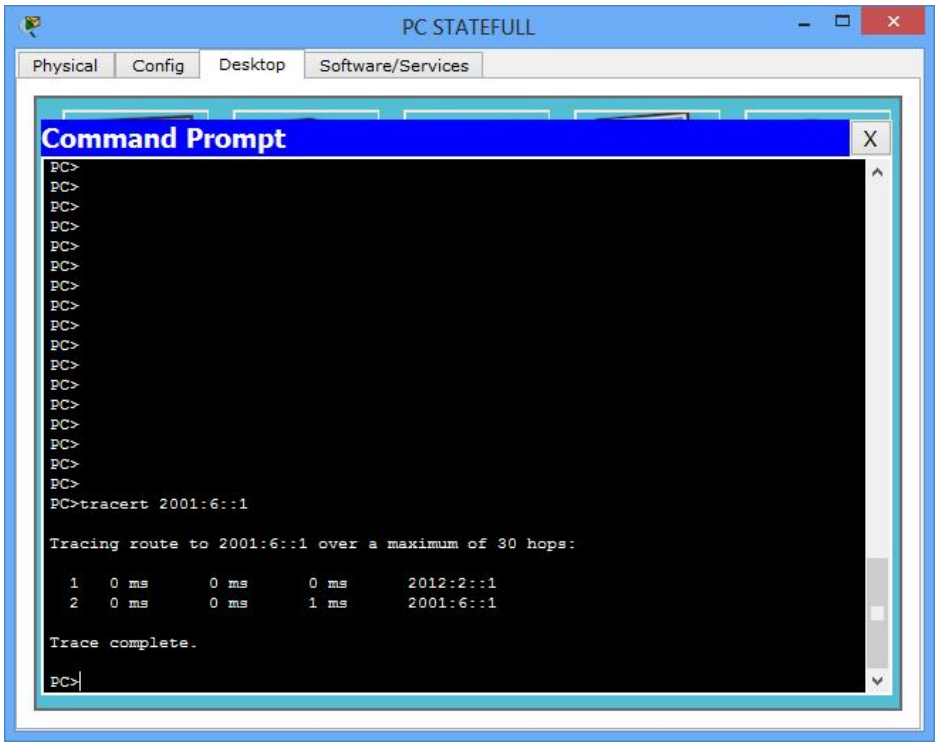

Figura 5.11 - Tracert do PC STATEFULL para o PC STATELESS.

A Figura 5.12 mostra o caminho que o PC que está na rede STETELESS precisa realizar para alcançar o *Router Externo* que tem um endereço IPv6 de uma rede distinta a sua.

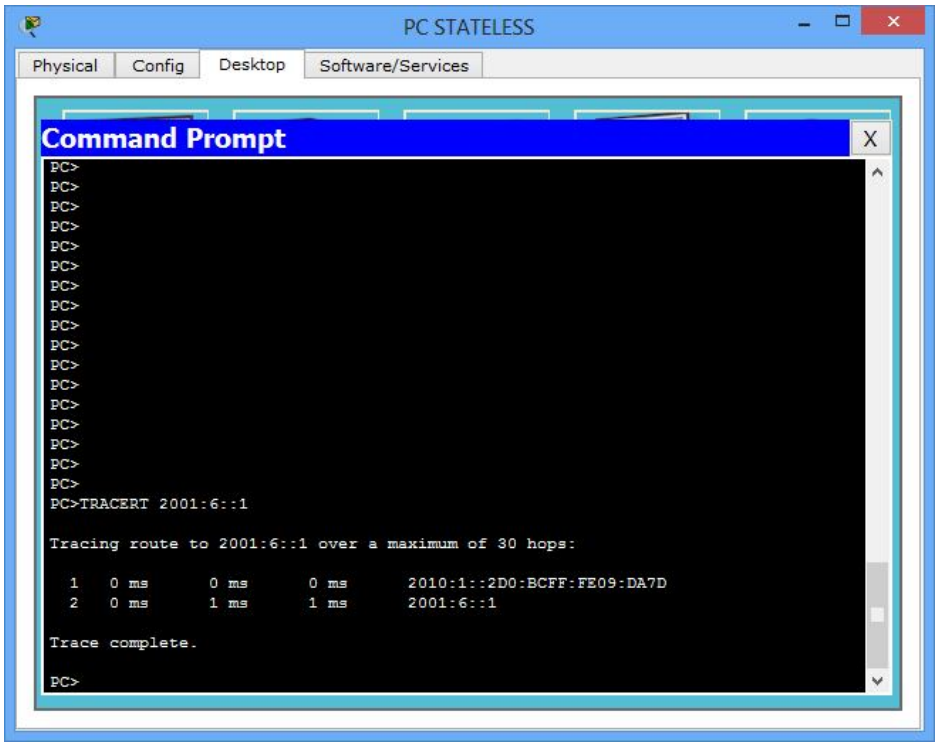

Figura 5.12 - Tracert do PC STATELESS para o roteador Router Externo IPv4.

5.3 CONFIGURANDO PILHA DUPLA

Após as configurações realizadas temos o seguinte cenário: a empresa IPv6 conseguindo se comunicar com o seu ISP assim como a empresa IPv4, mas elas não conversam entre sim, funcionam independentemente.

A empresa IPv6 ainda não consegue se comunicar com a empresa IPv4, isso porque os protocolos IPv6 e IPv4 são incompatíveis, para que elas consigam conversar será necessário configurar um NAT-PT e uma técnica de pilha dupla na empresa IPv4.

Já que será configurado um NAT-PT na empresa IPv4 não será necessário configurá-lo na empresa IPv6, por dois motivos. Se configurar na rede IPv6 não será possível divulgar a rede IPv4 a não ser que configure a pilha dupla nela. O segundo motivo é que o interesse em não ficar isolada do mundo é da empresa no modelo IPv4, então ela terá que se adaptar a nova realidade do mundo.

Para viabilizar a comunicação entre redes e Internet funcionando nos dois protocolos os ISP irão se adaptar a nova realidade; já existem alguns com técnicas de tunelamento, pilha dupla para comportar as duas redes.

O ISP deste cenário fictício ainda não foi configurado com pilha dupla, ao configurá-lo com pilha dupla ele conseguirá rotear pacotes de rede para os dois protocolos, mas não fará eles conversarem entre si.

Para configurar pilha dupla no ISP *Router Externo IPv4* basta adicionar um endereço IPv6 na interface que tem conexão com o IPv4 e na Empresa IPv4 também. Como já foi configurado também o roteamento dinâmico RIP e RIPng basta habilitá-los.

```
Externo-IPv4(config)# interface Serial0/0/0
Externo-IPv4(config-if)# IPv6 address 2001:B:B:B::2/64
Externo-IPv4(config-if)#  IPv6 rip rIPv6 enable
```

```
INTERNET(config)# IPv6 unicast-routing
INTERNET(config-rtr)# IPv6 router rip rIPv6
INTERNET(config-rtr)# exit
INTERNET(config)# interface Serial0/0/0
INTERNET(config-if)#  IPv6 enable
INTERNET(config-if)#  IPv6 address 2001:B:B:B::1/64
```

```
INTERNET(config-if)# IPv6 rip rIPv6 enable
```

Após configurar um endereço IPv6 no roteador INTERNET juntamente com o RIPng já é possível verificar a tabela de roteamento IPv6 nos roteadores:

```
Externo-IPv6#show IPv6 route
IPv6 Routing Table - 8 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
       U - Per-user Static route, M - MIPv6
       I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary
       O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
       ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
       D - EIGRP, EX - EIGRP external
C   2001:6::/64 [0/0]
     via ::, Serial0/0/0
L   2001:6::2/128 [0/0]
     via ::, Serial0/0/0
R   2001:B:B:B::/64 [120/2]
     via FE80::2E0:F7FF:FE15:C102, Serial0/0/0
C   2010:1::/64 [0/0]
     via ::, GigabitEthernet0/0.6
L   2010:1::2D0:BCFF:FE09:DA7D/128 [0/0]
     via ::, GigabitEthernet0/0.6
C   2012:2::/64 [0/0]
     via ::, GigabitEthernet0/0.60
L   2012:2::1/128 [0/0]
     via ::, GigabitEthernet0/0.60
L   FF00::/8 [0/0]
     via ::, Null0

Externo-IPv4>show IPv6 route
IPv6 Routing Table - 7 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
       U - Per-user Static route, M - MIPv6
       I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary
       O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
       ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
       D - EIGRP, EX - EIGRP external
```

```
C   2001:6::/64 [0/0]
     via ::, Serial0/0/1
L   2001:6::1/128 [0/0]
     via ::, Serial0/0/1
C   2001:B:B:B::/64 [0/0]
     via ::, Serial0/0/0
L   2001:B:B:B::2/128 [0/0]
     via ::, Serial0/0/0
R   2010:1::/64 [120/2]
     via FE80::201:43FF:FE20:AA74, Serial0/0/1
R   2012:2::/64 [120/2]
     via FE80::201:43FF:FE20:AA74, Serial0/0/1
L   FF00::/8 [0/0]
     via ::, Null0

INTERNET>show IPv6 route
IPv6 Routing Table - 6 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
       U - Per-user Static route, M - MIPv6
       I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary
       O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
       ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
       D - EIGRP, EX - EIGRP external
R   2001:6::/64 [120/2]
     via FE80::2E0:F7FF:FE15:C101, Serial0/0/0
C   2001:B:B:B::/64 [0/0]
     via ::, Serial0/0/0
L   2001:B:B:B::1/128 [0/0]
     via ::, Serial0/0/0
R   2010:1::/64 [120/3]
     via FE80::2E0:F7FF:FE15:C101, Serial0/0/0
R   2012:2::/64 [120/3]
     via FE80::2E0:F7FF:FE15:C101, Serial0/0/0
L   FF00::/8 [0/0]
     via ::, Null0
```

Após esta configuração a empresa IPv6 conseguirá estabelecer conexão com a empresa IPv4 através da rede IPv6.

A Figura 5.13 mostra a conexão da empresa IPv6 com o roteador da empresa IPv4 configurado com pilha dupla, ou seja, com endereços IPv6 e IPv4 na interface externa a sua rede.

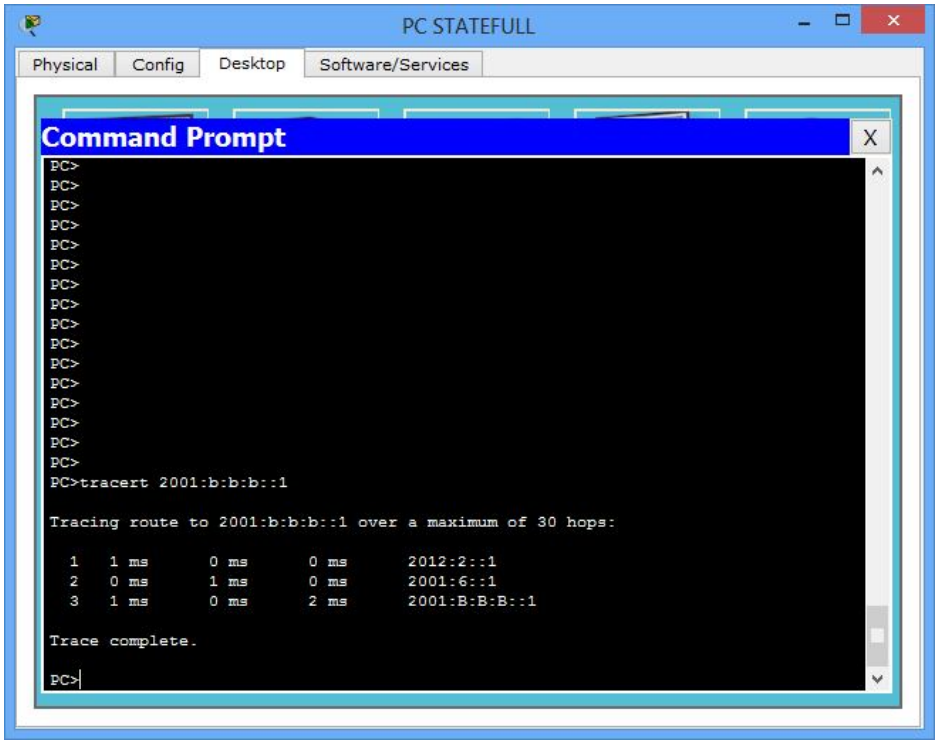

Figura 5.13 – Tracert do PC STATEFULL para o roteador Router Internet.

5.4 ISP

O Roteador *Router Externo IPv4* neste cenário fictício está representando o ISP da rede.

Todas as configurações dele já foi realizada para estabelecer conexão e convergência com as empresas IPv4 e IPv6.

Para verificar a configuração deste roteador, consultar o Apêndice.

```
Externo-IPv4#show running-config
```

5.5 CONFIGURANDO NAT-PT

Após todas as configurações realizadas ainda não é possível os *hosts* da empresa IPv6 acessarem os *hosts* da empresa IPv4. Uma solução seria habilitar pilha dupla na rede interna IPv4, mas isso gera uma inconveniência. Toda a infraestrutura deve ser duplicada, todos os *hosts* devem ter os dois protocolos IPv4 e IPv6, dificultando assim a sua gerência e controles de acessos. Para evitar duas infraestruturas para serem gerenciadas, ter dois problemas, ter duas redes a empresa IPv4 vai ser configurada com NAT-PT

A configuração estática servirá para estabelecer uma conexão imediata dos serviços mais essenciais ou para um acesso direto ao outro roteador e imediatamente sem a necessidade de aguardar uma tradução dinamicamente.

Configurado a tradução estática de dos endereços IPv4 para os endereços IPv6:

```
INTERNET(config)# IPv6 nat v4v6 source 172.16.4.2 2013::4:2
```

Configurado a tradução estática de 1:1 dos endereços IPv6 para os endereços IPv4:

```
INTERNET(config)# IPv6 nat v6v4 source 2001:6::2 192.168.6.2
INTERNET(config)# IPv6 nat v6v4 source 2012:2::1 192.168.6.1
```

Abaixo será configurado NAT-PT dinamicamente, onde ele traduzirá os endereços IPv4 para uma faixa de endereços IPv6 e vice-versa.

