UNIVERSIDADE TECNOLÓGICA FEDERAL DO PARANÁ
DIRETORIA DE PESQUISA E PÓS-GRADUAÇÃO
DEPARTAMENTO ACADÊMICO DE ELETRÔNICA
CURSO DE ESPECIALIZAÇÃO SEMIPRESENCIAL EM GERENCIAMENTO DE SERVIDORES E EQUIPAMENTOS DE REDES

FERNANDA ROSÁ

PROJETO DE IMPLEMENTAÇÃO DE UMA TOPOLOGIA DE REDE UTILIZANDO IPv6 EM PILHA DUPLA EM VLANS NO INSTITUTO FEDERAL DE SANTA CATARINA – CAMPUS JARAGUÁ DO SUL

MONOGRAFIA DE ESPECIALIZAÇÃO

CURITIBA
2016

FERNANDA ROSÁ

PROJETO DE IMPLEMENTAÇÃO DE UMA TOPOLOGIA DE REDE UTILIZANDO IPv6 EM PILHA DUPLA EM VLANS NO INSTITUTO FEDERAL DE SANTA CATARINA – CAMPUS JARAGUÁ DO SUL

Monografia de Especialização, apresentada ao Curso de Especialização Especialista em Gerenciamento de Servidores e Equipamentos de Redes, do Departamento Acadêmico de Eletrônica da Universidade Tecnológica Federal do Paraná – UTFPR, como requisito parcial para obtenção do título de Especialista.
Orientador: Fabiano Scriptore de Carvalho

CURITIBA
2016

RESUMO

ROSÁ, Fernanda. **Projeto de Implementação de uma Topologia de Rede Utilizando IPv6 em Pilha Dupla em VLANs no Instituto Federal De Santa Catarina – Campus Jaraguá do Sul.** 2016. 66 f. Monografia (Curso de Especialização em Gerenciamento de Servidores e Equipamentos de Redes), Departamento Acadêmico de Eletrônica, Universidade Tecnológica Federal do Paraná. Curitiba, 2016.

Esta monografia aborda o estudo de maneira teórica do protocolo IPv4, o funcionamento do sistema de endereçamento e as estratégias que possibilitaram o prolongamento de sua vida útil, do protocolo IPv6, endereçamento e suas diferenças em relação ao IPv4 e as estratégias de migração, e do funcionamento das VLANs. Em seguida será feita a configuração da rede proposta, com adaptações, para que seja possível de ser feita no simulador Cisco *Packet Tracer*, mostrando os comandos necessários para a configuração dos *switches* e roteador para a rede do Instituto Federal de Santa Catarina – Campus Jaraguá do Sul, seguidos de testes para demostrar a conectividade em IPv4 e IPv6 entre computadores de mesma VLAN, entre VLANs diferentes e para um roteador representando as redes externas, de modo que possa facilmente ser adaptado para utilização em outros campus e instituições.

Palavras chave: IPv4. IPv6. VLAN. Configuração.

ABSTRACT

ROSÁ, Fernanda. **Implementation Project Using an IPv6 Dual-Stack in VLANs Network Topology at Instituto Federal De Santa Catarina – Campus Jaraguá do Sul.** 2016. 66 f. Monografia (Curso de Especialização em Gerenciamento de Servidores e Equipamentos de Redes), Departamento Acadêmico de Eletrônica, Universidade Tecnológica Federal do Paraná. Curitiba, 2016.

This monograph deals with the theoretical study of the IPv4 protocol, the operation of the addressing system and the strategies that allowed the extension of its useful life, the IPv6 protocol, addressing and their differences in relation to IPv4 and migration strategies, and the VLANs operation. And then, the proposed network configuration will be made, with adaptations, to be possible that it can be done in the Cisco Packet Tracer simulator, showing the necessary commands for the configuration of the switches and router for the network of the Instituto Federal de Santa Catarina – Campus Jaraguá do Sul, followed by tests to demonstrate IPv4 and IPv6 connectivity between computers on the same VLAN, between different VLANs and to a router representing the external networks, so that it can be easily adapted for use in others campuses and institutions.

Keywords: IPv4. IPv6. VLAN. Configuration.

LISTA DE FIGURAS

LISTA DE TABELAS

LISTA DE SIGLAS

ARP	Address Resolution Protocol
ARPA	Advanced Research Projects Agency
CIDR	Classless Inter-Domain Routing
DHCP	Dynamic Host Configuration Protocol
FDDI	Fiber Distributed Data Interface
IANA	Internet Assigned Numbers Authority
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IFSC	Instituto Federal de Santa Catarina
IOS	Internetwork Operation System
IP	Internet Protocol
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
LACNIC	Latin America and Caribbean Network Information Centre
MAC	Media Access Control
NAT	Network Address Translator
NIC.br	Núcleo de Informação e Coordenação do Ponto BR
RFC	Request For Comments
RIR	Regional Internet Registry
RNP	Rede Nacional de Ensino e Pesquisa
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
VLAN	Virtual Local Area Network

LISTA DE ABREVIATURAS

add	address
conf t	configure terminal
en	enable
encap	encapsulation
ex	exit
fa	fastethernet
g	gigabitethernet
int	interface
net	network
runn	running-config
sh	show
shut	shutdown
swi	switchport

SUMÁRIO

1 INTRODUÇÃO

Todo e qualquer dispositivo que se conecta à Internet precisa de um endereço único que o identifique. Atualmente o protocolo de endereçamento usado é o Internet *Protocol version* 4 (IPv4), mas conforme previsto pelo Núcleo de Informação e Coordenação do Ponto BR (NIC.br), antes da metade de 2017, não haverá mais endereços IPv4 disponíveis no *Latin America and Caribbean Network Information Centre (*LACNIC), o qual é a entidade responsável por gerenciar os endereços Internet *Protocol* (IP) na América Latina e Caribe. Soluções paliativas como o *Classless Inter-Domain Routing* (CIDR), o *Dynamic Host Configuration Protocol* (DHCP) e o *Network Address Translator* (NAT) já estão sendo usadas desde a década de 1990, sendo que o NAT tem a desvantagem de quebra o modelo fim-a-fim da Internet, o que dificulta o funcionamento de algumas aplicações e algumas técnicas de segurança.

A solução definitiva é migrar para o Internet *Protocol version* 6 (IPv6), um protocolo de endereçamento padronizado em 1998, que possibilita 340.282.366.920.938.463.463.374.607.431.768.211.456 endereços diferentes, enquanto o IPv4 possibilita apenas 4.294.967.296 endereços. Há várias estratégias de migração, e para o cenário proposto o método de pilha dupla foi considerado o mais adequado, pois mantendo os dois protocolos em paralelo é possível o acesso aos serviços em IPv4 e em IPv6 sem a necessidade de configurar túneis, protocolos adicionais ou fazer configurações em outros locais.

Com o crescimento das redes e a necessidade da rede proposta ser utilizada por alunos, docentes, técnicos administrativos e comunidade externa, é necessário limitar o acesso à rede conforme as necessidades de cada público, um meio de aumentar a segurança e desempenho da mesma é utilizar *Virtual Local Area Networks* (VLANs), que consiste em separar a rede em grupos lógicos diferentes, facilitando a administração e alterações e inclusões de membros. O tráfego entre VLANs é restringido, obrigando o tráfego de uma VLAN a passar por roteamento para acessar outra VLAN, deste modo permitindo a aplicação de regras de acesso.

Nesta monografia serão abordados os passos e procedimentos necessários

para a configuração de IPv6 em pilha dupla com segmentação da rede proposta em VLANs.

1.1 PROBLEMA

O cenário proposto é o de uma rede que está passando por reestruturação, com aproximadamente 200 computadores divididos em diversos locais, e diversos equipamentos trazidos pelos alunos, servidores e comunidade externa que se conectam via rede sem fio, na qual já se utiliza uma solução Cisco que não será alterada.

A rede atual tem sérios problemas de gerenciamento e desempenho por causa do uso de equipamentos de rede antigos e inadequados, como *hubs* recebidos de doação da receita federal há mais de 10 anos, além da falta de estruturação do cabeamento e da ausência de documentação, o que torna o processo de descoberta de falhas lento e trabalhoso. Com o projeto de cabeamento estruturado a ser feito, também devem ser feitas trocas dos equipamentos de rede, e com o recebimento de um bloco IPv6 da Rede Nacional de Ensino e Pesquisa (RNP) tem-se a necessidade de fazer a configuração dos mesmos.

Neste contexto, no ambiente de simulação *Packet Tracer* da Cisco, este trabalho pretende criar um passo a passo para a configuração dos *switches* e roteador uma rede dividida em VLANs e que permita conectividade em IPv6, criando assim um modelo que possa ser adaptado para ser utilizado em outros campi e instituições.

1.2 OBJETIVOS

Nesta seção serão apresentados os objetivos gerais e específicos deste trabalho.

1.2.1 Objetivo Geral

Fazer o projeto de uma infraestrutura de rede em um ambiente de simulação, para posterior implementação nos equipamentos, utilizando a configuração de uma rede com os protocolos IPv4/IPv6 em pilha dupla, segmentada em VLANs para ser utilizada no Instituto Federal de Santa Catarina – Campus Jaraguá do Sul.

1.2.2 Objetivos Específicos

- Demonstrar os conceitos dos protocolos IPv4;
- Demonstrar os conceitos dos protocolos IPv6;
- Demonstrar conceitos dos métodos de migração;
- Demonstrar os conceitos de VLANs;
- Demonstrar as configurações necessárias para criação de VLANs;
- Demonstrar as configurações necessárias para permitir o uso do IPv6.

1.3 JUSTIFICATIVA

Num mundo onde há cada vez mais dispositivos conectados à Internet, é uma questão de tempo até o protocolo IPv6 necessitar ser totalmente implementado, já que, segundo o NIC.br, mesmo com as estratégias usadas para possibilitar a sobrevida do IPv4, em poucos meses não haverá mais endereços IPv4 disponíveis. Entre as estratégias de migração possíveis a pilha dupla é a que se mostra mais adequada ao cenário proposto, além de ser a recomendada pela Cisco, pois permite acessibilidade às redes e serviços IPv4 e IPv6, sem necessidade de configurar protocolos adicionais ou fazer configurações no provedor ou em outras redes.

Com o crescimento das redes e a necessidade de ser utilizada por tipos de

usuários diferentes, utilizar VLANs é um meio de segmentar a rede em grupos lógicos, o que permite melhorar o desempenho da mesma, reduzindo o tráfego desnecessário através da diminuição do tamanho do domínio de *broadcast*, e segurança, pela facilidade de aplicação de regras distintas de acesso à rede aos vários grupos, facilitando assim, a criação de perfis de acesso diferenciado conforme o grupo ao qual o usuário pertence.

1.4 ESTRUTURA DO TRABALHO

O trabalho terá a estrutura abaixo apresentada.

Capítulo 1 – Introdução: serão apresentados o tema, o problema, os objetivos, a justificativa da pesquisa e a estrutura geral do trabalho.

Capítulo 2 – Fundamentação teórica: serão abordados os conceitos dos protocolos IPv4, CIDR, DHCP, NAT, IPv6 e VLANs.

Capítulo 3 – Desenvolvimento: será mostrado a rede proposta, o planejamento e os comandos necessários para a criação das VLANs e para permitir a conectividade em IPv4 e IPv6.

Capítulo 4 – Considerações finais: serão retomados os objetivos da pesquisa, mostrando como os resultados foram atingidos. Além disso serão sugeridos outros trabalhos que poderiam se seguir a este.

2 FUNDAMENTAÇÃO TEÓRICA

2.1 IPv4

Com a necessidade de interligar os computadores dos centros militares e de pesquisa, a *Advanced Research Projects Agency* (ARPA) do Departamento de Defesa dos Estados Unidos, iniciou em 1966 um projeto de sistema de comunicação e controle distribuído que foi chamado de ARPANET, e tinha como objetivo formar uma rede que continuasse funcionando mesmo com a queda de algum dos computadores.

Diversos protocolos de comunicação foram utilizados, mas ao chegar a 562 computadores em 1983, o *Transmission Control Protocol/Internet Protocol* (TCP/IP) foi adotado, pois eliminava restrições dos protocolos anteriores, permitindo assim um crescimento ordenado da rede. Em 1981, na *Request For Comments* (RFC) 791, foi definido o protocolo IP versão 4, que é utilizado até hoje e fornece a possibilidade de transferir grandes blocos de dados fragmentados em pacotes menores para poderem ser transmitidos em redes de baixa largura de banda e um sistema de endereçamento que permite identificar origem e destino dos pacotes.

A figura a seguir apresenta a estrutura do cabeçalho do pacote de Internet.

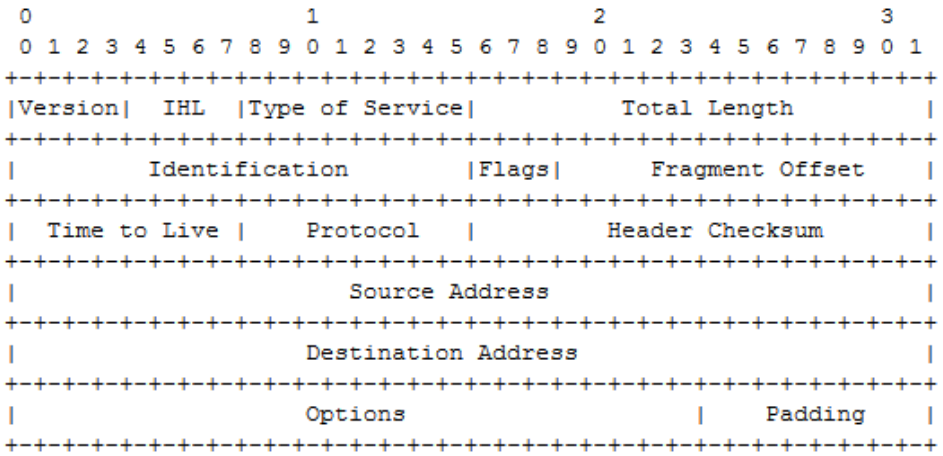

Figura 1 - Cabeçalho do Protocolo IPv4
Fonte: RFC 791.

Version: Versão do Protocolo, usa 4 bits.

IHL: Comprimento do cabeçalho de Internet, em grupos de 32 bits, usa 4 bits.

Type of Service: Indica a procedência e um resumo dos parâmetros de qualidade de serviço desejado, usa 8 bits. Atualmente esse campo é chamado de Serviços Diferenciados e indica a prioridade de cada pacote.

Total Length: Indica o comprimento total do pacote em octetos, usa 16 bits.

Identification: Valor atribuído pelo remetente para identificar os fragmentos de um pacote, usa 16 bits.

Flags: Usado para indicar fragmentação, usa 3 bits.

Fragment Offset: Indica a sequência no pacote ao que fragmento pertence e é medido em unidades de 8 octetos, usa 13 bits.

Time to Live: Indica o tempo máximo que é permitido ao pacote permanecer no sistema até ser entregue ao destino, usa 8 bits.

Protocol: Indica o protocolo do próximo nível usado na parte de dados do pacote, os valores para cada protocolo são especificados pela RFC 790, usa 8 bits.

Header Checksum: Usado para verificação de erros no cabeçalho, usa 16 bits

Source Address: Endereço de origem, usa 32 bits.

Destination Address: Endereço de destino, usa 32 bits.

Options: Opções adicionais, podem ou não aparecer nos pacotes, tamanho variável.

Padding: Usado apenas para garantir que o cabeçalho tenha um tamanho que seja múltiplo de 32 bits, tamanho variável.

2.1.1 Endereçamento

A definição do sistema de endereçamento IP foi feita pela RFC 790, e fornece flexibilidade na atribuição de endereços, permitindo redes grandes e pequenas usarem o mesmo sistema de endereçamento.

