Jordao Dos Santos Coana

ESTUDO DA MIGRAÇÃO DA REDE CORPORATIVA IPv4 A IPv6:

Estudo de caso do EXB- Servicos

Licenciatura em Informática

Universidade Pedagógica de Maputo

2021

Jordao dos Santos Coana

ESTUDO DA MIGRAÇÃO DA REDE CORPORATIVA IPv4 A IPv6:

Estudo de caso do EXB- Servicos

Monografia Científica a ser apresentada no Departamento de Informática na Faculdade de Engenharias e Tecnologias da UP-Maputo, para obtenção de grau de Licenciatura em Informática

Supervisor:

dr. Faizal Licumba

Universidade Pedagógica de Maputo

2021

Índice

Índice iii
Lista de Tabelas v
Lista de Figuras vi
Lista de abreviaturas e siglas vii
Declaração ix
Dedicatória x
Agradecimentos xi
Resumo xii
Abstract xiii
CAPÍTULO I: INTRODUÇÃO 13
1.1 Problema de Pesquisa 14
1.2 Justificativa 15
1.3 Objectivos 17
1.3.1 Objectivo Geral 17
1.3.2 Objectivos Específicos 17
1.4 Questões de Pesquisa 17
1.5 Hipóteses 18
1.6 METODOLOGIA DA PESQUISA 18
1.6.1 Métodos de Pesquisa 18
CAPÍTULO II: REVISÃO BIBLIOGRÁFICA / FUNDAMENTAÇÃO TEORICA 20
2.1 Redes de Computadores 20
2.2 Internet 20
2.3 Histórico e arquitectura da rede TCP/IP 20
2.4 Protocolo 23
2.5 Protocolo da Internet Versão Quatro (IPv4) 23
2.5.1 Formato do Cabeçalho do IPv4 24
2.5.2 Endereçamento do Protocolo de Internet versão quatro 26
2.5.3 Tipos de Endereços IPv4 27
2.5.4 Esgotamento e Medidas IPv4 28
2.6 Protocolo de Internet Versão Seis (IPv6) 30

2.6.1 Cabeçalho de Extensão do Protocolo IPv6 32
2.6.2 Formato do Cabeçalho de IPv6 32
2.6.3 Endereçamento IPv6 34
2.6.4 Estrutura do Endereçamento do IPv6 34
2.6.5 Tipos de Endereços IPv6 35
2.6.5.1 Unicast 35
2.6.5.2 Anycast 37
2.6.5.3 Multicast 37
2.6.6 Segurança do Protocolo IPv6 38
2.6.7 Mobilidade IPv6 39
2.7 Tipos de Simuladores 39
CAPÍTULO IV: APRESENTAÇÃO, ANÁLISE E DISCUSSÃO DOS RESULTADOS DA PESQUISA 40
4.1 Levantamento da situação actual da rede EXB na versão do IPv4 40
4.1.1 Apresentação da EXB Serviços 40
4.1.2 Levantamento da situação actual da Rede sob ponto de vista de Hardware 40
4.1.3 Software que suporta a Rede 41
4.1.4 Segurança da rede 42
4.1.5 Gestão e roteamento de pacotes da rede 42
4.1.6 Acessso a Rede 44
4.1.1 Cenário actual da rede da Fidelidade 45
4.2 Identificação das características técnicas de protocolo de Internet IPv6 45
4.3 Redesenho da rede com IPv6 46
4.4 Resultado da simulação virtual da rede com IPv6 46
CAPÍTULO V: CONCLUSÃO, RECOMENDAÇÕES E LIMITAÇÕES 48
Recomendações 48
REFERÊNCIAS BIBLIOGRÁFICAS 49
Outros Documentos Consultados: 50

Lista de Tabelas

Tabela 1: Cabeçalho de IPv4 25
Tabela 2: Formato de endereço IPv4 27
Tabela 3: Cabeçalho de IPv6 32
Tabela 4: Cabeçalho IPv4 - Remoção de campos para o IPv6 33

Lista de Figuras

Figura 1: Descrição das arquitecturas OSI e TCP/IP 21
Figura 2: Demonstração do NAT 30
Figura 3: Esquema da actual da REDe EXB 40
Figura 4: Infraestrutura da Rede 41
Figura 5: Infraestrutura de Rede de Segurança 43
Figura 6: Cenário actual da redecom IPv4 45
Figura 7: Cenário proposto para a rede com IPv6 46

Lista de abreviaturas e siglas

ARP – Address Resolution Protocol

BGP – Border Gateway Protocol

CCNA – Cisco Certified Network Associate

CISCO – Corps Information System Control Officer

CIUP – Centro de Informática da Universidade Pedagógica

CTA – Corpo Técnico Administrativo

DHCP – Dynamic Host Configuration Protocol

DNS – Domain Nome Services

EN1 - Estrada Nacional número 1

FTP – File Transfer Protocol

GNS3 – Graphical Network Simulator-3

GNU – Gnu's Not Unix

HTTP –Hypertext Transfer Protocol

IANA – Internet Assigned Number Authority

ICMP - Internet Control Message Protocol

ICT – Information and Communication Technologies

IETF - Internet Engieneering Task Force

IP – Internet Protocol

IPsec – Internet Protocol Security

IPv4 – Protocolo de Internet versão quatro

IPv6 – Protocolo de Internet versão seis

ISP – Internet Service Provider

LACNIC - Latin America and Caribbean Network Information Centre

LAN – Local Area Network

MPLS – Multi-Protocol Label Switching

MS - Microsoft Office

NAT – Network Address Translation

OSPF – Open Shortest Path First

Pág – Páginas

PC – Personal Computer

QoS – Qualidade de Serviços

RARP – Reserve Address Resolution Protocol

RFC - Request For Comments

Lista de abreviaturas e siglas (Cont.)

RIP – Routing Information Protocol

SIGEUP – Sistema de Gestão da Universidade Pedagógica

SMTP – Simple Mail Transfer Protocol

UP - Universidade Pedagógica

VoIP – Voice over IP

WAN – Wide Area Network

Declaração

Declaro que esta Monografia é resultado da minha investigação pessoal e das orientações do meu supervisor, o seu conteúdo é original e todas as fontes consultadas estão devidamente mencionadas no texto, nas notas e na bibliografia final.

Declaro ainda que este trabalho não foi apresentado em nenhuma outra instituição para obtenção de qualquer grau académico.

Maputo, Junho de 2021

_____

(Jordão dos Santos Coana)

Dedicatória

Dedico este trabalho a minha família Coana, em especial aos meus pais, meu filho e minha esposa que todo momento estiveram presente nesta jornada académica.

Agradecimentos

A Universidade Pedagógica e a todos docentes da Escola Superior Técnica, em particular do Departamento de Informática, por ter dado espaço para minha prática da pesquisa, aos técnicos do Centro de Informática da UP e a direcção em geral pelo acompanhamento e ensinamentos nesta longa e dura caminhada.

Aos meus Filhos, pelo apoio moral, financeiro e espiritual para que eu pudesse chegar no fim nessa longa e dura caminhada.

Ao Professores e Mestres pelas observações dadas ao longo da realização do trabalho.

Aos meus colegas da turma INF2015, em espacial a a minha turma, pelas dicas e colaborações preciosas.

Aos meu amigos que incansavelmente me apoiou e deu-me forças para não recuar, alimentando a esperança.

Como não posso contemplar todos aqui, os meus agradecimentos para todos que directa ou indirectamente, contribuíram para a realização deste trabalho e no meu sucesso académico.

Resumo

Com o esgotamento de IPv4 o uso do NAT já não é mais solução, não sendo a migração, encontra-se a rede EXB Serviços com maior número de dispositivos e vários serviços, o que leva a insuficiências de endereços. O problema de partida para a realização deste trabalho é a procura de estratégias da migração da rede UPNet de protocolo de Internet versão quatro (IPv4) para protocolo de Internet versão seis (IPv6).

O objectivo geral deste trabalho é analisar estratégias de migração da Rede de Protocolo de Internet versão quatro (IPv4) à versão seis (IPv6).

Para a materialização da pesquisa foi, por um lado, usada a abordagem qualitativa para avaliação da Rede antes e depois da migração. Por outro lado foi usada a abordagem quantitativa para a análise de dados e, na base de pesquisas bibliográficas em materiais específicos da área de redes, livros que abordam protocolos de comunicação, também em documentos que tratam da migração de IPv4-IPv6, relatório anual da Movitel, monografias já defendidas na área de Informática com informações relacionadas ao com o tema em pesquisa e a simulação da rede antes e depois da migração.

Os resultados de destaque da pesquisa são:

• Um desenho e uma demonstração da gama de endereços da nova rede com IPv6.

• Um desenho de estratégias de migração da Rede IPv4 para IPv6, demonstrando que a estratégia pilha dúpla e tunelamento são as principais.

Palavras-Chave**:** ***Redes, Internet, IP (Internet Protocol), IPv4, IPv6*****.**

Abstract

With the depletion of IPv4 and the use of NAT is no longer a solution behind migration, the EXB Services network is available with more devices and various services, which leads to address the shortcomings. The initial problem for the accomplishment of this work is the search of strategies of migration of the Network version of the protocol Internet version four (IPv4) to the six version of the protocol Internet (IPv6).

The general objective of this work is to analyze the migration strategies of version four of the Internet Protocol (IPv4) for version six (IPv6).

For the materialization of the research, a qualitative approach was used to evaluate before and after the migration, quantitative for data analysis and on the basis of bibliographical research in specific materials in the area of networks, books that deal with communication protocols, also in related documents to migration. of the IPv4-IPv6, annual report of the Network, monographs already defended in the area of Informatics with information related to the topic in research and the simulation of EXB before and after the migration.

The highlights of the survey are:

- *A design and demonstration of the range of addresses of the new network with IPv6.*
- *A design of Netowk migration strategies from IPv4 to IPv6, demonstrating that the stack and tunneling strategy are the main ones*

*Keywords**: **Networks, Internet, IP (Internet Protocol), IPv4, IPv6.***

CAPÍTULO I: INTRODUÇÃO

A Internet é uma rede que interconecta milhões de computadores no mundo inteiro, onde para que haja a comunicação na rede, cada dispositivo necessita de um endereço único, o chamado Protocolo de Internet (IP), com função principal a interligação dos dispositivos na rede.

No início da década de 90 ficou evidente que o IP atingirá um estado crítico. Se nada fosse feito, a quantidade de endereços disponíveis se extinguiria rapidamente. Houve então o surgimento de soluções relativamente fáceis tais como C**IDR** (**Classless Inter-Domain Routing**) e o **NAT,** esta auxiliou preventivamente no problema do esgotamento do espaço de endereçamento do IPv4, mas ele apresentou várias incompatibilidades com vários protocolos, por exemplo, no FTP. Foi daí que surgiu o IPv6, que é a resposta de insuficiência de endereços IP.

Sendo a rede corporativa de Internet da Fidelidade, uma rede de computadores que usa o endereçamento IPv4 para a transferência de dados, partilha de informação e acesso a Internet, a rede dá suporte a todos serviços Offline e Online da instituição. Neste âmbito, surge o presente trabalho que tem como tema "Estudo da migração da Rede de IPv4 a IPv6: estudo de caso do Fidelidade Seguros".

O presente trabalho surge da necessidade de solucionar o problema de insuficiência de endereços IPs, na rede de Internet da EXB Serviços, que é uma unidade central de apoio a seguros.

O objectivo geral deste trabalho é analisar estratégias de migração da rede de Protocolo de Internet versão quatro (IPv4) a versão seis (IPv6).

Para o alcance do objectivo acima referido, a pesquisa foi feita através das abordagens qualitativa e quantitativa assim como através de pesquisas bibliográficas em materiais específicos de área de redes, livros que abordam protocolos de comunicação, também em documentos que abordam a migração de IPv4 - IPv6, relatório anual da EXB Serviços.

1.1 Problema de Pesquisa

GIL (2008) diz que o primeiro procedimento adoptado numa pesquisa bibliográfica, como em qualquer outro tipo de pesquisa, consiste na formulação do problema que se deseja investigar.

MARCONI & LAKATOS (2003:97) descrevem o problema como sendo o que dita a pesquisa, e que toda investigação nasce de algum problema teórico/prático sentido. Este dirá o que é relevante ou irrelevante observar, os dados que devem ser seleccionados.