Este comando servirá como prefixo para os endereços que serão traduzidos dos endereços IPv4 para o IPv6:

```
INTERNET(config)# IPv6 nat prefix 2013::/96
```

O comando a seguir procurará em uma ACL uma faixa de *hosts* e traduzi-los para uma faixa de endereços IPv6:

```
INTERNET(config)# IPv6 nat v4v6 source list 1 pool IPv4_IPv6
```

Esta ACL está permitindo todos os *hosts* contidos entre 172.16.0.1 ao 172.16.7.254:

```
INTERNET(config)# access-list 1 permit 172.16.0.0 0.0.7.255
```

O próximo comando define a faixa de endereços para qual os endereços IPv4 serão traduzidos, como o prefixo anteriormente utilizou um /96 só sobram /32 para o total de 128 bits.

```
INTERNET(config)# IPv6 nat v4v6 pool IPv4_IPv6 2013::4:16 2013::4:FFFF prefix-length 32
```

A ACL nomeada abaixo servirá para permitir todos os endereços IPv6:

```
INTERNET(config)# IPv6 access-list trafego_nat_IPv6
INTERNET(config-IPv6-acl)# permit IPv6 any any
```

Abaixo segue o comando para traduzir todos os endereços IPv6 para uma faixa de endereços IPv4:

```
INTERNET(config)# IPv6 nat v6v4 source list trafego_nat_IPv6 pool IPv6_IPv4
```

Em seguida é definido a faixa de endereços que a tradução de IPv6 para IPv4 irá utilizar:

```
INTERNET(config)# IPv6 nat v6v4 pool IPv6_IPv4 192.168.6.16 192.168.6.32 prefix-length 24
```

Após definir as faixas de endereços que serão traduzidas é necessário informar em quais interfaces utilizarão o NAT-PT.

```
INTERNET(config)# interface GigabitEthernet0/0.10
INTERNET(config-subif)# IPv6 nat
INTERNET(config-subif)# exit
INTERNET(config)# interface GigabitEthernet0/0.100
INTERNET(config-subif)# IPv6 nat
INTERNET(config-subif)# exit
INTERNET(config)# interface GigabitEthernet0/0.1000
INTERNET(config-subif)# IPv6 nat
```

```
INTERNET(config-subif)# exit
INTERNET(config)# interface Serial0/0/0
INTERNET(config-subif)# IPv6 nat
```

Após ser habilitado o NAT-PT nas interfaces será necessário criar uma *interface loopback.* Esta interface virtual servirá para divulgar os endereços traduzidos para os outros roteadores, pois as traduções foram realizadas para endereços que não foram divulgados. Se não habilitar esta interface e divulgar a rede não haverá comunicação com os outros *hosts* ou roteadores.

```
INTERNET(config)# interface Loopback0
INTERNET(config-if)# ip address 192.168.6.254 255.255.255.0
INTERNET(config-if)# IPv6 address 2013::4:1/64
```

Agora para que estas redes 192.168.6.254/24 e 2013::4:1/64 sejam divulgadas tem que habilitar o RIP e o RIPng.

```
INTERNET(config)# router rip
INTERNET(config-router)# network 192.168.6.0
```

```
INTERNET(config)# interface Loopback0
INTERNET(config-if)# IPv6 rip rIPv6 enable
```

5.6 CONFIGURANDO O ISATAP

O ISATAP é um exemplo de uma das técnicas de transição por túnel. Foi escolhida esta opção devido a sua compatibilidade com o roteador da CISCO e com a versão 6.01 do Cisco Packet Tracer

A proposta do ISATAP é prover uma conexão IPv6 sobre uma IPv4 através de um túnel aonde necessitará de um cliente ISATAP e um servidor ISATAP, estes clientes e servidores irão adicionar e retirar informações do cabeçalho IPv6 juntamente com o IPv4.

Por que configurar o ISATAP?

Ao configurar a Pilha Dupla (*Dual Stack*) foi optado por não duplicar toda a infraestrutura da empresa que está com rede sobre IPv4, optando-a apenas entre o Roteador da Empresa e o seu ISP para realizar o tratamento de protocolos IPv4 e IPv6. Com isso, apenas o roteador conseguiria receber pacotes IPv6, devido a Pilha Dupla, mas os *hosts* de sua

rede não teriam conectividade com IPv6. Desta forma foi implementado o NAT-PT, para traduzir os endereços da rede IPv4 em endereços IPv6 e para garantir a conexão de volta foi feito um NAT-PT de IPv6 para IPv4 também. Desta forma a rede já haveria convergência entre elas, porém o que aconteceria com *host's* novos? Ou se não fosse conhecido a tradução dos endereços?

Para que haja conexão através do NAT-PT o micro necessita saber qual endereço ele deverá acessar. Da rede IPv4 o usuário necessitará saber qual o endereço IPv4 traduzido referente ao IPv6 da outra rede. Para solucionar estas questões foi implementada uma técnica de tunelamento, aonde o equipamento faz um túnel com um servidor e troca informações, funcionando desta forma como uma pilha dupla sobre a rede IPv4.

Abaixo seguem as configurações necessárias e realizadas para prover uma conexão via CLIENTE ISATAP e SERVIDOR ISATAP

Foi escolhido para ser cliente ISATAP o roteador *Router Internet* que está na empresa IPv4 representada pela cor azul de acordo com a figura 4.1, pois a conexão interna de sua rede é sobre IPv4, a sua conexão externa é IPv4 e IPv6, a fim de demonstrar que o pacote IPv6 passou sobre o IPv4, foi selecionada uma conexão aonde não tivesse nenhum IPv6 configurado.

Para configurar o ISATAP primeiramente será configurado o servidor no *Router Internet.* Adicionando uma interface Tunel e habilitando o modo do túnel nesta interface.

Criando a interface para realizar o túnel

```
INTERNET(config)#  interface Tunnel 0
```

Não há necessidade de IPv4, deve-se retirar o IPv4 e adicionar um endereço IPv6.

```
INTERNET(config-if)#   no ip address
INTERNET(config-if)#  ipv6 enable
INTERNET(config-if)#   ipv6 address 2014::/64 eui-64
```

Configurando o túnel no modo ISATAP

```
INTERNET(config-if)#   tunnel mode ipv6ip isatap
```

Configuração para retirar a supressão de descoberta de vizinhança. Este modo permite que o cliente ISATAP realize um RS e o túnel informe o seu endereço como *gateway* da rede.

```
INTERNET(config-if)#   no ipv6 nd ra suppress
```

Após configurar o túnel tem que informar qual interface de origem interpretará o cabeçalho ISATAP

```
INTERNET(config-if)#   tunnel source GigabitEthernet0/0.10
```

Poderia selecionar a interface GigabitEthernet0/0, porém ao fazer isso estaria habilitando toda a rede interna a habilitar um cliente ISATAP, como a rede está segmentada em VLANs foi habilitado apenas em uma subinterface destinada a uma única VLAN.

Com estas configurações os *hosts* da REDE ESTAGIARIO ainda não conseguirão acessar a rede IPv6, isso ocorre porque a rede que o túnel se encontra é uma rede desconhecida para o roteador *Router Externo* IPv6. Para ele aprender a rota basta divulgara a rede Tunel através do RIPng.

```
INTERNET(config-if)#   ipv6 rip ripv6 enable
```

Agora é necessário habilitar um cliente ISATAP no *host* para ter conectividade com uma rede IPv6. No cliente é necessário inserir os seguintes comandos no *prompt* para habilitar a interface ISATAP:

```
netsh interface isatap set state enabled
```

Após habilitar a interface ISATAP é necessário informar para onde ela será roteada informando o ip do servidor ISATAP.

```
netsh interface isatap set router 172.16.0.1:
```

A Figura 5.14 mostra a configuração realizada para que a conexão via ISATAP. Comando executados no *prompt* de comando do PC estagiário. Qualquer computador da rede da empresa IPv4, representada pela zona azul da figura 4.1, poderá utilizar este comando com o intuito de estabelecer uma conexão ISATAP.

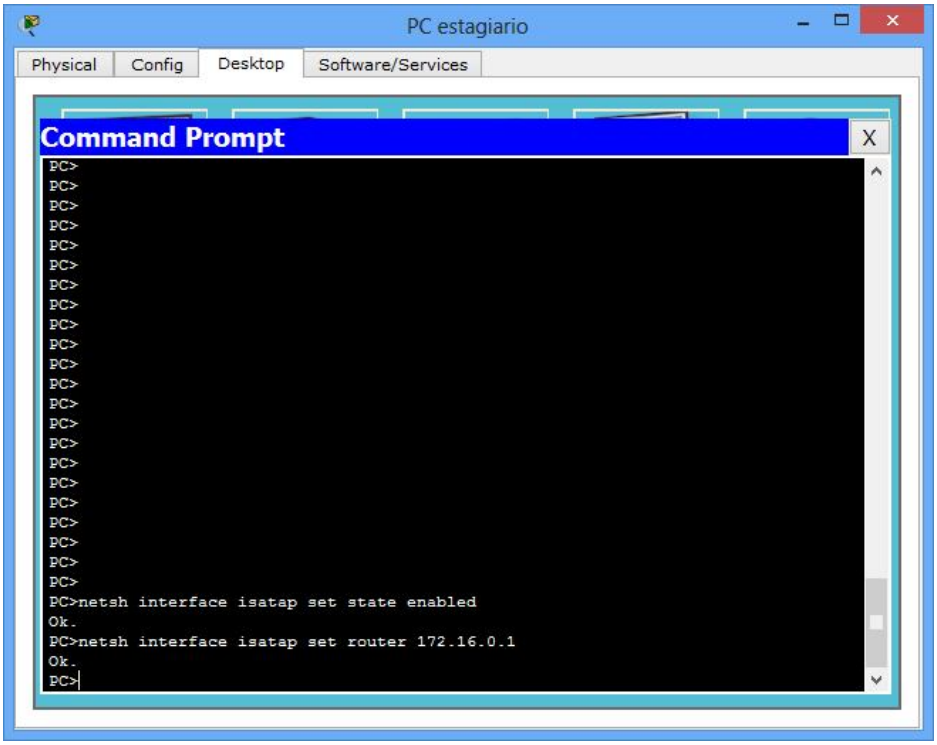

Figura 5.14 – Configurando a interface ISATAP no cliente PC ESTAGIARIO.

Ao configurar a interface ISATAP e informar a rota para o servidor ISATAP o comando ipconfig /all irá trazer informações sobre a conexão via ISATAP e o IPv6 *address* atribuído, como pode ser verificado na figura 5.15.

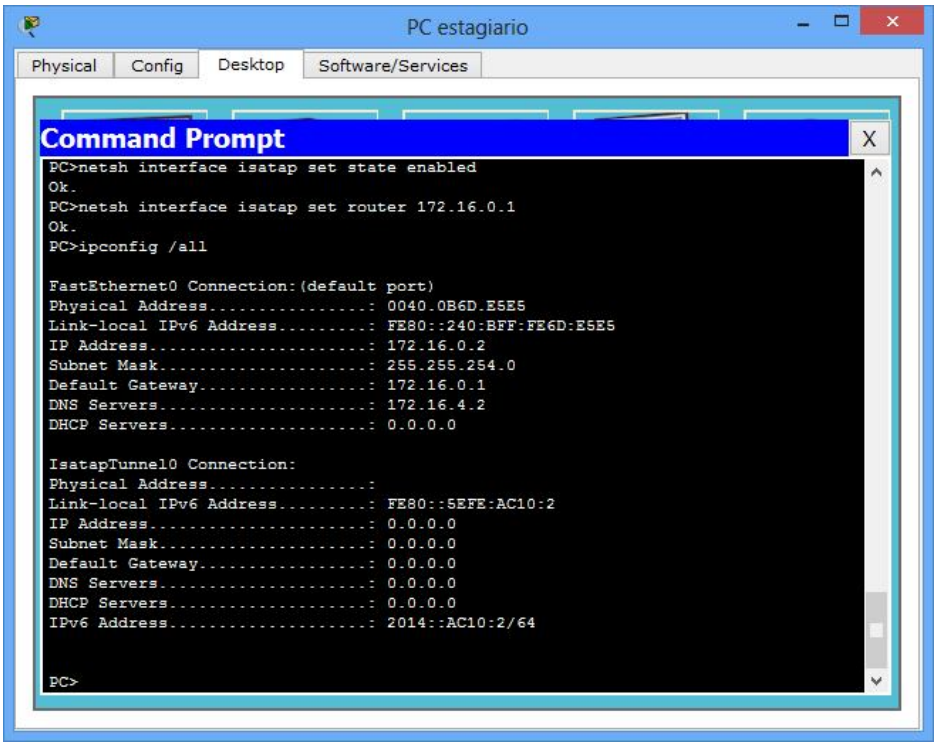

Figura 5.15 – Demonstra a configuração de IPs do host PC ESTAGIARIO.

Após esta configuração foi adicionado um servidor com o *service* de DNS na rede IPv4 e um servidor HTTP na rede IPv6 para verificar a saída do equipamento através do túnel.

A Figura 5.16 mostra as configurações do servidor DNS da empresa IPv4, aonde tem entradas IPv4 e IPv6, a fim de demonstrar a conexão utilizando NAT-PT e ISATAP.

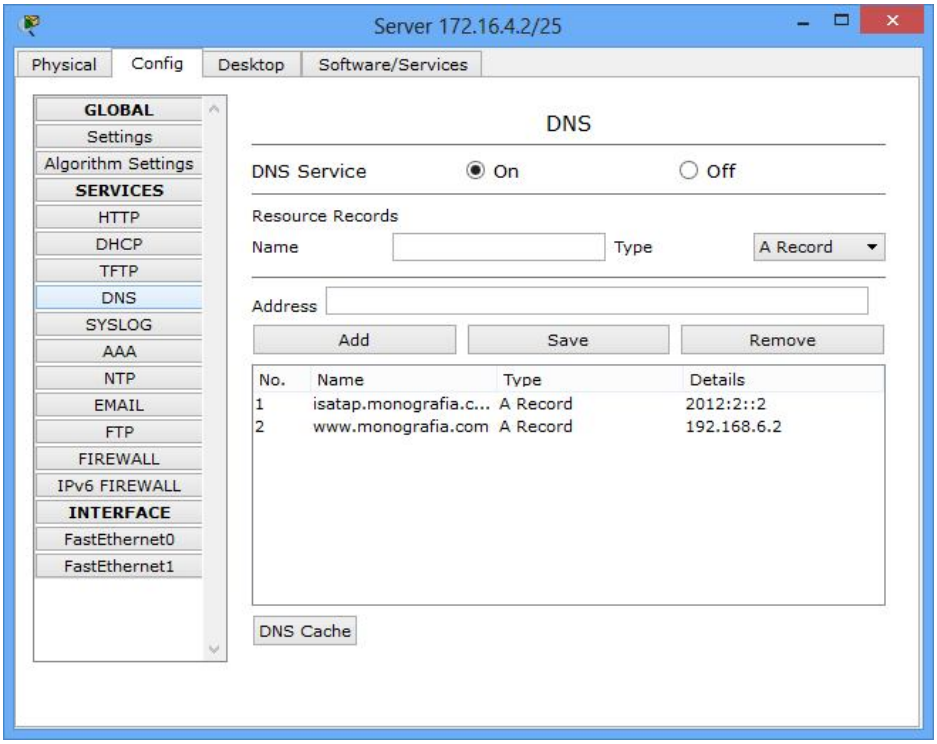

Figura 5.16 – Demonstra a configuração de DNS do servidor da rede IPv4.

Configurado no servidor da empresa IPv6 o serviço HTTP. Este servidor servirá para realizar os testes de acesso da rede sobre IPv4 e IPv6 acessando o site www.monografia.com.

Para utilizar esses serviços basta inserir o servidor e nas opções de configurações do equipamento habilitar o serviço HTTP para porta 80 e HTTPS para a porta 443. O seu conteúdo pode ser alterado conforme a necessidade e desejo no formato html.

A Figura 5.17 mostra a configuração do servidor HTTP da empresa IPv6 . Este servidor servirá a página de internet seja ela requisitada pela técnica de tradução ou tunelamento.