Os endereços são divididos em classes, os de classe A usam 7 bits para rede e 24 para *host*, permitindo 128 endereços de rede e 16.777.216 endereços de

host, os de classe B usam 14 bits para rede e 16 para *host*, permitindo 16.348 endereços de rede e 65.536 endereços de *host*, os de classe C usam 21 bits para rede e 8 para *host*, permitindo 2.097.152 endereços de rede e 256 endereços de *host*.

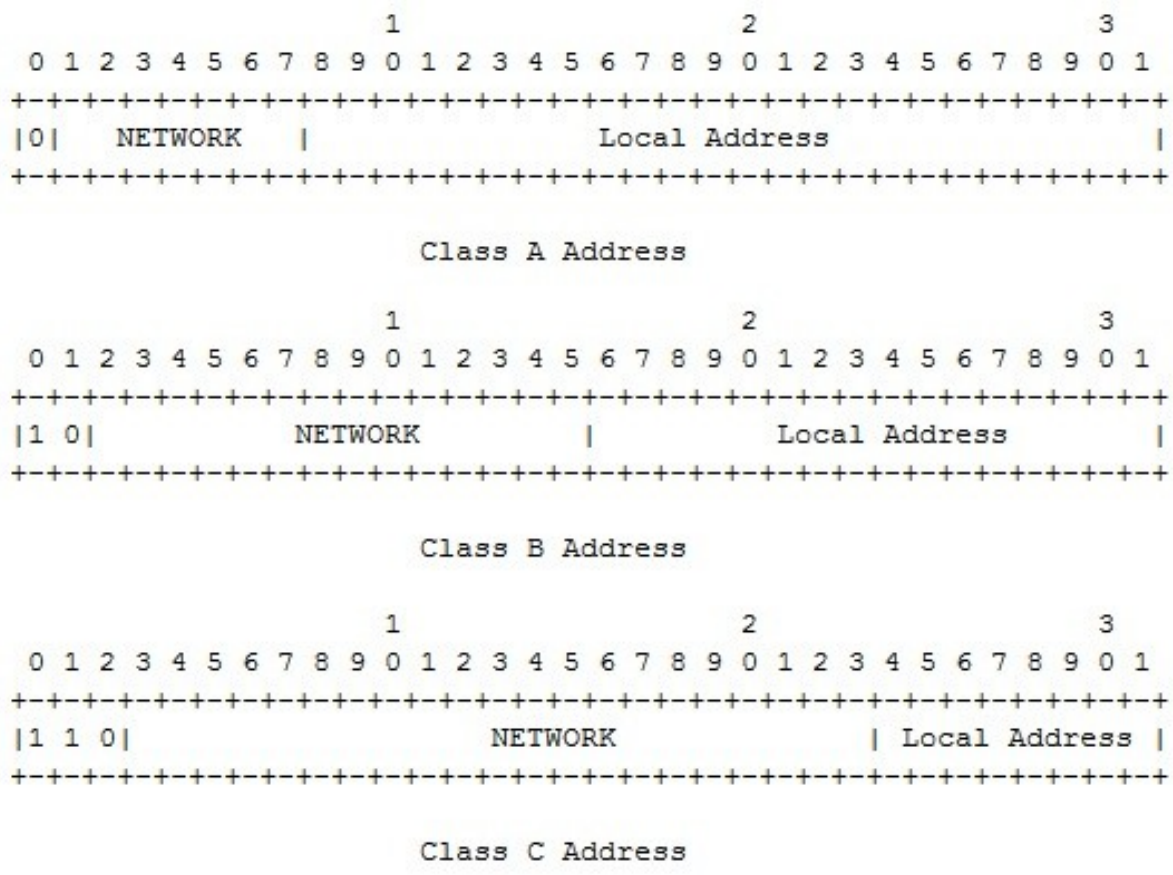

Figura 2 - Sistema de Endereçamento IP
Fonte: RFC 790.

Para permitir a utilização de redes de tamanhos diferentes das classes A, B e C, é necessário diferenciar a parte do endereço que representa a rede da parte do endereço que representa os *hosts*, para isso é usado o prefixo de rede, também chamado de máscara de rede e é representado por “/n”, onde n é o número de bits que correspondem a parte de rede do endereço. Outra forma de representar a máscara de rede é usando a mesma notação do endereço IPv4 colocando 255 na parte que representa rede e 0 na parte que representa o *host*, por exemplo a máscara de rede de um endereço /8 pode ser representada por 255.0.0.0, de um

endereço /16 pode ser escrita como 255.255.0.0, de um endereço /24, 255.255.255.0 ou um endereço /26, 255.255.255.192.

2.1.1.1 Endereços IPv4 de uso especial

Há faixas de endereços de uso restrito definidas inicialmente pela RFC 3330 atualmente as faixas IPv4 reservadas, conforme descrito na RFC 6890 são:

Dentro das classes A, B e C, há uma faixa de endereços, definida pela RFC 1918, reservada para uso privado que são 10.0.0.0 a 10.255.255.255 (10.0.0.0/8), 172.16.0.0 a 172.31.255.255 (172.16.0.0/12) e 192.168.0.0 a 192.168.255.255 (192.168.0.0/16), esses endereços devem ser usados apenas em redes internas, pois não são roteáveis na Internet.

A RFC 6598 definiu o bloco 100.64.0.0/10 como sendo destinado para uso somente nas redes dos provedores de serviços.

Outra faixa reservada, definida pela RFC 1112, é a de *loopback*, 127.0.0.0 a 127.255.255.255 que é usada pelos hosts para encaminhar tráfego para si mesmos, facilitando a comunicação entre aplicações e serviços TCP/IP num mesmo dispositivo.

A RFC 3927 definiu a faixa de 169.254.0.0 a 169.254.255.255 (169.254.0.0/16) para *link-local* e geralmente é atribuída a um *host* pelo seu sistema operacional quando o mesmo não consegue um endereço pelo DHCP, ou em links ponto-a-ponto.

O bloco de endereços 192.0.0.0/24, foi definida na RFC 5736, para uso de atribuições de protocolo IETF.

A faixa 192.0.0.0/29 é atribuída pela RFC 6333 como de uso para *Dual-Stack Lite*, para ajudar a manter o funcionamento do IPv4 enquanto incentiva a adoção do IPv6.

Na RFC 5737, os blocos 192.0.2.0/24, 198.51.100.0/24 e 203.0.113.0/24, chamados respectivamente de *Test-Net*-1, *Test-Net*-2 e *Test-Net*-3, foram definidos como de uso para documentação.

Outra faixa restrita é a 192.88.99.0/24, definida na RFC 3068, para divulgar

rotas IPv4 *6to4* para roteadores de retransmissão disponíveis.

A RFC 2544 definiu o bloco 198.18.0.0/15 para uso em testes de desempenho de equipamentos de rede.

Os endereços de 240.0.0.0 a 255.255.255.254 são definidos como reservados para uso futuro pela RFC 1112.

Além desses, na RFC 3171, o bloco 224.0.0.0/4 é atribuído para uso *multicast*, ou seja, para endereçar um grupo de *hosts*.

Outros endereços de uso especial, são o endereço de rede, no qual a parte relativa ao *host* é composta de zeros e é usado para identificar a rede, e o endereço de *broadcast*, no qual a parte referente ao *host* é composta por bits 1 e é usado para enviar pacotes para todos os *hosts* da rede, definido na RFC 0919.

2.1.2 CIDR

Apesar de a divisão por classes permitir redes de diversos tamanhos, com o aumento da Internet descobriu-se que essa divisão não era eficiente. Em 1990 já haviam estudos indicando que futuramente haveria falta de endereços e problemas com o aumento da tabela de roteamento além da capacidade de *software, hardware* e pessoas para gerenciá-las na época. Para resolver o problema a curto prazo, a RFC 1519, publicada em 1993, que foi substituída pela RFC 4632 em 2006, definiu o CIDR.

Conforme descrito na RFC, o CIDR resolve o problema das tabelas de roteamento e a proximidade de exaustão de endereçamento da classe B e ajuda a retardar o problema da falta de endereços geral, deste modo permitindo que a Internet continue funcionando enquanto se trabalha em uma solução de longo prazo. O CIDR flexibiliza o tamanho das máscaras de rede, permitindo, por exemplo, a agregação de 4 redes /24 em uma única rede /22.

A figura seguinte mostra todas as possibilidades de prefixos do CIDR relacionando-as com a quantidade possível de endereços em cada rede e a quantidade possível de redes.

notation	addrs/block	# blocks	
n.n.n.n/32	1	4294967296	"host route"
n.n.n.x/31	2	2147483648	"p2p link"
n.n.n.x/30	4	1073741824	
n.n.n.x/29	8	536870912	
n.n.n.x/28	16	268435456	
n.n.n.x/27	32	134217728	
n.n.n.x/26	64	67108864	
n.n.n.x/25	128	33554432	
n.n.n.0/24	256	16777216	legacy "Class C"
n.n.x.0/23	512	8388608	
n.n.x.0/22	1024	4194304	
n.n.x.0/21	2048	2097152	
n.n.x.0/20	4096	1048576	
n.n.x.0/19	8192	524288	
n.n.x.0/18	16384	262144	
n.n.x.0/17	32768	131072	
n.n.0.0/16	65536	65536	legacy "Class B"
n.x.0.0/15	131072	32768	
n.x.0.0/14	262144	16384	
n.x.0.0/13	524288	8192	
n.x.0.0/12	1048576	4096	
n.x.0.0/11	2097152	2048	
n.x.0.0/10	4194304	1024	
n.x.0.0/9	8388608	512	
n.0.0.0/8	16777216	256	legacy "Class A"
x.0.0.0/7	33554432	128	
x.0.0.0/6	67108864	64	
x.0.0.0/5	134217728	32	
x.0.0.0/4	268435456	16	
x.0.0.0/3	536870912	8	
x.0.0.0/2	1073741824	4	
x.0.0.0/1	2147483648	2	
0.0.0.0/0	4294967296	1	"default route"

Figura 3 - CIDR
Fonte: RFC 4632.

2.1.3 DHCP

Outra solução paliativa proposta em 1993 foi o DHCP na RFC 1541, que consiste de um mecanismo de alocação de endereços e entrega de parâmetros de configuração aos *hosts*, deste modo habilitando o reúso de endereços IP.

2.1.4 NAT

Em 1994, na RFC 1631, foi proposto o NAT que permite que os endereços IP privados possam ser convertidos para um endereço público. Esta solução foi pensada tomando como fato que dentro de uma rede, apenas uns poucos *hosts* se comunicam com redes externas ao mesmo tempo, assim um número limitado de endereços seria capaz de fornecer conectividade às redes externas a um número muito maior de *hosts*.

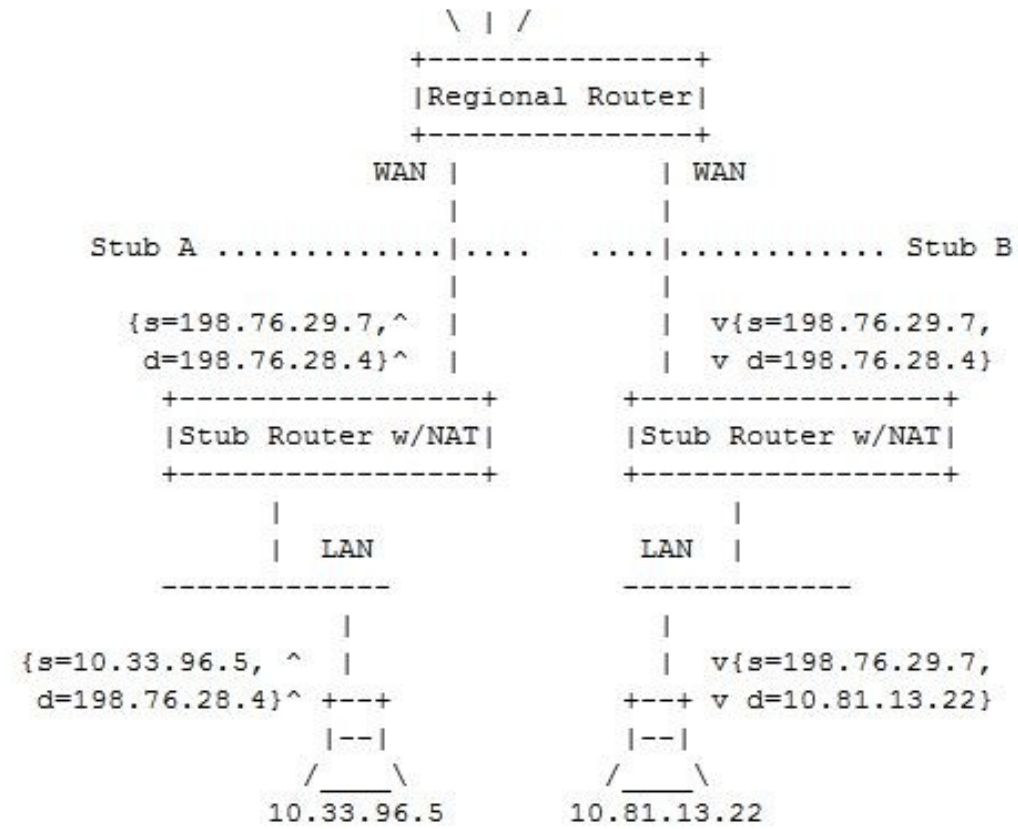

Figura 4 - NAT
Fonte: RFC 1631.

Por exemplo, na figura acima o *host* da rede A que usa o IP privado 10.33.96.5 manda um arquivo para o *host* 198.76.28.4, o roteador converte o

endereço privado para um endereço público da rede disponível, no caso, 198.76.29.7 e manda o arquivo para a rede 198.76.29.0, ao chegar, o roteador B consulta sua tabela NAT e ao encontrar uma entrada que corresponda ao IP de destino, no caso o *host* 10.81.13.22, encaminha o arquivo para o destino.

Assim, mesmo uma empresa grande que necessitasse de um /8 para sua rede, poderia utilizar um /24 para conexão com a Internet. O problema é que para cada *host* que quisesse acesso à Internet em determinado momento, seria necessário um IP público, por exemplo, se há 10 IPs públicos disponíveis e em um momento 11 tentassem acessar a Internet, o 11º ficaria sem acesso. Para resolver esse problema, em 2001, na RFC 3022, foi proposto uma forma adicional de NAT, o *Network Address Port Translator*, também chamado de PAT ou sobrecarga de NAT, que permite múltiplas conexões com apenas 1 endereço IP, utilizando o número de porta TCP/UDP da sessão para diferenciar as conexões.

NAT

Pool de endereços globais internos	Endereço local interno
209.165.200.226	192.168.10.10
209.165.200.227	192.168.10.11
209.165.200.228	192.168.10.12
209.165.200.229	192.168.10.13

PAT

Endereço global interno	Endereço local interno
209.165.200.226:1444	192.168.10.10:1444
209.165.200.226:1445	192.168.10.11:1444
209.165.200.226:1555	192.168.10.12:1555
209.165.200.226:1556	192.168.10.13:1555

Figura 5 - Tabela NAT x Tabela PAT
Fonte: ACADEMIA CISCO (CCNA, 2016, módulo 4, cap 5.1.2.5).

Todas essas medidas ajudaram a retardar o problema da falta de endereços

IP, mas conforme colocado na RFC 6264, a exaustão de endereços IPv4 livres da *Internet Assigned Numbers Authority* (IANA), se deu em fevereiro de 2011, e segundo o IPv6.br, nos Registros Regionais de Internet (RIR), principalmente no LACNIC, o esgotamento é iminente, sendo necessário adotar uma nova medida, o IPv6.

