Aprimorando o desempenho e a segurança das redes locais universitárias com a utilização das técnicas de VLAN

Ciro Ferreira de Carvalho Júnior Correio
Instituto Federal de Educação, Ciência e Tecnologia do Tocantins (IFTO)
(cirofcjr@ifto.edu.br)

Kely Rejane Souza dos Anjos de Carvalho Correio
Universidade Federal do Tocantins (UFT)
(kelyrejanecarvalho@gmail.com)

Resumo: Este trabalho consiste em apresentar as características de uma rede de computadores de abrangência local (LAN), assim como também demonstrar o funcionamento de uma Rede Local Virtual – VLAN e mostrar até que ponto as VLANs podem melhorar ou não no desempenho e na segurança de uma rede local corporativa ou universitária. Foi realizado um levantamento bibliográfico para fundamentar e embasar o entendimento de redes locais (LAN) e redes locais virtuais (VLAN), tornando possível ao leitor entender melhor o conceito e funcionamento destas redes. Para a realização deste artigo foram utilizados dois switches da marca 3com com suporte ao protocolo VLAN e um computador, denominado Servidor com o Sistema Operacional – Debian. Ao final, os resultados obtidos foram satisfatórios, uma vez que foram verificadas melhorias gerais de desempenho ao reduzir significativamente o domínio de broadcast, e também melhorias na segurança da informação ao segmentar logicamente os usuários por grupos ou funções, podendo inclusive criar regras de acesso para cada rede virtual entre si ou entre as redes virtuais e a Internet, por meio de um *firewall*.

Palavras-chave: VLAN; protocolo 802.1q; switch, rede local.

Abstract: This paper aims to present the characteristics of a local area network (LAN), as well as demonstrate the operation of a Virtual Local Area Network (VLAN) and show the extent to which VLANs can improve performance and security of a VLAN corporate or university local network. A bibliographic survey was carried out to support the understanding of local area networks (LAN) and local virtual networks (VLANs), making it possible for the reader to better understand the concept and functioning of these networks. To accomplish the objective of this article, it were used two switches of the mark 3com with support to VLAN protocol and a computer, denominated Server with the Operating System - Debian. Ultimately,, the results were satisfactory, since general performance improvements were verified by significantly reducing the broadcast domain, as well as improvements in information security by logically segmenting users by groups or functions, and might even create access rules for each virtual network to each other or between virtual networks and the Internet, through a firewall.

Keywords: VLAN; protocol 802.1q; switch, LAN.

1. INTRODUÇÃO

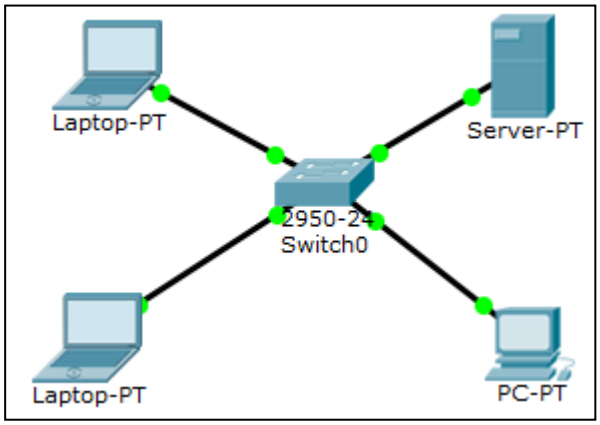
Para entender melhor o conceito de VLAN (Rede Local Virtual) é necessário entender alguns conceitos iniciais, como LAN (*Local Area Network*), e *broadcast,* que é quando uma mensagem emitida por um dispositivo no enlace pode ser recebida por todos os demais dispositivos em um segmento. Kurose e Ross (2006) afirmam que “o **enlace *broadcast*** pode ter vários nós remetentes e receptores,

todos conectados ao mesmo canal de transmissão único e compartilhado". (KUROSE E ROSS, 2006, p. 337).

Uma LAN é uma rede de dados tolerante a falhas e de alta velocidade, que cobre uma área geográfica relativamente pequena. Tipicamente interconecta estações de trabalho, computadores pessoais, impressoras e outros dispositivos. As LANs trazem muitas vantagens aos usuários, incluindo acesso compartilhado de dispositivos e aplicações, troca de arquivos entre os usuários conectados, e a comunicação entre usuários por meio de correio eletrônico e outras aplicações. (Cisco Systems, 2012).