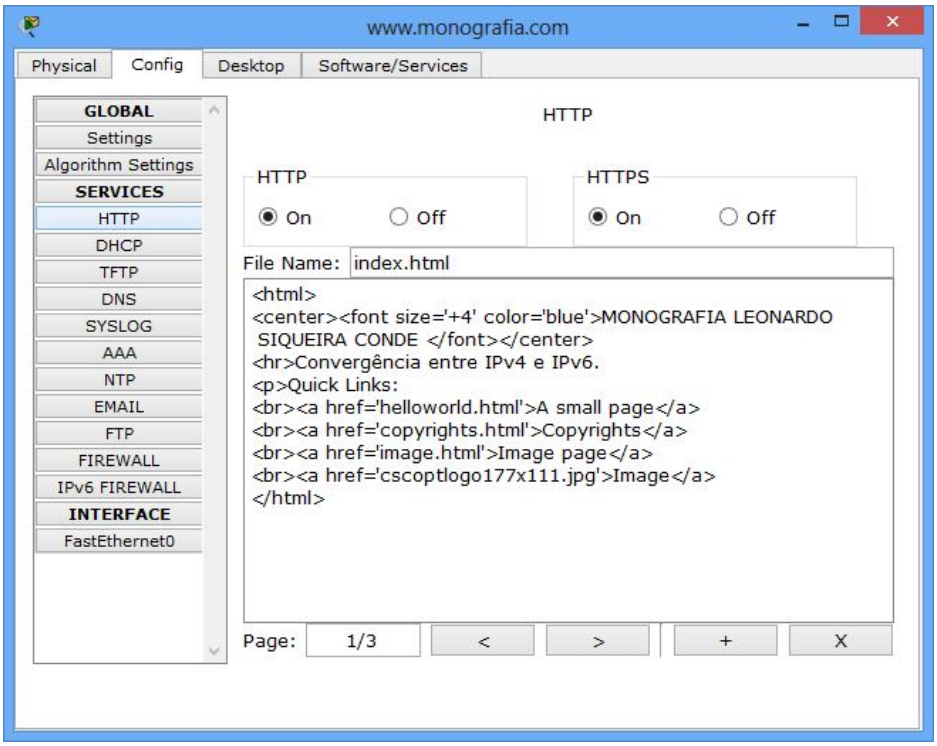

Figura 5.17 –Configuração de HTTP do servidor da rede IPv6.

Com estas configurações o *host* PC ESTAGIARIO conseguirá acessar o *site* isatap.monografia.com que se encontra na rede IPv6, mas não só o site como qualquer equipamento da rede IPv6.

Após as configurações de pilha dupla, NAT-PT e ISATAP, a topologia ficará de acordo com a figura 5.18:

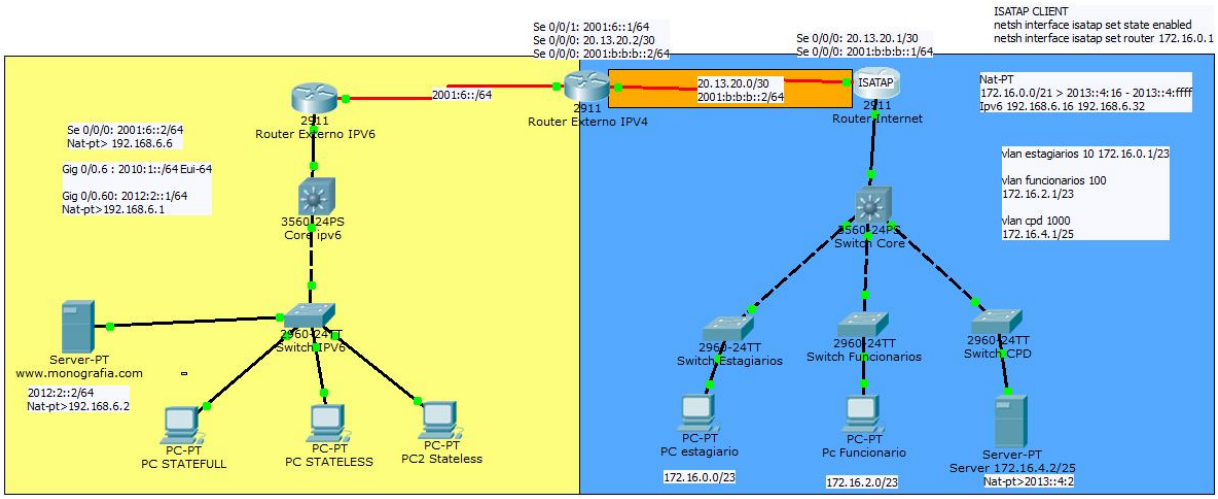

Figura 5.18 - Topologia completa

5.7 TESTANDO A CONVERGÊNCIA ENTRE AS REDES IPV4 E IPV6

Para testar a convergência foi feito um *tracert* do PC STATEFULL localizado na rede IPv6 para o endereço da PILHA DUPLA da rede IPv4 (2001:b:b:b::1) e para tradução do Server-PT localizado na rede IPv4 (2013::4:2<=>172.16.4.2)

A figura 5.19 mostra o *tracert* sendo realizado da rede IPv6 para um endereço traduzindo na rede IPv4, havendo total convergência entre as duas redes.

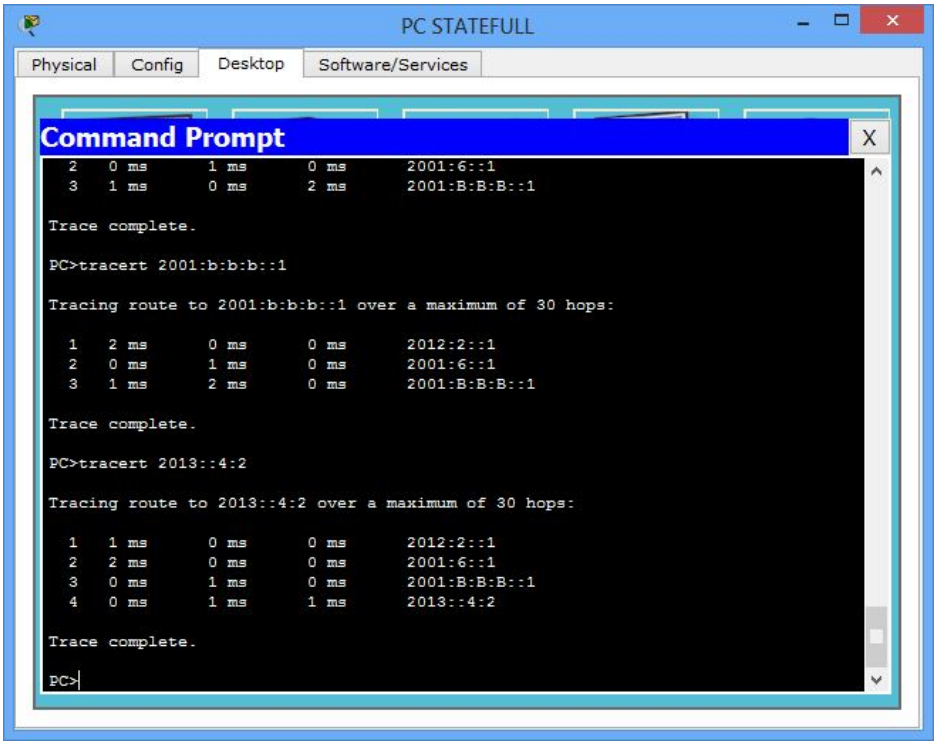

Figura 5.19 - Tracert para os endereços localizados na rede IPv4.

Para verificar quais endereços foram traduzidos para efetuar testes de conexão foi necessário verificar a tabela de tradução de endereços do IPv6:

```
INTERNET#show IPv6 nat translations
INTERNET#show IPv6 nat translations
Prot  IPv4 source          IPv6 source
---   ---                  ---
---   172.16.4.2           2013::4:2

---   192.168.6.18         2012:2::A
---   172.16.4.2           2013::4:2

---   192.168.6.2          2001:6::2
```

```
---  172.16.4.2          2013::4:2

---  192.168.6.1         2012:2::1
---  ---                 ---

---  192.168.6.18        2012:2::A
---  ---                 ---

---  192.168.6.2         2001:6::2
---  ---                 ---
```

Da Tabela de tradução IPv6 serão utilizados os seguintes endereços para criar um PDU complexo e testar um *telnet* da rede IPv4 para IPv6:

```
---  192.168.6.18        2012:2::A
---  172.16.4.2          2013::4:2
```

Após analisar os endereços traduzidos foi criado um *complex* PDU para fazer um *telnet* do equipamento de IP 172.16.4.2 para o equipamento de IP 2012:2::A, como pode ser visto e verificado na figura 5.20 e 5.21.

A figura 5.21 ilustra o telnet sendo realizado para o endereço IPv6 traduzido para o IPv4 192.168.6.18. Para que o pacote consiga voltar, foi necessário configurar um NAT para o endereço de volta 172.16.4.2 traduzido para 2013::4:2. Se o endereço de origem não tivesse o NAT-PT configurado o pacote chegaria ao destino, mas não retornaria.

Origem: 172.16.4.2 , NAT-PT v4v6 2013::4:2

Destino: 2012:2::A, NAT-PT v6v4 192.168.6.18

O NAT-PT ocorre após o pacote passar e ser analisado pelo roteador da rede IPv4 *Router Internet* ilustrado na fiugra 4.1.

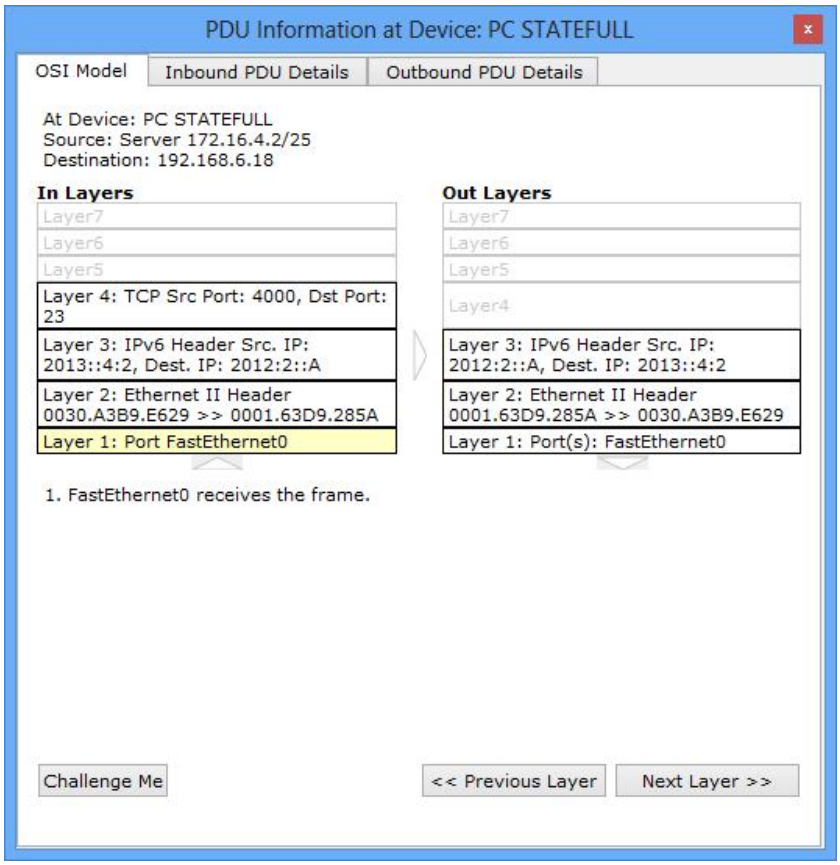

Figura 5.20 - *Telnet* para o equipamento

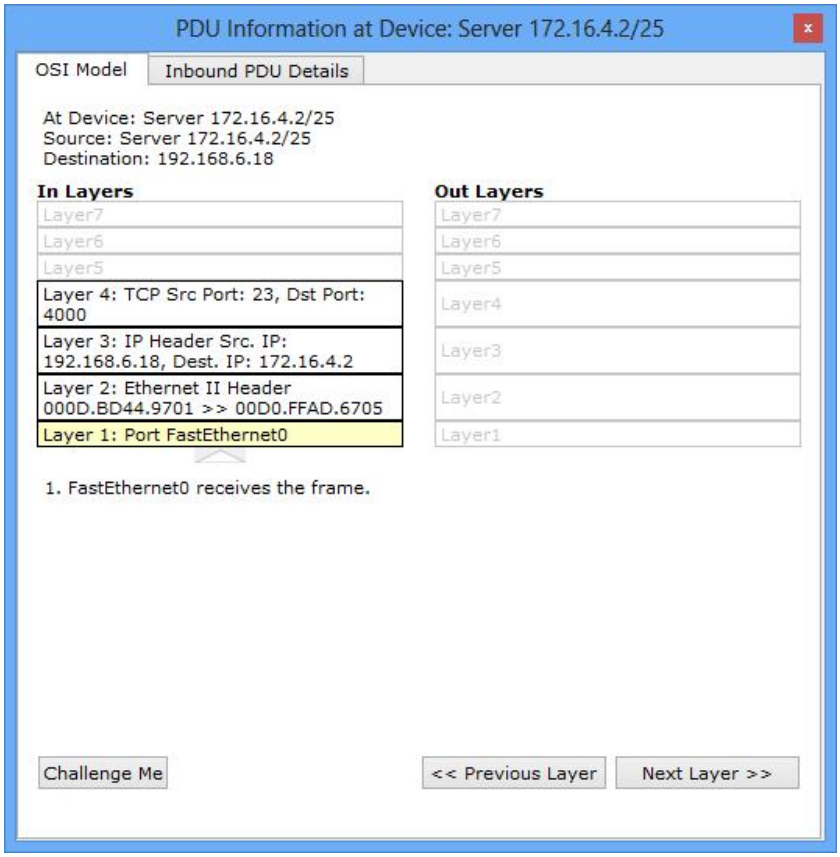

Figura 5.21 - Resposta para a solicitação do *telnet*

Desta forma, isso demonstra total integração entre as duas redes utilizando pilha dupla e tradução de endereços.

5.7.1 Testando a conexão ISATAP

Foram executados testes de convergências, extraídos os vídeos e documentados na pasta “Video - TESTES REALIZADOS” da mídia em anexo.

Foi aberto no *browser* do PC ESTAGIARIO e digitado o endereço isatap.monografia.com. Este endereço consultará o DNS da rede, conforme mostrado na figura 5.22.