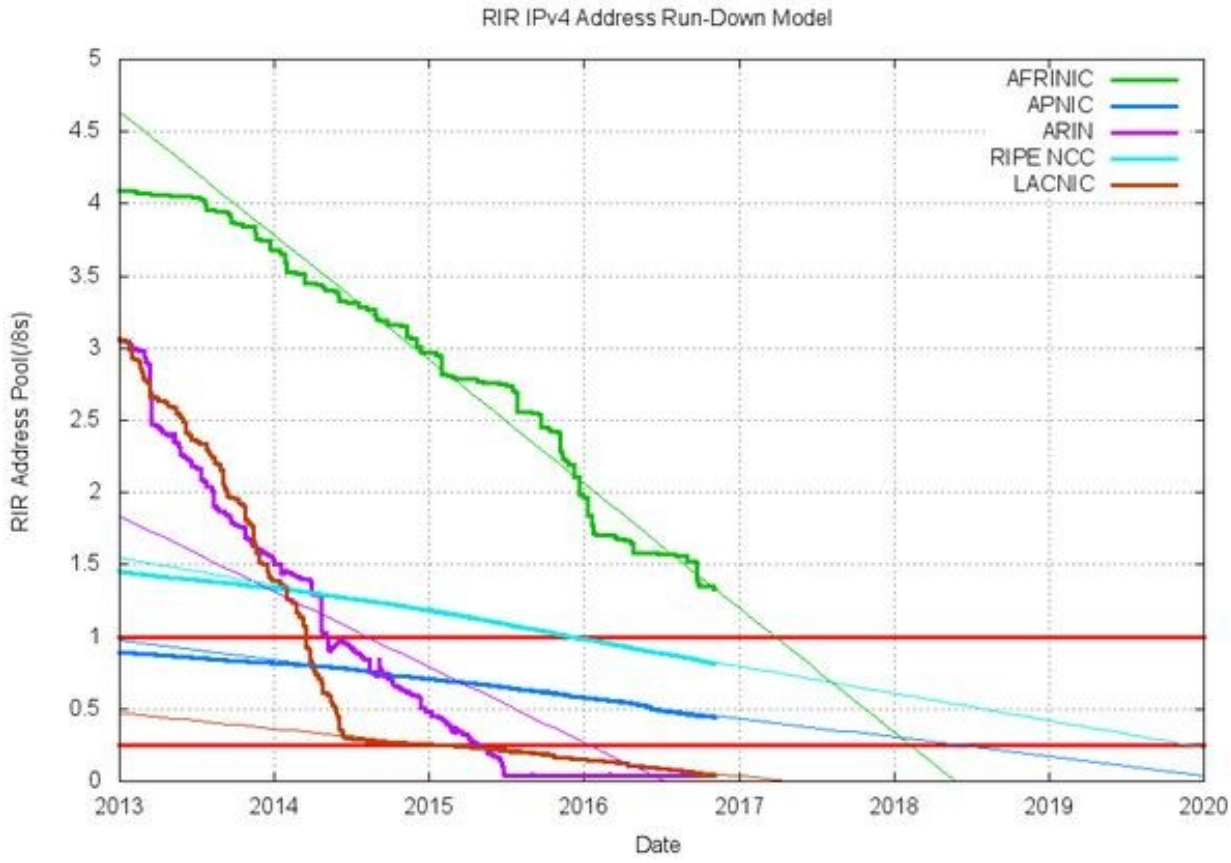

Figura 6 - Previsão de esgotamento do IPv4
Fonte: IPv6.Br.

2.2 IPv6

Em 1993, diversas pesquisas começaram a ser feitas para criar um novo protocolo de endereçamento e em 1995 foi publicada a primeira proposta do IPv6 na RFC 1883, e na RFC 1884 a arquitetura de endereçamento. Em 1998, a RFC 2460 fez algumas alterações no Protocolo IPv6, e é a versão utilizada até hoje.

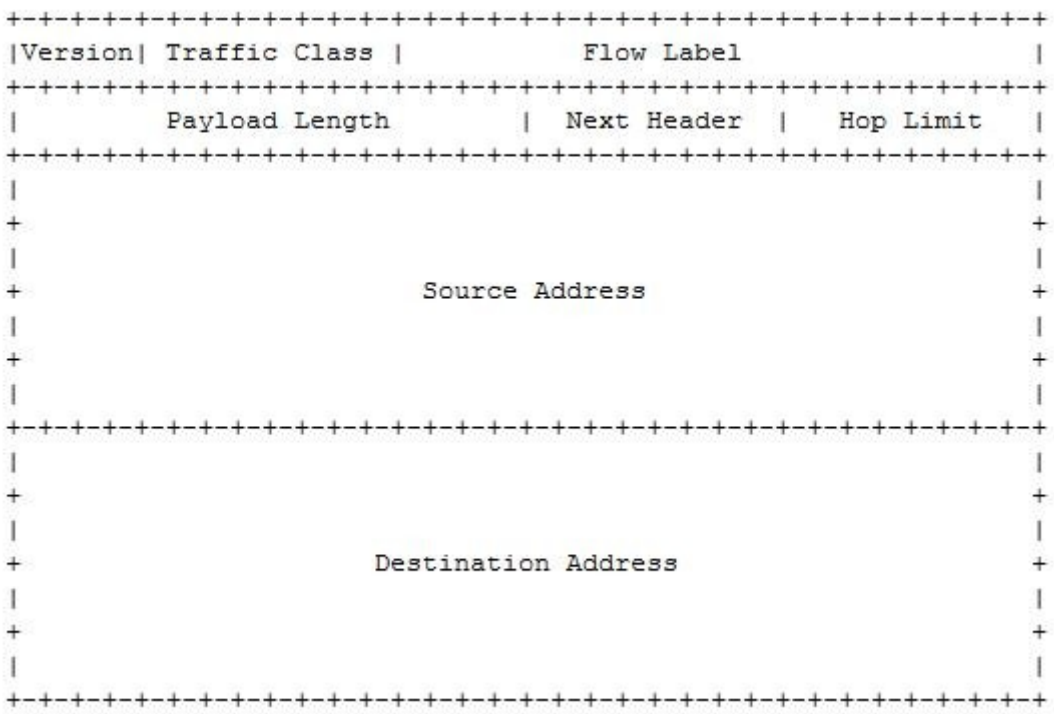

Figura 7 - Cabeçalho IPv6
Fonte: RFC 2460.

Version: versão do protocolo de Internet, usa 4 bits.

Traffic Class: Usado para diferenciar entre classes ou prioridades, usa 8 bits.

Flow Label: Controle de fluxo, usa 20 bits.

Payload Length: Tamanho da carga do pacote, ou seja, o tamanho do pacote menos os 60 bytes do cabeçalho IPv6, em octetos, usa 16 bits.

Next Header: Identifica o cabeçalho imediatamente subsequente ao cabeçalho IPv6, usa 8 bits.

Hop Limit: Decrementa 1 a cada roteador que encaminha o pacote, se chegar a 0 o pacote é descartado, usa 8 bits.

Source Address: Endereço de origem do pacote, usa 128 bits.

Destination Address: Endereço de destino do pacote, usa 128 bits.

2.2.1 Endereçamento

Desde 1995, algumas alterações foram feitas e a RFC 4291 é a que define a arquitetura de endereçamento atualmente. Endereços IPv6 tem 128 bits e são divididos em três tipos:

Unicast: identificam apenas 1 interface, um pacote enviado para um endereço *unicast* será enviado apenas para a interface a qual o endereço é atribuído.

Anycast: identifica um grupo de interfaces, um pacote enviado para um endereço *anycast* será entregue a uma das interfaces a qual o endereço é atribuído.

Multicast: identifica um grupo de interfaces, um pacote enviado a um endereço *multicast* será entregue a todas as interfaces a qual o endereço é atribuído.

Não há endereços de *broadcast* no IPv6, sua função foi superada pelos endereços *multicast*.

Diferentemente do IPv4, no IPv6, os endereços são representados textualmente na forma hexadecimal e divididos por dois pontos ":" em 8 grupos de 4 caracteres, correspondendo cada caractere a 4 bits, conforme recomendação da RFC 5952. Não há diferenciação entre letras maiúsculas ou minúsculas.
Exemplos:

0123:4567:0000:0000:0123:4567:89AB:CDEF
0000:0001:0002:0003:0004:0005:0006:0007:
0000:0000:0000:0000:0000:0000:0000:0001
1234:0000:0249:0047:0000:0000:0000:ABCD

Para facilitar a escrita foi definido que é possível suprimir zeros em dois casos:
1º - Zeros à esquerda em cada grupo podem ser omitidos.

123:4567:0:0:123:4567:89AB:CDEF
0:1:2:3:4:5:6:7

0:0:0:0:0:0:0:1
1234:0:249:47:0:0:0:ABCD

2° - Grupos contíguos de zeros podem ser representados por “::”, essa substituição pode acontecer apenas uma vez, para evitar interpretações ambíguas.

123:4567::123:4567:89AB:CDEF
::1:2:3:4:5:6:7
::1
1234:0:249:47::ABCD ou 1234::249:47:0:0:0:ABCD

O prefixo de rede IPv6 tem representação semelhante a notação CIDR do IPv4 “/n” sendo escrita logo após o endereço de rede.

2.2.1.1 Endereços IPv6 de uso especial

Assim como o IPv4, o IPv6 também tem alguns endereços de uso restrito, listados na RFC 6890, que são os seguintes:

::1/128 é o endereço de *loopback* – RFC 4291
::/128 é o endereço não especificado – RFC 4291
64:FF9B::/96 é a faixa usada para tradução entre IPv4 e IPv6 – RFC6052.
::FFFF:0:/96 são endereços mapeados do IPv4 – RFC4291
100::/64 é o prefixo para descarte de pacotes - RFC 6666
2001::/23 - endereços IPv6 para registro de propósito especial da IANA – RFC 4773
2001::/32 é o bloco Teredo, podem ser divulgados quando um local está oferecendo um serviço de transmissão ou retransmissão Teredo – RFC 4380
2001:2::/48 é exclusiva para uso em testes de desempenho em equipamentos de rede – RFC 5180
2001:DB8::/32 é o prefixo de documentação, proposto para ser usado em manuais,

RFCs, etc – RFC 3849
2001:10::/28 são endereços *Overlay Routable Cryptographic Hash Identifiers*, são usados como identificadores e não são roteáveis. - RFC 4843
2002::/16 são endereços *6to4*, podem ser divulgados quando um local está executando transmissão ou retransmissão *6to4* – RFC 3056
FC00::/7 são endereços únicos locais – RFC4193
FE80::/10 são endereços de *Link local* – RFC 4291

2.2.1.1 Configuração de endereços IPv6

Segundo a Cisco (ACADEMIA CISCO, 2016), descreve no módulo 2, capítulo 10, há diferentes maneiras diferentes de configurar endereçamento IPv6 dinâmico: configuração automática (SLAAC) ou DHCP para IPv6. No SLAAC apenas as mensagens de anúncio do roteador são utilizadas para obter as configurações de endereçamento da rede. O DHCPv6 é definido na RFC 3315 e pode ser configurado para funcionar semelhante ao DHCP tradicional (DHCPv6 *Statefull*), onde o computador receberá todas as configurações de endereçamento de um servidor, ou pode ser utilizado o DHCPv6 *Stateless*, em que as configurações de prefixo de rede e *gateway* serão obtidas através de anúncios do roteador e configurações adicionais, como servidor de DNS, serão fornecidas pelo DHCP.

2.3 MÉTODOS DE MIGRAÇÃO

O IPv6 resolve o problema da falta de endereços, mas não é compatível com o IPv4 e antes que o IPv4 possa ser definitivamente abandonado, o IPv6 precisa ser configurado nos roteadores e servidores, em todas as redes, públicas e privadas.

Para facilitar a transição, em 1996 dois métodos de transição foram propostos pela RFC 1933, pilha dupla e tunelamento, desde então diversas ferramentas de migração foram criados e revisados. Os métodos de migração se

agrupam em:

2.3.1 Tradução

Permite que uma rede que usa apenas uma versão, continue funcionando através de uma rede que usa somente a outra, vários mecanismos já foram criados, sendo o mais recente o 464XLAT, descrito na RFC 6877, e que usa um tradutor nas instalações do cliente que traduz 1 IPv4 privado para 1 IPv6 global e vice-versa, e um tradutor do lado do provedor que traduz n IPv6 globais para 1 IPv4 global e vice-versa.

2.3.2 Tunelamento

Há vários mecanismos de tunelamento, e é recomendado pela *Internet Engineering Task Force* (IETF) na RFC 6180 apenas quando duas redes que usam apenas uma versão do protocolo IP precisam se conectar através de uma rede que use apenas a outra versão, por exemplo encapsulando pacotes IPv6 com um cabeçalho IPv4 para transportá-los através de uma rede somente IPv4.

2.3.3 Pilha dupla

É o método no qual o IPv4 e o IPv6 são configurados em paralelo na rede, não há necessidade de configurações ou protocolos adicionais e suporta todos os tipos de equipamentos e aplicações sem restrições.

Como no cenário trabalhado, a rede interna passará a usar IPv6 e acessa a Internet através de um provedor que também suporta IPv6 o método de migração recomendado pela RFC 6180 é o de Pilha Dupla.

2.3 VLANs

Quanto maior uma rede, maior é o impacto que *broadcasts* causam no desempenho da mesma. Mensagens de *broadcast*, são utilizadas, por exemplo, por um computador para solicitar um endereço IP a um servidor de DHCP, ou pelo *Address Resolution Protocol* (ARP), que é usado pelos *switches* para relacionar endereços lógicos e físicos a ele conectados. O domínio de *broadcast*, normalmente é o roteador da rede e uma mensagem de *broadcast* é encaminhada a todos os equipamentos dentro do domínio, sendo reencaminhada pelos *switches* inclusos.

As VLANs, foram padronizadas pela *Institute of Electrical and Electronics Engineers* (IEEE) na 802.1q, e segundo a Cisco (ACADEMIA CISCO, 2016), descreve no módulo 2, capítulo 3, as VLANs permitem várias vantagens como a possibilidade de dividir o domínio de *broadcast* em vários menores, aumentando seu desempenho, possibilitando uma melhor organização da rede e facilitando a aplicação de regras de acesso diferenciadas às mesmas. Cada VLAN é uma rede lógica diferente e mesmo que várias delas usem o mesmo *switch*, é necessário que pacotes de uma rede passem por um roteador para poderem ser encaminhadas a outra.

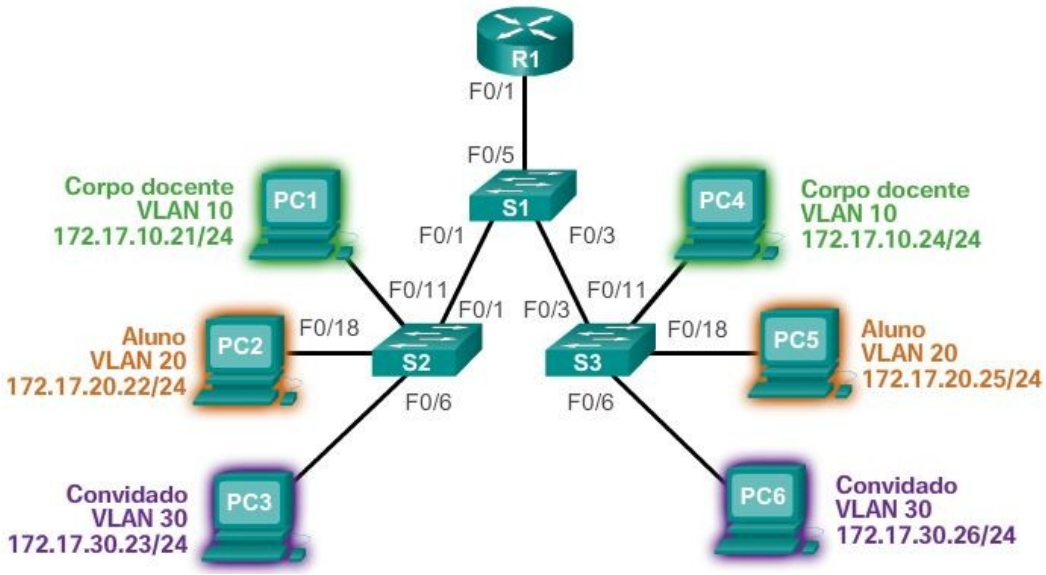

Figura 8 - Exemplo de rede com VLANs
Fonte: ACADEMIA CISCO (CCNA, 2016, módulo 2, cap 3.1.1.2).