Os autores anteriormente citados convergem na ideia segundo a qual o problema é uma dificuldade de real importância, na qual requer uma investigação a procura da solução c

A REDE EXB Serviços é uma infra-estrutura física da rede corporativa de dados, vídeo e voz da Instituição, que é gerida por endereços IP, vem para responder a disponibilidade e consistência dos serviços informáticos oferecidos, reduzindo custos, e gerando maior produtividade nos estudantes, nos gestores até aos colaboradores e pesquisadores (Citar Alguem *et al*., 2014).

A mesma rede funciona e dá suporte a vários serviços da rede, dentre os quais: serviços de Internet, Vídeo-conferências, VOIP, Sinalética Digital e E-mail corporativo usando o IPv4.

O protocolo IPv4 é o mais usado e mostrou-se muito robusto, sendo de fácil implantação e interoperabilidade. Entretanto, durante o seu projecto original não se previa alguns aspectos relativos ao crescimento exponencial das redes e um possível esgotamento de endereços IP. Utiliza 32 bits para endereçamentos representados em 4 segmentos de números decimais variando de 0 a 255, onde parte do endereço identifica a rede e outra parte a estação. Os 32 bits de endereçamento, possibilitam gerar mais de 4 biliões de endereços distintos (OMAR, 2017).

Devido ao crescimento da instituição, o número dos utilizadores conectados na rede e os dispositivos também ligados na rede são enormes necessitando desta forma uma gama de endereços e que a qualidade de serviços seja verificada, permitindo que o nível da administração da infra-estrutura da rede e o uso dos equipamentos sejam os desejados. Assim, prevê-se o esgotamento de endereço IP na rede, havendo necessidade de migração de IPv4 para IPv6.

Assim, a questão de partida para a realização deste trabalho é: *Quais são as estratégias da migração da rede de protocolo de Internet versão quatro (IPv4) para protocolo de Internet versão seis (IPv6)?*

1.2 Justificativa

LAKATOS & MARCONI (2005: 219) afirmam que a justificativa é o único item do projecto que apresenta respostas à questão por quê? E que geralmente é o elemento que contribui mais directamente na aceitação da pesquisa pela (s) pessoa (s) ou entidades que vão financiá-la.

GIL (2002: 162) defende que a justificava trata-se de uma apresentação inicial do projecto, que pode incluir factores que determinaram a escolha do tema, sua relação com a experiência profissional ou académica do autor, assim como sua vinculação à área temática da pesquisa.

A EXB Serviços, desde que concebeu a rede corporativa de Internet, tem o suporte do Protocolo de Internet da versão quatro, onde segundo JAMHOUR (2008:8), alerta do esgotamento do primeiro bloco de endereços IPv4 os quais pertenciam a própria IANA. Como no geral, a quantidade de alocações vem crescendo a cada ano, deve-se esperar que o esgotamento do bloco IANA aconteça muito em breve (as últimas estimativas eram de 2011). Quando o bloco IANA estiver totalmente exaurido, não haverá possibilidade de novas alocações para as autoridades de registo regionais. Isto significa que a IANA não terá mais a possibilidade de suprir as necessidades de crescimentos de áreas emergentes representadas pelo LACNIC (América Latina) e AfriNIC (África).

Sendo que na rede jamais podem-se encontrar dois dispositivos com os mesmos endereços IP operando, o papel fundamental dos endereços é distinguir entre quaisquer equipamentos de uma mesma rede, como uma forma de garantir também a segurança de informação (MADEIROS, 2010).

O objectivo do autor ao trazer esse tema é contribuir para a melhoria de qualidade de serviços informáticos e responder à futura demanda das necessidades dos utilizadores e no ponto de vista de migração da versão IPv4 para versão IPv6. Após a migração espera-se que haja um maior benefício no melhoramento do desempenho. Isso vai trazer a abrangência de todos serviços fornecidos pela EXB Serviços, não só, que a instituição esteja já doptada de todas ferramentas e que responda com exactidão às necessidades previamente estabelecidas na concepção da rede.

O presente trabalho é importante no processo de ensino, pesquisa e extensão na formação de qualidade, isto é, com o acesso à rede de Internet assim como a partilha exaustiva de ficheiros

dos pesquisadores internos e internacionais através da rede de Internet leva a um alto nível de aprendizagem assim como de pesquisa, tomando em consideração o outro ponto importante é o facto de acesso a informação, obras e pesquisas diárias na Internet. Através da rede de Internet pode-se proporcionar o incentivo pela leitura e pela aprendizagem, conta também com abrangência do ensino.

Com a presente abordagem, este tema visa contribuir na carreira como pesquisador e como estudante de Informática, trazendo um contributo para a casa que lhe acolheu durante a formação académica. Por outro lado durante a formação, o autor foi percebendo a necessidade de pesquisar um assunto de interesse institucional e como uma marca de não só se limitar em se formar, mas sim, na contribuição do crescimento da instituição.

É de salientar que o uso de IPv6 é um mecanismo de fácil adaptação para os técnicos e os usuários da rede, ajudando assim a responder as necessidades diárias das solicitações feitas ao departamento do acesso a rede, pelos directores e CTA.

1.3 Objectivos

1.3.1 Objectivo Geral

O objectivo geral do trabalho é estudar as estratégias de migração da rede da EXB Serviços de Protocolo de Internet versão quatro (IPv4) a versão seis (IPv6).

1.3.2 Objectivos Específicos

Os objectivos específicos do trabalho são:

- Fazer o levantamento da situação actual da rede na versão do IPv4 sob ponto de vista de Hardware, Software, Segurança, Gestão e QoS;
- Identificar as características técnicas do protocolo de Internet IPv6;
- Redesenhar/o a rede com IPv6;
- Simular virtualmente a rede com IPv6;
- Desenhar as principais estratégias de migração da rede em IPv4 para IPv6.

1.4 Questões de Pesquisa

As questões de pesquisa levantadas para este trabalho são:

- Qual é a situação actual da rede?
- Quais são as características técnicas do protocolo de Internet IPv6?

- Que tipo de estrutura deverá ter a nova rede com IPv6?
- Qual é o simulador que permite criar topologias com variadas infra-estruturas de redes e que permite comunicação de dados?
- Quais são as principais estratégias da migração de IPv4 para IPv6?

1.5 Hipóteses

Segundo os objectivos específicos da pesquisa, definimos as seguintes hipóteses:

- A rede usa actualmente o Protocolo de Internet IPv4 para dar suporte aos serviços, visto que o protocolo não tem maior número de endereços e encontra-se em esgotamento.
- Das várias características, o IPv6 tem a capacidade de endereçamento, suporte para tráfego com a garantia de qualidade de serviços, maior número de endereços disponíveis.
- A nova rede da Fidelidade com IPv6 tem uma estrutura de Rede Convencional com sustentação técnica e padronização dos protocolos, meios de comunicação remodeladas ou redefinidas dando origem a novos serviços.
- O simulador que permite criar topologias com variadas infra-estruturas de redes e comunicação de dados é o Cisco Packet-Trace.
- As estratégias de migração de IPv4 para IPv6 na rede são uma pilha dúpla, tunelamento e tradução.

1.6 METODOLOGIA DA PESQUISA

O capítulo da metodologia fundamenta a organização dos dados, articulando-os com a fundamentação teórica, resultante da revisão da literatura da temática da investigação. Qualquer procedimento empírico prevê que sejam tomadas opções metodológicas, para que o investigador, ou seja, o pesquisador possa utilizar o método científico com rigor e honestidade, e ainda utilizar os recursos de forma produtiva e eficiente. (MARCONI & LAKATOS, 2003)

1.6.1 Métodos de Pesquisa

Para o presente trabalho recorreu-se a metodologias qualitativa e quantitativa que a seguir descrevemos:

a) Pesquisa Qualitativa

Neste tipo de pesquisa, GIL (1999) considera que há uma relação dinâmica entre o mundo real e o sujeito, isto é, um vínculo indissociável entre o mundo objectivo e a subjectividade do sujeito que não pode ser traduzida em números. A interpretação dos fenómenos e a atribuição de

significados são básicos no processo de pesquisa qualitativa.

O autor entende o método qualitativo como sendo aquele que leva a perceber a Rede da Fidelidade durante o processo da migração em termo da qualidade de sinal e de serviços fornecidos.

b) Pesquisa Quantitativa

GERHARDT & SILVEIRA (2009:33) caracterizam a pesquisa quantitativa, como sendo as raízes no pensamento positivista lógico, tende a enfatizar o raciocínio dedutivo, as regras da lógica e os atributos mensuráveis da experiência humana. Por outro lado, a pesquisa qualitativa tende a salientar os aspectos dinâmicos, holísticos e individuais da experiência humana e utiliza procedimentos estruturados e instrumentos formais para colecta de dados.

Para o autor, o método quantitativo é aquele que fornece os dados numéricos, sistemáticos e estatísticos da amostra, onde apresentamos os resultados de dados estatísticos dos utilizadores da rede antes e depois da migração concordando desta forma com GERHARDT & SILVEIRA (2009).

CAPÍTULO II: REVISÃO BIBLIOGRÁFICA / FUNDAMENTAÇÃO TEORICA

Este capítulo aborda os diferentes conceitos associados ao tema e à recolha de informação de várias obras e artigos científicos para fundamentação do problema do estudo.

2.1 Redes de Computadores

Uma rede de computadores é o conjunto de ligações de dois ou mais computadores para permitir a partilha de recursos e troca de informações entre as máquinas (FERNANDES, 2016, p.1).

A rede de computadores consiste nas ligações entre dois ou mais computadores e dispositivos (equipamentos) completamente acoplados através de recursos de comunicação, geograficamente distribuídos, permitindo a troca de dados entre estas unidades através de um sistema de comunicação e optimizando recursos de *hardware* e *software* (MORAIS *et al*., 2012, p.13).

O autor entende que rede de computadores é formada por dois ou mais computadores interligados, tornando-os capazes de se comunicar, e usam protocolos comuns, sendo esses protocolos um conjunto de regras e códigos em comum concordando assim com MORAIS *et al*., 2012.

2.2 Internet

PAMPLONA (2014) defende que Internet é uma organização livre, nenhum grupo a controla ou a mantém economicamente. Pelo contrário, muitas organizações privadas, universidades e agências governamentais sustentam ou controlam parte dela. Todos trabalham juntos, numa aliança organizada, livre e democrática.

A Internet é um grande conjunto de redes de computadores interligado pelo mundo inteiro; de forma integrada viabilizando a conectividade independente do tipo de máquina que seja utilizada. Para manter essa multi-compatibilidade usa-se um conjunto de protocolos e serviços em comum, podendo assim, os usuários conectados a ele usufruir de serviços de informação de alcance mundial.

2.3 Histórico e arquitectura da rede TCP/IP

Durante o desenvolvimento das arquitecturas que seriam padronizadas para as redes, como TCP/IP, foi desenvolvido também um modelo chamado OSI pela ISO, o modelo OSI segundo

alguns pesquisadores como o "*Tenenbaum*" não se pode clamar de arquitectura, pois ele não especifica os serviços e protocolos exactos que devem ser usados em cada camada (OMAR, 2017).

No modelo OSI (*Open Systems Interconnection*) é um conjunto de protocolos abertos (normas que podem ser adoptadas livremente) para o fabrico de equipamentos e desenvolvimento de *software*, destinados a funcionar em rede. Este modelo subdivide-se, no processo global da comunicação de dados entre computadores, em sete níveis ou camadas. Cada uma das quais tem funções específicas.

OSI é um conjunto de protocolos, e sim de um modelo para o desenvolvimento de uma arquitectura de rede flexível, robusta e de operação conjunta, facilitando a interconexão de sistemas distintos, tudo partindo da divisão das camadas tem como uma das vantagem decompor as comunicações de rede em partes menores e mais simples, facilitando a sua análise. A arquitectura ganhou o nome de arquitectura da rede TCP/IP partindo do modelo de referência OSI como ilustra a baixo.