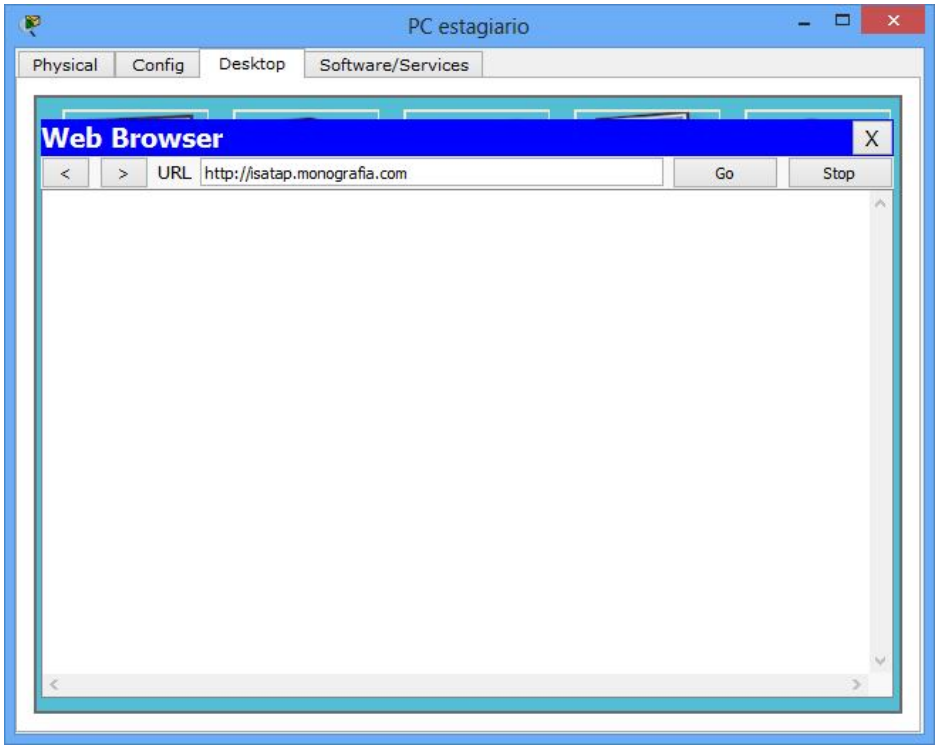

Figura 5.22 – *Browse* do PC estagiário tentando conexão com o endereço isatp.monografia.com

Ao observar o pacote solicitando conexão na sua rede local para trazer o endereço e o IP de destino do endereço desejado. A Figura 5.23 mostra a requisição feita para o servidor DNS, o qual irá responder com o endereço do servidor HTTP da rede IPv6.

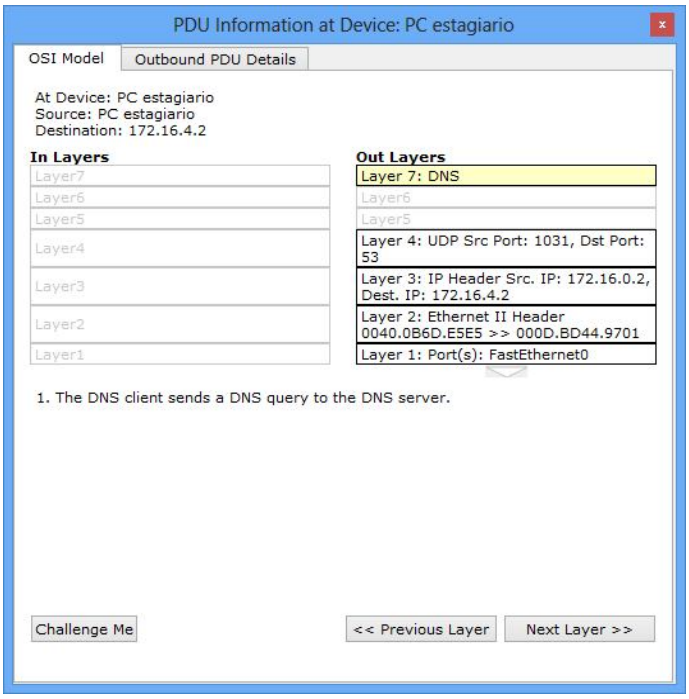

Figura 5.23 – Solicitação para o DNS para resolver o endereço isatap.monografia.com

Ao resolver a requisição, o DNS responderá com o endereço de destino para isatap.monografia.com com o IP 2012: 2::2 conforme a Figura 5.24.

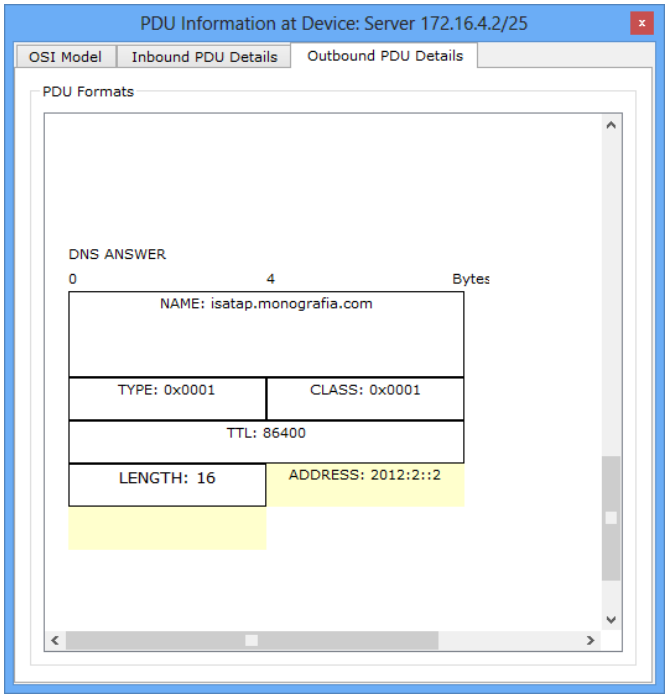

Figura 5.24 – Resposta a solicitação DNS com o IP da página.

A figura a seguir (5.25) mostra o pacote com os dois cabeçalhos, IPv4 e IPv6 para acesso à página isatap.monografia.com:

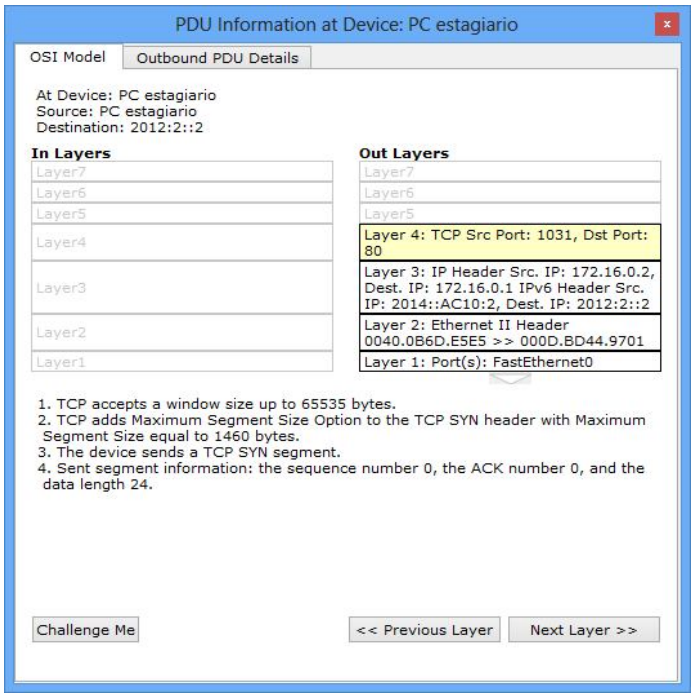

Figura 5.25 – Os dois cabeçalhos IPv4 e IPv6, ISATAP TUNEL

O pacote ao chegar no *router* INTERNET ele irá retirar o cabeçalho IPv4 e deixar apenas o IPv6, conforme mostrado nas figuras a seguir (5.26. e 5.27):

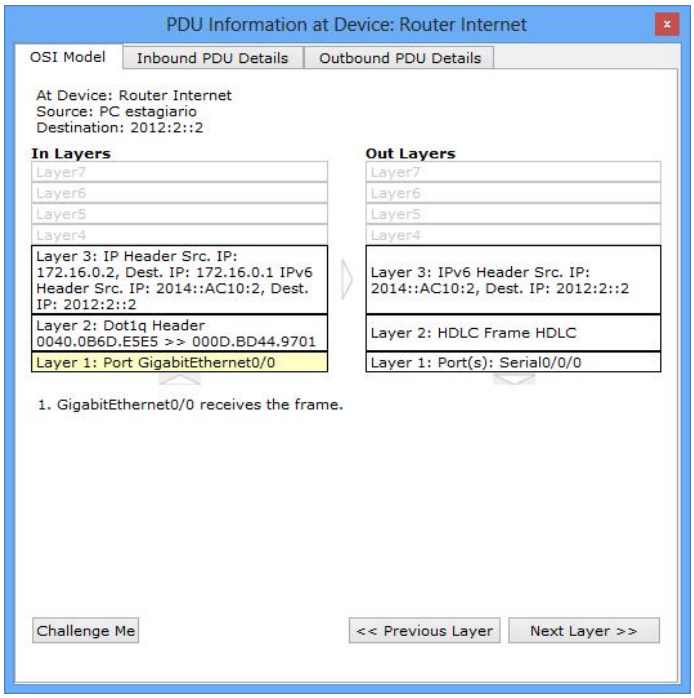

Figura 5.26 – Demonstra alteração do cabeçalho da mensagem com destino para 2012:2::2

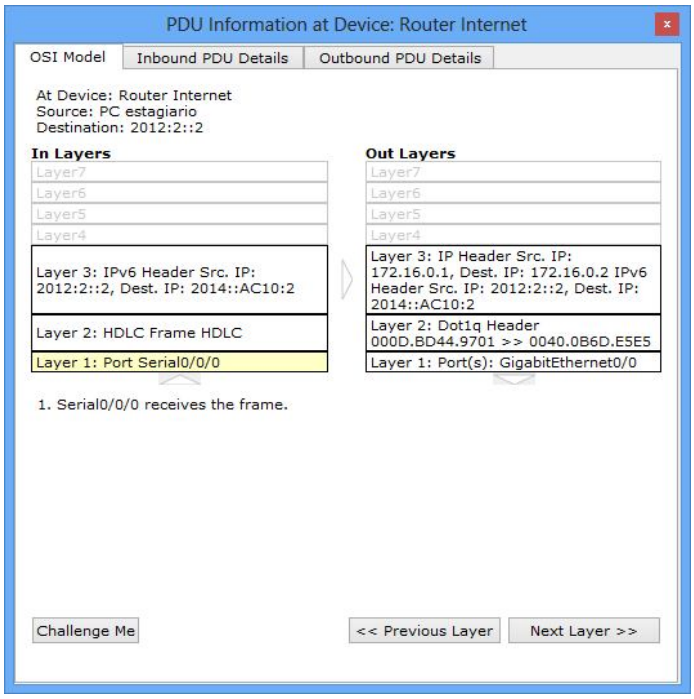

Figura 5.27 – Como o pacote é montado da rede IPv6 para o host 172.16.0.2

Em seguida demonstra o que acontece quando a solicitação chega ao servidor HTTP na rede IPv6 com a solicitação de acesso ao isatap.monografia.com, conforme a figura 5.28.

A origem do pacote foi destinada pelo um endereço IPv6 gerado pelo ISATAP no qual o servidor deve encaminhar a requisição HTTP.

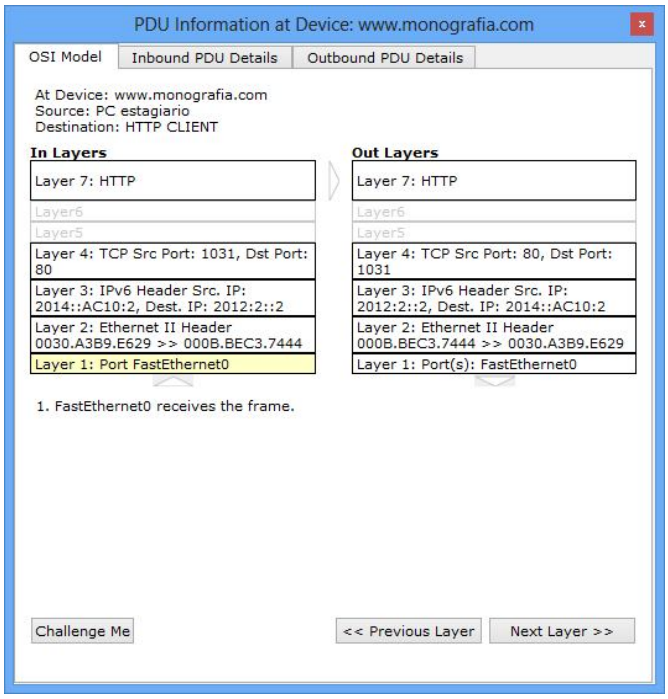

Figura 5.28 – Requisição HTTP no servidor da rede IPv6

O pacote ao passar novamente pelo roteador que está com o ISATP SERVER configurado irá associar acrescentando novamente o endereço de origem IPv4 para que o pacote alcance o equipamento PC estagiário.

Em seguida o comportamento do pacote ao receber a resposta do servidor HTTP com a página aberta, mostrado nas figuras 5.29 e 5.30.

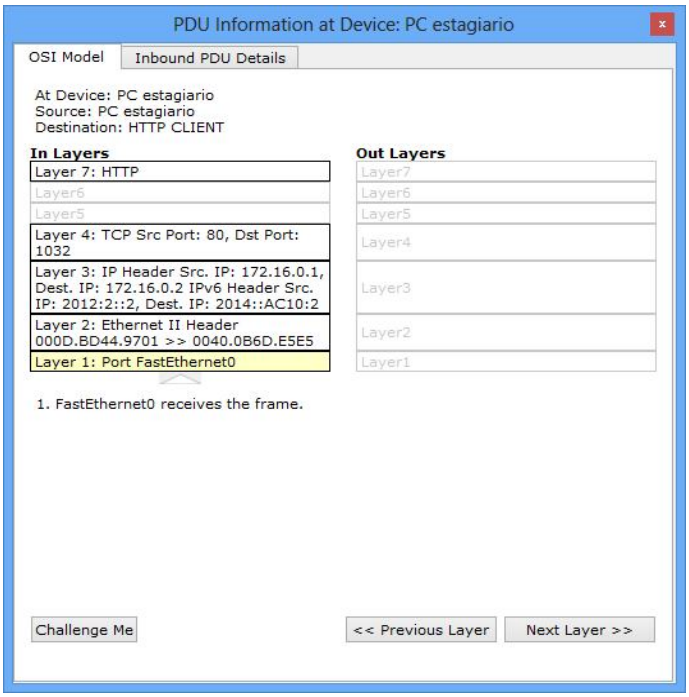

Figura 5.29 - Retorno da solicitação HTTP via ISATAP

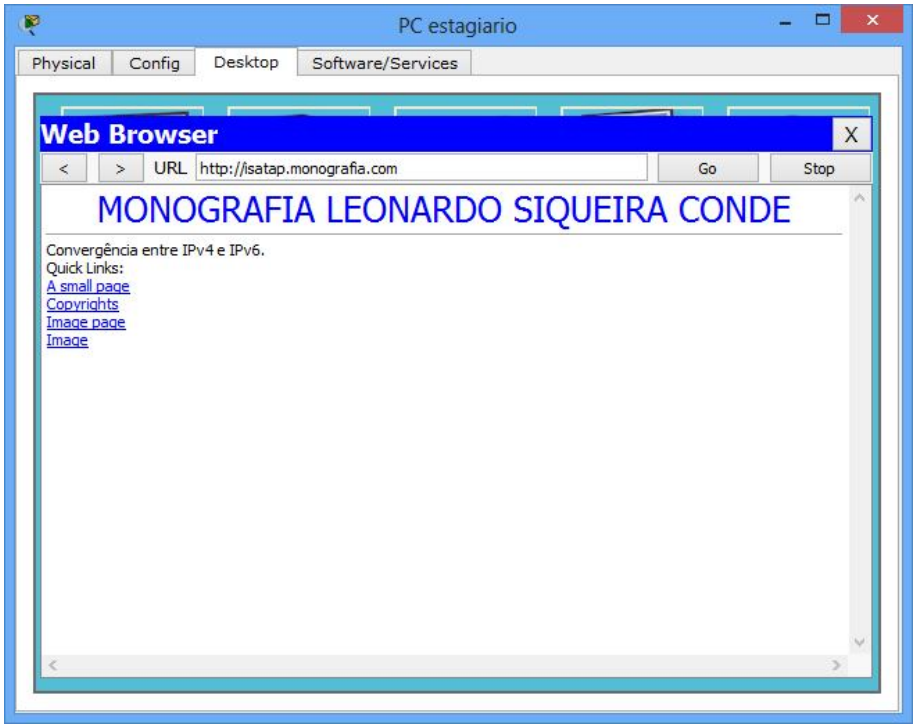

Figura 5.30 – Resultado da requisição HTTP via ISATAP.