Na figura acima, para o pc1 enviar uma mensagem ao pc4, a mesma sai do computador 1 passa pelo S2, o S1 encaminha para o S3 que manda a mensagem para o computador 4, mas se o computador 1 quiser mandar uma mensagem para o computador 2, é obrigatório que a mensagem passe pelo roteador, indo do S2 para o S1 e pro roteador, que verifica se a mensagem pode ser encaminhada, caso haja regras de acesso, e se permitido, encaminha o pacote de volta para S1 e então S2 que o entrega ao pc 2. Há diversos tipos de VLANs:

A VLAN padrão é a qual todas as portas de um *switch* pertencem, enquanto não for feita outra configuração, nos *switches* Cisco a VLAN padrão é a VLAN 1.

VLAN de dados são as VLANs configuradas para o transporte de dados para usuários e são as usadas para separar os usuários em grupos.

VLAN de gerência é a configurada para permitir o acesso aos gerenciamento do *switch*, configurando uma interface virtual e seu endereço IP é possível que o *switch* seja acessado pela rede.

VLAN nativa são as atribuídas à porta de tronco, que são utilizadas para o transporte de tráfego de várias VLANs entre *switches*. São os troncos que estendem as VLANs pela rede e podem ser usadas entre quaisquer equipamentos com placas de rede que suportem o 802.1Q.

VLAN de voz é a usada para o VoIP, e é colocado em uma VLAN separada da de dados porque o tráfego de voz requer prioridade de transmissão e garantia de largura de banda para assegurar a qualidade.

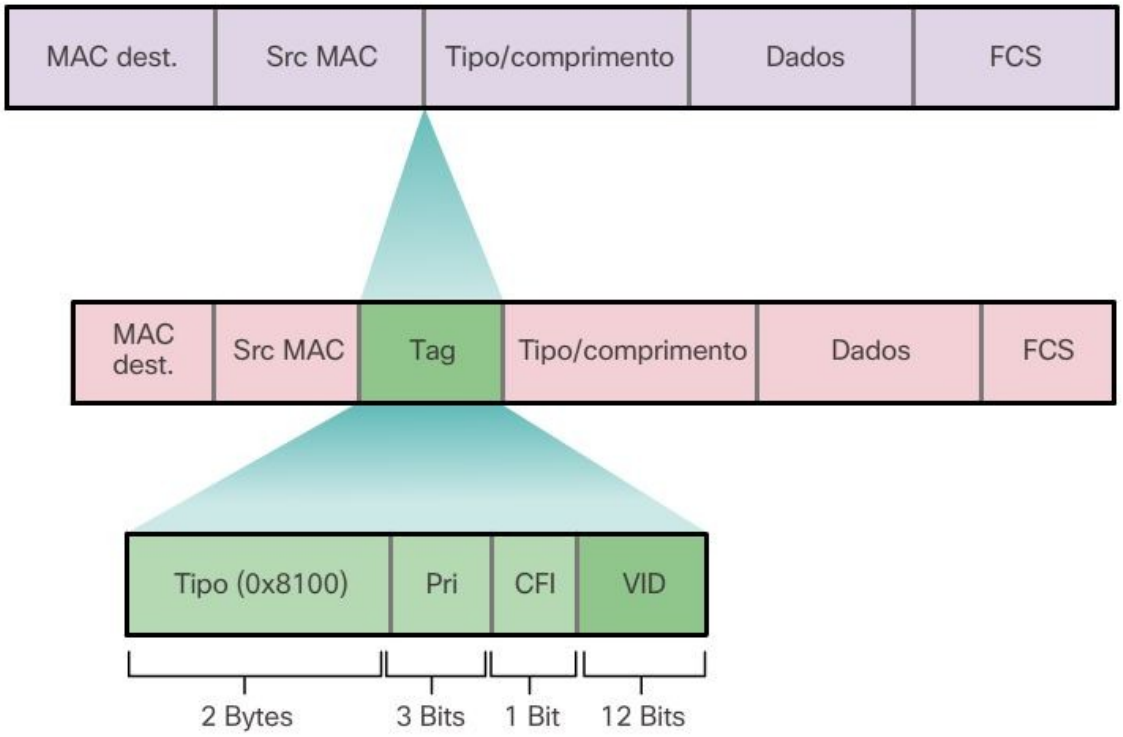

Figura 9 - Quadro Ethernet 802.1Q
Fonte: ACADEMIA CISCO (CCNA, 2016, módulo 2, cap 3.1.2.3).

Switches trabalham na camada de enlace, portanto as informações referentes à VLAN são inseridas no cabeçalho do quadro *ethernet* ao ser recebido pelo *switch*. Esse processo chamado de marcação inclui quatro bytes após o endereço MAC de origem, divididos nos seguintes campos:

Type – Identificação do protocolo de Tag, usa 2 bytes.

User Priority – usado para definir a prioridade do serviço, usa 3 bits.

Canonical Format Identifier – permite o transporte de quadros *Token Ring* atravé de redes *Ethernet*, usa 1 bit.

VID – o número de identificação da VLAN, usa 12 bits.

As VLANs também podem ser divididas em sendo de intervalo normal, de 1 até 1005, sendo as 1002, 1003, 1004 e 1005 reservadas para *Token Ring* e *Fiber Distributed Data Interface* (FDDI), e de intervalo estendido, de 1006 até 4096.

3 DESENVOLVIMENTO

Este capítulo apresenta o cenário proposto e como são feitas as configurações de VLAN e IPv6.

3.1 CENÁRIO PROPOSTO E PLANEJAMENTO

Considerando o projeto de rede do Campus, apresentado na figura a seguir, e tendo em vista a necessidade de conectar 17 *switches* de acesso, com várias VLANs na maioria deles, optou-se por usar um *switch* de camada 3 para conectá-los, já que o mesmo tem uma grande quantidade de portas e permite o roteamento entre as VLANs. No *Packet Tracer* o *switch* de camada 3 disponível é o 3560, para os s*witches* de acesso foram usados o 2960, e o roteador usado foi o 2911.

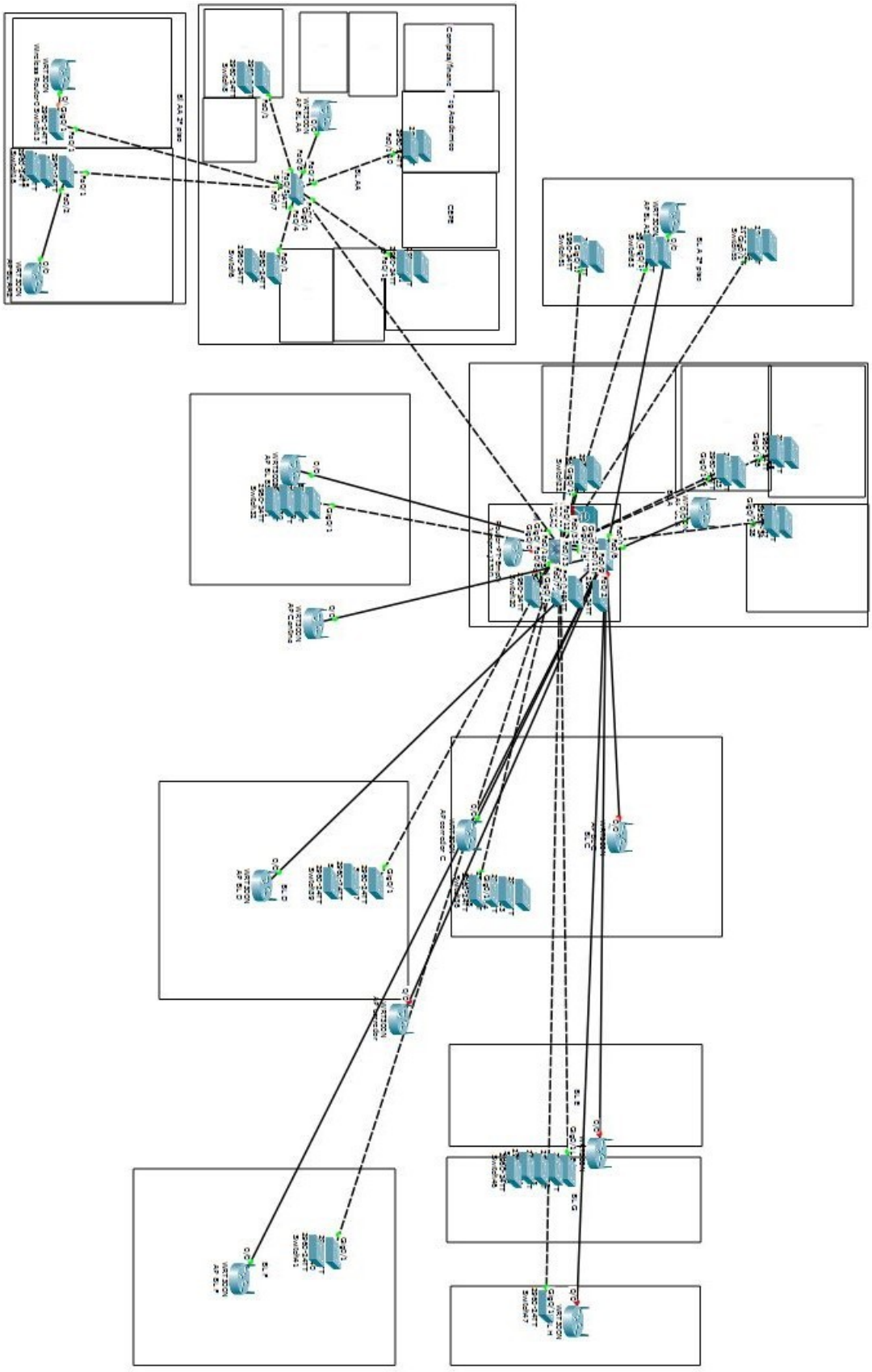

Figura 10 - Projeto de rede do Campus
Fonte: Autoria própria.

Nos locais em que há mais de um *switch*, eles serão interligados via empilhamento, por isso, para simplificar será feita a configuração de apenas um. Além disso, este trabalho se limita à configuração das VLANs e do IPv6 em pilha dupla, nos *switches* e roteador, por isso configurações relativas à segurança, como senha de acesso aos dispositivos e listas de controle de acesso não serão abordadas. Deste modo os equipamentos a serem configurados, são mostrados na figura abaixo.

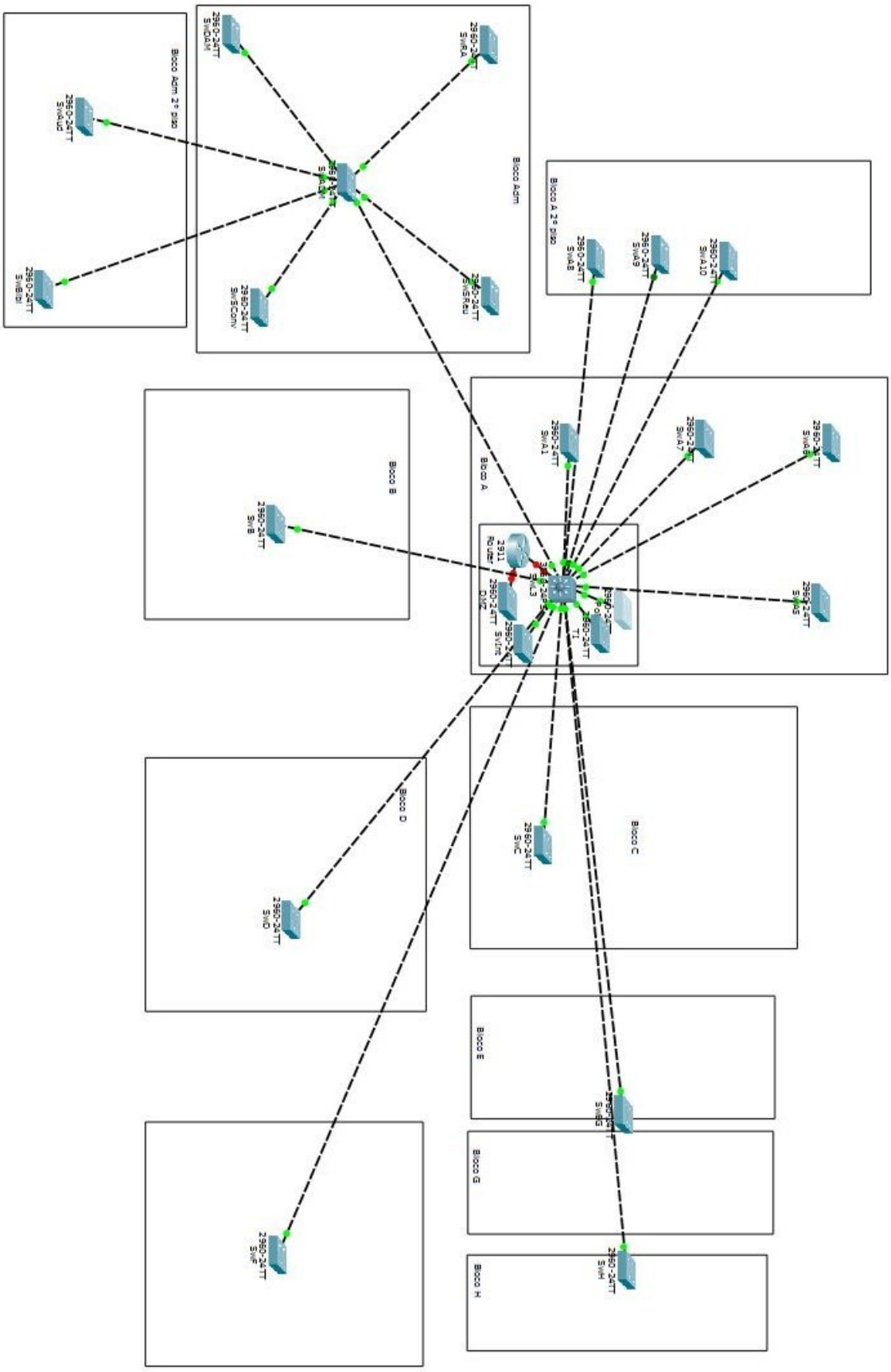

Figura 11 – Equipamentos a serem configurados
Fonte: Autoria própria.

Antes de configurar as VLANs nos equipamentos é necessário decidir quantas e quais as VLANs que serão necessárias. Com base em um estudo realizado com os analistas e técnicos em tecnologia da informação do IFSC a fim de fazer um documento para padronizar a criação e uso de VLANs no IFSC, conforme a tabela de modelo resumido, do capítulo 4 Modelo Final do documento, em anexo, definiu-se a proposta apresentada na tabela abaixo para aplicação no Câmpus.