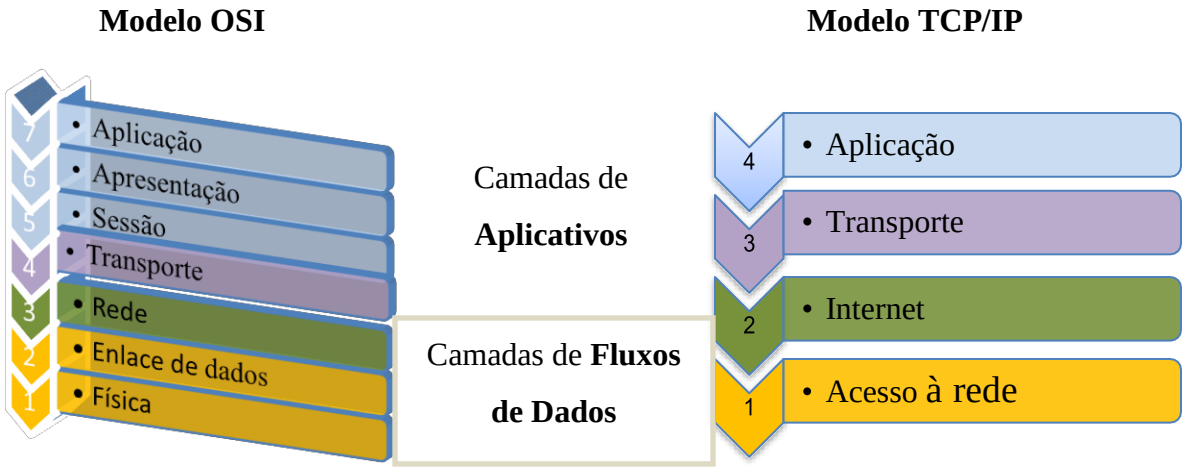


Figura 1: Descrição das arquitecturas OSI e TCP/IP

Fonte: Adaptada segundo comparação dos modelos OSI e TCP (2018)

Seria difícil falar do modelo TCP/IP sem mencionar o modelo de referência OSI, porém, no que concerne ao modelo OSI (criado em 1970 e formalizado em 1983), este é um modelo de referência da ISO que tinha como principal objectivo ser um modelo *standard* para protocolos de comunicação entre os mais diversos sistemas. Para garantir a comunicação *end-to-end* e a percepção do modelo OSI, MACAMO (2018:9) explica, as seguintes camadas e suas funções:

1) – **Física:** A camada física é a mais baixa da hierarquia e nela é determinado como serão realizadas as transferências de bits através de um canal de comunicação.

2) **- Enlace de Dados:** Nesta camada é onde há detecção/Correcção de erros, fragmentação dos dados em quadros, ocorrem também algum controle de fluxo.
3) **– Rede:** É nesta camada onde há controlo a operação da sub-rede, há também roteamento e controle de congestionamento.
4) **– Transporte:** Nesta camada se estabelece a comunicação ponto-a-ponto e estabelecimento/encerramento de conexão.
5) **- Sessão:** é a camada onde existe o estabelecimento de sessão entre máquinas diferentes e provê serviços aperfeiçoados tais como **login remoto** e **transferência de arquivos.**
6) **– Apresentação: S**e relaciona com a sintaxe/semântica dos dados, codificação dos dados: computadores diferentes podem ter codificações diferentes e criptografia.
7) **– Aplicação:** A camada 7 é a mais próxima do usuário, porque mostra todos os aplicativos e que têm acesso à rede. Temos como exemplo um usuário acesa a internet, ele utiliza um *browser,* que usará o protocolo de aplicação chamado *HTTP* que posteriormente "fará contacto com o servidor para buscar a página desejada".

OMAR (2017:11) demostra que a arquitectura do modelo TCP/IP é constituída por quatro camadas, em comparação com o modelo de referência OSI que é constituído por sete camadas, conforme ilustra a figura 1. Actualmente usa-se a arquitectura TCP/IP, onde encontram-se as quatro camadas, sendo cada uma responsável pela execução de tarefas distintas, para garantir a integridade e entrega dos dados transferidos pelo Protocolo, a saber:

1) Camada de acesso a Rede: é também chamada de interface da rede, estabelece a base do modelo TCP/IP, agrupando as camadas Física e de Enlace do padrão OSI. Desta forma, suas funções de **formatação** e **endereçamento** dos dados para o meio de transmissão, com base em endereços de hardware (físico), e verificação de erros dos dados entregues no destino.

2) **Camada de Rede (Internet):** Esta camada está relacionada à camada de rede do modelo OSI e tem a finalidade de fornecer e tratar endereços lógicos de origem e destino, independentes de *hardware*, possibilitando a compatibilidade na comunicação entre diferentes plataformas, que não se encontram conectadas localmente e com a função de endereçamento lógico efectuado pelo *Internet Protocol* (IP).

3) Camada de Transporte: Função de transporte incluindo os mecanismos necessários que garantem a entrega sequencial de dados, sem erros e sem falhas.

4) Camada de Aplicação: Esta camada faz a comunicação entre os programas e os protocolos de transporte no TCP/IP.

Arquitectura TCP/IP (*Transmission Control Protocol/Internet Protocol)* é um conjunto de padrões e protocolos de comunicação de dados utilizados na interconexão e endereçamento de computadores e redes onde cada computador deve ter um módulo de *software* TCP/IP em seu sistema operativo e aplicativos para se comunicar com outros dispositivos e redes TCP/IP. (TCP & COLOMBO, 2015).

TCP (*Transmission Control Protocol*): é o protocolo responsável pelo controle de qualidade da comunicação entre a origem (transmissor) e o destino final (receptor).

IP (*Internet Protocol*) realiza o endereçamento nas redes de forma que os dados cheguem a seu destino.

Em uma comunicação TCP/IP, por uma única conexão física, podemos ter diferentes serviços (aplicações) simultâneos compartilhando essa conexão. Isso é possível porque cada aplicação possui um canal lógico específico, que é uma numeração específica denominada de "porta" que a diferencia de outras aplicações (TCP & COLOMBO, 2015).

2.4 Protocolo

FERNANDES (2016:3) diz que Protocolo é uma convenção que controla e possibilita uma conexão, comunicação, transferência de dados entre dois sistemas computacionais. De maneira simples, um protocolo pode ser definido como "as regras que governam" a sintaxe, semântica e sincronização da comunicação.

Protocolo é um conjunto de regras que definem o modo como se dará a comunicação entre as partes envolvidas, que pode ser por *hardware* ou *software* (NIPASSA, 2011).

O autor concordando com Nipassa, salienta que um protocolo em uma rede de computadores é um conjunto de regras e convenções que definem a comunicação dos dispositivos em uma rede.

2.5 Protocolo da Internet Versão Quatro (IPv4)

Segundo NETO (2011), o IPv4 foi desenvolvido originalmente para o uso académico e com o aumento do uso da Internet, e principalmente com uso comercial foi necessário que se desenvolvessem mecanismos de segurança que garantissem a confidencialidade e autenticidade das comunicações, onde temos o exemplo da implementação do IPSec que propicia a criptografia

dos dados trafegados na rede, mas esbarra na limitação de seu uso com NAT. Encontramos algumas características de IPv4 que identificam o protocolo desde a sua implementação, as seguintes:

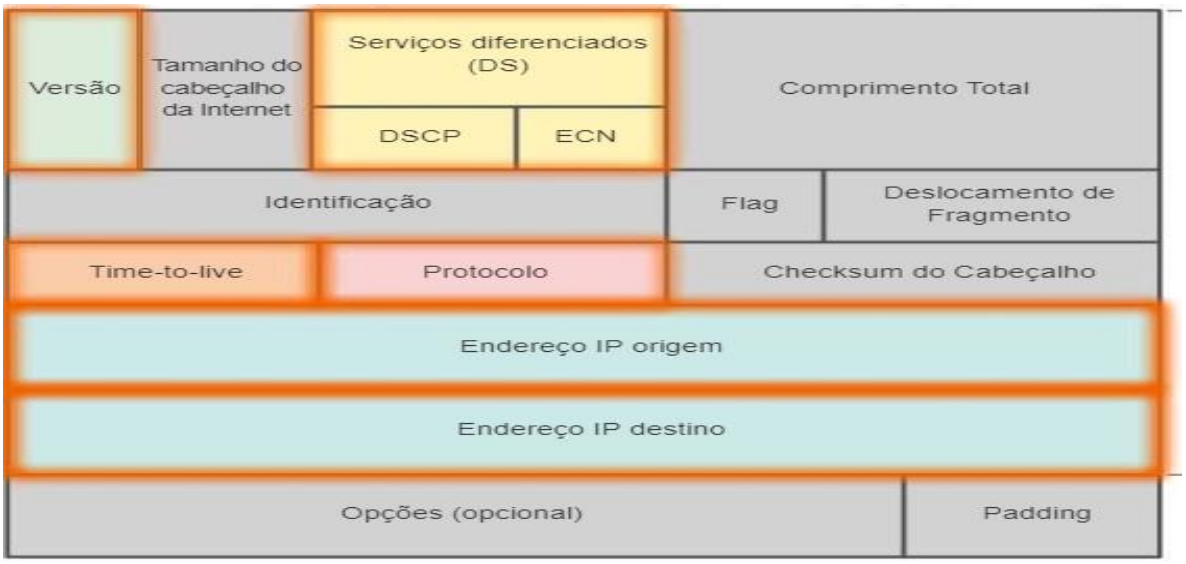
a) **Sem conexão –** A conexão não é estabelecida antes do envio dos pacotes de dados, onde os pacotes IP são enviados sem notificar a sua chegada para *host* final. A entrega de pacotes sem conexão pode resultar na chegada dos pacotes do destino fora de sequência.
b) **Serviço de melhor esforço -** O IP conseguiria funcionar com grande eficiência na camada da rede, se incluísse um cabeçalho de confiabilidade no protocolo da camada 3, as comunicações que não requerem conexão ou confiabilidade seriam sobrecarregadas com o consumo de largura de banda e o atraso produzido por este cabeçalho.
c) **Independente do meio físico –** O IPv4 opera independentemente do meio físico que transporta os dados nas camadas inferiores da pilha de protocolo. Qualquer pacote IP individual pode ser passado electricamente por cabo como os sinais ópticos nas fibras ou sem fio como sinais de rádio.

2.5.1 Formato do Cabeçalho do IPv4

Um pacote IPv4 é composto por um cabeçalho e um campo de dados que contém os dados provenientes da camada superior (transporte). A estrutura de um pacote IPv4, incluindo cabeçalho e campo de dados, é mostrada na tabela 1.

A tabela 1 ilustra o cabeçalho de Protocolo de Internet versão quatro e os campos que o compõem.

Tabela 1: Cabeçalho de IPv4



Fonte: http://jkolb.com.br/protocolo-ip-IPv4-e-IPv6 (Capturado aos 15-06-2018)

Como esta ilustrada na tabela 1, OMAR (2018) diz que o cabeçalho IPv4 é composto por 12 campos fixos, que podem ou não conter opções responsáveis por fazer com que o tamanho, varie de 20 a 60 Bytes. Estes campos são destinados a transmitir informações sobre:

- **Versão –** Possui um valor binário de 4 bits que identifica a versão do pacote IP, em pacotes IPv4;
- **Tamanho do cabeçalho da Internet (IHL) –** Possui um valor binário de 4 bits que indica o número de palavras de 32 bits no cabeçalho. O valor do IHL varia devido aos campos () Opções e de Padding. O valor mínimo desse campo é 5 (isto é, 5×32 = 160 bits = 20 bytes) e o valor máximo é 15 (isto é, 15×32 = 480 bits = 60 bytes);
- **Serviço diferenciado (DS) -** Anteriormente chamava-se de campo Tipo de Serviço (ToS), o campo DS é um campo de 8 bits usado para determinar a prioridade de cada pacote. Os primeiros 6 bits identificam o valor do ponto de códigos de serviços diferenciados que é usado por um mecanismo de qualidade de serviço (QoS).
    - **Comprimento Total -** Conhecido como o comprimento do pacote, esse campo de 16 bits define o tamanho total do pacote (fragmento), incluindo cabeçalho e dados, em bytes. O pacote de comprimento mínimo é 20 bytes (cabeçalho de 20 bytes + dados de 0 bytes) e o máximo é 65.535 bytes;

- **Identificação -** Neste campo encontram-se 16 bits, identifica exclusivamente o segmento de um pacote de IP original;
- **Flags -** Esse campo de 3 bits identifica como o pacote é fragmentado. É usado com os campos de deslocamento de fragmento e identificação para ajudar a reconstruir o fragmento dentro do pacote original;
- **Deslocamento de fragmento -** Esse campo é de 13 bits, identifica a ordem na qual o fragmento do pacote deve ser colocado na reconstrução do pacote original desfragmentado;
- **Time-to-live (TTL) -** Possui um valor binário de 8 bits que é usado para limitar a vida de um pacote. Ele é especificado em segundos mas é geralmente conhecido como a contagem de saltos. O remetente do pacote define o valor inicial do Time-to-live (TTL) e diminui em um de cada vez que o pacote for processado por um roteador, ou por salto.
- **Protocolo -** o valor binário de 8 bits indica o tipo de payload de dados que o pacote está carregando, que permite que a camada de rede passe os dados para o protocolo apropriado das camadas superiores.
- **Checksum do cabeçalho -** O campo de 16 bits é usado para verificar erros do cabeçalho IP. O checksum do cabeçalho é recalculado e comparado ao valor no campo checksum. Se os valores não coincidem, o pacote é descartado;
- **Endereço IP origem -** Contém um valor binário de 32 bits que representa o endereço IP origem do pacote;
- **Endereço IP origem -** Contém um valor binário de 32 bits que representa o endereço IP destino do pacote;
- **Padding** - É um campo que contém bit **0** que estendem o cabeçalho para torná-lo múltiplo de 32 bits. Assim, o campo Padding somente é usado quando o campo opções, que é variável, não é múltiplo de 32 bits.