Como pode ser visto na Figura 1, a LAN é composta por todos os *hosts* (dispositivos) que estão conectados no mesmo segmento físico através de um comutador e que estão no mesmo domínio de *broadcast,* que é o segmento lógico onde todos os dispositivos possam se comunicar diretamente sem a necessidade de um roteador, e pode ser chamado também de enlace *broadcast*.

Figura 1: **Exemplo de LAN**



Fonte: próprio autor

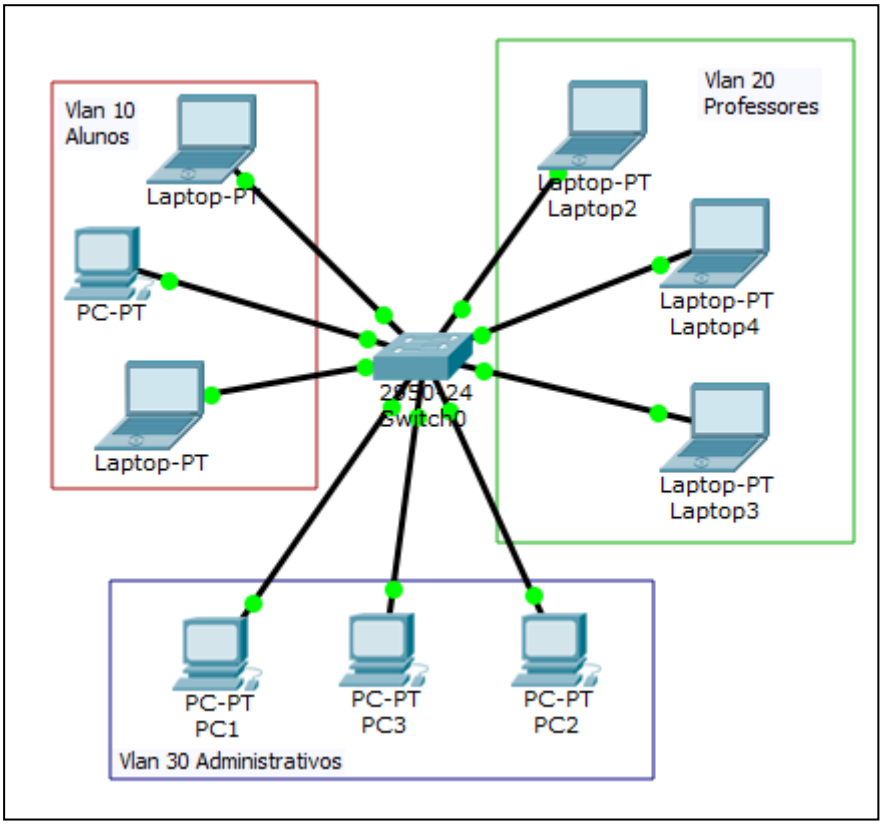
Em redes de computadores o *broadcast* é utilizado, por exemplo, para uma requisição DHCP (*Dynamic Host Configuration Protocol* - Protocolo de Configuração Dinâmica de *Host*) onde o dispositivo cliente envia esta requisição para todos os *hosts* na rede no intuito de descobrir quem é o servidor DHCP na rede. Outro fator relevante é que o *broadcast* normalmente não é transmitido além dos roteadores, já que os mesmos não encaminham tráfego deste tipo. Desse modo tal tráfego é limitado apenas à segmentação da rede local.

As redes locais são necessárias em qualquer empresa, residência ou escritório para o compartilhamento de recursos físicos e lógicos como Internet e

dados digitais em geral e impressoras de rede. Enquanto que a VLAN (*Virtual Local Area Network*), que é formada por várias LANs logicamente segmentadas, é normalmente utilizada em ambientes corporativos.

Podem-se destacar algumas vantagens das VLANs como a segmentação lógica da rede física, a segurança e a flexibilidade de administração da mesma. Observando a figura 2, tem-se o exemplo de uma VLAN básica. Percebe-se que os computadores estão na mesma infraestrutura física, mas segmentados de acordo com cada VLAN.