Tabela 1 – Relação de VLANs e endereços IPv4 e IPv6

vlan	local	endereços IPv4	endereços IPv6
1	**TI**		
100	DMZ – site	172.20.1.0/24	2001:0db8:1f5c:100::/64
105	BD – Ldap	172.20.2.0/24	2001:0db8:1f5c:105::/64
110	serv internos – ponto, antivírus, arquivos	172.20.3.0/24	2001:0db8:1f5c:110::/64
120	tic	172.20.5.0/24	2001:0db8:1f5c:120::/64
2	**ADM**		
200	direção	172.20.10.0/24	2001:0db8:1f5c:200::/64
210	TAES	172.20.15.0/24	2001:0db8:1f5c:210::/64
220	Docentes	172.20.20.0/24	2001:0db8:1f5c:220::/64
290	servidores – áreas comuns	172.20.25.0/24	2001:0db8:1f5c:290::/64
3	**Acadêmico**		
301	laboratório A1	172.20.31.0/24	2001:0db8:1f5c:301::/64
302	laboratório A5	172.20.32.0/24	2001:0db8:1f5c:302::/64
303	laboratório A6	172.20.33.0/24	2001:0db8:1f5c:303::/64
304	laboratório A7	172.20.34.0/24	2001:0db8:1f5c:304::/64
310	laboratório física	172.20.40.0/24	2001:0db8:1f5c:310::/64
311	laboratório química	172.20.41.0/24	2001:0db8:1f5c:311::/64
312	laboratório fios	172.20.42.0/24	2001:0db8:1f5c:312::/64
350	Biblioteca – alunos	172.20.50.0/24	2001:0db8:1f5c:350::/64
360	salas de aula	172.20.60.0/25	2001:0db8:1f5c:360::/64
4	**Acadêmico e Visitante (490-499)**		
490	recepção	172.20.70.0/24	2001:0db8:1f5c:490::/64
491	auditório	172.20.80.0/24	2001:0db8:1f5c:491::/64
5	**Wifi**		
520	IFSC-ADM	172.20.100.0/24	2001:0db8:1f5c:520::/64
530	IFSC-ALUNOS	172.20.104.0/21	2001:0db8:1f5c:530::/64
540	IFSC-VISITANTE	172.20.120.0/24	2001:0db8:1f5c:540::/64
7	**VoIP**		
700	voip	172.20.140.0/24	2001:0db8:1f5c:700::/64
710	videoconfêrencia	172.20.141.0/24	2001:0db8:1f5c:710::/64
8	**Impressoras**	172.20.150.0/24	2001:0db8:1f5c:800::/64
9	**Gerência**	172.20.254.0/24	2001:0db8:1f5c:900::/64

Fonte: Autoria própria.

Definidas as VLANs, é necessário decidir quantos usuários serão atendidos em cada pra saber qual a quantidade mínima necessária de endereços e então definir o endereço de rede e a máscara para cada uma. Depois é necessário saber quais VLANs cada equipamento deverá permitir acesso com base em que usuários estarão conectados em cada *switch*.

Tabela 2 – Relação de switches e VLANs

SwRA	210, 490, 700, 800, 900
SwDAM	200, 210, 700, 800, 900
SwSReu	200, 210, 290, 490, 700, 710, 800, 900
SwSConv	200, 290, 700, 900
SwBibl	210, 350, 520, 530, 540, 700, 800, 900
SwAud	491, 520, 530, 540, 900
SwADM	200, 210, 290, 350, 490, 491, 520, 530, 540, 700, 710, 800, 900
SwA1	301, 900
SwA5	302, 900
SwA6	303, 900
SwA7	304, 900
SwA8	220, 700, 900
SwA9	220, 700, 800, 900
SwA10	312, 360, 900
SwB	210, 220, 360, 700, 710, 800, 900
SwC	210, 360, 700, 800, 900
SwD	210, 220, 360, 700, 800, 900
SwEG	210, 220, 310, 311, 360, 700, 800, 900
SwF	210, 360, 700, 900
SwH	360, 900
SwTI	120, 700, 900
SwPoE	520, 530, 540, 900
SwSvInt	105, 110, 900
SwDMZ	100, 900

Fonte: Autoria própria.

3.2 CONFIGURAÇÃO DE VLANS

Existem três principais modos no *Internetwork Operation System*, no primeiro, indicado por um sinal de maior após o nome do dispositivo “>”, é o modo executivo do usuário, em que é possível apenas o uso do *ping*, alguns comandos *show* e o *enable*, que é o comando para passar ao segundo modo, que é o executivo

privilegiado, indicado pela cerquilha após o nome do dispositivo “#”, neste modo é permitido verificar as configurações do equipamento através dos comandos *show*, usar o *debug* para verificar a operação, salvar as configurações, recarregar o sistema, entre vários outros comandos, para passar ao modo de configuração global é necessário digitar “*configure terminal*”, indicado pelo (config)# após o nome do dispositivo, neste modo é feito a maioria das configurações além de permitir a passagem para modos de configuração específicos, como modo de configuração de *interface*. Como o IOS permite a abreviação dos comandos, muitos deles serão utilizados de forma abreviada.

3.2.1 Configuração dos switches de acesso

Para começar uma boa prática é dar um nome ao equipamento, para o qual se usa o comando “*hostname”*.

Tabela 3 – Mudar o nome do switch

Switch>**en**
Switch#**conf t**
Switch(config)#**hostname SwRA**

Fonte: Autoria própria.

A *interface gigabit* 0/1 é a que está conectada ao *switch* principal, portando deve ser configurada como *trunk* para permitir a passagem do tráfego das VLANs nele configuradas, além disso a VLAN nativa deve ser configurada na porta *trunk*. Para isso depois de entrar no modo de configuração da *interface* é necessário colocá-la no modo tronco, depois configurar a VLAN nativa e então quais as VLANs que serão permitidas no tronco. O comando *exit* é usado para voltar ao modo anterior.

Tabela 4 – Configurar a porta trunk

SwRA(config)**#int g0/1**
SwRA(config-if)**#swi mode trunk**
SwRA(config-if)**#swi trunk native vlan 99**
SwRA(config-if)**#swi trunk allowed vlan 210,490,700,800,900**
SwRA(config-if)**#ex**

Fonte: Autoria própria.

Para criar as VLANs basta digitar "*vlan*" e o número da mesma, após isso o *prompt* entra no modo de configuração da VLAN onde é possível nomeá-la.

Tabela 5 – Criar as VLANs

SwRA(config)**#vlan 210**
SwRA(config-vlan)**#name Taes**
SwRA(config-vlan)**#vlan 490**
SwRA(config-vlan)**#name Recepcao**
SwRA(config-vlan)**#vlan 700**
SwRA(config-vlan)**#name Voip**
SwRA(config-vlan)**#vlan 800**
SwRA(config-vlan)**#name Impressoras**
SwRA(config-vlan)**#vlan 900**
SwRA(config-vlan)**#name Gerencia**
SwRA(config-vlan)**#ex**

Fonte: Autoria própria.

Depois de criadas as VLANs é preciso atribuí-las às portas do *switch*, o que é feito no modo de configuração da *interface*. É possível configurar várias de uma vez utilizando o comando "*interface range*", então configura-se a *interface* para o modo de acesso e se atribuiu uma VLAN. Neste caso resolveu-se atribuir três *interfaces* para cada VLAN. No caso da VLAN para VoIP no comando *switchport* se indica que a VLAN é de voz.

Tabela 6 – Atribuir VLANs às portas

(continua)

SwRA(config)**#int range fa0/1 -3**
SwRA(config-if-range)**#swi mode access**
SwRA(config-if-range)**#swi access vlan 210**
SwRA(config-if-range)**#int range fa0/4 - 6**

Tabela 6 – Atribuir VLANs às portas

(conclusão)

```
SwRA(config-if-range)#swi mode access
SwRA(config-if-range)#swi access vlan 490
SwRA(config-if-range)#int range fa0/7 - 9
SwRA(config-if-range)#swi mode access
SwRA(config-if-range)#swi voice vlan 700
SwRA(config-if-range)#int range fa0/10 - 12
SwRA(config-if-range)#swi mode access
SwRA(config-if-range)#swi access vlan 800
SwRA(config-if-range)#ex
```

Fonte: Autoria própria.

A VLAN de gerência é usada para acesso ao equipamento através da rede, portanto a mesma não é configurada em uma porta física e sim em uma *interface* virtual, também chamada de SVI. Para isso primeiro é preciso criar a *interface* virtual através do "*interface* vlan", então adicionar um endereço IP e máscara de rede e ligar a interface com o comando "*no shutdown*".

Tabela 7 – Configurar SVI

```
SwRA(config)#int vlan 900
SwRA(config-if)#ip add 172.20.254.15 255.255.255.0
SwRA(config-if)#no shut
SwRA(config-if)#ex
```

Fonte: Autoria própria.

Para permitir que o *switch* seja gerenciado através de uma rede que não esteja diretamente conectada é necessário configurar o *gateway* padrão, que é o endereço do roteador ao qual o *switch* está conectado, e é o endereço pelo qual o *switch* encaminha as mensagens nele geradas.

Tabela 8 – Configurar o gateway

```
SwRA(config)#ip default-gateway 172.20.254.254
```

Fonte: Autoria própria.

Para verificar as VLANs é possível usar o comando *show* vlan.

```
SwRA#sh vlan

VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                                 Fa0/17, Fa0/18, Fa0/19, Fa0/20
                                                 Fa0/21, Fa0/22, Fa0/23, Fa0/24
                                                 Gig0/1, Gig0/2
210  Taes                              active    Fa0/1, Fa0/2, Fa0/3
490  Recepcao                          active    Fa0/4, Fa0/5, Fa0/6
700  Voip                              active    Fa0/7, Fa0/8, Fa0/9
800  Impressoras                       active    Fa0/10, Fa0/11, Fa0/12
900  Gerencia                          active
1002 fddi-default                      active
1003 token-ring-default                active
1004 fddinet-default                   active
1005 trnet-default                     active

VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------
1    enet  100001     1500  -      -      -        -    -        0      0
210  enet  100210     1500  -      -      -        -    -        0      0
490  enet  100490     1500  -      -      -        -    -        0      0
700  enet  100700     1500  -      -      -        -    -        0      0
800  enet  100800     1500  -      -      -        -    -        0      0
900  enet  100900     1500  -      -      -        -    -        0      0
1002 fddi  101002     1500  -      -      -        -    -        0      0
1003 tr    101003     1500  -      -      -        -    -        0      0
1004 fdnet 101004     1500  -      -      -        ieee -        0      0
1005 trnet 101005     1500  -      -      -        ibm  -        0      0

Remote SPAN VLANs
------------------------------------------------------------------------------

Primary Secondary Type              Ports
------- --------- ----------------- ------------------------------------------
SwRA#
```

Figura 12 – Show VLAN
Fonte: Autoria própria.

Como mostrado na figura, as portas as quais não foram atribuídas nenhuma VLAN, continuam na VLAN 1. Para evitar utilização indevida é possível desligar a *interface* com o comando *shutdown*.

Outro comando que pode ser usado para verificar as configurações feitas é o *show running-config*.

```
SwRA#sh runn
Building configuration...

Current configuration : 2018 bytes
!
version 12.2
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname SwRA
!
!
!
!
!
spanning-tree mode pvst
!
interface FastEthernet0/1
 switchport access vlan 210
 switchport mode access
!
interface FastEthernet0/2
 switchport access vlan 210
 switchport mode access
!
interface FastEthernet0/3
 switchport access vlan 210
 switchport mode access
!
interface FastEthernet0/4
 switchport access vlan 490
 switchport mode access
!
interface FastEthernet0/5
 switchport access vlan 490
 switchport mode access
!
interface FastEthernet0/6
 switchport access vlan 490
 switchport mode access
!
interface FastEthernet0/7
 switchport access vlan 700
 switchport mode access
!
interface FastEthernet0/8
 switchport access vlan 700
 switchport mode access
!
interface FastEthernet0/9
 switchport access vlan 700
 switchport mode access
!
interface FastEthernet0/10
 switchport access vlan 800
 switchport mode access
!
interface FastEthernet0/11
```

Figura 13 – Show running-config
Fonte: Autoria própria.

```
 switchport access vlan 800
 switchport mode access
!
interface FastEthernet0/12
 switchport access vlan 800
 switchport mode access
!
interface FastEthernet0/13
 shutdown
!
interface FastEthernet0/14
 shutdown
!
interface FastEthernet0/15
 shutdown
!
interface FastEthernet0/16
 shutdown
!
interface FastEthernet0/17
 shutdown
!
interface FastEthernet0/18
 shutdown
!
interface FastEthernet0/19
 shutdown
!
interface FastEthernet0/20
 shutdown
!
interface FastEthernet0/21
 shutdown
!
interface FastEthernet0/22
 shutdown
!
interface FastEthernet0/23
 shutdown
!
interface FastEthernet0/24
 shutdown
!
interface GigabitEthernet0/1
 switchport trunk native vlan 99
 switchport trunk allowed vlan 210,490,700,800,900
 switchport mode trunk
!
interface GigabitEthernet0/2
!
interface Vlan1
 no ip address
 shutdown
!
interface Vlan900
 mac-address 0002.162a.7301
 ip address 172.20.254.15 255.255.255.0
```

Figura 14 – Continuação show running-config
Fonte: Autoria própria.

Há ainda diversos outros comandos que podem ser utilizados para verificação.

3.2.2 Configuração do switch central

Para que as VLANs funcionem é necessário configurar também o equipamento que fará o roteamento entre as VLANs, neste caso um *switch* multicamada, também chamado de *switch layer* 3.

Tabela 9 – Mudar o nome do switch L3

Switch(config)**#hostname SwL3**

Fonte: Autoria própria.

Como esse é o *switch* que vai fazer o roteamento, todas as VLANs vão passar por ele, sendo necessário criar todas as VLANs.

Tabela 10 – Criar as VLANs no SwL3

(continua)

SwL3(config)**#vlan 100**
SwL3(config-vlan)**#name DMZ**
SwL3(config-vlan)**#vlan 105**
SwL3(config-vlan)**#name BD**
SwL3(config-vlan)**#vlan 110**
SwL3(config-vlan)**#name SvInt**
SwL3(config-vlan)**#vlan 120**
SwL3(config-vlan)**#name TI**
SwL3(config-vlan)**#vlan 200**
SwL3(config-vlan)**#name Direcao**
SwL3(config-vlan)**#vlan 210**
SwL3(config-vlan)**#name Taes**
SwL3(config-vlan)**#vlan 220**
SwL3(config-vlan)**#name Docentes**
SwL3(config-vlan)**#vlan 290**
SwL3(config-vlan)**#name Servidores**
SwL3(config-vlan)**#vlan 301**
SwL3(config-vlan)**#name A1**
SwL3(config-vlan)**#vlan 302**

Tabela 10 – Criar as VLANs no SwL3

(conclusão)

```
SwL3(config-vlan)#name A5
SwL3(config-vlan)#vlan 303
SwL3(config-vlan)#name A6
SwL3(config-vlan)#vlan 304
SwL3(config-vlan)#name A7
SwL3(config-vlan)#vlan 310
SwL3(config-vlan)#name Fisica
SwL3(config-vlan)#vlan 311
SwL3(config-vlan)#name Quimica
SwL3(config-vlan)#vlan 312
SwL3(config-vlan)#name Fios
SwL3(config-vlan)#vlan 350
SwL3(config-vlan)#name Biblioteca
SwL3(config-vlan)#vlan 360
SwL3(config-vlan)#name Salas_Aula
SwL3(config-vlan)#vlan 490
SwL3(config-vlan)#name Recepcao
SwL3(config-vlan)#vlan 491
SwL3(config-vlan)#name Auditorio
SwL3(config-vlan)#vlan 520
SwL3(config-vlan)#name Wifi_Adm
SwL3(config-vlan)#vlan 530
SwL3(config-vlan)#name Wifi_Alunos
SwL3(config-vlan)#vlan 540
SwL3(config-vlan)#name Wifi_Visitante
SwL3(config-vlan)#vlan 700
SwL3(config-vlan)#name Voip
SwL3(config-vlan)#vlan 710
SwL3(config-vlan)#name Videoconferencia
SwL3(config-vlan)#vlan 800
SwL3(config-vlan)#name Impressoras
SwL3(config-vlan)#vlan 900
SwL3(config-vlan)#name Gerencia
```

Fonte: Autoria própria.

Para cada VLAN é necessário uma *interface* virtual, com endereço IP configurado para servir de *gateway* para as VLANs. Nas *interfaces* que recebem requisição de DHCP é necessário adicionar o comando ip *helper-address* que permite o encaminhamento de mensagens de *broadcast* como as de requisição de endereço enviadas pelo DHCP para um endereço ip específico.