2.5.2 Endereçamento do Protocolo de Internet versão quatro

Dentro de uma rede TCP/IP, cada computador recebe um endereço IP único que o identifica na rede.

Um endereço IP é um identificador de um dispositivo pertencente a uma rede de computadores. Também conhecido como endereço lógico, pode conter endereços reservados, que são utilizados dentro de uma rede local, também conhecidos como não-roteáveis e endereços IP's válidos, utilizados publicamente, inclusive no acesso à Internet (FERNANDES, 2010).

O endereço IPv4 é um número de 32 bits com 4 conjuntos de 8 bits (4x8=32). A estes conjuntos de 4 bits dá-se o nome de **octeto**. Exemplo de IPV4 é: ***192.168.0.2***

Para as redes do IPv4 foram definidas 5 classes a saber: A, B, C, D, E, **classes de endereços**, de modo a permitir uma maior gama de endereços. Vamos concentrar-nos nas primeiras três classes sendo as mais usadas.

As redes foram divididas em classes e cada uma delas tem a sua máscara padrão, como a Classe A com máscara /8, Classe B com máscara /16 e Classe C com máscara /24.

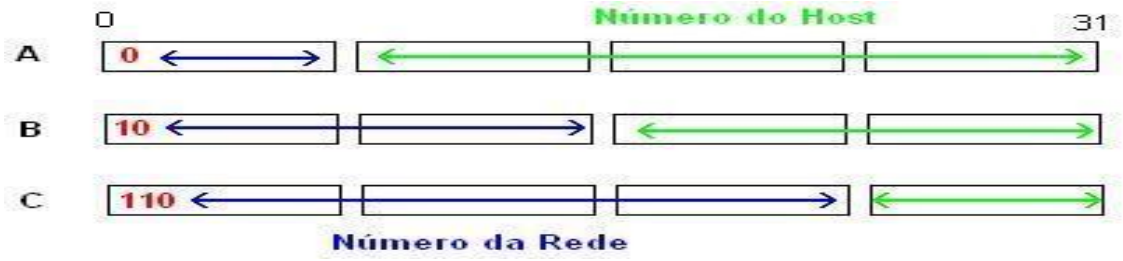
Classe A: com máscara /8 onde apenas o primeiro octeto identifica a rede e os últimos três octetos identificam os *hosts*; isto quer dizer que poderíamos ter no máximo 254 (o 0 e o 255 não contam) redes e 256x256x254. Assim encontramos mais de 16 milhões de endereços, e muitas das grandes empresas de tecnologias mundiais conhecidas até hoje, basearam-se nessa vantagem.

Classe B: os dois primeiros octetos identificam a rede e os outros dois identificam os *hosts*; neste caso, podemos ter mais redes, mas menos *hosts* em cada rede.

Classe C: os três primeiros octetos identificam as redes possíveis e apenas o último octeto identifica os *hosts*; aqui, podemos ter muito menos *hosts* em cada rede (254), mas muitas redes.

A tabela que se segue demonstra o formato de um endereço IPv4 de 32 bits divididos em quatro octetos exemplificando as três classes onde encontramos os endereços de rede e endereços de *hosts*.

Tabela 2: Formato de endereço IPv4



Fonte: https://pt.wikipedia.org/wiki/Endere%C3%A7o_IP#/media/File:Mascara.JPG (Capturado aos 13-06-2018)

2.5.3 Tipos de Endereços IPv4

Os tipos de endereço IPv4 que encontramos são os seguintes:

- Endereços da Rede: Os endereços da rede identificam a própria rede e não uma interface da rede específica. É representado por todos os bits de *host* com o valor zero e é o primeiro IP de uma rede ou Sub-rede.

- Endereços de Host: Os endereços de *host* identificam uma interface da rede específica ou um *host* dentro de uma rede. Os endereços de *host* vão do primeiro IP após o endereço da rede (endereços da rede+1) ao penúltimo IP (endereço de *broadcast* – 1), ou seja, é o número anterior ao endereço de *broadcast.*

- Endereços de Broadcast: Os endereços de *broadcast* são especiais e reservados para se enviar a todas as máquinas na rede específica, representado por todos os bits de *host* com o valor 1 (um).

- Endereços Experimentais: Os endereços no bloco 240.0.0.0 a 255.255.255.254 são listados como reservados para uso futuro (RFC 3330,2002). Actualmente, esses endereços podem ser usados apenas para fins de pesquisa ou de experimentação, mas não podem ser usados em uma rede IPv4.

- Endereços Unicast: As comunicações *unicast* são usadas para a comunicação máquina-a-máquina. Os endereços *unicast* identificam de forma unívoca a interface de uma máquina. Um pacote enviado para um endereço *unicast* é apenas recebido pela interface que tem associado tal endereço.

- Endereços Multicast: Um endereço *multicast* identifica um grupo de interfaces, podendo cada interface pertencer a outros grupos. Os pacotes enviados para esses endereços são entregues a todas as interfaces que fazem parte do "grupo".

2.5.4 Esgotamento e Medidas IPv4

Conforme as análises feitas nas politicas que existiam para a rede Internet e uma observação devido ao rápido crescimento que a rede apresentava, foi previsto que esse crescimento em pouco tempo, em épocas próximas os endereços IPv4 apresentariam dificuldades e não seriam suficientes para endereçamento mundial que crescia. Uma das causas dessa insuficiência era o desperdício de endereços no início das redes.

Existem três (3) medidas tomadas para se conter a disponibilização dos endereços IPv4 nas redes, a saber:

a) CIDR (*Classless Inter-Domain Routing*)

Durante o princípio de alocação de endereços às empresas, foi feita através de classes que tinham suas máscaras de tamanho padrão e achou-se um desperdício de endereços, em

publicação feita em 09/1993 a CIDR que permitia ter máscaras da rede variável em qualquer classe para o tamanho da rede que acha desejável (OMAR, 2017).

As Máscara padrão de IP das classes mais usadas em IPv4 são:

- **Máscaras da Classe A** 255.0.0.0 ou seja máscara /8 → Mais de 16.000.000 de endereços.
- **Máscaras de Classe B** 255.255.0.0 ou seja máscara /16 → Mais de 65.000 endereços.
- **Máscaras de Classe C** 255.255.255.0 ou seja máscara /24 → 254 endereços.

b) DHCP (*Dynamic Host Configuration Protocol*)

O DHCP é um protocolo do serviço TCP/IP que permite atribuir um IP e outras configurações a computadores em uma rede.

c) NAT (*Network Address Translation*)

NAT é uma função de roteador na qual endereços IP (e possivelmente números de porta) de datagramas IP são substituídos no limite de uma rede privada; NAT é um método que permite que *hosts* em redes privadas se comuniquem com *hosts* na Internet; o NAT é executado em roteadores que conectam redes privadas à Internet pública, para substituir o par de porta de endereço IP de um pacote IP por outro par de porta de endereço IP (GOMES et al., 2012).

Existem três tipos de NAT:

- **NAT Estático** – É o mapeamento um-para-um de um endereço IP privado para um endereço IP público. O NAT estático é útil quando um dispositivo da rede dentro de uma rede privada precisa ser acessível pela Internet.
- **NAT Dinâmico** – O NAT dinâmico pode ser definido como mapeamento de um endereço IP privado para um endereço IP público a partir de um grupo de endereços IP públicos chamados de NAT pool. Dynamic NAT estabelece um mapeamento um-para-um entre um endereço IP privado para um endereço IP público. O mapeamento público para privado pode variar com base no endereço IP público disponível na *pool* do NAT.
- **NAT sobrecarga (PAT)** – Este tipo de NAT mais conhecido por PAT (Port Address Translator) é outro tipo de NAT dinâmico, que pode mapear vários endereços IP privados para um único endereço IP público usando uma tecnologia conhecida como Port Address Translation.

Na figura 2 podemos verificar o princípio do funcionamento do NAT entre a Internet e os nossos computadores.

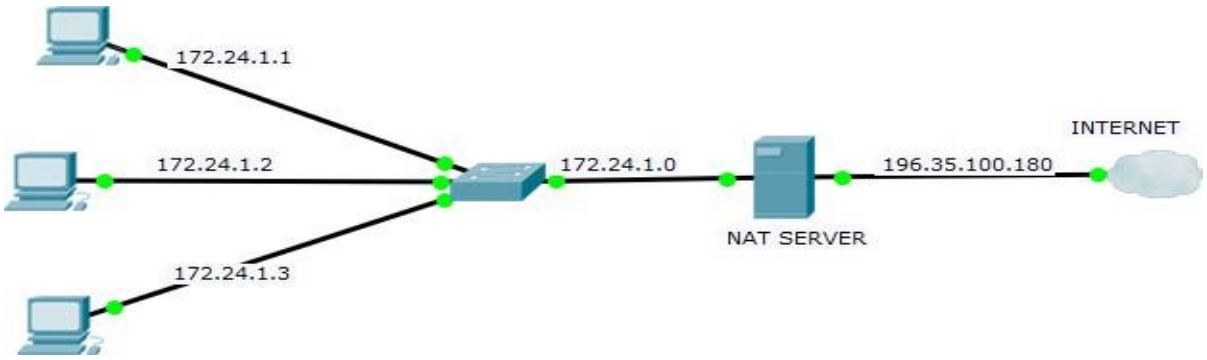


Figura 2: Demonstração do NAT

Fonte: Adaptada segundo o funcionamento do NAT (2018)

A Internet desde a sua criação não era para serviços comerciais como destacamos actualmente, se não apenas para comunicações militares, porém, com o tempo abrangia vários ramos tais como científicos, culturais, comerciais e mais usando o protocolo de internet IPv4, entretanto, com o desenvolvimento e a necessidade dos serviços de internet o IPv4 encontra-se esgotado devido ao número de endereços que se dispõem e a necessidade nos últimos dias é incontornável.

2.6 Protocolo de Internet Versão Seis (IPv6)

O IPv6 (*Internet Protocol Version 6*) é a solução dos vários problemas do IPv4 desde o número limitado de endereços disponíveis e segurança. Várias são as melhorias em relação ao IPv4 em áreas tais como a auto configuração de roteamento e da rede.

Segundo TANENBAUM (2003) citado por PAMPLONA&TOKUNAGA (2014), o IP versão 6 começou a ser desenvolvido no início da década de 1990, com o objectivo de ser a solução definitiva para o esgotamento de endereços IP na Internet e as principais modificações foram o aumento de endereços, a simplificação do cabeçalho, melhor suporte para as opções oferecidas e o avanço na questão de segurança.

O protocolo IPv6 tem endereços mais longos que o IPv4, eles têm 16 bytes, ou seja, têm 128 bits maiores em relação aos 32 de IPv4.

O protocolo é escrito só no formato hexadecimal com capacidades de endereçar mais de 3.400.000.000.000.000.000.000.000.000.000 (cerca de 340 undecilhoes) de endereços *hosts*.

O sistema de numeração hexadecimal é um sistema de base dezasseis, onde a base de número 16 do sistema de numeração utiliza os números de 0 à 9 e as letras de A à F.

Por ser um sistema que tem menor anotações para o endereço IPv6 foi escolhido o hexadecimal. Exemplo de caso seria necessário representar um endereço IPv6 em binário com 128 bits, o endereço ficaria:

11000000.10101000.00000000.00000000.00000000.00000000.00000000.00000000.
00000000.00000000.00000000.00000000.00000000.00000000.00000000.00000001

Ou seria em decimal: 192.168.0.0.0.0.0.0.0.0.0.0.1, onde em hexadecimal ficaria: C0A8.0000.0000.0000.0000.0000.0000.0001, na sua forma abreviada hexadecimal IPv6 fica: C0A8::1.

O IPv6 não tem máscara da rede, pois a máscara da sub-rede de um tamanho de 128 bits seria complicado, somente existem os prefixos da rede /64, /32, /127.