CONSIDERAÇÕES FINAIS

6.1 CONCLUSÕES

No estudo realizado foi demonstrada a utilização do protocolo TCP/IP (Transmission Control Protocol / Internet Protocol) IPv4 e IPv6 e a convergência entre eles.

Com o começo da distribuição do último lote de endereços IPv4 - no dia 1º de fevereiro de 2011 - onde dois blocos foram entregues à APNIC, entidade que administra os endereços IP no sudeste asiático e Oceania, iniciou-se a fase de exaustão dos endereços IPv4. Com isso, foi verificada a necessidade de utilização do endereçamento IPv6 para suprir essa falta de endereçamento.

A migração é um passo necessário para muitas empresas, mas elas não demonstram estarem preocupadas. Porém, a migração torna-se indispensável a cada dia que se passa. Como foi visto, o protocolo IPv6 tem recursos avançados podendo ser muito mais explorado. Os provedores sabem que terão que se adequar a nova realidade, alguns já começaram a migração e a fornecer serviços, como túneis e interfaces configuradas com IPv6 para fornecerem conexão para futuras empresas. Grandes empresas como o Facebook e o Google já fornecem serviço sobre IPv6.

Uma vez que a maioria das pessoas e empresas ainda utilizam o IPv4, eles ainda não estão preparadas para suportar comunicações em IPv6. Faz se necessário o aprimoramento em termos de técnicas de transição e implementação de redes sobre IPv6, buscando, assim, o melhor entendimento e soluções que o protocolo fornece.

A migração de IPv4 para IPv6 será lenta e gradual. Algumas empresas talvez não utilizarão IPv6 internamente, devido à existência de equipamentos obsoletos e incompatíveis com o novo protocolo, ou simplesmente irão aguardar as primeiras migrações e acompanharem a solução dos problemas iniciais, pois na adoção do recente protocolo poderão surgir novos problemas de segurança e novas funcionalidades.

Para suprir a necessidade dessa comunicação, este trabalho demonstrou a possibilidade de utilização dos protocolos de endereçamento IPv4 e IPv6 simultaneamente através da utilização do método de transição denominado Pilha Dupla, NAT-PT e ISATAP.

Portanto, através das análises realizadas nos cenários, foi verificado que o referido método permite que os roteadores recebam e transmitam pacotes tanto IPv4 quanto IPv6 e

que o IPv6 funciona perfeitamente nos protocolos de roteamento dinâmico e na tradução de endereços. Desta forma facilita e abre caminho para a migração e utilização futura somente do endereçamento IPv6.

A descrição do cenário apresentado demonstrou convergência entre as duas redes.

6.2 SUGESTÕES PARA TRABALHOS FUTUROS

Para trabalhos futuros sugere-se demonstrar outras técnicas em conjunto com as apresentadas neste trabalho. Técnicas de tunelamento como ISATAP juntamente com as opções de segurança que o IPv6 proporciona.

Se possível, ainda, a utilização de um roteador físico, pois o GNS3 (emulador de rede) ao utilizar vários roteadores consome muito processo do equipamento, não sendo possível simular perfeitamente a rede com uma quantidade muito grande de roteadores.

A simulação pelo *packet tracer* é limitada. Sugiro utilizar o sistema FreeBSD que já tem nativo a tradução de endereços e tunelamento 6in4 e 4in6.

Com o FreeBSD é possível demonstrar mais técnicas de tunelamento e ele faz o papel de roteador da rede.

Explorar segurança e possíveis falhas de segurança do protocolo IPv6.

REFERÊNCIAS

BUARQUE, Daniel. http://g1.globo.com/mundo/noticia/2011/10/populacao-mundial-chega-7-bilhoes-de-pessoas-diz-onu.html. Acesso em: 20 de abril de 2013.

BURGESS, Mark. Princípios de Administração de Redes e Sistemas. 2ª ed. São Paulo: LTC, 2006.

CISCO . ISATAP - Interface and Hardware Component Configuration Guide, Cisco IOS XE Release 3S. Disponível em http://www.cisco.com/en/US/docs/ios-xml/ios/interface/configuration/xe-3s/ip6-isatap-xe.html#GUID-C13E0DD3-1DBD-46E0-956C-4ACE2CB0C5FB. Acesso em: 22 de maio 2013

CISCO. Cisco Networking Academy. Disponível em http://www.cisco.com/web/learning/netacad/index.html. Acesso em: 03 de março de 2013.

CISCO. Cisco Networking Academy. Disponível em http://www.cisco.com/web/learning/netacad/index.html. Acesso em: 20 de fevereiro de 2013.

CISCO. Implementing DHCP for IPv6. Disponível em http://www.cisco.com/en/US/docs/ios-xml/ios/ipv6/configuration/15-2mt/ip6-dhcp.html. Acesso em: 20 de abril de 2013

COMER, D. E. Computer Networks and Internets with Internet Applications. 4ª ed. Englewood Cliffs, NJ: Prentice Hall, 2003.

DAS, KAUSHIK, Stateless Auto Configuration, disponível em http://IPv6.com/articles/general/Stateless-Auto-Configuration.htm. Acesso em: 22 de março de 2013

FOROUZAN, B. Protocolo TCP/IP. 3ª ed. Mcgraw-hill Interamericana, 2010.

IETF. The Internet Engineering Task Force. Disponível em http://www.ietf.org. Acesso em: 05 de maio de 2013

IPV6.BR, EQUIPE disponível em 15 de maio de 2012 em http://ipv6.br/entenda/introducao/. Acesso em: 12 de maio de 2013.

IPv6.BR, EQUIPE. Disponível em http://ipv6.br/entenda/transicao/. Acesso em: 15 de maio de 2013.

MICROSOFT. Disponível em http://technet.microsoft.com/pt-br/library/cc778502(v=ws.10).aspx. Acesso em: 23 de maio de 2013

MORIMOTO, Carlos E.. Disponível em http://www.hardware.com.br/termos/tcp-ip. Acesso em 08 de dezembro de 2011.

RFC 0791. Protocol Specification. Disponível em http://tools.ietf.org/html/rfc791. Acesso em: 03 de fevereiro de 2013

RFC 2462. IPv6 Stateless Address Autoconfiguration. Disponível em http://tools.ietf.org/html/rfc2462. Acesso em: 07 de maio de 2013

RFC 3330. Special-Use IPv4 Addresses. Disponível em http://www.rfc-editor.org/rfc/rfc3330.txt. Acesso em: 05 de março de 2013

RFC 4861. Neighbor Discovery for IP version 6 (IPv6). Disponível em http://tools.ietf.org/html/rfc4861. Acesso em: 16 de maio de 2013

RIBEIRO, EFRÉM. IBGE aponta que 76,9% das empresas brasileiras usaram Internet. Disponível em http://www.meionorte.com/efremribeiro/ibge-aponta-que-76-9-das-empresas-brasileiras-usaram-internet-233698.html. Acesso em: 05 de março de 2013.

SMETANA, George Marcel M. A. .http://www.abusar.org.br/ftp/pitanga/Redes/ArtigoIP.pdf. Acesso em 18 de dezembro de 2012.

SOUZA, Jorge Moreira. Qualidade de Serviço (QoS) I: Dependabilidade: Teleco – Informação em Telecomunicações. 2005.

TANENBAUM, Andrew S. Redes de Computadores. http://IPv6.br/. Acesso em: 05 de dezembro de 2012.

APÊNDICES

APÊNDICE A

1. SWITCH ESTAGIÁRIOS – running-config

Abaixo se pode verificar a configuração do *switch* estagiarios após as configurações aplicadas. Estas configurações auxiliam no entendimento e resolução de futuros problemas de convergência. Nesta configuração pode-se verificar a associação das VLANs nas portas deste *switch.*

```
“
version 12.2
no service timestamps log datetime msec
no service timestamps debug datetime msec
NA no service password-encryption
!
hostname sw-estagiarios
!
spanning-tree mode pvst
!
interface FastEthernet0/1
 switchport mode trunk
!
interface FastEthernet0/2
 switchport access vlan 10
 switchport mode access
!
interface FastEthernet0/3
 switchport access vlan 10
 switchport mode access
!
interface FastEthernet0/4
 switchport access vlan 10
 switchport mode access
!
interface FastEthernet0/5
 switchport access vlan 10
 switchport mode access
!
interface FastEthernet0/6
```

```
 switchport access vlan 10
 switchport mode access
!
interface FastEthernet0/7
 switchport access vlan 10
 switchport mode access
!
interface FastEthernet0/8
 switchport access vlan 10
 switchport mode access
!
interface FastEthernet0/9
 switchport access vlan 10
 switchport mode access
!
interface FastEthernet0/10
 switchport access vlan 10
 switchport mode access
!
interface FastEthernet0/11
 switchport access vlan 10
 switchport mode access
!
interface FastEthernet0/12
 switchport access vlan 10
 switchport mode access
!
interface FastEthernet0/13
 switchport access vlan 10
 switchport mode access
!
interface FastEthernet0/14
 switchport access vlan 10
 switchport mode access
!
interface FastEthernet0/15
 switchport access vlan 10
 switchport mode access
!
```

```
interface FastEthernet0/16
 switchport access vlan 10
 switchport mode access
!
interface FastEthernet0/17
 switchport access vlan 10
 switchport mode access
!
interface FastEthernet0/18
 switchport access vlan 10
 switchport mode access
!
interface FastEthernet0/19
 switchport access vlan 10
 switchport mode access
!
interface FastEthernet0/20
 switchport access vlan 10
 switchport mode access
!
interface FastEthernet0/21
 switchport access vlan 10
 switchport mode access
!
interface FastEthernet0/22
 switchport access vlan 10
 switchport mode access
!
interface FastEthernet0/23
 switchport access vlan 10
 switchport mode access
!
interface FastEthernet0/24
 switchport access vlan 10
 switchport mode access
!
interface GigabitEthernet1/1
!
interface GigabitEthernet1/2
```

```
!
interface Vlan1
 no ip address
 shutdown
!
line con 0
!
line vty 0 4
 login
line vty 5 15
 login
!
End”
```

2. SWITCH FUNCIONÁRIOS – running-config

Neste *switch* foi configurada a VLAN 100 destinada a rede para os funcionários da rede IPv4 representado pela cor azul da figura 4.1.

```
“
hostname sw-funcionarios
!
spanning-tree mode pvst
!
interface FastEthernet0/1
 switchport mode trunk
!
interface FastEthernet0/2
 switchport access vlan 100
 switchport mode access
!
interface FastEthernet0/3
 switchport access vlan 100
 switchport mode access
!
interface FastEthernet0/4
 switchport access vlan 100
 switchport mode access
```

```
!
interface FastEthernet0/5
 switchport access vlan 100
 switchport mode access
!
interface FastEthernet0/6
 switchport access vlan 100
 switchport mode access
!
interface FastEthernet0/7
 switchport access vlan 100
 switchport mode access
!
interface FastEthernet0/8
 switchport access vlan 100
 switchport mode access
!
interface FastEthernet0/9
 switchport access vlan 100
 switchport mode access
!
interface FastEthernet0/10
 switchport access vlan 100
 switchport mode access
!
interface FastEthernet0/11
 switchport access vlan 100
 switchport mode access
!
interface FastEthernet0/12
 switchport access vlan 100
 switchport mode access
!
interface FastEthernet0/13
 switchport access vlan 100
 switchport mode access
!
interface FastEthernet0/14
 switchport access vlan 100
```

```
 switchport mode access
!
interface FastEthernet0/15
 switchport access vlan 100
 switchport mode access
!
interface FastEthernet0/16
 switchport access vlan 100
 switchport mode access
!
interface FastEthernet0/17
 switchport access vlan 100
 switchport mode access
!
interface FastEthernet0/18
 switchport access vlan 100
 switchport mode access
!
interface FastEthernet0/19
 switchport access vlan 100
 switchport mode access
!
interface FastEthernet0/20
 switchport access vlan 100
 switchport mode access
!
interface FastEthernet0/21
 switchport access vlan 100
 switchport mode access
!
interface FastEthernet0/22
 switchport access vlan 100
 switchport mode access
!
interface FastEthernet0/23
 switchport access vlan 100
 switchport mode access
!
interface FastEthernet0/24
```

```
 switchport access vlan 100
 switchport mode access
!
interface GigabitEthernet1/1
!
interface GigabitEthernet1/2
!
interface Vlan1
 no ip address
 shutdown
!
!
line con 0
!
line vty 0 4
 login
line vty 5 15
 login
!
!
End”
```

3. SWITCH CPD – running-config

Nas configurações abaixo podem ser verificados os comandos utilizados para a configuração e atribuição da VLAN 1000 nas portas deste *switch.*

```
“
hostname sw-CPD
!
spanning-tree mode pvst
!
interface FastEthernet0/1
 switchport mode trunk
!
interface FastEthernet0/2
 switchport access vlan 1000
 switchport mode access
```

```
!
interface FastEthernet0/3
 switchport access vlan 1000
 switchport mode access
!
interface FastEthernet0/4
 switchport access vlan 1000
 switchport mode access
!
interface FastEthernet0/5
 switchport access vlan 1000
 switchport mode access
!
interface FastEthernet0/6
 switchport access vlan 1000
 switchport mode access
!
interface FastEthernet0/7
 switchport access vlan 1000
 switchport mode access
!
interface FastEthernet0/8
 switchport access vlan 1000
 switchport mode access
!
interface FastEthernet0/9
 switchport access vlan 1000
 switchport mode access
!
interface FastEthernet0/10
 switchport access vlan 1000
 switchport mode access
!
interface FastEthernet0/11
 switchport access vlan 1000
 switchport mode access
!
interface FastEthernet0/12
 switchport access vlan 1000
```

```
 switchport mode access
!
interface FastEthernet0/13
 switchport access vlan 1000
 switchport mode access
!
interface FastEthernet0/14
 switchport access vlan 1000
 switchport mode access
!
interface FastEthernet0/15
 switchport access vlan 1000
 switchport mode access
!
interface FastEthernet0/16
 switchport access vlan 1000
 switchport mode access
!
interface FastEthernet0/17
 switchport access vlan 1000
 switchport mode access
!
interface FastEthernet0/18
 switchport access vlan 1000
 switchport mode access
!
interface FastEthernet0/19
 switchport access vlan 1000
 switchport mode access
!
interface FastEthernet0/20
 switchport access vlan 1000
 switchport mode access
!
interface FastEthernet0/21
 switchport access vlan 1000
 switchport mode access
!
interface FastEthernet0/22
```

```
 switchport access vlan 1000
 switchport mode access
!
interface FastEthernet0/23
 switchport access vlan 1000
 switchport mode access
!
interface FastEthernet0/24
 switchport access vlan 1000
 switchport mode access
!
interface GigabitEthernet1/1
!
interface GigabitEthernet1/2
!
interface Vlan1
 no ip address
 shutdown
!
line con 0
!
line vty 0 4
 login
line vty 5 15
 login
!
!
end
”
```