Tabela 11 – Configurar as SVIs no SwL3

(continua)

```
SwL3(config)#int vlan 100
SwL3(config-if)#ip add 172.20.1.1 255.255.255.0
SwL3(config-if)#int vlan 105
SwL3(config-if)#ip add 172.20.2.1 255.255.255.0
SwL3(config-if)#int vlan 110
SwL3(config-if)#ip add 172.20.3.1 255.255.255.0
SwL3(config-if)#int vlan 120
SwL3(config-if)#ip add 172.20.5.1 255.255.255.0
SwL3(config-if)#ip helper-address 172.20.0.1
SwL3(config-if)#int vlan 200
SwL3(config-if)#ip add 172.20.10.1 255.255.255.0
SwL3(config-if)#ip helper-address 172.20.0.1
SwL3(config-if)#int vlan 210
SwL3(config-if)#ip add 172.20.15.1 255.255.255.0
SwL3(config-if)#ip helper-address 172.20.0.1
SwL3(config-if)#int vlan 220
SwL3(config-if)#ip add 172.20.20.1 255.255.255.0
SwL3(config-if)#ip helper-address 172.20.0.1
SwL3(config-if)#int vlan 290
SwL3(config-if)#ip add 172.20.25.1 255.255.255.0
SwL3(config-if)#ip helper-address 172.20.0.1
SwL3(config-if)#int vlan 301
SwL3(config-if)#ip add 172.20.31.1 255.255.255.0
SwL3(config-if)#ip helper-address 172.20.0.1
SwL3(config-if)#int vlan 302
SwL3(config-if)#ip add 172.20.32.1 255.255.255.0
SwL3(config-if)#ip helper-address 172.20.0.1
SwL3(config-if)#int vlan 303
SwL3(config-if)#ip add 172.20.33.1 255.255.255.0
SwL3(config-if)#ip helper-address 172.20.0.1
SwL3(config-if)#int vlan 304
SwL3(config-if)#ip add 172.20.34.1 255.255.255.0
SwL3(config-if)#ip helper-address 172.20.0.1
SwL3(config-if)#int vlan 310
SwL3(config-if)#ip add 172.20.40.1 255.255.255.0
SwL3(config-if)#ip helper-address 172.20.0.1
SwL3(config-if)#int vlan 311
SwL3(config-if)#ip add 172.20.41.1 255.255.255.0
SwL3(config-if)#ip helper-address 172.20.0.1
SwL3(config-if)#int vlan 312
SwL3(config-if)#ip add 172.20.42.1 255.255.255.0
SwL3(config-if)#ip helper-address 172.20.0.1
SwL3(config-if)#int vlan 350
SwL3(config-if)#ip add 172.20.50.1 255.255.255.0
SwL3(config-if)#ip helper-address 172.20.0.1
SwL3(config-if)#int vlan 360
SwL3(config-if)#ip add 172.20.60.1 255.255.255.0
SwL3(config-if)#ip helper-address 172.20.0.1
SwL3(config-if)#int vlan 490
SwL3(config-if)#ip add 172.20.70.1 255.255.255.0
SwL3(config-if)#ip helper-address 172.20.0.1
SwL3(config-if)#int vlan 491
SwL3(config-if)#ip add 172.20.80.1 255.255.255.0
SwL3(config-if)#ip helper-address 172.20.0.1
```

Tabela 11 – Configurar as SVIs no SwL3

(conclusão)

```
SwL3(config-if)#int vlan 520
SwL3(config-if)#ip add 172.20.100.1 255.255.255.0
SwL3(config-if)#ip helper-address 172.20.0.1
SwL3(config-if)#int vlan 530
SwL3(config-if)#ip add 172.20.104.1 255.255.248.0
SwL3(config-if)#ip helper-address 172.20.0.1
SwL3(config-if)#int vlan 540
SwL3(config-if)#ip add 172.20.120.1 255.255.255.0
SwL3(config-if)#int vlan 700
SwL3(config-if)#ip add 172.20.140.1 255.255.255.0
SwL3(config-if)#int vlan 710
SwL3(config-if)#ip add 172.20.141.1 255.255.255.0
SwL3(config-if)#int vlan 800
SwL3(config-if)#ip add 172.20.150.1 255.255.255.0
SwL3(config-if)#int vlan 900
SwL3(config-if)#ip add 172.20.254.254 255.255.255.0
```

Fonte: Autoria própria.

Também é necessário configurar as portas que fazem ligação com os demais *switches*.

Tabela 12 – Configurar portas trunk no SwL3

(continua)

```
SwL3(config)#int fa0/1
SwL3(config-if)#swi mode trunk
SwL3(config-if)#swi trunk native vlan 99
SwL3(config-if)#swi trunk allowed vlan 200,210,290,350,490,491,520,530,540,700,710,800,900
SwL3(config-if)#int fa0/2
SwL3(config-if)#swi mode trunk
SwL3(config-if)#swi trunk native vlan 99
SwL3(config-if)#swi trunk allowed vlan 301,900
SwL3(config-if)#int fa0/3
SwL3(config-if)#swi mode trunk
SwL3(config-if)#swi trunk native vlan 99
SwL3(config-if)#swi trunk allowed vlan 302,900
SwL3(config-if)#int fa0/4
SwL3(config-if)#swi mode trunk
SwL3(config-if)#swi trunk native vlan 99
SwL3(config-if)#swi trunk allowed vlan 303,900
SwL3(config-if)#int fa0/5
SwL3(config-if)#swi mode trunk
SwL3(config-if)#swi trunk native vlan 99
SwL3(config-if)#swi trunk allowed vlan 304,900
SwL3(config-if)#int fa0/6
SwL3(config-if)#swi mode trunk
SwL3(config-if)#swi trunk native vlan 99
```

Tabela 12 – Configurar portas trunk no SwL3

(conclusão)

```
SwL3(config-if)#swi trunk allowed vlan 220,700,900
SwL3(config-if)#int fa0/7
SwL3(config-if)#swi mode trunk
SwL3(config-if)#swi trunk native vlan 99
SwL3(config-if)#swi trunk allowed vlan 220,700,800,900
SwL3(config-if)#int fa 0/8
SwL3(config-if)#swi mode trunk
SwL3(config-if)#swi trunk native vlan 99
SwL3(config-if)#swi trunk allowed vlan 312,360,900
SwL3(config-if)#int fa0/9
SwL3(config-if)#swi mode trunk
SwL3(config-if)#swi trunk native vlan 99
SwL3(config-if)#swi trunk allowed vlan 210,220,360,700,710,800,900
SwL3(config-if)#int fa0/10
SwL3(config-if)#swi mode trunk
SwL3(config-if)#swi trunk native vlan 99
SwL3(config-if)#swi trunk allowed vlan 210,360,700,800,900
SwL3(config-if)#int fa0/11
SwL3(config-if)#swi mode trunk
SwL3(config-if)#swi trunk native vlan 99
SwL3(config-if)#swi trunk allowed vlan 210,220,360,700,800,900
SwL3(config-if)#int fa0/12
SwL3(config-if)#swi mode trunk
SwL3(config-if)#swi trunk native vlan 99
SwL3(config-if)#swi trunk allowed vlan 210,220,310,311,360,700,800,900
SwL3(config-if)#int fa0/13
SwL3(config-if)#swi mode trunk
SwL3(config-if)#swi trunk native vlan 99
SwL3(config-if)#swi trunk allowed vlan 210,360,700,900
SwL3(config-if)#int fa0/14
SwL3(config-if)#swi mode trunk
SwL3(config-if)#swi trunk native vlan 99
SwL3(config-if)#swi trunk allowed vlan 360,900
SwL3(config-if)#int fa0/15
SwL3(config-if)#swi mode trunk
SwL3(config-if)#swi trunk native vlan 99
SwL3(config-if)#swi trunk allowed vlan 120,700,900
SwL3(config-if)#int fa0/16
SwL3(config-if)#swi mode trunk
SwL3(config-if)#swi trunk native vlan 99
SwL3(config-if)#swi trunk allowed vlan 520,530,540,900
SwL3(config-if)#int fa0/17
SwL3(config-if)#swi mode trunk
SwL3(config-if)#swi trunk native vlan 99
SwL3(config-if)#swi trunk allowed vlan 105,110,900
```

Fonte: Autoria própria.

A função de roteamento não vem ativada por padrão, para ativá-la é necessário o comando “ip *routing*”.

Tabela 13 – Ativar o roteamento no SwL3

SwL3(config)**#ip routing**

Fonte: Autoria própria.

Para que o *switch* possa encaminhar o tráfego com destino externo é necessário configurar uma porta como porta roteada para que passe a se comportar como uma porta de roteador, o que deve ser feito através do comando “no *switchport*, após é preciso configurar um endereço IP para a mesma.

Tabela 14 – Configurar porta roteada no SwL3

SwL3(config)**#int g0/1** SwL3(config-if)**#no swi** SwL3(config-if)**#ip add 172.20.0.2 255.255.255.0** SwL3(config-if)**#no shut**

Fonte: Autoria própria.

Além disso é preciso configurar uma rota padrão, que é a que diz para onde encaminhar qualquer pacote cujo destino não seja uma rede diretamente conectada. Para configurar rotas se usa o comando “ip *route*” seguido do endereço da rede de destino e sua máscara e o IP do próximo salto ou a interface de saída, para rota padrão se usa máscara e endereço “0.0.0.0”.

Tabela 15 – Configurar rota padrão no SwL3

SwL3(config)**#ip route 0.0.0.0 0.0.0.0 172.20.0.1**

Fonte: Autoria própria.

É possível verificar as rotas através do comando “*show* ip *route*”.

```
SwL3#sh ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS
inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is 172.20.0.1 to network 0.0.0.0

     172.20.0.0/16 is variably subnetted, 26 subnets, 2 masks
C       172.20.0.0/24 is directly connected, GigabitEthernet0/1
C       172.20.2.0/24 is directly connected, Vlan105
C       172.20.3.0/24 is directly connected, Vlan110
C       172.20.5.0/24 is directly connected, Vlan120
C       172.20.10.0/24 is directly connected, Vlan200
C       172.20.15.0/24 is directly connected, Vlan210
C       172.20.20.0/24 is directly connected, Vlan220
C       172.20.25.0/24 is directly connected, Vlan290
C       172.20.31.0/24 is directly connected, Vlan301
C       172.20.32.0/24 is directly connected, Vlan302
C       172.20.33.0/24 is directly connected, Vlan303
C       172.20.34.0/24 is directly connected, Vlan304
C       172.20.40.0/24 is directly connected, Vlan310
C       172.20.41.0/24 is directly connected, Vlan311
C       172.20.42.0/24 is directly connected, Vlan312
C       172.20.50.0/24 is directly connected, Vlan350
C       172.20.60.0/24 is directly connected, Vlan360
C       172.20.70.0/24 is directly connected, Vlan490
C       172.20.80.0/24 is directly connected, Vlan491
C       172.20.100.0/24 is directly connected, Vlan520
C       172.20.104.0/21 is directly connected, Vlan530
C       172.20.120.0/24 is directly connected, Vlan540
C       172.20.140.0/24 is directly connected, Vlan700
C       172.20.141.0/24 is directly connected, Vlan710
C       172.20.150.0/24 is directly connected, Vlan800
C       172.20.254.0/24 is directly connected, Vlan900
S*   0.0.0.0/0 [1/0] via 172.20.0.1

SwL3#
```

Figura 15 – Tabela de roteamento do SwL3
Fonte: Autoria própria.

3.2.1 Configuração do roteador

Para que todas essas VLANs possam se comunicar com as redes externas é necessário também configurar o roteador. Além da rota padrão é necessário que o roteador consiga encaminhar o tráfego externo para o *switch* encaminhar para as VLANs o que pode ser feito sumarizando as redes em uma única rota /16.

Tabela 16 – Configurar rota padrão no roteador

Router(config)**#ip route 172.20.0.0 255.255.0.0 172.20.0.2**
Router(config)**#ip route 0.0.0.0 0.0.0.0 200.0.0.1**

Fonte: Autoria própria.

Também é necessário configurar a DMZ que é o local da rede onde ficarão os servidores que necessitam ficar abertos ao acesso externo, como os onde ficam as páginas web e por isso são conectados a uma interface diferente do roteador.

Tabela 17 – Configurar a DMZ no roteador

```
Router(config)#int g0/1
Router(config-if)#no shut
Router(config-if)#ex
Router(config)#int g0/1.100
Router(config-subif)#encap dot1q 100
Router(config-subif)#ip add 172.20.1.1 255.255.255.0
Router(config-subif)#ex
```

Fonte: Autoria própria.

Ao verificar a tabela de roteamento do roteador é possível ver a rota para as redes internas que foi configurada manualmente, as três interfaces diretamente conectadas e a rota padrão.

```
Router#sh ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is 200.0.0.1 to network 0.0.0.0

     172.20.0.0/16 is variably subnetted, 5 subnets, 3 masks
S       172.20.0.0/16 [1/0] via 172.20.0.2
C       172.20.0.0/24 is directly connected, GigabitEthernet0/2
L       172.20.0.1/32 is directly connected, GigabitEthernet0/2
C       172.20.1.0/24 is directly connected, GigabitEthernet0/1.1
L       172.20.1.1/32 is directly connected, GigabitEthernet0/1.1
     200.0.0.0/24 is variably subnetted, 2 subnets, 2 masks
C       200.0.0.0/24 is directly connected, GigabitEthernet0/0
L       200.0.0.2/32 is directly connected, GigabitEthernet0/0
S*   0.0.0.0/0 [1/0] via 200.0.0.1

Router#
```

Figura 16 – Tabela de Roteamento do Roteador
Fonte: Autoria própria

Para que os computadores obtenham um endereço ip automaticamente é necessário ter um servidor de DHCP, é preciso configurar uma instância para cada

VLAN, o que pode ser feito no roteador ou em algum computador. Neste caso foi feita a configuração no roteador. Para configurar o roteador como servidor de DHCP é necessário criar um pool de endereços e definir qual o endereço e máscara serão alocados e qual será o roteador padrão, é recomendável definir alguns endereços como reservados, o que pode ser feito através do comando “ip dhcp *excluded-address*”, e é possível também definir o endereço do servidor DNS.

Tabela 18 – Configurar o DHCP

```
Router(config)#ip dhcp excluded-address 172.20.31.1 172.20.31.5
Router(config)#ip dhcp pool A1
Router(dhcp-config)#net 172.20.31.0 255.255.255.0
Router(dhcp-config)#default-router 172.20.31.1
Router(dhcp-config)#dns-server 172.20.1.2
Router(dhcp-config)#end
```

Fonte: Autoria própria.

Para que os computadores da rede interna sejam capazes de se comunicar com a Internet é necessário ainda configurar o NAT no roteador. Para isso é necessário criar um *pool* de endereços públicos, criar uma *access list* que dê permissão para os computadores da rede interna e associar o *pool* com a *access list* criada, a palavra “*overload*” é a que ativa a sobrecarga de NAT, e é necessário identificar com os comandos ip nat *inside* e ip nat *outside* quais são as interfaces ligadas à rede interna e externa.

Tabela 19 – Configurar o NAT

```
Router(config)#ip nat pool POOL-NAT 200.0.0.50 200.0.0.254 netmask 255.255.255.0
Router(config)#access-list 1 permit 172.20.0.0 0.0.255.255
Router(config)#ip nat inside source list 1 pool POOL-NAT overload
Router(config)#int g0/2
Router(config-if)#ip nat inside
Router(config-if)#ex
Router(config)#int g0/0
Router(config-if)#ip nat outside
```

Fonte: Autoria própria.

3.3 CONFIGURAÇÃO DE IPv6

O Packet tracer possui algumas limitações e nele o switch 3560 não aceita comandos para a configuração de IPv6, por isso, erá utilizado no lugar um roteador 2911.

Os roteadores não vem com o roteamento para IPv6 habilitado por padrão, para habilitá-lo é necessário utilizar o comando “IPv6 *unicast-routing*”.

Tabela 20 – Habilitar o roteamento IPv6

Router(config)**#ipv6 unicast-routing**

Fonte: Autoria própria.

Para configurar a rota padrão IPv6 o comando é o “ipv6 route”.