Para tornar o endereço IPV6 mais curto e agradável existem regras de abreviação na anotação de endereços, tais como:

1ª Regra – Omitir os zeros a esquerda do endereço

Em cada um dos quartetos podemos omitir os zeros a esquerda. Exemplo:

Endereço: 2001:0DB8:CAFE:0000:0000:0000:0000:0001/64 - Aplicando a 1ª regra o endereço fica: 2001:DB8:CAFÉ:0:0:1/64.

2ª Regra – Omitir as sequências de zeros

Podemos omitir uma sequência de quartetos de zeros representado por **(::)** dois pontos dúplos. Exemplo:

Endereço: 2001:0DB8:CAFÉ:0000:0000:0000:0000:0001/64 - Aplicando 2ª regra o endereço fica: 2001:0DB8;CAFE::0001/64.

Sendo assim, pode-se aplicar as duas regras, tornando o endereço IPv6 mais simples, assim teremos: 2001:DB8:CAFE::1/64.

Mais informações sobre algumas designações:

• RFC 1380 - *IESG Deliberations on Routing and Addressing*

• RFC 1918 - *Address Allocation for Private Internets*

• RFC 2131 - *Dynamic Host Configuration Protocol*

• RFC 2775 - *Internet Transparency*

• RFC 2993 - *Architectural Implications of NAT*

• RFC 3022 - *Traditional IP Network Address Translator (Traditional NAT)*

• RFC 3027 - *Protocol Complications with the IP Network Address Translator*

• RFC 4632 - *Classless Inter-domain Routing (CIDR): The Internet Address Assignment and Aggregation Plan.*

2.6.1 Cabeçalho de Extensão do Protocolo IPv6

VUMO (2018) diz que actualmente, encontramos 6 tipos de cabeçalhos de extensão que são:

a) **Hop-by-hop options**: Permite incluir campos adicionais com informações que serão analisadas pelos roteadores ao longo do caminho do pacote.

b) **Destination options**: Permite incluir campos adicionais que são interpretados pelo destino final, sendo ignorados pelos roteadores ao longo do caminho.

c) **Fragmentation**: Inclui os campos de fragmentação que foram removidos do IPv4.

d) **Authentication (AH + ESP)**: Inclui campos para autenticação dos pacotes IPv6. Corresponde ao protocolo AH do IPsec.

e) **Encrypted security payload**: Inclui campos para criptografia do pacote IPv6.

f) **Routing**: inclui campos que permitem definir de forma total ou parcial a sequência de roteadores que o pacote deverá percorrer para chegar ao seu destino.

2.6.2 Formato do Cabeçalho de IPv6

O IPv6 permite criar cabeçalhos de tamanho variável, de acordo com as necessidades específicas do pacote que está sendo enviado. Essa melhoria foi implementada pela introdução de cabeçalhos opcionais especializados e denominados cabeçalhos de expansão (extension headers). Além disso, alguns campos pouco usados do IPv4 foram eliminados, como ilustra a figura abaixo que representa o cabeçalho de IPv6.

Tabela 3: Cabeçalho de IPv6

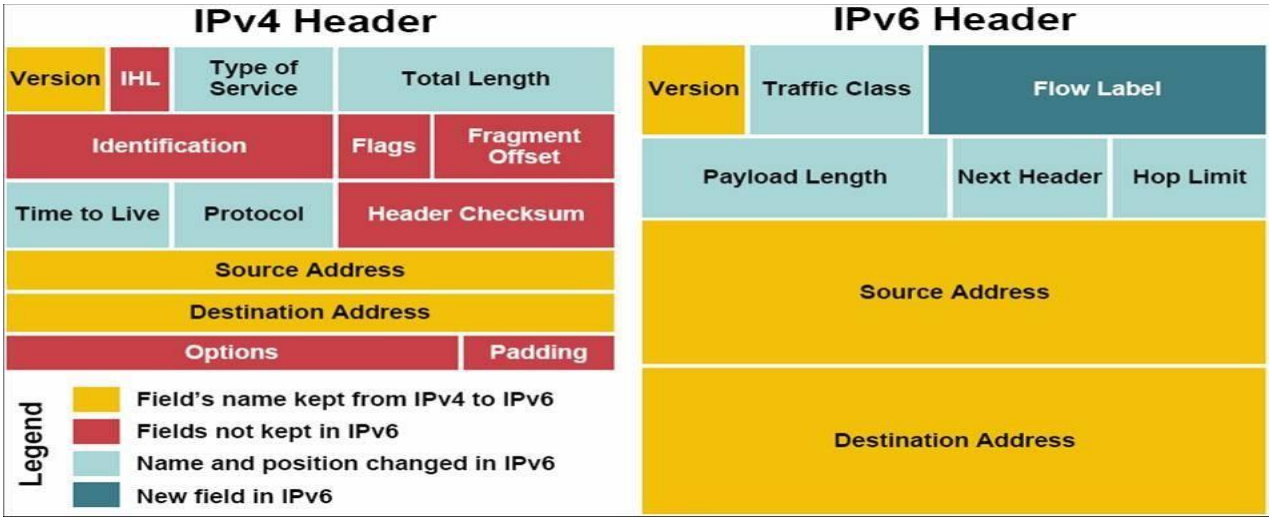
<table>
<tr><td>Version</td><td colspan="2">Traffic Class</td><td colspan="2">Flow Label</td></tr>
<tr><td colspan="3">Playload Length</td><td>Next Header</td><td>Hop Limit</td></tr>
<tr><td colspan="5">Source Address</td></tr>
<tr><td colspan="5">Destination Adrress</td></tr>
</table>

Fonte: Adaptada segundo o cabeçalho IPv4 depois da remoção de alguns campos (2018)

Algumas mudanças foram realizadas no formato do cabeçalho base do IPv6 de modo a torná-lo mais simples. A tabela a seguir ilustra identificação desses campos.

Visto que foram removidos espaços no cabeçalho IPv4 e outros acrescentados no cabeçalho IPv6, a tabela que se segue demonstra a comparação dos dois cabeçalhos.

Tabela 4: Cabeçalho IPv4 - Remoção de campos para o IPv6



Fonte: https://www.gta.ufrj.br/ensino/eel879/trabalhos_vf_2009_2/priscilla/ipv6_cabecalho.html (Capturado aos 20-08-2018)

VUMO (2018) afirma que o número de campos de IPv4 foi reduzido para apenas oito em IPv6 e o tamanho foi fixado em 40 Bytes. Além disso, ele ficou mais flexível e eficiente com a adição de cabeçalhos de extensão que não precisam ser processados por roteadores intermediários. Os campos do cabeçalho IPv6 são:

- **Version (4 bits)** - Indica a versão do protocolo.
- **Trafic Class (8 bits)** - Utilizado na priorização de tráfego no IPv6.
- **Flow Label (20 bits)** - Usado para a Qualidade de Serviço em fluxos de dados.
- **Payload Length (16 bits)** - Tamanho (em bytes) da área de dados do pacote. Guarda certa similaridade ao *Total Length Field* do IPv4, mas se diferencia desse por tratar apenas da área de dados.
- **Next Header (8 bits)** - Especifica o protocolo encapsulado na área de dados ou, opcionalmente, um cabeçalho de extensão do IPv6.

- **Hop Limit (8 bits)** - Número máximo de nós que um pacote pode passar até ser descartado.
- **Source Address (128 bits)** - Endereço de origem.
- **Destination Address (128 bits)** - Endereço de destino.

2.6.3 Endereçamento IPv6

O protocolo IPv6 apresenta como principal característica e justificativa maior para o seu desenvolvimento, o aumento no espaço para endereçamento. Por isso, é importante conhecer as diferenças entre os endereços IPv4 e IPv6, saber reconhecer a sintaxe dos endereços IPv6 e conhecer os tipos de endereços IPv6 existentes e suas principais características.

O IPv6 possui um espaço para endereçamento de 128 bits, sendo possível obter 340.282.366.920.938.463.463.374.607.431.768.211.456 endereços (2128). Este valor representa aproximadamente 79 octilhões (7,9×1028) de vezes que a quantidade de endereços IPv4 representa, também, mais de 56 octilhões (5,6×1028) de endereços por ser humano na terra, considerando-se a população estimada em 6 bilhões de habitantes.

O IPv6 é representado por 8 campos de endereços de 16 bits (em forma hexadecimal), separados por dois pontos:

- 2001:0DB8:0000:CAFE:0000:0000:087C:140b
- 2001:DB8:0:CAFE::087C:140b

• Prefixos

– Como o CIDR (IPv4)

– Exemplo: **2001:db8:12::/48**

URL: - http://[2001:DB8:CAFE::20]:8080

- http://[2001:DB8:CAFE::20]/index.html

2.6.4 Estrutura do Endereçamento do IPv6

Um dos principais motivos da criação de um novo protocolo IP deu-se devido ao esgotamento dos endereçamentos IPv4. Com isso, foi revista toda a estrutura dos endereços no IPv6 que agora possuem 128 bits de endereçamentos, contra os 32 bits do seu antecedor, o IPv4. Isso representa algo em torno de 3,4x1038 de endereços IP’s, enquanto o IPv4 disponibiliza algo em torno de 4,3 bilhões de endereços IP’s. Para se ter uma ideia, actualmente existem aproximadamente 7,4 bilhões de pessoas no mundo, isso daria algo em torno de 4,5x1028 de endereços IPv6 por pessoa no mundo (COELHO & GOMES, 2016).

A autoconfiguração faz uso das funcionalidades dos endereçamentos *unicast* link local FE:80::/64 para as comunicações iniciais entre os elementos do mesmo enlace.

2.6.5 Tipos de Endereços IPv6

Segundo a RFC 2374, uma mesma interface, que utiliza o protocolo IPv6, pode utilizar mais de um endereço, diferentemente do IPv4, onde tal característica só era possível em roteadores. Essa característica é importante porque na versão 6 algumas aplicações, servem em geral para o controlo.

Segundo VUMO (2018) no IPv6 existem 3 tipos de endereços:

- ✓ **Unicast;**
- ✓ **Anycast;**
- ✓ **Multicast**.

Outra característica marcante do IPv6 é que não existem mais os endereços *broadcast,* que endereçavam todos os *hosts* de um mesmo domínio de colisão, isto é, um pacote com endereço de destino do tipo *broadcast* era enviado para todos os *hosts* do seu domínio de colisão.

2.6.5.1 Unicast

Os endereços de *unicast* são responsáveis por endereçar um *host* de maneira única na rede. Identificam apenas uma interface, onde um pacote destinado a um endereço *unicast* é enviado directamente para interface associada a esse endereço. Por outro lado os endereços *unicast* são associados a uma única interface de um computador ou roteador. Foram definidos pela RFC 2374 vários tipos de endereços de *unicast* que são:

Agregatable Global Unicast Address, Loopback Address, Unspecified Address, NSAP Address, IPX Address, Site-local Unicast Address, Link-local Unicast Address e IPv4- compatible IPv6 Address. A descrição de cada endereço é a seguinte:

a) Agregatable Global Unicast Address

Este tipo de endereço *unicast* é equivalente ao endereço global *unicast* usado em IPv4. Sendo assim é o endereço que será usado globalmente na Internet. Essa estrutura de endereços globais permite uma agregação de prefixos de roteamento que limitam o número de entradas nas tabelas de rotas. A estrutura deste tipo de endereço é dividida em 4 níveis, o primeiro é o FP – *Format Prefix*, que indica justamente que se trata de um endereço do tipo *Global Unicast* (VUMO, 2018).

O segundo campo é chamado *Global Routing Prefix*, e é destinado a identificação dos ISP´s – *Internet Service Provider*. O terceiro campo *Subnet ID* também foi apresentado anteriormente como sendo o campo *Site ID* da estrutura de hierarquização do endereço IPv6, o último nível é o *Interface ID* (OMAR, 2017).

b) Loopback Address

Este tipo de endereço, como o próprio nome já diz, é o endereço da própria interface. Porém, ele só pode ser usado quando um nó envia um pacote para ele mesmo. No IPv4 este tipo de endereço era geralmente o 127.0.0.1, em IPv6 é indicado por: **0:0:0:0:0:0:0:1** ou simplesmente**: ::1** (CILENTO, 2017).