4. SWITCH CORE – running-config

Abaixo segue a configuração do switch core da rede IPv4 e pode se verificar os comandos utilizados para associar as portas deste switch no modo *trunk* para transportar todas as VLANs.

```
“
```

```
hostname sw-core
!
spanning-tree mode pvst
!
interface FastEthernet0/1
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface FastEthernet0/2
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface FastEthernet0/3
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface FastEthernet0/4
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface FastEthernet0/5
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface FastEthernet0/6
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface FastEthernet0/7
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface FastEthernet0/8
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface FastEthernet0/9
 switchport trunk encapsulation dot1q
 switchport mode trunk
```

```
!
interface FastEthernet0/10
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface FastEthernet0/11
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface FastEthernet0/12
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface FastEthernet0/13
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface FastEthernet0/14
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface FastEthernet0/15
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface FastEthernet0/16
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface FastEthernet0/17
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface FastEthernet0/18
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface FastEthernet0/19
 switchport trunk encapsulation dot1q
```

```
 switchport mode trunk
!
interface FastEthernet0/20
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface FastEthernet0/21
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface FastEthernet0/22
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface FastEthernet0/23
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface FastEthernet0/24
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface GigabitEthernet0/1
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface GigabitEthernet0/2
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface Vlan1
 no ip address
 shutdown
!
ip classless
!
line con 0
!
line aux 0
```

```
!
line vty 0 4
 login
!
end
”
```

5. SWITCH IPV6 – running-config

A saída do *commando show* running-config mostra as configurações utilizadas neste switch. A VLAN 60 foi aplicada nas interfaces do switch no modo de acesso e no modo *trunk* com o *switch* CORE da rede IPv6.

```
“
hostname sw-IPv6
!
spanning-tree mode pvst
!
interface FastEthernet0/1
 switchport access vlan 60
 switchport mode access
!
interface FastEthernet0/2
 switchport access vlan 60
 switchport mode access
!
interface FastEthernet0/3
 switchport access vlan 6
 switchport mode access
!
interface FastEthernet0/4
 switchport access vlan 6
 switchport mode access
!
interface FastEthernet0/5
!
interface FastEthernet0/6
!
```

```
interface FastEthernet0/7
!
interface FastEthernet0/8
!
interface FastEthernet0/9
!
interface FastEthernet0/10
!
interface FastEthernet0/11
!
interface FastEthernet0/12
!
interface FastEthernet0/13
!
interface FastEthernet0/14
!
interface FastEthernet0/15
!
interface FastEthernet0/16
!
interface FastEthernet0/17
!
interface FastEthernet0/18
!
interface FastEthernet0/19
!
interface FastEthernet0/20
!
interface FastEthernet0/21
!
interface FastEthernet0/22
!
interface FastEthernet0/23
!
interface FastEthernet0/24
!
interface GigabitEthernet1/1
 switchport mode trunk
!
```

```
interface GigabitEthernet1/2
!
interface Vlan1
 no ip address
 shutdown
!
!
line con 0
!
line vty 0 4
 login
line vty 5 15
 login
!
end
```

6. SWITCH CORE IPV6 – running-config

Neste *switch* foram configuradas as portas no modo *trunk* utilizando o encapsulamento dot1q. Configuração necessária para transportar mais de uma VLAN utilizando apenas uma porta.

```
 “
hostname core-IPv6
!
spanning-tree mode pvst
!
!
!
!
interface FastEthernet0/1
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface FastEthernet0/2
 switchport trunk encapsulation dot1q
 switchport mode trunk
```

```
!
interface FastEthernet0/3
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface FastEthernet0/4
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface FastEthernet0/5
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface FastEthernet0/6
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface FastEthernet0/7
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface FastEthernet0/8
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface FastEthernet0/9
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface FastEthernet0/10
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface FastEthernet0/11
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface FastEthernet0/12
 switchport trunk encapsulation dot1q
```

```
 switchport mode trunk
!
interface FastEthernet0/13
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface FastEthernet0/14
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface FastEthernet0/15
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface FastEthernet0/16
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface FastEthernet0/17
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface FastEthernet0/18
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface FastEthernet0/19
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface FastEthernet0/20
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface FastEthernet0/21
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface FastEthernet0/22
```

```
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface FastEthernet0/23
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface FastEthernet0/24
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface GigabitEthernet0/1
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface GigabitEthernet0/2
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface Vlan1
 no ip address
 shutdown
!
ip classless

!
line con 0
!
line aux 0
!
line vty 0 4
 login
!
End
”
```

7. ROTEADOR EXTERNO IPV6 – running-config

Configurações aplicadas no roteador externo. Configurações necessárias para prover convergência entre redes distintas sobre IPv6 e saída da rede para outras redes. Configurada a interface com sub-interfaces para acessos às redes das VLANs 6 e 60. Configurado o roteamento dinâmico para divulgação e troca de tabela de roteamento. Configurado o roteamento dinâmico RIPng.

```
“
hostname Externo-IPv6
!
IPv6 unicast-routing
!
IPv6 dhcp pool dhcpv6
 prefix-delegation pool dhcpv6 lifetime 3600 3600
!
IPv6 local pool dhcpv6 2012:2::/120 124
!
license udi pid CISCO2911/K9 sn FTX1524C6KA
!
spanning-tree mode pvst
!
interface GigabitEthernet0/0
 no ip address
 duplex auto
 speed auto
!
interface GigabitEthernet0/0.6
 description IPv6 stateless
 encapsulation dot1Q 6
 no ip address
 IPv6 address 2010:1::/64 eui-64
 IPv6 rip rIPv6 enable
 IPv6 enable
!
interface GigabitEthernet0/0.60
 description statefull
 encapsulation dot1Q 60
```

```
 no ip address
 IPv6 address 2012:2::1/64
 IPv6 rip rIPv6 enable
 IPv6 enable
 IPv6 dhcp server dhcpv6
!
interface GigabitEthernet0/1
 no ip address
 duplex auto
 speed auto
 shutdown
!
interface GigabitEthernet0/2
 no ip address
 duplex auto
 speed auto
 shutdown
!
interface Serial0/0/0
 no ip address
 IPv6 address 2001:6::2/64
 IPv6 rip rIPv6 enable
 clock rate 64000
!
interface Serial0/0/1
 no ip address
 IPv6 rip rIPv6 enable
 shutdown
!
interface Vlan1
 no ip address
 shutdown
!
router rip
 version 2
 network 20.0.0.0
 no auto-summary
!
IPv6 router rip rIPv6
```

```
!
ip classless
!
line con 0
!
line aux 0
!
line vty 0 4
 login
!
end
”
```

8. ROTEADOR EXTERNO IPV4 – running-config

Seguem as configurações deste roteador, abaixo seguem os comandos aplicados e necessários para o correto funcionamento do roteador. Estes comandos permitem total convergência entre as redes IPv4 e IPv6 pela pilha dupla.

```
“
hostname Externo-IPv4
!
IPv6 unicast-routing
!
license udi pid CISCO2911/K9 sn FTX1524DG51
!
spanning-tree mode pvst
!
interface GigabitEthernet0/0
 no ip address
 duplex auto
 speed auto
 shutdown
!
interface GigabitEthernet0/1
 no ip address
 duplex auto
```

```
 speed auto
 shutdown
!
interface GigabitEthernet0/2
 no ip address
 duplex auto
 speed auto
 shutdown
!
interface Serial0/0/0
 ip address 20.13.20.2 255.255.255.252
 IPv6 address 2001:B:B:B::2/64
 IPv6 rip rIPv6 enable
 IPv6 enable
!
interface Serial0/0/1
 no ip address
 IPv6 address 2001:6::1/64
 IPv6 rip rIPv6 enable
 IPv6 enable
!
interface Vlan1
 no ip address
 shutdown
!
router rip
 version 2
 network 20.0.0.0
 no auto-summary
!
IPv6 router rip rIPv6
!
ip classless

!
line con 0
!
line aux 0
!
```

```
line vty 0 4
 login
!
End
”
```

9. ROTEADOR INTERNET – running-config

Neste Roteador foram configurados Pilha Dupla, NAT, NAT-PT, ISATAP, RIP e RIPng. Abaixo seguem as configurações aplicadas e necessárias para que os serviços possam funcionar corretamente:

```
hostname INTERNET
!


ipv6 unicast-routing


!
license udi pid CISCO2911/K9 sn FTX1524QA1M
!
spanning-tree mode pvst
!
interface Loopback0
 ip address 192.168.6.254 255.255.255.0
 ipv6 address 2013::4:1/64
 ipv6 rip ripv6 enable
!
interface Tunnel0
 no ip address
 mtu 1476
 no ipv6 nd ra suppress
 ipv6 address 2014::/64 eui-64
 ipv6 rip ripv6 enable
 ipv6 enable
 tunnel source GigabitEthernet0/0.10
 tunnel mode ipv6ip isatap
!
!
interface GigabitEthernet0/0
```

```
 no ip address
 duplex auto
 speed auto
!
interface GigabitEthernet0/0.10
 description Estagiarios
 encapsulation dot1Q 10
 ip address 172.16.0.1 255.255.254.0
 ip nat inside
 ipv6 nat
!
interface GigabitEthernet0/0.100
 description Funcionarios
 encapsulation dot1Q 100
 ip address 172.16.2.1 255.255.254.0
 ip nat inside
 ipv6 nat
!
interface GigabitEthernet0/0.1000
 description CPD
 encapsulation dot1Q 1000
 ip address 172.16.4.1 255.255.255.128
 ip nat inside
 ipv6 nat
!
interface GigabitEthernet0/1
 no ip address
 duplex auto
 speed auto
 shutdown
!
interface GigabitEthernet0/2
 no ip address
 duplex auto
 speed auto
 shutdown
!
interface Serial0/0/0
 ip address 20.13.20.1 255.255.255.252
```

```
 ip nat outside
 ipv6 address 2001:B:B:B::1/64
 ipv6 rip ripv6 enable
 ipv6 nat
 ipv6 enable
 clock rate 64000
!
interface Serial0/0/1
 no ip address
 shutdown
!
interface Vlan1
 no ip address
 shutdown
!
router rip
 version 2
 network 20.0.0.0
 network 172.16.0.0
 network 192.168.6.0
 no auto-summary
!
ipv6 router rip ripv6
!
ip nat inside source list 10 interface Serial0/0/0 overload
ip classless
!
!
access-list 10 permit 172.16.0.0 0.0.7.255
access-list 1 permit 172.16.0.0 0.0.7.255
ipv6 nat v4v6 source 172.16.4.2 2013::4:2
ipv6 nat v6v4 source 2012:2::1 192.168.6.1
ipv6 nat v6v4 source 2001:6::2 192.168.6.6
ipv6 nat v6v4 source 2012:2::2 192.168.6.2
ipv6 nat v4v6 source list 1 pool ipv4_ipv6
ipv6 nat v6v4 pool ipv6_ipv4 192.168.6.16 192.168.6.32 prefix-length 24
ipv6 nat v6v4 source list trafego_nat_ipv6 pool ipv6_ipv4
ipv6 nat v4v6 pool ipv4_ipv6 2013::4:16 2013::4:FFFF prefix-length 32
ipv6 nat prefix 2013::/96
```

```
ipv6 access-list trafego_nat_ipv6
 permit ipv6 any any
!


line con 0
!
line aux 0
!
line vty 0 4
 login
!
!
!
end
```

APÊNDICE B

LEITURA COMPLEMENTAR – CONFIGURANDO ROTEAMENTO DINÂMICO EM IPV6

Construída uma topologia para demonstrar o roteamento dinâmico RIP, OSPF e EIGRP para IPv6.

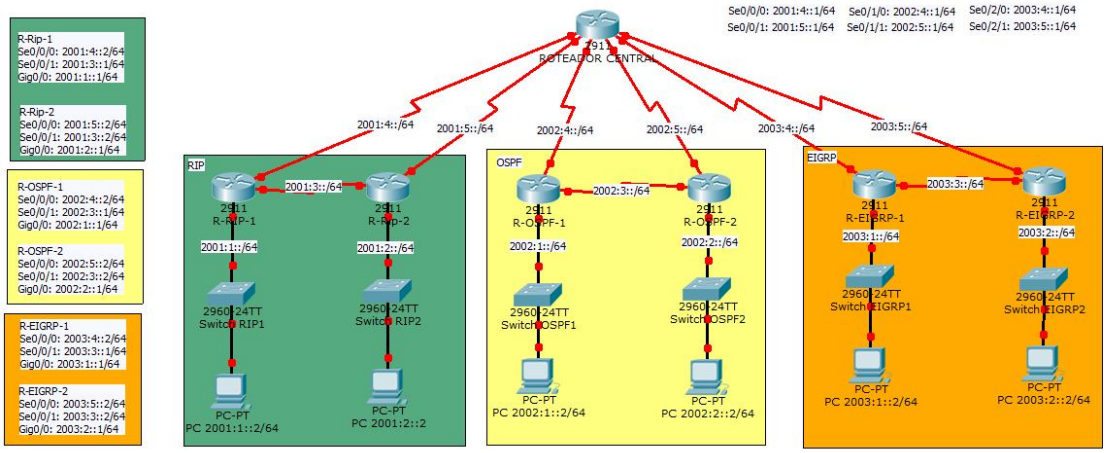

Figura - demonstra a topologia montada, mas com as interfaces desligadas.

Primeiro passo após construir a topologia é endereçar todos os equipamentos em redes diferentes para que haja conexão

Endereçamentos dos roteadores

R-RIP-1

ROETADOR	R-RIP-1 - R-CENTRAL	R-RIP-1 - R-RIP-2	R-RIP-1 - PC
IPv6	2001:4::2/64 - 2001:4::1/64	2001:3::1/64 - 2001:3::2/64	2001:1::1/64 - 2001:1::2/64

R-RIP-2

ROETADOR	R-RIP-2 - R-CENTRAL	R-RIP-2 - R-RIP-1	R-RIP-2 - PC
IPv6	2001:5::2/64 - 2001:5::1/64	2001:3::2/64 - 2001:3::1/64	2001:2::1/64 - 2001:2::2/64

R-OSPF-1

ROETADOR	R-OSPF-1 - R-CENTRAL	R-OSPF-1 - R-OSPF-2	R-OSPF-1 - PC
IPv6	2002:4::2/64 - 2002:4::1/64	2002:3::1/64 - 2002:3::2/64	2002:1::1/64 - 2002:1::2/64

R-OSPF-2

ROETADOR	R-OSPF-2 - R-CENTRAL	R-OSPF-2 - R-OSPF-1	R-OSPF-2 - PC
IPv6	2002:5::2/64 - 2002:5::1/64	2002:3::2/64 - 2002:3::1/64	2002:2::1/64 - 2002:2::2/64

R-EIGRP-1

ROETADOR	R-EIGRP-1 - R-CENTRAL	R-EIGRP-1 - R-EIGRP-2	R-EIGRP-1 - PC
IPv6	2003:4::2/64 - 2003:4::1/64	2003:3::1/64 - 2003:3::2/64	2003:1::1/64 - 2003:1::2/64

R-EIGRP-2

ROETADOR	R-EIGRP-1 - R-CENTRAL	R-EIGRP-1 - R-EIGRP-2	R-EIGRP-1 - PC
IPv6	2003:5::2/64 - 2003:5::1/64	2003:3::2/64 - 2003:3::1/64	2003:2::1/64 - 2003:2::2/64

Após Endereçar as conexões todos os roteadores e ligar as suas interfaces eles conseguirão comunicação entre si, mas não alcançarão roteadores ou computadores mais distantes, dispositivos que não estão diretamente conectados e em subredes distintas.