Figura 2: **Exemplo básico de VLAN**



Fonte: próprio autor

O conceito de rede local é de um ambiente confiável, em que não é preciso implementar um nível de segurança extremo, por ser considerado um ambiente em que todos os usuários são supostamente conhecidos. Mas a partir do momento em que as empresas ou instituições de ensino passaram a usar os recursos da rede em larga escala, tais como compartilhamento de dados, impressoras e internet, surgiu então a necessidade de uma segurança maior.

Em uma rede local a falta de segurança é evidente. Suponhamos que em uma instituição de ensino houvesse apenas uma LAN e os dados dos alunos

ficassem em um computador nesta rede local, como mostra a figura 1. Percebe-se que estes dados estão sujeitos à interceptação e, até mesmo, à alteração sem o consentimento da instituição.

Uma forma de resolver este problema é fazer uma segregação física e colocar os alunos em outra LAN, diferente da rede dos administrativos ou professores. Só que para isso é necessário ao menos um *switch, dispositivo concentrador,* ou um roteador, responsável por definir a melhor rota entre um dispositivo de origem e outro de destino, em cada rede local.

Nesse contexto surge a necessidade de usar VLAN. Uma vez que as redes podem ser segmentadas de forma lógica. Desse modo, pode haver uma melhoria da segurança e a redução da quantidade de equipamentos na rede, facilitando o gerenciamento das redes.

O objetivo principal deste artigo é mostrar uma melhora significativa de desempenho e segurança em redes corporativas com o uso de VLAN. Primeiramente, na seção 2, discute-se a fundamentação teórica. Em seguida, são abordados alguns aspectos relacionados aos protocolos IEEE 802.1q e *Inter-Switch Link* (ISL) da empresa Cisco Systems, ambos tratam sobre VTP (VLAN *Trunking Protocol*) e o cabeçalho ethernet II. Na seção 3, são descritas as metodologias utilizadas. Por sua vez, na seção 4 são apresentados os resultados em gráficos e tabelas para facilitar o entendimento. Por fim, na seção 5, são apresentadas as considerações finais e na seção 6, as referências.

2. FUNDAMENTAÇÃO TEÓRICA

Uma rede de computadores comutada é definida como a interligação de dois ou mais dispositivos entre si. Esta ligação pode ser com cabo ou com a ausência deste, que são as redes *wireless* ou sem fio. Pode-se ligar os computadores diretamente entre si ou por meio de um dispositivo concentrador.

Esta pesquisa tem como embasamento teórico a comparação entre os protocolos ISL (Cisco Systems) e 802.1q (IEEE). Na parte prática foi implementado um rede utilizando o protocolo 802.1q. Para que não fossem usados vários

roteadores, foi criado um *trunk* (tronco) onde os dados de todas as VLANs trafegam. Economizando, assim, tanto portas dos switches como dispositivos roteadores.

Já a base prática desta pesquisa foi uma configuração de dois *switches* com três VLANs diferentes e um servidor, com a distribuição Linux Debian, onde foram configurados os serviços de DNS, DHCP, *proxy*, *firewall* e roteamento entres as redes virtuais. Essas rotas também poderiam ser configuradas diretamente nos próprios *switches*. Mas foram configurados no servidor para que as regras do *firewall* tivessem efeito e assim uma melhor segurança e controle do que trafega entre as redes.

Dentre os vários protocolos citados nas literaturas para configurar VLAN, foram escolhidos dois para detalhamento (ISL e 802.1q) e um deles, o protocolo 802.1q, foi utilizado a configuração prática.

Segundo Birkner (2003), anteriormente, os comutadores Cisco utilizavam apenas um método patenteado chamado *Link* entre Comutadores (ISL). Na prática isto significava que o emprego de VLAN era patenteado. Além disso, a inclusão do "ID VLAN" no cabeçalho pode resultar em um quadro "gigante", que o Ethernet interpreta como um erro. (BIRKNER, 2003, P. 62).

A problemática maior é que em uma rede de grande porte, a empresa que fosse implementar as técnicas de VLAN em seus equipamentos ficariam reféns de uma marca em específico. Ou seja, se a empresa possuir comutadores da marca Cisco a mesma não poderia agregar à sua rede comutadores da marca 3Com, TP-Link ou Intelbras dentre outras.