Este endereço não pode ser associado a nenhuma interface física, nem como endereço de fonte, nem como endereço de destino, mas pode ser imaginado como sendo de uma interface virtual, a interface *loopback*. Um pacote IPv6 com endereço destino do tipo *loopback address* também não deve deixar o próprio *host*, sendo que esse endereço nunca será repassado por um roteador IPv6 (VUMO, 2018).

c) Unspecified Address

Este tipo de endereço indica exactamente a falta de um endereço. Ele nunca deverá ser utilizado como um endereço válido para nenhum *host*. A sua utilidade é para que estações que ainda não foram inicializadas, sejam identificadas com endereços deste tipo, ou seja, *hosts* que ainda não tenham aprendido seus próprios endereços globais, utilizem tais endereços para se autoconfigurar. Além disso, esse tipo de endereço não deve ser utilizado como endereço de destino ou em cabeçalho de roteamento de pacotes IPv6. Seu formato é o seguinte: **0:0:0:0:0:0:0:0** ou simplesmente**: ::** (CILENTO, 2017).

d) Site Local Unicast Address

O endereço do tipo *Site Local* é similar aos endereços privados usados em IPv4, como as redes 10.0.0.0 /8, 172.16.0.0/16 e 198.168.0.0/16. Estes endereços podem ser usados para uma comunicação restrita dentro de um domínio específico.

Este tipo de endereço é identificado pelo prefixo **FEC0::/10** ou **1111111011** em binário**.** Ele pode ser definido para uso interno numa organização através da concatenação do campo de SLA (16 bits) com a identificação da interface (64 bits). Este tipo de endereçamento pode ser considerado como privado, visto que ele está restrito a um domínio sem ligação à Internet. Desta forma, ele não pode ser anunciado externamente por roteadores (MADEIROS, 2010).

e) Link Local Unicast Address

Este tipo de endereço é automaticamente configurado em qualquer *host* IPv6 através da conjugação do seu prefixo **FE80::/10** ou **1111111010** em binário. Estes endereços são utilizados nos processos de configuração dinâmica automática (autoconfiguração) e no processo de descoberta de elementos na hierarquia de roteamento (VUMO, 2018).

f) IPv4-compatible IPv6 Address

PAMPLONA (2014) Circunda que este tipo de endereço é usado em IPv6 como um mecanismo de transição entre IPv6 e IPv4. É utilizado como endereços de destino e origem em *tunnel* (encapsulamento de um protocolo sobre outro) IPv6 sobre IPv4. É representado por um endereço IPv6 cujos últimos 32 bits são um endereço IPv4. Desta forma, anexando-se um prefixo nulo (96 bits de zeros) a um endereço IPv4 (32 bits), obtém-se o seguinte formato: **0:0:0:0:0:0:192.168.30.1** ou no seu formato abreviado **::192.168.30.1**

2.6.5.2 Anycast

O *anycast* é um endereço compartilhado por mais de um elemento da rede. Os endereços *anycast* tiram proveito do facto das rotas IP sempre utilizarem o caminho mais curto. Desta forma, um pacote para um endereço *anycast* será sempre enviado para o elemento da rede que esteja mais próximo da origem (JAMHOUR, 2008).

2.6.5.3 Multicast

Os endereços de *multicast* podem estar associados a interfaces de múltiplos computadores ou roteadores. Exemplos de endereços *multicast* são aqueles que representam roteadores ou servidores DHCP, isto é, um roteador além do endereço *multicast*, também responde a um endereço *multicast* que é comum a todos os roteadores. O mesmo raciocínio se aplica a servidores DHCP e muitos outros serviços que precisam ser localizados automaticamente (HEIDRICH, 2011).

VUMO (2018) diz que nos endereços *multicast* encontramos faixa de endereçamento com maior espaço de endereçamento, onde visa a criação facilitada de classes de endereçamento. Tais classes, mais apropriadamente denominadas de faixas de endereçamento, são registadas junto à IETF, apresentados na lista a seguir as principais faixas e os respectivos prefixos IPv6:

1- **0000::/8** Reservado
2- **0000::/96** Endereços IPv6 compatíveis com IPv4

3- **::FFFF:0:0/96** Endereços IPv4 mapeados em IPv6
4- **0200::/8** NSAP (não usado)
5- **0400::/8** IPX (não usado)
6- **2000::/3** Endereços roteáveis na Internet (prefixos **2xxx** e **3xxx**)
7- **FE80::/10** Endereços da rede local (automáticos, estáticos ou *stateless*)
8- **FEC0::/19** Endereços do site local
9- **FF00::/8** *Multicast*

Dentro dos endereços *Multicast* já reservados, podemos identificar alguns endereços especiais utilizados para funções específicas (todos de *lifetime* permanente):

- FF01::1 – Indica todas as interfaces de escopo local, isto é, somente as interfaces de um mesmo *host*.
- FF02::1 – Indica todas as interfaces de um escopo de enlace local, isto é, todos os *hosts* de um mesmo domínio de colisão.
- FF01::2 – Indica todos os roteadores dentro de um escopo local, isto é, todas as interfaces de um mesmo roteador.
- FF02::2 – Indica todos os roteadores dentro de um escopo de enlace local, isto é, todos os roteadores interligados por um mesmo enlace.
- FF05::2 – Indica todos os roteadores dentro de um escopo *site* local, isto é, todos os roteadores que possuem um mesmo *site ID*.
- FF02::1:FFxx:xxxx – Endereço especial chamado de *Solicited-Node Multicast Address*, onde xx:xxxx representam os últimos 24 *bits* do endereço IPv6 *Unicast* do *host*.

2.6.6 Segurança do Protocolo IPv6

O protocolo IPv6 não é necessariamente mais seguro que o IPv4, por ser relativamente um protocolo novo; existe menos vulnerabilidades conhecidas comparado ao IPv4 que é muito mais antigo e utilizado. Porém, algo que ajuda na segurança dos dados está na obrigatoriedade de todos os equipamentos que suportam o IPv6 também terem suporte nativo ao protocolo IPsec (IP Security Protocol), mas não necessariamente ao utilizar o protocolo IPv6, o IPsec estará habilitado e funcionando automaticamente. O IPsec precisa ser configurado manualmente para funcionar.

2.6.7 Mobilidade IPv6

A RFC 6275 descreve o Mobile IPv6 como um protocolo que possibilita a um *host* móvel movimentar-se entre duas redes distintas sem perder a conectividade. Seum *host* móvel conecta a uma outra rede, ele irá precisar de um novo endereço IP. O endereço IP móvel aborda o desafio de movimentar um *host* de uma rede para outra sem perder a conexão adicionando a interface deste *host* um novo endereço IP.

2.7 Tipos de Simuladores

Simuladores são *softwares* que nos permitem virtualizar vários serviços. Desta forma encontramos os seguintes simuladores:

a) O Cisco Packet Tracer

O *Packet Tracer* é um simulador desenvolvido pela *Cisco Systems* para ser utilizado como ferramenta no *Networking Academy* (NetAcad), um programa mundial de treinamento de novos profissionais na área de redes e comunicação de dados. O *NetAcad* está difundido por vários países (SOUSA & CABRAL, 2017).

b) Graphical Network Simulator-3

O GNS3 é um simulador de redes (ou ambiente de simulação de redes) bastante "real", que emula os mais diversos equipamentos activos de uma rede: *routers, switchs, PCs*, etc. Considerando por exemplo um router, o *GNS*3 permite-nos emular o IOS (sistema operativo dos equipamentos Cisco) de um router real e proceder às respectivas configurações. Estas configurações podem posteriormente ser importadas para um *router* de uma rede real (SOUSA et al., 2017).

O GNS3 é um aplicativo gratuito sob licença da GNU que provê a interface gráfica que permite ao usuário construir a topologia da rede que pretende configurar. Ele reúne diversos emuladores de sistemas operacionais.

O autor destaca o simulador *Cisco Packet-Trace* para permitir a virtualização por permitir simular o comportamento de roteadores, computadores, servidores dentre outros dispositivos da CISCO, mesmo dispositivos usados na rede. A simulação é fidedigna de um roteador físico do mesmo modelo.

A configuração de IPv6 pode ser feita na rede LAN da rede, uma vez que é da rede *LAN* que se tem o total privilégio de administração e não existe restrição de endereços IPv6, pode também ser feito na rede *WAN*, nas interfaces *loopbacks* da rede que vão aos ISPs.

CAPÍTULO IV: APRESENTAÇÃO, ANÁLISE E DISCUSSÃO DOS RESULTADOS DA PESQUISA

Neste capítulo apresentamos, analisamos e discutimos os resultados da pesquisa segundo a ordem dos objectivos específicos.

4.1 Levantamento da situação actual da rede EXB na versão do IPv4

Com relação a rede é essencial a sua apresentação de forma detalhada.

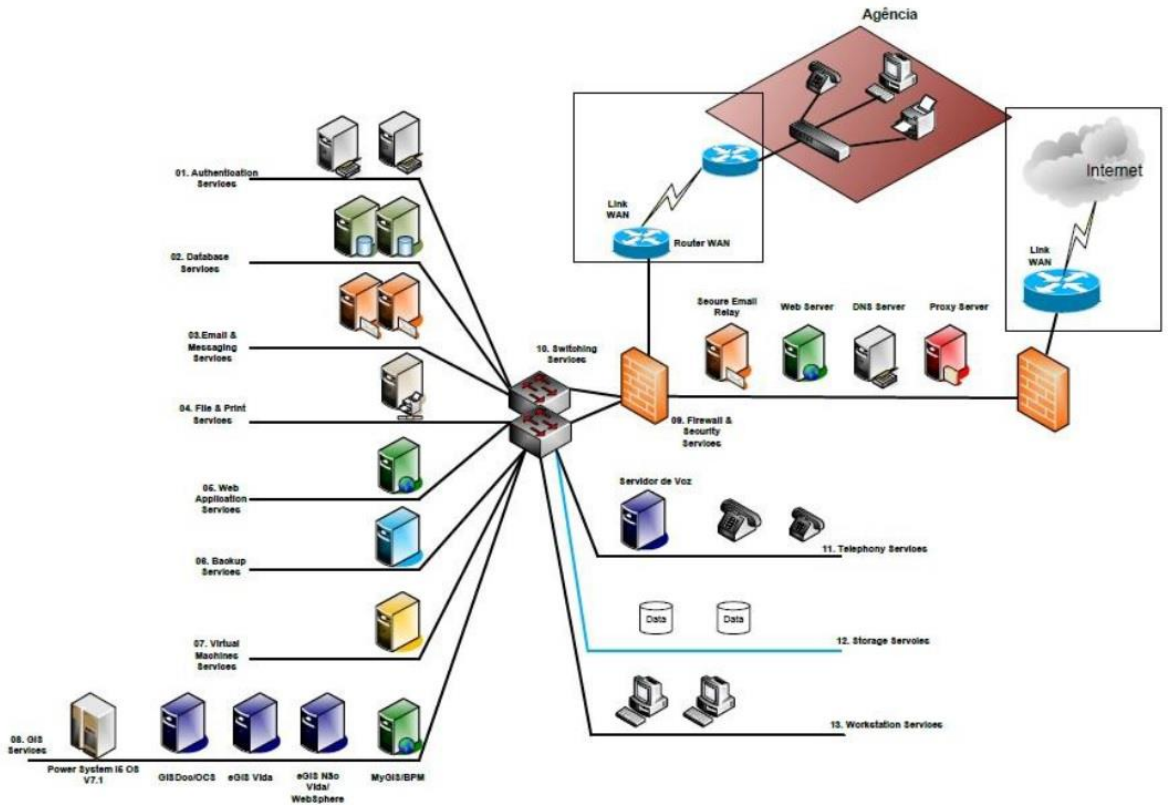


Figura 3: Esquema da actual da REDe EXB

4.1.1 Apresentação da EXB Serviços

A rede é a denominação que foi atribuída à rede , cujo objectivo é permitir que todos os utilizadores estejam ligados numa única rede de computadores. A rede está segmentada em todos blocos do edificio e que este projecto da segmentação da rede nos blocos está sendo realizado pela direção telecomunicações, uma unidade orgânica que responde pela informática a nível da Companhia (xxxx, 2018).

4.1.2 Levantamento da situação actual da Rede sob ponto de vista de Hardware

No que diz respeito a *hardware* como referenciamos nos recursos materiais, usa todos

equipamentos adequados para uma infra-estrutura de rede.

Para xxx (2018), actualmente é suportada por três (ou dois) provedores de Internet que são MOVITEL, dispondo cada um de seu modem, e está conectado a um *router* específico, oferecendo por sua vez endereços IPv4, como ilustra a figura , sendo assim, a rede ilustrada na figura 5 apresenta as unidades, totalmente separadas. O sinal chega no *router*, este que é segmentado para *switchs Cisco*, onde são criadas as *Vlans*, e feito o respectivo encaminhamento.