Ao ligar as interfaces os indicadores de conexão ficarão verdes conforme a seguinte figura:

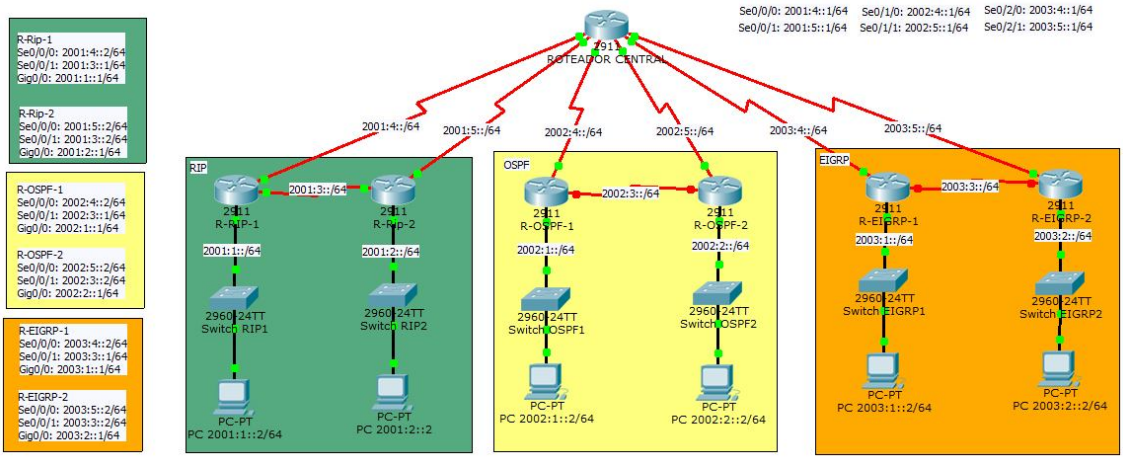

Figura - interfaces ligadas após endereçamento

Feitos testes de ICMPv6 para testar as conexões entre dispositivos para mostrar que sem um roteamento dinâmico ou estático os dispositivos só alcançam outros dispositivos diretamente conectados e pertencentes a mesma REDE.

Demonstrado o ICMPv6 na REDE VERDE que será configurado o RIPv6. O ICMPv6 só terá sucesso em dispositivos diretamente conectados e pertencentes a mesma rede, as outras redes terão o mesmo comportamento, .

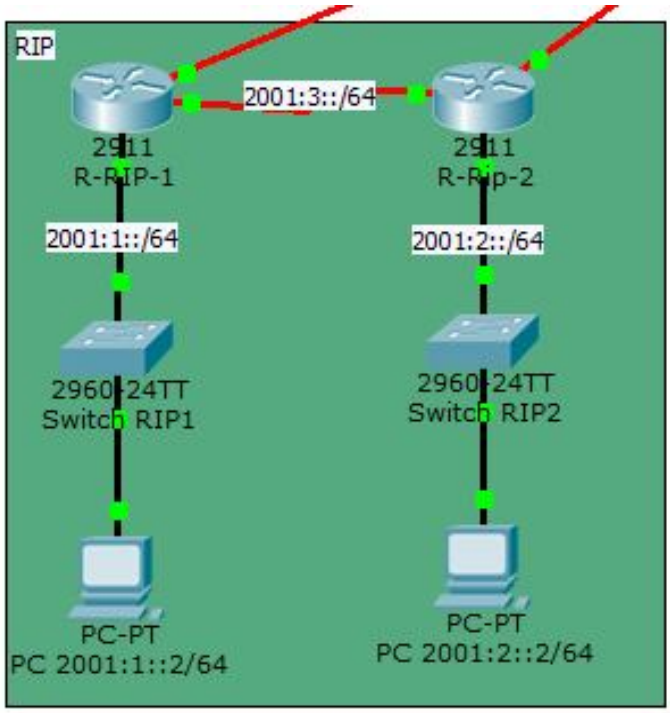

Figura - topologia do RIP

Fire	Last Status	Source	Destination	Type
	Successful	PC 2001:1::2/64	R-RIP-1	ICMPv6
	Successful	PC 2001:2::2/64	R-Rip-2	ICMPv6

ICMPv6 mostrando conectividade dos PC com os seus roteadores

Fire	Last Status	Source	Destination	Type
	Successful	R-RIP-1	R-Rip-2	ICMPv6
	Successful	R-RIP-1	ROTEADOR CENTRAL	ICMPv6
	Successful	R-Rip-2	ROTEADOR CENTRAL	ICMPv6

ICMPv6 mostrando conectividade entre os roteadores diretamente conectados

Fire	Last Status	Source	Destination	Type
	Failed	PC 2001:1::2/64	ROTEADOR CENTRAL	ICMPv6
	Failed	PC 2001:2::2/64	ROTEADOR CENTRAL	ICMPv6

ICMPv6 mostrando que não foi possível alcançar o próximo roteador 2001:4::1/64 e 2001:5::1/64

A tabela de roteamento demonstra com quem é possível estabelecer uma conexão. Abaixo seguem as Tabelas de roteamento dos roteadores R-RIP-1, R-RIP-2 e ROTEADOR CENTRAL.

```
R-RIP-1#show ipv6 route
IPv6 Routing Table - 7 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
       U - Per-user Static route, M - MIPv6
       I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary
       O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
       ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
       D - EIGRP, EX - EIGRP external
C   2001:1::/64 [0/0]
     via ::, GigabitEthernet0/0
L   2001:1::1/128 [0/0]
     via ::, GigabitEthernet0/0
C   2001:3::/64 [0/0]
     via ::, Serial0/0/1
L   2001:3::1/128 [0/0]
     via ::, Serial0/0/1
C   2001:4::/64 [0/0]
     via ::, Serial0/0/0
L   2001:4::2/128 [0/0]
     via ::, Serial0/0/0
L   FF00::/8 [0/0]
     via ::, Null0
```

Tabela de roteamento ipv6 do roteador R-RIP-1

```
R-RIP-2#show ipv6 route
IPv6 Routing Table - 7 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
       U - Per-user Static route, M - MIPv6
       I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary
       O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
       ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
       D - EIGRP, EX - EIGRP external
C   2001:2::/64 [0/0]
     via ::, GigabitEthernet0/0
L   2001:2::1/128 [0/0]
     via ::, GigabitEthernet0/0
C   2001:3::/64 [0/0]
     via ::, Serial0/0/1
L   2001:3::2/128 [0/0]
     via ::, Serial0/0/1
C   2001:5::/64 [0/0]
     via ::, Serial0/0/0
L   2001:5::2/128 [0/0]
     via ::, Serial0/0/0
L   FF00::/8 [0/0]
     via ::, Null0
```

Tabela de roteamento ipv6 do roteador R-RIP-2

```
R-CENTRAL#show ipv6 route
IPv6 Routing Table - 13 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
       U - Per-user Static route, M - MIPv6
       I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary
       O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
       ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
       D - EIGRP, EX - EIGRP external
C   2001:4::/64 [0/0]
     via ::, Serial0/0/0
L   2001:4::1/128 [0/0]
     via ::, Serial0/0/0
C   2001:5::/64 [0/0]
     via ::, Serial0/0/1
L   2001:5::1/128 [0/0]
     via ::, Serial0/0/1
C   2002:4::/64 [0/0]
     via ::, Serial0/1/0
L   2002:4::1/128 [0/0]
     via ::, Serial0/1/0
C   2002:5::/64 [0/0]
     via ::, Serial0/1/1
L   2002:5::1/128 [0/0]
     via ::, Serial0/1/1
C   2003:4::/64 [0/0]
     via ::, Serial0/2/0
L   2003:4::1/128 [0/0]
     via ::, Serial0/2/0
C   2003:5::/64 [0/0]
     via ::, Serial0/2/1
L   2003:5::1/128 [0/0]
     via ::, Serial0/2/1
L   FF00::/8 [0/0]
     via ::, Null0
```

Tabela de roteamento ipv6 do roteador ROTEADOR CENTRAL

Para que as redes possam acessar dispositivos que não estão diretamente conectados e em redes diferentes será utilizado roteamento dinâmico para divulgar as redes para outros roteadores e construir tabelas de roteamento automaticamente.

1 – CONFIGURANDO O RIPv6

Para configurar o rip será necessário ativar o roteamento na versão ipv6 com o seguinte comando no modo de configuração do roteador:

```
Roteador(config)#ipv6 unicast-routing
```

Atribuir um nome para o roteamento rip

```
Roteador(config)# ipv6 router rip <nome>
```

<nome> - nome a ser atribuído para identificar o rip

Neste exemplo o roteamento rip terá o nome ripv6

```
Roteador(config)# ipv6 router rip ripv6
```

Após atribuir um nome ao roteamento RIPng (RIPv6) ele deverá ser ativado em todas as interfaces que deseja divulgar as redes.

```
R-RIP-1(config)#interface Serial0/0/0
R-RIP-1(config-if)# ipv6 rip ripv6 enable
R-RIP-1(config-if)#interface Serial0/0/1
R-RIP-1(config-if)# ipv6 rip ripv6 enable
R-RIP-1(config-if)#interface GigabitEthernet0/0
R-RIP-1(config-if)# ipv6 rip ripv6 enable
```

```
R-RIP-2(config)#interface Serial0/0/0
R-RIP-2(config-if)# ipv6 rip ripv6 enable
R-RIP-2(config-if)#interface Serial0/0/1
R-RIP-2(config-if)# ipv6 rip ripv6 enable
R-RIP-2(config-if)#interface GigabitEthernet0/0
R-RIP-2(config-if)# ipv6 rip ripv6 enable
```

```
R-CENTRAL(config)#interface Serial0/0/0
R-CENTRAL(config-if)# ipv6 rip ripv6 enable
R-CENTRAL(config-if)#interface Serial0/0/1
R-CENTRAL(config-if)# ipv6 rip ripv6 enable
```

Após estas configurações será possível alcançar dispositivos mais distantes, dispositivos que não estão diretamente conectados, em redes distintas e que estejam na tabela de roteamento.

Fire	Last Status	Source	Destination	Type
	Successful	PC 2001:1::2/64	ROTEADOR CENTRAL	ICMPv6
	Successful	PC 2001:2::2/64	ROTEADOR CENTRAL	ICMPv6
	Successful	PC 2001:2::2/64	PC 2001:1::2/64	ICMPv6

Figura demonstra os dispositivos alcançando redes distintas e que não estão diretamente conectadas

Com o RIPng configurado para divulgar as redes a tabela de roteamento dos roteadores aprenderão as redes distantes e que utilizem o rip para divulgá-las

```
R-RIP-1#show ipv6 route
IPv6 Routing Table - 9 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
       U - Per-user Static route, M - MIPv6
       I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary
       O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
       ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
       D - EIGRP, EX - EIGRP external
C   2001:1::/64 [0/0]
     via ::, GigabitEthernet0/0
L   2001:1::1/128 [0/0]
     via ::, GigabitEthernet0/0
R   2001:2::/64 [120/2]
     via FE80::2E0:8FFF:FEE9:D6DB, Serial0/0/1
C   2001:3::/64 [0/0]
     via ::, Serial0/0/1
L   2001:3::1/128 [0/0]
     via ::, Serial0/0/1
C   2001:4::/64 [0/0]
     via ::, Serial0/0/0
L   2001:4::2/128 [0/0]
     via ::, Serial0/0/0
R   2001:5::/64 [120/2]
     via FE80::2E0:8FFF:FEE9:D6DB, Serial0/0/1
     via FE80::20C:CFFF:FE65:3AB1, Serial0/0/0
L   FF00::/8 [0/0]
     via ::, Null0
```

Figura mostra as redes aprendidas pelo rip no roteador R-RIP-1

```
R-RIP-2#show ipv6 route
IPv6 Routing Table - 9 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
       U - Per-user Static route, M - MIPv6
       I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary
       O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
       ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
       D - EIGRP, EX - EIGRP external
R   2001:1::/64 [120/2]
     via FE80::2E0:F9FF:FEDC:C202, Serial0/0/1
C   2001:2::/64 [0/0]
     via ::, GigabitEthernet0/0
L   2001:2::1/128 [0/0]
     via ::, GigabitEthernet0/0
C   2001:3::/64 [0/0]
     via ::, Serial0/0/1
L   2001:3::2/128 [0/0]
     via ::, Serial0/0/1
R   2001:4::/64 [120/2]
     via FE80::2E0:F9FF:FEDC:C202, Serial0/0/1
     via FE80::290:2BFF:FE45:5D53, Serial0/0/0
C   2001:5::/64 [0/0]
     via ::, Serial0/0/0
L   2001:5::2/128 [0/0]
     via ::, Serial0/0/0
L   FF00::/8 [0/0]
     via ::, Null0
```

Figura mostra as redes aprendidas pelo rip no roteador R-RIP-2

```
R-CENTRAL#show ipv6 route
IPv6 Routing Table - 16 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
       U - Per-user Static route, M - MIPv6
       I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary
       O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
       ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
       D - EIGRP, EX - EIGRP external
R   2001:1::/64 [120/2]
     via FE80::2E0:F9FF:FEDC:C201, Serial0/0/0
R   2001:2::/64 [120/2]
     via FE80::210:11FF:FE52:E921, Serial0/0/1
R   2001:3::/64 [120/2]
     via FE80::2E0:F9FF:FEDC:C201, Serial0/0/0
     via FE80::210:11FF:FE52:E921, Serial0/0/1
C   2001:4::/64 [0/0]
     via ::, Serial0/0/0
L   2001:4::1/128 [0/0]
     via ::, Serial0/0/0
C   2001:5::/64 [0/0]
     via ::, Serial0/0/1
L   2001:5::1/128 [0/0]
     via ::, Serial0/0/1
C   2002:4::/64 [0/0]
     via ::, Serial0/1/0
L   2002:4::1/128 [0/0]
     via ::, Serial0/1/0
C   2002:5::/64 [0/0]
     via ::, Serial0/1/1
L   2002:5::1/128 [0/0]
     via ::, Serial0/1/1
C   2003:4::/64 [0/0]
     via ::, Serial0/2/0
L   2003:4::1/128 [0/0]
     via ::, Serial0/2/0
C   2003:5::/64 [0/0]
     via ::, Serial0/2/1
L   2003:5::1/128 [0/0]
     via ::, Serial0/2/1
L   FF00::/8 [0/0]
     via ::, Null0
```

Figura mostra as redes aprendidas pelo rip no roteador R-CENTRAL

2 – CONFIGURANDO O OSPFv3

O OSPFv3 é a versão do OSPFv2 compatível com IPv6, para implementá-lo é muito parecido com o rip, com algumas funções a mais.