Tabela 21 – Configurar rota padrão IPv6 no roteador

Router(config)**#ipv6 route ::/0 2001:DB8:200::1**

Fonte: Autoria própria.

Na interface que irá se comunicar com o roteador do provedor é necessário configurar um endereço IPv6 o que deve ser feito com o comando “IPv6 add”.

Tabela 22 – Adicionar o endereço IPv6 na interface

Router(config)**#int g0/0** Router(config-if)**#ipv6 add 2001:db8:200::2/64**

Fonte: Autoria própria.

Com o endereço e o roteamento configurado no roteador, resta apenas configurar o DHCP, que será utilizado apenas para distribuir o endereço do DNS. Para configurar o DHCP stateless é necessário criar um pool e, neste caso, configurar o endereço do servidor de DNS e dentro da subinterface da VLAN, além das configurações de endereçamento, indicar o pool de DHCP e o comando “IPv6 nd other-config-flag” que é o que indica que a mensagem de anúncio do roteador deve conter instruções para se utilizar configurações adicionais de um servidor de DHCP.

Tabela 23 – Habilitar o DHCP para IPv6

```
Router(config)#ipv6 dhcp pool POOL_IPv6
Router(config-dhcpv6)#dns-server 2001:db8:1f5c:100::2
Router(config-dhcpv6)#ex
Router(config)#int g0/1
Router(config-if)#no shut
Router(config-if)#int g0/1.301
Router(config-subif)#encap dot1q 301
Router(config-subif)#ip add 172.20.31.1 255.255.255.0
Router(config-subif)#ipv6 add 2001:db8:1f5c:301::1/64
Router(config-subif)#ipv6 dhcp server POOL_IPv6
Router(config-subif)#ipv6 nd other-config-flag
Router(config-subif)#ex
```

Fonte: Autoria própria.

3.4 TESTES DE CONECTIVIDADE

Após feitas as configurações no SwL3 e nos demais switches já é possível que computadores em VLANs diferentes conversem entre si. Para fins de teste foram conectados alguns computadores, sendo três no SwF, dois deles nas portas pertencentes à VLAN 210, configurados com os ips 172.20.15.6 e 172.20.15.7, e um na em uma porta pertencente à VLAN 360, um computador com o ip 172.20.60.7, um computador em uma porta pertencente à VLAN 210 no SwD, com o ip 172.20.15.10 e um computador no SwEG, em uma porta pertencente à VLAN 360 com o ip 172.20.60.10, para realização de testes com *ping* e *tracert*.

```
C:\>ping 172.20.15.7

Pinging 172.20.15.7 with 32 bytes of data:

Reply from 172.20.15.7: bytes=32 time=1ms TTL=128
Reply from 172.20.15.7: bytes=32 time<1ms TTL=128
Reply from 172.20.15.7: bytes=32 time<1ms TTL=128
Reply from 172.20.15.7: bytes=32 time<1ms TTL=128

Ping statistics for 172.20.15.7:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>ping 172.20.15.10

Pinging 172.20.15.10 with 32 bytes of data:

Reply from 172.20.15.10: bytes=32 time<1ms TTL=128
Reply from 172.20.15.10: bytes=32 time<1ms TTL=128
Reply from 172.20.15.10: bytes=32 time<1ms TTL=128
Reply from 172.20.15.10: bytes=32 time=14ms TTL=128

Ping statistics for 172.20.15.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 14ms, Average = 3ms

C:\>ping 172.20.60.7

Pinging 172.20.60.7 with 32 bytes of data:

Reply from 172.20.60.7: bytes=32 time=4ms TTL=127
Reply from 172.20.60.7: bytes=32 time<1ms TTL=127
Reply from 172.20.60.7: bytes=32 time<1ms TTL=127
Reply from 172.20.60.7: bytes=32 time<1ms TTL=127

Ping statistics for 172.20.60.7:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 4ms, Average = 1ms

C:\>ping 172.20.60.10

Pinging 172.20.60.10 with 32 bytes of data:

Reply from 172.20.60.10: bytes=32 time<1ms TTL=127
Reply from 172.20.60.10: bytes=32 time<1ms TTL=127
Reply from 172.20.60.10: bytes=32 time<1ms TTL=127
Reply from 172.20.60.10: bytes=32 time<1ms TTL=127

Ping statistics for 172.20.60.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Figura 17 – Teste de conectividade usando o ping
Fonte: Autoria própria.

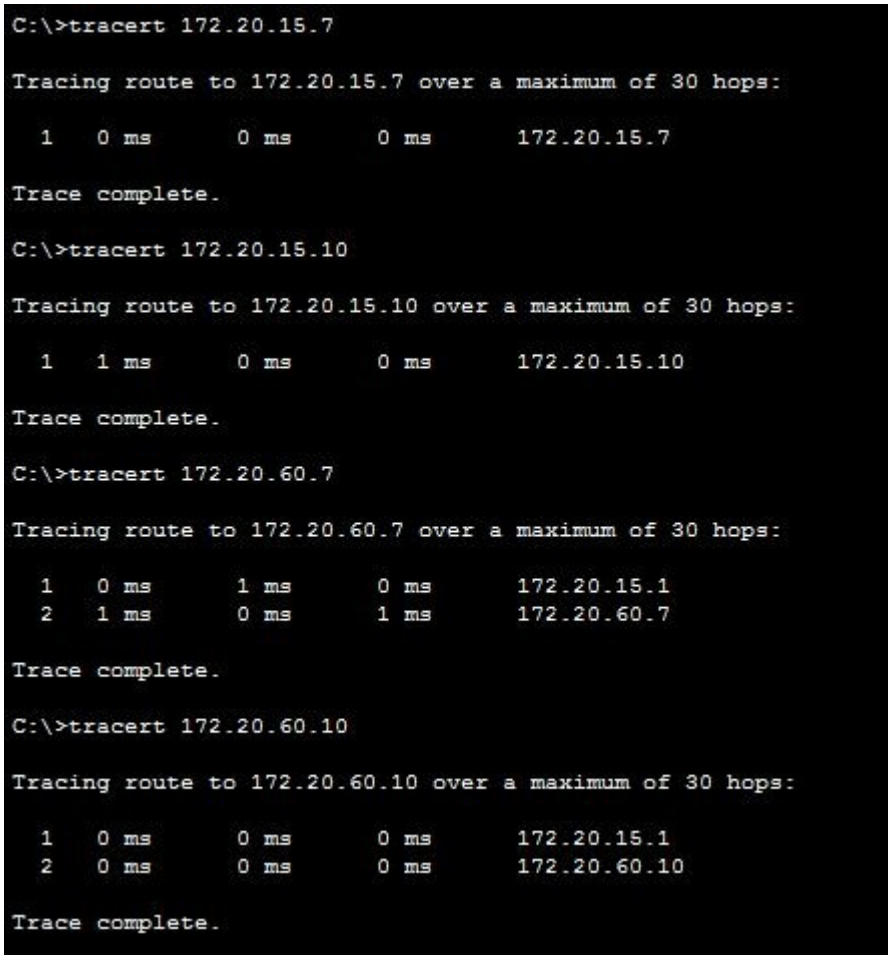

Figura 18 – Teste de conectividade usando tracert
Fonte: Autoria própria.

Nas saídas dos comandos *tracert* é possível notar que para os pacotes com destino a um computador de outro *switch*, o que torna necessário a ida do mesmo até o SwL3, apenas um salto é necessário, já para pacotes com destino a computadores de outra VLAN, mesmo que conectados no mesmo *switch* é necessário passar por roteamento.

É possível também testar a conectividade diretamente do *prompt* do *switch*. No exemplo mostrado na figura 17 a seguir, foram usados os comandos *ping* e *traceroute* no SwBibl para testar a conectividade à SVI da Vlan de gerência do SwC e a um computador conectado ao SwA1 em que todas as portas com exceção do tronco foram designadas para a VLAN 301.

```
SwBibl#ping 172.20.254.10

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.20.254.10, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/1 ms

SwBibl#ping 172.20.31.10

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.20.31.10, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/1 ms

SwBibl#traceroute 172.20.254.10
Type escape sequence to abort.
Tracing the route to 172.20.254.10

  1   172.20.254.10   10 msec   0 msec    0 msec
SwBibl#traceroute 172.20.31.10
Type escape sequence to abort.
Tracing the route to 172.20.31.10

  1   172.20.254.254  0 msec    0 msec    0 msec
  2   172.20.31.10    0 msec    0 msec    0 msec
SwBibl#
```

Figura 19– Teste de conectividade do SwBibl
Fonte: Autoria própria.

Para fins de teste um segundo roteador foi conectado para simular uma rede externa e configurado com o ip 200.0.0.1. Para verificar foi usado o comando *tracert* a partir de um computador conectado à VLAN 301, no SwA1.

```
C:\>tracert 200.0.0.1

Tracing route to 200.0.0.1 over a maximum of 30 hops:

  1    0 ms      0 ms      0 ms      172.20.31.1
  2    0 ms      1 ms      0 ms      172.20.0.1
  3    0 ms      0 ms      0 ms      200.0.0.1