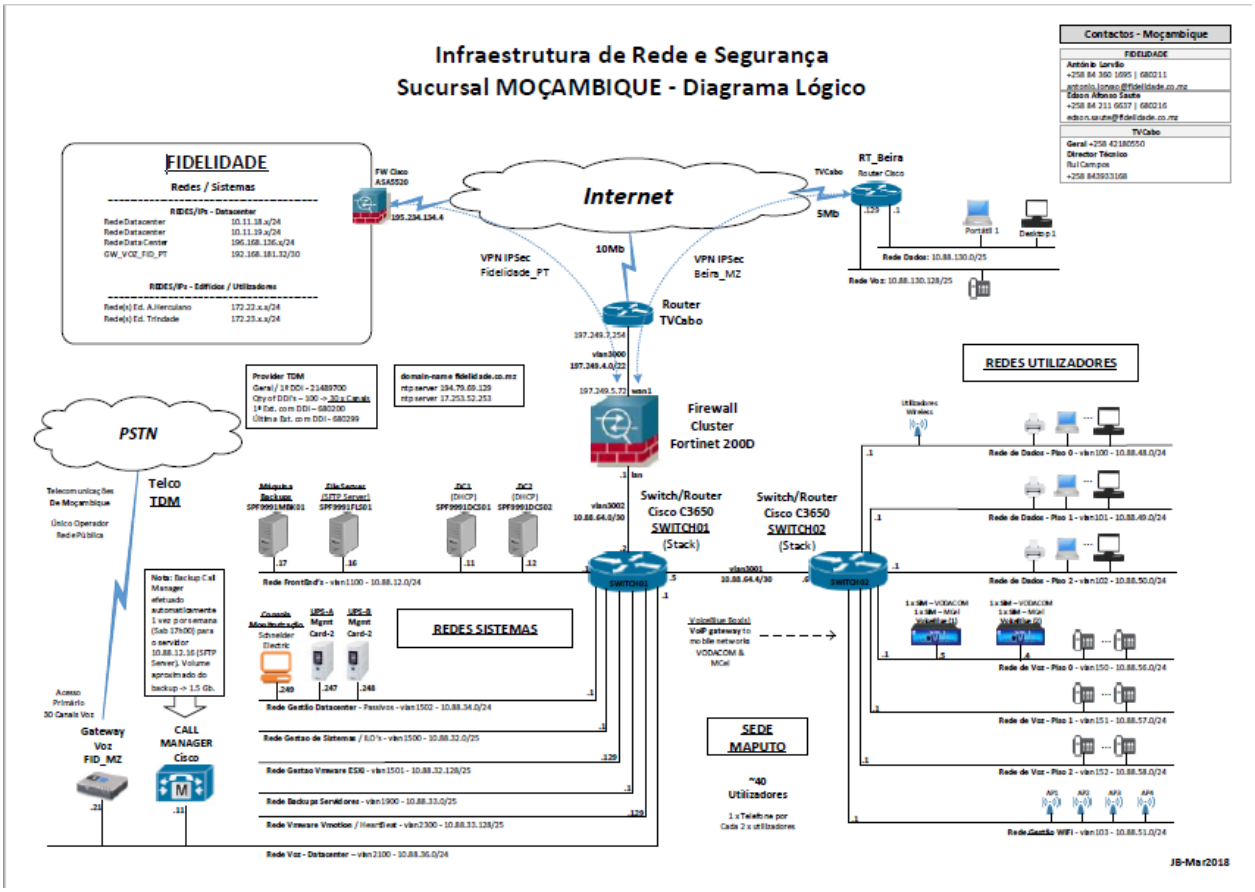


Figura 4: Infraestrutura da Rede

4.1.3 Software que suporta a Rede

Como apresentamos anteriormente o sinal é roteado e encaminhado, importa referir que os equipamentos usados para dar suporte a rede e os serviços nele patente, os *routers*, *switchs* não precisam de um *software* para o seu funcionamento. Dos vários serviços que são suportados pela rede, vários são os sistemas operativos usados, isto é, dependendo da complexidade do serviço e da necessidade de segurança do mesmo, os técnicos adequam aos *softwares* que permitem a segurança e integridade dos serviços.

4.1.4 Segurança da rede

xxxxxxx (2018) aponta que a segurança da rede é importante para garantir a protecção do património de uma empresa, credibilidade, vantagem competitiva, cumprimento das responsabilidades, continuidade da operação e actividade, pois se uma informação confidencial for obtida por uma pessoa que esteja ligada a concorrência de um negócio da empresa, esta pode deixar de exercer suas actividades pela insegurança de informação.

A segurança tem sido o problema que prevalece em quase todas as redes da internet que dia pôs dia nascem, isto é, sempre existem tentativas de invasão. Este dilema traz sempre um desafio aos técnicos e ao departamento.

A segurança na rede é garantida a partir de ferramentas específicas, e que a maior parte dos equipamentos usados por sua vez permite uma segurança interna, também são usadas senhas para permitir a privacidade ao acesso.

4.1.5 Gestão e roteamento de pacotes da rede

Durante o inquérito feito aos técnicos do centro de informática sob ponto de vista de dificuldades de gestão de *IP,* eles apontam não enfrentar nenhuma dificuldade na gestão de endereços IPv4 visto que a criação das sub-redes para a rede local ajuda a descongestionar a rede e a resolver o problema de endereços *IP*, e que com as politicas usadas na rede que no melhoramento de largura de banda ajuda nas horas do pico é gerido também através dos roteadores e *switchs* na base de *Vlans* para a distribuição da rede nos blocos como ilustra a figura 6, é usado o mecanismo de roteamento para gerir o tráfego e encaminhamento de pacotes dentro da rede.

Quando um *host* envia um pacote para outro *host*, ele usa a tabela de roteamento para determinar para onde enviar o pacote. Se o *host* destino estiver em uma rede remota, o pacote será encaminhado para o endereço de um dispositivo de *gateway*. O roteador procura sua tabela de roteamento para determinar para onde encaminhar pacotes. Sendo assim, o roteador precisa saber para onde encaminhar o pacote destino na rede usando assim a tabela de roteamento.

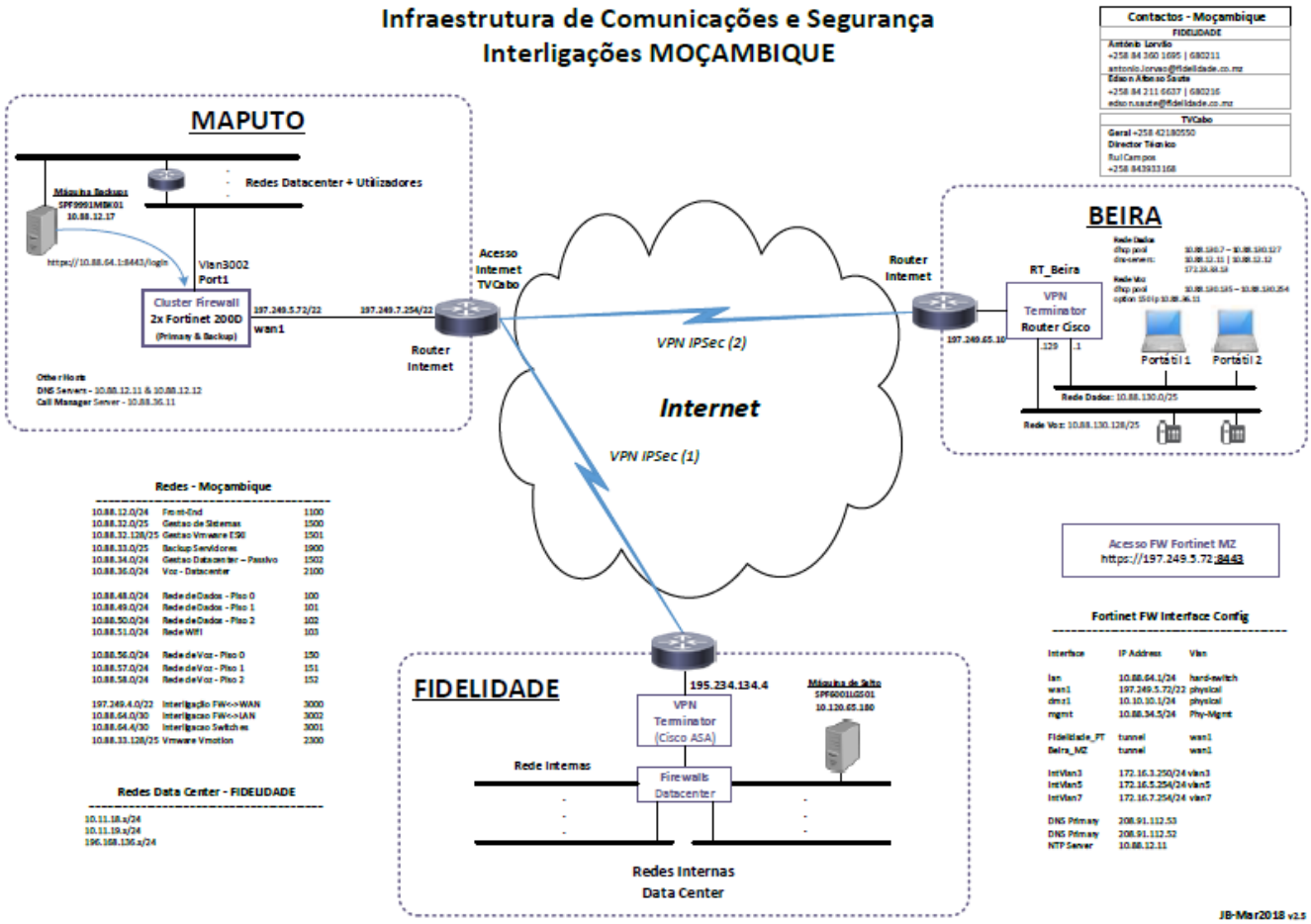


Figura 5: Infraestrutura de Rede de Segurança

O roteamento de pacotes actua-se ao nível 3 do modelo OSI e usa endereços lógicos para identificar as redes e os dispositivos das redes, todos os dispositivos da rede que queiram comunicar entre si têm de ser identificados com único endereço lógico.

4.1.6 Acessso a Rede

A rede encontra-se disponível para os colaboradores, clientes, Chefes dos departamentos, Corpo Técnico Administrativo (CTA) da companhia, assim como fora, por outra a rede é acessível para toda comunidade académica sendo ou não da Fildelidade. Importa referir que dos serviços suportados pela rede não são todos serviços que são de acesso livre, tanto dentro e acesso fora da rede, alguns serviços são exclusivamente para os internos. Exemplo serviços de *Wireless* para estudantes são permitidos somente os cadastrados para ter acesso a rede *Wi-Fi* mas temos serviços como página web é de acesso a todos.