Assim como para configurar o RIPng necessita habilitar o roteamento para IPv6 com o comando ipv6 unicast-routing no modo de configuração do roteador

```
Roteador(config)#ipv6 unicast routing
```

Pode-se ter várias instâncias do OSPF configurado em um roteador com configurações distintas, neste caso iremos usar todas com um mesmo **process id igual a um.**

```
Roteador(config)# ipv6 router ospf 1
```

Importante identificar cada roteador com um **id** do ospf e segmentar o OSPF em áreas

```
Roteador(config-rtr)#  router-id 3.3.3.3
```

Para habilitar o OSPFv3 assim como no RIPng é necessário habilitá-lo na interface a qual deseja que divulgue a rede.

```
Roteador(config)# interface <[giga / serial / fast]> <[0-1]/[0-2]/[0-2]>
Roteador(config-if)# ipv6 ospf <id> area <[0-4294967295]>
        Ex:   Roteador(config)# interface serial 0/0/0
              Roteador(config-if)# ipv6 ospf 1 area 0
```

Em seguida será mostrada a configuração de cada roteador que utilizará o OSPF

```
R-OSPF-1(config)# ipv6 unicast-routing
R-OSPF-1(config)# ipv6 router ospf 1
R-OSPF-1(config-rtr)# router-id 1.1.1.1
R-OSPF-1(config)# interface GigabitEthernet0/0
R-OSPF-1(config-if)# ipv6 ospf 1 area 3
R-OSPF-1(config)# interface Serial0/0/0
R-OSPF-1(config-if)# ipv6 ospf 1 area 1
R-OSPF-1(config)# interface Serial0/0/1
R-OSPF-1(config-if)# ipv6 ospf 1 area 0
```

```
R-OSPF-2(config)# ipv6 unicast-routing
R-OSPF-2(config)# ipv6 router ospf 1
R-OSPF-2(config-rtr)# router-id 2.2.2.2
R-OSPF-2(config)# interface GigabitEthernet0/0
R-OSPF-2(config-if)# ipv6 ospf 1 area 4
R-OSPF-2(config)# interface Serial0/0/0
R-OSPF-2(config-if)# ipv6 ospf 1 area 2
R-OSPF-2(config)# interface Serial0/0/1
R-OSPF-2(config-if)# ipv6 ospf 1 area 0
```

```
R-OSPF-2(config)# ipv6 unicast-routing
R-CENTRAL(config)# ipv6 router ospf 1
R-CENTRAL(config-rtr)# router-id 3.3.3.3
R-CENTRAL(config)# interface Serial0/1/0
R-CENTRAL(config-if)# ipv6 ospf 1 area 1
```

```
R-CENTRAL(config)# interface Serial0/1/1
R-CENTRAL(config-if)# ipv6 ospf 1 area 2
```

Após estas configurações a tabela de roteamento já foi reconstruída e divulgada as redes para os roteadores via OSPF

```
R-OSPF-1#show ipv6 route
IPv6 Routing Table - 9 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
       U - Per-user Static route, M - MIPv6
       I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary
       O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
       ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
       D - EIGRP, EX - EIGRP external
C   2002:1::/64 [0/0]
     via ::, GigabitEthernet0/0
L   2002:1::1/128 [0/0]
     via ::, GigabitEthernet0/0
OI  2002:2::/64 [110/65]
     via FE80::260:2FFF:FE93:8871, Serial0/0/1
C   2002:3::/64 [0/0]
     via ::, Serial0/0/1
L   2002:3::1/128 [0/0]
     via ::, Serial0/0/1
C   2002:4::/64 [0/0]
     via ::, Serial0/0/0
L   2002:4::2/128 [0/0]
     via ::, Serial0/0/0
OI  2002:5::/64 [110/128]
     via FE80::260:2FFF:FE93:8871, Serial0/0/1
L   FF00::/8 [0/0]
     via ::, Null0
```

Figura mostra tabela de roteamento do roteador R-OSPF-1

```
R-OSPF-2#show ipv6 route
IPv6 Routing Table - 9 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
       U - Per-user Static route, M - MIPv6
       I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary
       O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
       ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
       D - EIGRP, EX - EIGRP external
OI  2002:1::/64 [110/65]
     via FE80::230:A3FF:FE44:B47B, Serial0/0/1
C   2002:2::/64 [0/0]
     via ::, GigabitEthernet0/0
L   2002:2::1/128 [0/0]
     via ::, GigabitEthernet0/0
C   2002:3::/64 [0/0]
     via ::, Serial0/0/1
L   2002:3::2/128 [0/0]
     via ::, Serial0/0/1
OI  2002:4::/64 [110/128]
     via FE80::230:A3FF:FE44:B47B, Serial0/0/1
C   2002:5::/64 [0/0]
     via ::, Serial0/0/0
L   2002:5::2/128 [0/0]
     via ::, Serial0/0/0
L   FF00::/8 [0/0]
     via ::, Null0
```

Figura mostra tabela de roteamento do roteador R-OSPF-2

Após a configuração do OSPF o comando show ipv6 route no roteador R-CENTRAL terá a seguinte saída:

```
R-CENTRAL>show ipv6 route
IPv6 Routing Table - 19 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
       U - Per-user Static route, M - MIPv6
       I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary
       O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
       ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
       D - EIGRP, EX - EIGRP external
R   2001:1::/64 [120/2]
     via FE80::2E0:F9FF:FEDC:C201, Serial0/0/0
R   2001:2::/64 [120/2]
     via FE80::210:11FF:FE52:E921, Serial0/0/1
R   2001:3::/64 [120/2]
     via FE80::2E0:F9FF:FEDC:C201, Serial0/0/0
     via FE80::210:11FF:FE52:E921, Serial0/0/1
C   2001:4::/64 [0/0]
     via ::, Serial0/0/0
L   2001:4::1/128 [0/0]
     via ::, Serial0/0/0
C   2001:5::/64 [0/0]
     via ::, Serial0/0/1
L   2001:5::1/128 [0/0]
     via ::, Serial0/0/1
OI  2002:1::/64 [110/65]
     via FE80::20D:BDFF:FEEB:203D, Serial0/1/0
OI  2002:2::/64 [110/65]
     via FE80::2D0:FFFF:FE02:B014, Serial0/1/1
OI  2002:3::/64 [110/128]
     via FE80::2D0:FFFF:FE02:B014, Serial0/1/1
     via FE80::20D:BDFF:FEEB:203D, Serial0/1/0
C   2002:4::/64 [0/0]
     via ::, Serial0/1/0
L   2002:4::1/128 [0/0]
     via ::, Serial0/1/0
C   2002:5::/64 [0/0]
     via ::, Serial0/1/1
L   2002:5::1/128 [0/0]
     via ::, Serial0/1/1
C   2003:4::/64 [0/0]
```

```
    via ::, Serial0/2/0
L   2003:4::1/128 [0/0]
    via ::, Serial0/2/0
C   2003:5::/64 [0/0]
    via ::, Serial0/2/1
L   2003:5::1/128 [0/0]
    via ::, Serial0/2/1
L   FF00::/8 [0/0]
    via ::, Null0
```

3 – CONFIGURANDO O EIGRP IPv6

EIGRP é um protocolo de roteamento dinâmico da CISCO, sua configuração é muito parecida com a do OSPF, não há necessidade de dividir ou informar as áreas como no OSPF, porém existe a necessidade de liga-lo assim como as interfaces físicas.

```
R-EIGRP-1(config)#ipv6 unicast-routing
R-EIGRP-1(config)#ipv6 router eigrp 1
R-EIGRP-1(config-rtr)# router-id 1.1.1.1
R-EIGRP-1(config-rtr)#no shutdown
R-EIGRP-1(config)#interface GigabitEthernet0/0
R-EIGRP-1(config-if)# ipv6 eigrp 1
R-EIGRP-1(config)#interface Serial0/0/0
R-EIGRP-1(config-if)#ipv6 eigrp 1
R-EIGRP-1(config)#interface Serial0/0/1
R-EIGRP-1(config-if)#ipv6 eigrp 1
```

```
R-CENTRAL(config)#ipv6 router eigrp 1
R-CENTRAL(config-rtr)# router-id 3.3.3.3
R-CENTRAL(config-rtr)#no shutdown
R-CENTRAL(config)#interface Serial0/2/0
R-CENTRAL(config-if)#ipv6 eigrp 1
R-CENTRAL(config)#interface Serial0/2/1
R-CENTRAL(config-if)#ipv6 eigrp 1
```

Após as configurações nos roteadores os equipamentos conseguirão se comunicar com as redes divulgadas que estão mais distantes e indiretamente conectadas.

A seguir será mostrada a tabela de roteamento dos roteadores que utilizam EIGRP

```
R-EIGRP-1#show ipv6 route
IPv6 Routing Table - 9 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
       U - Per-user Static route, M - MIPv6
       I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary
       O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
       ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
       D - EIGRP, EX - EIGRP external
C   2003:1::/64 [0/0]
     via ::, GigabitEthernet0/0
L   2003:1::1/128 [0/0]
     via ::, GigabitEthernet0/0
D   2003:2::/64 [90/2170112]
     via FE80::2E0:F9FF:FECA:1E6, Serial0/0/1
C   2003:3::/64 [0/0]
     via ::, Serial0/0/1
L   2003:3::1/128 [0/0]
     via ::, Serial0/0/1
C   2003:4::/64 [0/0]
     via ::, Serial0/0/0
L   2003:4::2/128 [0/0]
     via ::, Serial0/0/0
D   2003:5::/64 [90/2681856]
     via FE80::2E0:F9FF:FECA:1E6, Serial0/0/1
     via FE80::206:2AFF:FE08:C501, Serial0/0/0
L   FF00::/8 [0/0]
     via ::, Null0
```

Figura mostra tabela de roteamento do roteador R-EIGRP-1

```
R-EIGRP-2>show ipv6 route
IPv6 Routing Table - 9 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
       U - Per-user Static route, M - MIPv6
       I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary
       O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
       ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
       D - EIGRP, EX - EIGRP external
D   2003:1::/64 [90/2170112]
     via FE80::20A:F3FF:FE02:4151, Serial0/0/1
C   2003:2::/64 [0/0]
     via ::, GigabitEthernet0/0
L   2003:2::1/128 [0/0]
     via ::, GigabitEthernet0/0
C   2003:3::/64 [0/0]
     via ::, Serial0/0/1
L   2003:3::2/128 [0/0]
     via ::, Serial0/0/1
D   2003:4::/64 [90/2681856]
     via FE80::20A:F3FF:FE02:4151, Serial0/0/1
     via FE80::260:5CFF:FE77:32AD, Serial0/0/0
C   2003:5::/64 [0/0]
     via ::, Serial0/0/0
L   2003:5::2/128 [0/0]
     via ::, Serial0/0/0
L   FF00::/8 [0/0]
     via ::, Null0
```

Figura mostra tabela de roteamento do roteador R-EIGRP-2

Após configurações em todos os roteadores a tabela de roteamento do roteador CENTRAL será enorme, conforme mostrado abaixo:

```
R-CENTRAL#show ipv6 route
IPv6 Routing Table - 22 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
```

```
       U - Per-user Static route, M - MIPv6
       I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary
       O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
       ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
       D - EIGRP, EX - EIGRP external
R   2001:1::/64 [120/2]
     via FE80::2E0:F9FF:FEDC:C201, Serial0/0/0
R   2001:2::/64 [120/2]
     via FE80::210:11FF:FE52:E921, Serial0/0/1
R   2001:3::/64 [120/2]
     via FE80::2E0:F9FF:FEDC:C201, Serial0/0/0
     via FE80::210:11FF:FE52:E921, Serial0/0/1
C   2001:4::/64 [0/0]
     via ::, Serial0/0/0
L   2001:4::1/128 [0/0]
     via ::, Serial0/0/0
C   2001:5::/64 [0/0]
     via ::, Serial0/0/1
L   2001:5::1/128 [0/0]
     via ::, Serial0/0/1
OI  2002:1::/64 [110/65]
     via FE80::20D:BDFF:FEEB:203D, Serial0/1/0
OI  2002:2::/64 [110/65]
     via FE80::2D0:FFFF:FE02:B014, Serial0/1/1
OI  2002:3::/64 [110/128]
     via FE80::2D0:FFFF:FE02:B014, Serial0/1/1
     via FE80::20D:BDFF:FEEB:203D, Serial0/1/0
C   2002:4::/64 [0/0]
     via ::, Serial0/1/0
L   2002:4::1/128 [0/0]
     via ::, Serial0/1/0
C   2002:5::/64 [0/0]
     via ::, Serial0/1/1
L   2002:5::1/128 [0/0]
     via ::, Serial0/1/1
D   2003:1::/64 [90/2170112]
     via FE80::203:E4FF:FEBB:DCC5, Serial0/2/0
D   2003:2::/64 [90/2170112]
     via FE80::260:47FF:FEC1:7209, Serial0/2/1
```

```
D   2003:3::/64 [90/2681856]
    via FE80::260:47FF:FEC1:7209, Serial0/2/1
    via FE80::203:E4FF:FEBB:DCC5, Serial0/2/0
C   2003:4::/64 [0/0]
    via ::, Serial0/2/0
L   2003:4::1/128 [0/0]
    via ::, Serial0/2/0
C   2003:5::/64 [0/0]
    via ::, Serial0/2/1
L   2003:5::1/128 [0/0]
    via ::, Serial0/2/1
L   FF00::/8 [0/0]
    via ::, Null0
```

Com as configurações realizadas permitirá apenas conexão nas redes RIP, OSPF e EIGRP, mas não entre elas.

Fire	Last Status	Source	Destination	Type
	Failed	R-RIP-1	R-OSPF-1	ICMPv6
	Failed	R-RIP-1	R-EIGRP-1	ICMPv6
	Failed	R-OSPF-1	R-EIGRP-1	ICMPv6

Figura ICMPv6 realizado entre os roteadores das redes RIP,OSPF e EIGRP

Isso porque os roteadores não conhecem a tabela de roteamento das outras redes. Para solucionar este problema basta criar uma rota padrão nos roteadores R-RIP-1, R-RIP-2, R-OSPF-1, R-OSPF-2, R-EIGRP-1 e EIGRP-2.

```
Router(config)#ipv6 route ::/0 serial 0/0/0
```

Escolhido fazer a rota padrão pela serial, pois nem sempre o ip do próximo salto - próximo roteador - será conhecido, ainda mais se tratando de redes IPv6.

Desta forma toda rota que não estiver em sua tabela de roteamento o pacote sairá pela interface serial 0/0/0 com a esperança de que o próximo roteador conheça ou tenha entradas em sua tabela de roteamento.

Como o roteador CENTRAL conhece todas as redes RIP, OSPF e EIGRP ele encaminhará para a rede correta.

Fire	Last Status	Source	Destination	Type
	Successful	R-RIP-1	R-OSPF-1	ICMPv6
	Successful	R-RIP-1	R-EIGRP-1	ICMPv6
	Successful	R-OSPF-1	R-EIGRP-1	ICMPv6

Figura ICMPv6 realizado entre os roteadores das redes RIP,OSPF e EIGRP