Trace complete.
```

Figura 20 – Teste com tracert para rede externa
Fonte: Autoria própria.

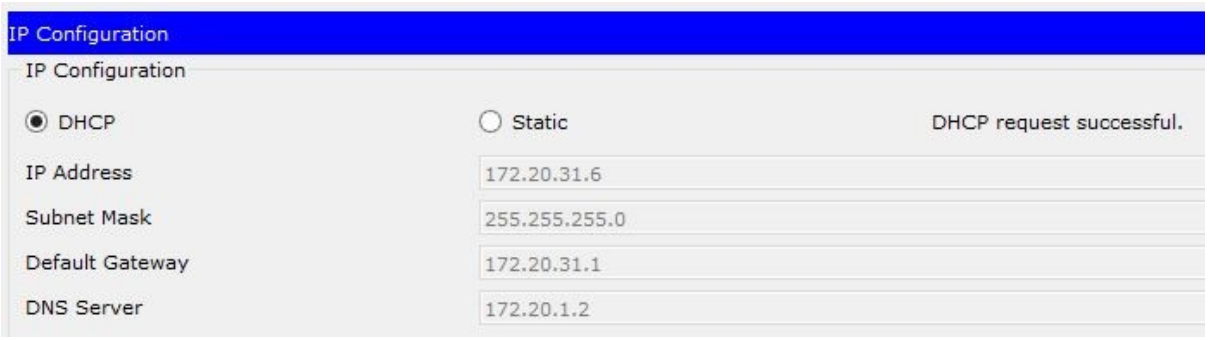

Figura 21 – Computador recebe endereço via DHCP
Fonte: Autoria própria.

Após feita a configuração do DHCP, na figura 21, é possível verificar no computador o recebimento do endereço IPv4, na figura 22 mostra o recebimento dos endereços depois de feita a configuração do DHCPv6.

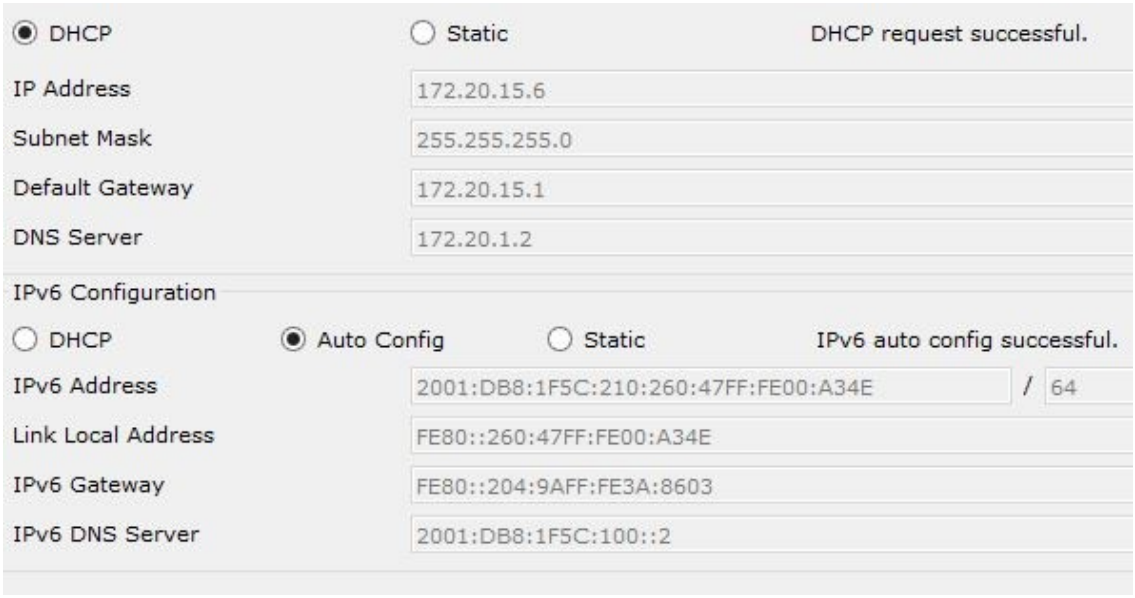

Figura 22 – Teste de DHCP e DHCPv6
Fonte: Autoria própria.

Após feitas as configurações foi colocado um computador na VLAN 210 no SwRa, que recebeu as configurações mostradas na figura acima. Para testar a conectividade foi usado o comando tracert para o endereço IPv4 e para o endereço IPv6. Na figura 23 é mostrado um teste de conectividade a um computador no SwBibl pertencente à mesma VLAN, na figura 24 foi testado a conexão a um

computador na VLAN 301 no SwA1 e na figura 25 ao roteador que representa as redes externas.

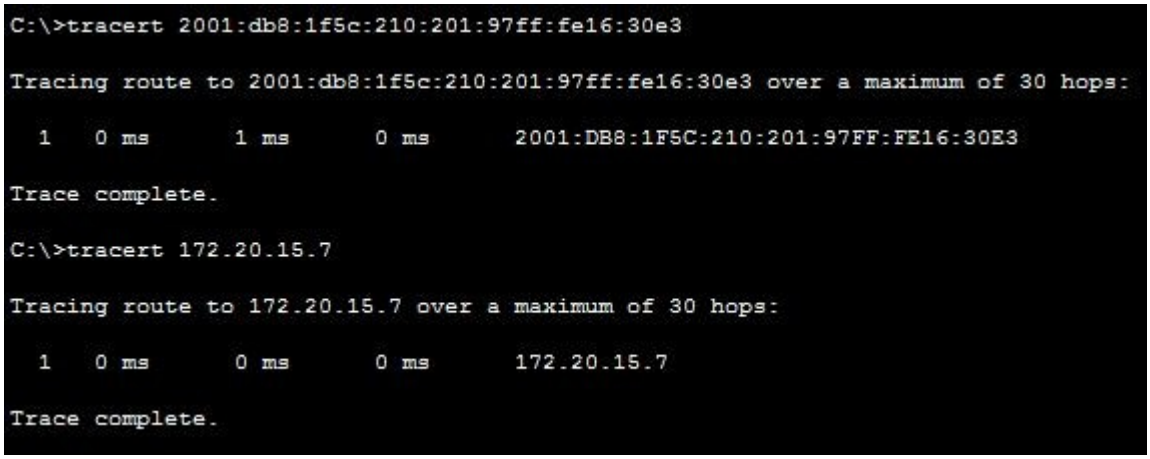

Figura 23 – Teste com tracert na mesma VLAN
Fonte: Autoria própria.

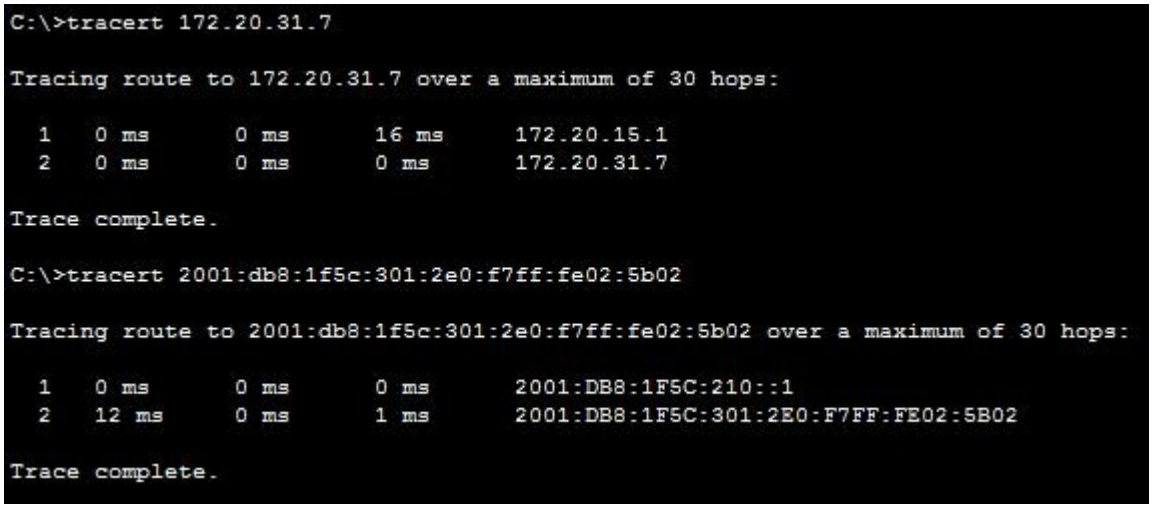

Figura 24 – Teste com tracert para VLAN diferente
Fonte: Autoria própria.

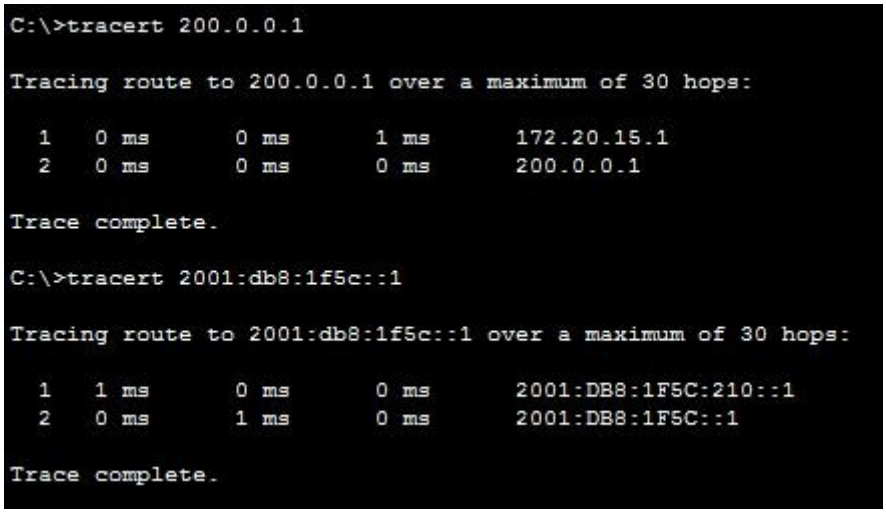

Figura 25 – Teste com tracert para roteador externo
Fonte: Autoria própria.

4 CONSIDERAÇÕES FINAIS

Após feitos os testes de conectividade, onde se pode ver que foram executados com sucesso, conclui-se que na simulação os objetivos gerais e específicos foram alcançados, mas como o *Packet Tracer* possui limitações, serão necessárias algumas mudanças ao aplicar nos equipamentos reais, como o switch 2960-X recebido pelo campus e em outros, já empenhados mas ainda não recebidos, de modo que o campus possa estar habilitado a acessar redes apenas IPv6.

Com a implementação da nova rede os problemas recorrentes de lentidão e as dificuldades de gerenciamento deverão ser sanados e problemas como um *loop* de rede em um *hub* que deixou o campus inteiro sem internet toda uma manhã não deverão voltar a acontecer, pois com a divisão em VLANs, os problemas ficarão restritos a apenas uma parte da rede, tornando-os fáceis de localizá-los e resolvê-los rapidamente, além de facilitar a implementação de políticas de segurança diferenciadas para os diversos públicos, de modo a impedir acessos indevidos entre os mesmos e acesso a conteúdo ilegal.

Outras configurações que não entraram no escopo deste trabalho e poderiam ser feitas em um trabalho futuro incluem configurações a serem feitas em outros equipamentos, como servidor de DNS, configurações de segurança dos equipamentos, como criptografia e usuários e senhas de acesso, que podem ser feitas manualmente em cada ou através de um servidor de autenticação, e configurações de controle de acesso, para definir as diferentes permissões para cada VLAN, que podem e/ou devem ser feitas, conforme as necessidades, no swittch multicamada, no roteador, num equipamento específico para *firewall* como o Cisco ASA 5505, utilizado no campus Jaraguá e alguns outros, ou ainda num serviço de firewall baseado em linux como o PfSense, utilizado em alguns outros campi.

REFERÊNCIAS BIBLIOGRÁFICAS

ACADEMIA CISCO. **CCNA.** Disponível em<http://cisco.ct.utfpr.edu.br/material/CCNA/2%20-%20Conceitos%20Essenciais%20de%20Roteamento%20e%20Switching/#3> Acesso em 29/10/2016.

ACADEMIA CISCO. **CCNA.** Disponível em<http://cisco.ct.utfpr.edu.br/material/CCNA/2%20-%20Conceitos%20Essenciais%20de%20Roteamento%20e%20Switching/#3.1.1.2> Acesso em 30/10/2016.

ACADEMIA CISCO. **CCNA.** Disponível em<http://cisco.ct.utfpr.edu.br/material/CCNA/2%20-%20Conceitos%20Essenciais%20de%20Roteamento%20e%20Switching/#3.1.2.3> Acesso em 30/10/2016.

ACADEMIA CISCO. **CCNA.** Disponível em<http://cisco.ct.utfpr.edu.br/material/CCNA/4%20-%20Conex%c3%a3o%20de%20Rede/#5.1.2.5> Acesso em 17/09/2016.

ACADEMIA CISCO. **CCNA.** Disponível em<http://cisco.ct.utfpr.edu.br/material/CCNA/2%20-%20Conceitos%20Essenciais%20de%20Roteamento%20e%20Switching/#10> Acesso em 12/11/2016.

DEFENSE Advanced Research Projects Agency. **Internet Protocol: Darpa Internet Program Protocol Specification.** Disponível em <https://tools.ietf.org/rfc/rfc791.txt>. Acesso em 02/09/2016.

IEEE Computer Society. LAN MAN Standards Committee. **IEEE Standards for Local and Metropolitan Area Networks: Bridges and Bridged Networks.** New York, 2014. 1832 p. Disponível em <http://standards.ieee.org/getieee802/download/802-1Q-2014.pdf> Acesso em 29/10/2016.

INTERNET Engineering Task Force (IETF). **464XLAT: Combination of Stateful and Stateless Translation.** Disponível em <https://tools.ietf.org/rfc/rfc6877.txt>. Acesso em 05/11/2016.

INTERNET Engineering Task Force (IETF). **A Discard Prefix for IPv6.** Disponível em <https://tools.ietf.org/rfc/rfc6666.txt>. Acesso em 29/10/2016.

INTERNET Engineering Task Force (IETF). **An Incremental Carrier-Grade NAT (CGN) for IPv6 Transition.** Disponível em <https://www.ietf.org/rfc/rfc6264.txt>. Acesso em 30/10/2016.

INTERNET Engineering Task Force (IETF). **A Recommendation for IPv6 Address Text Representation.** Disponível em <https://tools.ietf.org/rfc/rfc5952.txt>. Acesso em 08/10/2016.

INTERNET Engineering Task Force (IETF). **Dual-Stack Lite Broadband Deployments Folloeing IPv4 Exhaustion.** Disponível em <https://tools.ietf.org/rfc/rfc6333txt>. Acesso em 07/11/2016.

INTERNET Engineering Task Force (IETF). **Guidelines for Using IPv6 Transition Mechanisms During IPv6 Deployment.** Disponível em <https://tools.ietf.org/rfc/rfc6180.txt>. Acesso em 07/11/2016.

INTERNET Engineering Task Force (IETF). **IANA IPv4 Special Pourpose Address Registry.** Disponível em <https://tools.ietf.org/rfc/rfc5736.txt>. Acesso em 29/09/2016.

INTERNET Engineering Task Force (IETF). **IANA-Reserved IPv4 Prefix for Shared Address Space.** Disponível em <https://tools.ietf.org/rfc/rfc6598.txt>. Acesso em 28/09/2016.

INTERNET Engineering Task Force (IETF). **IPv6 Addressing of IPv4/IPv6 Translators.** Disponível em <https://tools.ietf.org/rfc/rfc6052.txt>. Acesso em 30/10/2016.

INTERNET Engineering Task Force (IETF). **Special-Purpose IP Address Registries.** Disponível em <https://tools.ietf.org/rfc/rfc6890.txt>. Acesso em 23/10/2016.

NETWORK Working Group. **Address Allocation for Private Internets.** Disponível em <https://tools.ietf.org/rfc/rfc1918.txt>. Acesso em 22/09/2016.

NETWORK Working Group. **Administration of the IANA Special Purpose IPv6**

Address Block. Disponível em <https://tools.ietf.org/rfc/rfc4773.txt>. Acesso em 29/10/2016.

NETWORK Working Group. **An Anycast Prefix for 6to4 Relay Routers.** Disponível em <https://tools.ietf.org/rfc/rfc3068.txt>. Acesso em 28/10/2016.

NETWORK Working Group. **An IPv6 Prefix for Overlay Routable Cryptographic Hash Identifiers (ORCHID).** Disponível em <https://tools.ietf.org/rfc/rfc4843.txt>. Acesso em 27/10/2016.

NETWORK Working Group. **Assigned Numbers.** Disponível em <https://tools.ietf.org/rfc/rfc790.txt>. Acesso em 03/09/2016.

NETWORK Working Group. **Basic Transition Mechanisms for IPv6 Hosts and Routers.** Disponível em <https://tools.ietf.org/rfc/rfc4213.txt>. Acesso em 01/11/2016.

NETWORK Working Group. **Benchmarking Methodology for Network Interconnect Devices.** Disponível em <https://tools.ietf.org/rfc/rfc2544.txt>. Acesso em 27/09/2016.

NETWORK Working Group. **Broadcasting Internet Datagrams.** Disponível em <https://tools.ietf.org/rfc/rfc0919.txt>. Acesso em 27/09/2016.

NETWORK Working Group. **Classless Inter-Domain Routing (CIDR): an Address Assignment and Aggregation Strategy.** Disponível em <https://tools.ietf.org/rfc/rfc1519.txt>. Acesso em 07/09/2016.

NETWORK Working Group. **Classless Inter-Domain Routing (CIDR): The Internet Address Assignment and Aggregation Plan.** Disponível em <https://tools.ietf.org/rfc/rfc4632.txt>. Acesso em 08/09/2016.

NETWORK Working Group. **Connection of IPv6 Domains via IPv4 Clouds.** Disponível em <https://www.ietf.org/rfc/rfc3056.txt>. Acesso em 02/11/2016.

NETWORK Working Group. **Dynamic Configuration of IPv4 Link-Local Addresses.** Disponível em <https://tools.ietf.org/rfc/rfc3927.txt>. Acesso em 28/09/2016.

NETWORK Working Group. **Dynamic Host Configuration Protocol.** Disponível em <https://tools.ietf.org/rfc/rfc1541.txt>. Acesso em 15/09/2016.

NETWORK Working Group. **Dynamic Host Configuration Protocol for IPv6 (DHCPv6).** Disponível em <https://www.ietf.org/rfc/rfc3315.txt>. Acesso em 12/11/2016.

NETWORK Working Group. **Host Extensions for IP Multicasting.** Disponível em <https://tools.ietf.org/rfc/rfc1112.txt>. Acesso em 28/09/2016.

NETWORK Working Group. **IANA Guidelines for IPv4 Multicast Address Assignments.** Disponível em <https://tools.ietf.org/rfc/rfc3171.txt>. Acesso em 26/09/2016.

NETWORK Working Group. **Internet Protocol, Version 6 (IPv6) Specification.** Disponível em <https://tools.ietf.org/rfc/rfc1883.txt>. Acesso em 02/10/2016.

NETWORK Working Group. **Internet Protocol, Version 6 (IPv6) Specification.** Disponível em <https://www.ietf.org/rfc/rfc2460.txt>. Acesso em 02/10/2016.

NETWORK Working Group. **IPv6 Address Prefix Reserved for Documentation.** Disponível em <https://tools.ietf.org/rfc/rfc3849.txt>. Acesso em 25/11/2016.

NETWORK Working Group. **IPv6 Benchmarking Methodology for Network Interconnect Devices.** Disponível em <https://www.ietf.org/rfc/rfc5180.txt>. Acesso em 28/109/2016.

NETWORK Working Group. **IP Version 6 Addressing Architecture.** Disponível em <https://tools.ietf.org/rfc/rfc1884.txt>. Acesso em 07/10/2016.

NETWORK Working Group. **IP Version 6 Addressing Architecture.** Disponível em <https://tools.ietf.org/rfc/rfc4291.txt>. Acesso em 08/10/2016.

NETWORK Working Group. **Special-Use IPv4 Addresses.** Disponível em <https://tools.ietf.org/rfc/rfc3330.txt>. Acesso em 23/09/2016.

NETWORK Working Group. **Teredo: Tunneling IPv6 over UDP through Network Address Translations (NATs).** Disponível em <https://tools.ietf.org/rfc/rfc4380.txt>. Acesso em 29/10/2016.

NETWORK Working Group. **The IP Network Address Translator (NAT).** Disponível em <https://www.ietf.org/rfc/rfc1631.txt>. Acesso em 17/09/2016.

NETWORK Working Group. **Traditional IP Network Address Translator (Traditional NAT).** Disponível em <https://www.ietf.org/rfc/rfc3022.txt>. Acesso em 17/09/2016.

NETWORK Working Group. **Transition Mechanisms for IPv6 Hosts and Routers.** Disponível em <https://tools.ietf.org/rfc/rfc1933.txt>. Acesso em 14/10/2016.

NETWORK Working Group. **Unique Local IPv6 Unicast Addresses.** Disponível em <https://tools.ietf.org/rfc/rfc4193.txt>. Acesso em 30/10/2016.

NIC.BR. Equipe IPv6.br. **Laboratório de IPv6: aprenda na prática usando um emulador de redes.** São Paulo: Novatec, 2015. 417 p.

NÚCLEO de Informação e Coordenação do Ponto BR. **Introdução.** Disponível em <http://IPv6.br/post/introducao/>. Acesso em 20/08/2016.

NÚCLEO de Informação e Coordenação do Ponto BR. **Previsão de esgotamento de endereços IPv4 nos RIR.** Disponível em <http://www.potaroo.net/tools/IPv4/plotend.png>. Acesso em 01/07/2016.

ANEXO A – PROJETO VLAN

4. MODELO FINAL

O modelo oficial de VLANs do IFSC, segue um padrão composto basicamente por 3 (três) dígitos, os quais se desdobram para oferecer uma estrutura escalável e ao mesmo tempo simples em termos administrativos. Abaixo é apresentado significado de cada dígito identificador:

ID	DESCRIÇÃO
Z . .	Dígito Identificador do Grupo Principal
. x .	Dígito que identifica uma subdivisão em blocos, porém limitados ao escopo do grupo principal.
. . y	Subdivisão do bloco

Tabela 01 – Dígitos identificadores

O “Dígito Identificador Principal” define os macro-grupos utilizados para a segmentação hierarquizada do modelo oficial, conforme segue comentado logo abaixo:

ID	GRUPO PRINCIPAL
0 x y	Enlaces
1 x y	DMZ, Servers, T.I.C.
2 x y	Administrativo
3 x y	Academico
4 x y	Academico & Visitante
5 x y	Wireless
6 x y	CFTV
7 x y	VoIP
8 x y	Impressora
9 x y	Gerencia

Tabela 02 – Modelo resumido