Lista de Serviços

Email
eGIS VIDA
eGIS Não Vida
Lync
Intranet
Acesso à Mail Box a partir da maquina física
Acesso aos discos de rede
VOZ
Internet
Impressora – Multifunções ligada à rede FM e operacional
Postos de trabalho integrados no domínio FM

4.1.1 Cenário actual da rede da Fidelidade

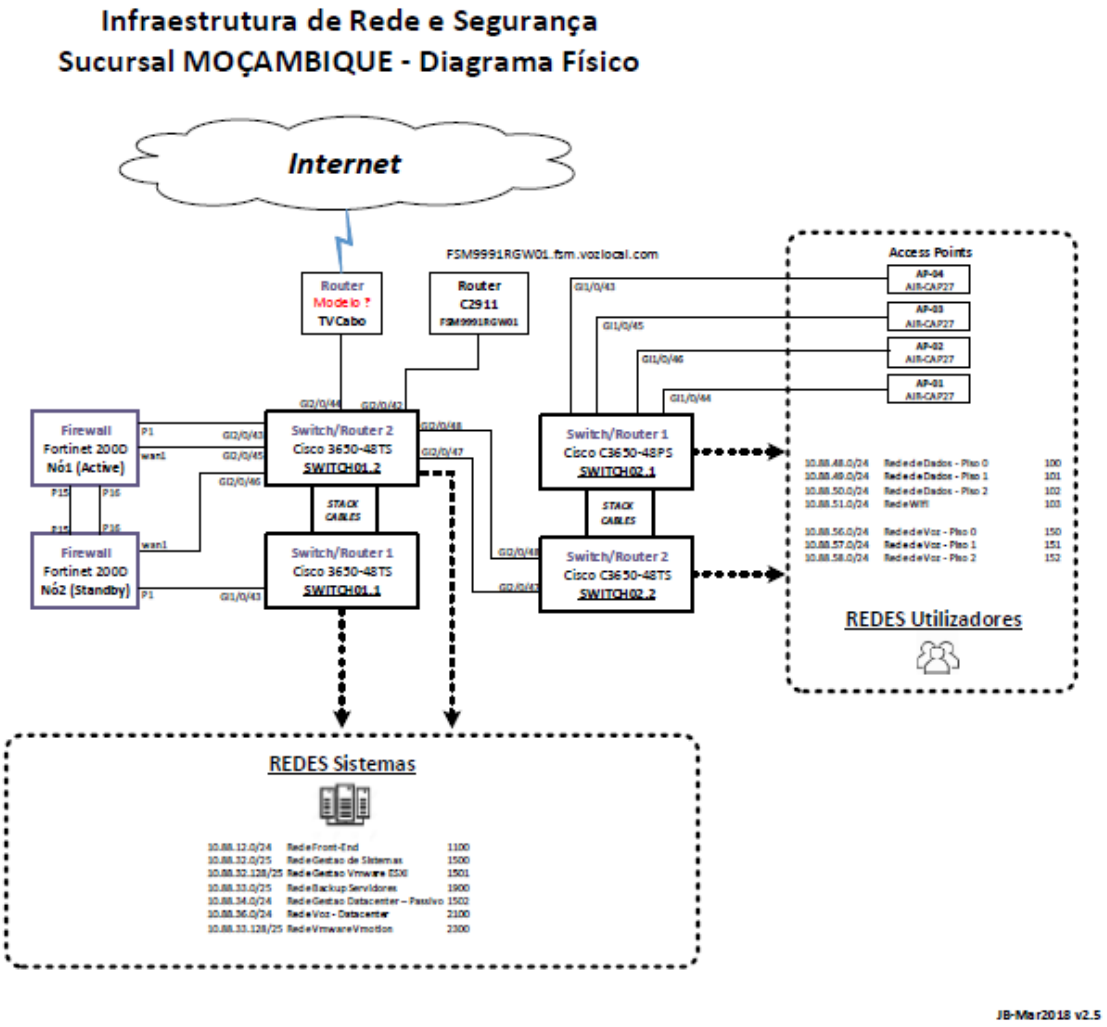


Figura 6: Cenário actual da redecom IPv4

Fonte: Autor

4.2 Identificação das características técnicas de protocolo de Internet IPv6

MORAIS (2018) apresenta as seguintes características técnicas do IPv6:

- Expansão das capacidades de endereçamento e *routing*;
- Simplificação do cabeçalho;
- Suporte para cabeçalho de extensão e de opções;
- Suporte para autenticação e privacidade;

- Suporte de auto-configuração;
- Suporte para selecção de rota pelo originador;
- Transição simples e flexível;
- Suporte para tráfego com garantia de qualidade de serviço;
- Mapeamento de endereços e Nomes;
- Encaminhamento;
- Fragmentação/Remontagem;
  Configuração automática de redes

4.3 Redesenho da rede com IPv6

A figura a baixo ilustra o cenário proposto para rede na versão IPv6 com vista a garantir a qualidade de serviços, segurança, mobilidade e acima de tudo melhor gestão na rede.

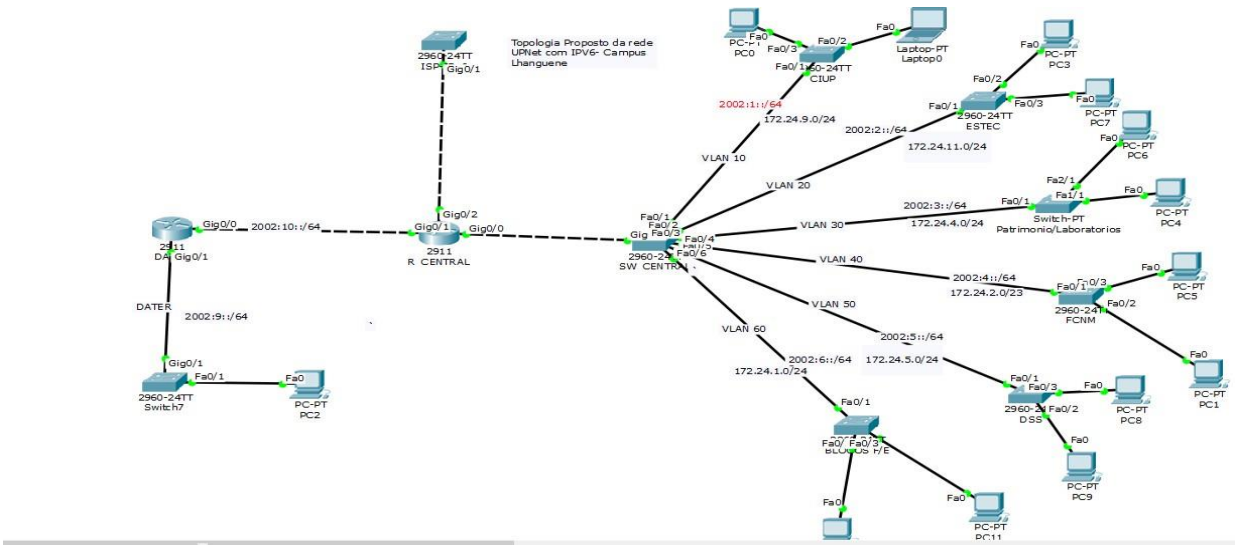


Figura 7: Cenário proposto para a rede com IPv6

Fonte: Autor

Na proposta, a rede está segmentada a partir de um *router* principal e um router que dará suporte apenas aos servidores.

Do *router* principal para o *switch* criamos *VLANs* que dão suporte aos blocos incorporando o IPv6, usando a técnica de pilha dúpla nos blocos.

4.4 Resultado da simulação virtual da rede com IPv6

Como forma de demostrar o cenário da migração de IPv4 para IPv6 primeiro foi virtualizado uma rede no *Cisco Packet Trecer*, com *routers Cisco 2911* e *switchs Cisco 2960* e testado fisicamente num dos blocos especificamente no xxxxxx como está ilustrada na figura 8.

CAPÍTULO V: CONCLUSÃO, RECOMENDAÇÕES E LIMITAÇÕES

Conclusão Segundo o problema de partida, os objectivos da pesquisa, as questões de pesquisa, as hipóteses e resultados da pesquisa, tiramos as seguintes conclusões: - A rede da EXB é uma infra-estrutura de rede que é suportada por provedoras de internet usando o protocolo IPv4, onde estes endereços são tidos como sendo de fácil uso, fácil cálculos de endereçamento por se apresentar apenas quatro octetos o que dita simplesmente 32 bits. Sendo assim, o IPv4 não possui um número maior de endereços, sendo que encontramo-nos numa altura em que a rede vai ganhando cada vez mais utilizadores e necessitando por este meio mais endereços IP. O IPv4 está em esgotamento e como mecanismo de garantir a resposta do esgotamento, partimos para a migração do mesmo, onde para a sua migração foi possível verificar que a maior parte dos equipamentos usados pela REDE, suportam a nova versão do protocolo IPv6 tanto em hardware, software. - Das características técnicas do IPv6 encontradas durante a realização do trabalho, existem as mais destacadas que são na maior parte capacidade de endereçamento e suporte de maior tráfego, por sua vez IPv6 possui um número de endereços quatro vezes maior (128 bits) que o IPv4, ilustrando desta forma o protocolo ideal para responder a futura procura dos serviços da EXB. - Uma das políticas do redesenho com IPv6 é que sustenta técnicas e padronização dos protocolos, onde uma das soluções do redesenho é a demonstração da separação das redes e integração dos dispositivos que simplesmente suportam o IPv6. Para simular a rede virtualmente, o Cisco Packet- Trace foi tido como o simples na aplicação e que respondeu a natureza da pesquisa. - As principais técnicas demonstradas e usadas neste trabalho para migração de IPv4 para IPv6 são a pilha dúpla, tunelamento e tradução. Contudo, foi possível comprovar todas as hipóteses deste trabalho, demonstrando que é possível com que a funcione com IPv6.

Recomendações

Findo o trabalho, foi possível perceber de alguns factores adversos para com a migração do IPv4 para IPv6, assim sendo, deixamos as seguintes recomendações: 56 – A EXB devia fazer o uso da técnica de pilha dúpla, tunelamento visto que, estas técnicas permitem a inclusão de todos equipamentos na rede tanto IPv4 assim como equipamentos que suportam apenas IPv6. - O Departamento de Informática devia fazer o uso deste material para a pesquisa e a criação do currículo que contemple cadeiras onde os estudantes irão aprender o IPv6 não de forma superficial como tem sido agora mas de forma profunda, pois presume-se que para os administradores da rede, haja futura procura de qualificados no endereçamento em IPv6. – A wmpresa devia fazer o uso de equipamentos CISCO, no processo de migração porque apesar de serem relativamente caros, são profissionais e são adequados para a implementação de IPv6 numa primeira fase.

REFERÊNCIAS BIBLIOGRÁFICAS

1. GERHARDT, Tatiana Engel e SILVEIRA, Denise Tolfo, Métodos de Pesquisa, 1.ed, UFRGS, Universidade Federal do Rio Grande do Sul, 2009.
2. GIL, António Carlos, Métodos e técnicas de pesquisa social. 5ª ed, Editora Atlas; São Paulo, 1999.
3. GIL, António Carlos. Como Elaborar Projectos de Pesquisa. 3ed, ATLAS S.A. São Paulo, 1996.
4. GIL, António Carlos. Como Elaborar Projectos de Pesquisa. 4ed, ATLAS S.A. São Paulo, 2002.
5. GIL, António Carlos. Métodos e técnicas de pesquisa social. 6ª ed, Editora Atlas; São Paulo, 2008.
6. GOMES, Alexandre José Camilo, TRINDADE, Carlod Botelho, Melhores Práticas de Migração de Rede IPV4 para IPV6, Inteligências em Telecomunicações, 2012.
7. JAMHOUR, Edgard, IPV6: Internet Protocol – Versão 6 e Mecanismos de Transição, 2008 MADEIROS, Aparecida, Lopes, SILVA, Maurício Rabelho. Evolução do Protocolo da Internet (IP): do IPV4 ao IPV6, Universidade do Estado do Rio Grande do Norte (UERN) e Universidade do Estado do Rio Grande do Norte (UERN) e Universidade Potiguar (UNP), Brasil, 2010.
8. MARCONI, Marina de Andrade e LAKATOS Eva Maria. Fundamentos de metodologia científica. São Paulo. 5ª Edição. Atlas Editora. 2003.
9. MARCONI, Marina de Andrade e LAKATOS Eva Maria. Fundamentos de metodologia científica: Técnicas de pesquisa. 7 ed. – São Paulo: Atlas, 2010.
10. NETO, Mário Cláudio Fellet. Planejamento Da Implantação De IPV6 Na Rede Corporativa Da Câmara Dos Deputados, Centro Universitário do Distrito Federal – UDF, Pós-Graduação Pesquisa e Extensão, Governança de TI no Sector Público. Brasília 2011.
11. PAMPLONA, Edno Gustavo, TOKUNAGA, Ricardo Kiyoshi. Transição IPV4/IPV6: Técnica De Tunelamento.

12. Universidade Tecnológica Federal Do Paraná, Departamento Académico De Electrónica, Curso Superior De Tecnologia Em Sistemas De Telecomunicações, Curitiba 2014.

Outros Documentos Consultados:

1. MACAMO, Xadreque. Identificar e implementar um mecanismo de autenticação centralizada na rede UPNet. Tese de licenciatura em Informática. Escola Superior Técnica. Maputo, Universidade Pedagógica, Universidade Pedagógica, 2018.
2. NIPASSA, Albertino J. André. Alternativas de segurança de redes Linux, proposta para implementação de um firewall e um servidor proxy. Tese de licenciatura em Informática. Escola Superior Técnica. Maputo, Universidade Pedagógica, 2011.
3. OMAR, Jaime Uirindi. Análise, migração e comunicação dos protocolos de Redes IPv4-IPv6. Tese de licenciatura em Informática. Escola Superior Técnica. Maputo, Universidade Pedagógica Universidade Pedagógica, 2017.
4. SINGO, Félix, JOVO, I. Cláudia, SAMBO, L. José, PORTUGAL, Yolanda, NHANISSE, Cacilda. Relatório Anual – 2013, Centro de Informática da Universidade Pedagógica – CIUP, Maputo, Agosto de 2014.