Com o advento do protocolo de arquitetura aberta para redes locais virtuais este problema foi sanado. Uma vez que este protocolo possui um padrão aberto em que as diversas empresas podem implementar o mesmo protocolo, tornando-as interoperáveis entre si.

Birkner (2003) afirma ainda que, hoje, felizmente, cada vez mais fabricantes, inclusive a Cisco, estão implementando o padrão 802.1Q. O ISL é um superconjunto de funcionalidades 802.1Q. A solução é que, se precisar de interoperabilidade VLAN entre vários fabricantes, você deve tratar de implementar o 802.1Q em sua rede. (BIRKNER, 2003, P. 62).

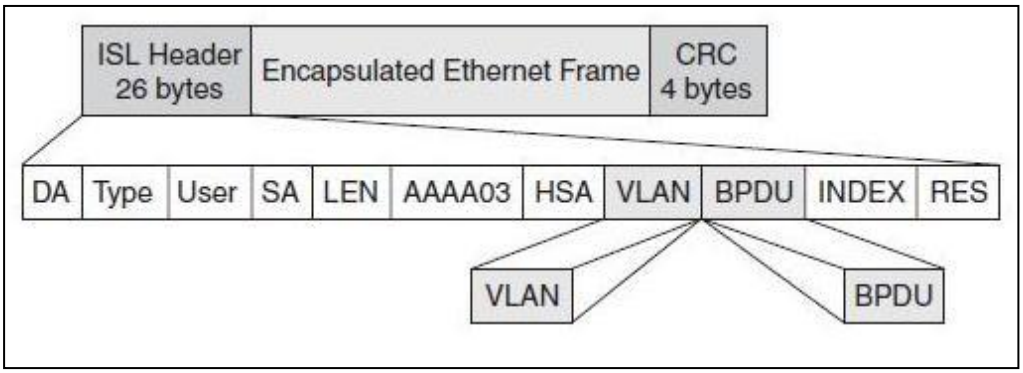
Esta funcionalidade permite o administrador da rede configurar as portas do comutador (*switch*) de forma individual, definindo os tipos de acordo com a

necessidade. Os tipos podem ser definidos como “porta de acesso” (*access port*), onde são ligados os dispositivos finais, como *notebooks*, computadores e impressoras, e a “porta tronco” (*trunk port*) que é utilizada para interligação entre os dispositivos comutadores e podem ser utilizadas para ligação dos comutadores com os roteadores.

2.1 O protocolo ISL – Inter-Switch Link

O protocolo *Inter-Switch Link - ISL* é um protocolo proprietário da Empresa Cisco. Ele é usado para manter uma ligação entre *switches* ou entre *switch* e roteador. A desvantagem imediata desse protocolo é porque ele é suportado apenas em *switches* da marca *Cisco*, o que obriga a empresa que adota o protocolo, de forma automática, a adotar a marca *Cisco* para toda a infraestrutura que for utilizar VLAN. Esse protocolo também modifica o cabeçalho *ethernet*.

Figura 3: Cabeçalho ISL



Fonte: Cisco.com

O ISL encapsula todo o quadro ethernet e adiciona um novo cabeçalho com 26 *bytes*, o que o torna consideravelmente mais pesado, uma vez que o tamanho aumenta até 26 *bytes* em cada quadro em relação ao cabeçalho *ethernet* original. O tamanho do cabeçalho encapsulado com ISL pode variar de 94 *bytes* até 1548 *bytes*, considerando estes dados, o aumento no tamanho vai de 1,7% até 27,7% em cada quadro apenas na camada dois do modelo OSI. Atualmente até mesmo a empresa *Cisco* já está com suporte ao protocolo padrão 802.1q da IEEE para seus *switches*.

2.2 O protocolo IEEE 802.1q

O protocolo 802.1q foi criado pelo Instituto de Engenheiros Eletricistas e Eletrônicos – IEEE e é mantido hoje como o protocolo padrão para a marcação de quadros *ethernet* e segmentação das redes em VLAN. Tem-se como vantagem imediata ser um padrão aberto, ou seja, qualquer empresa pode padronizar em seus equipamentos o suporte a VLAN com este protocolo.

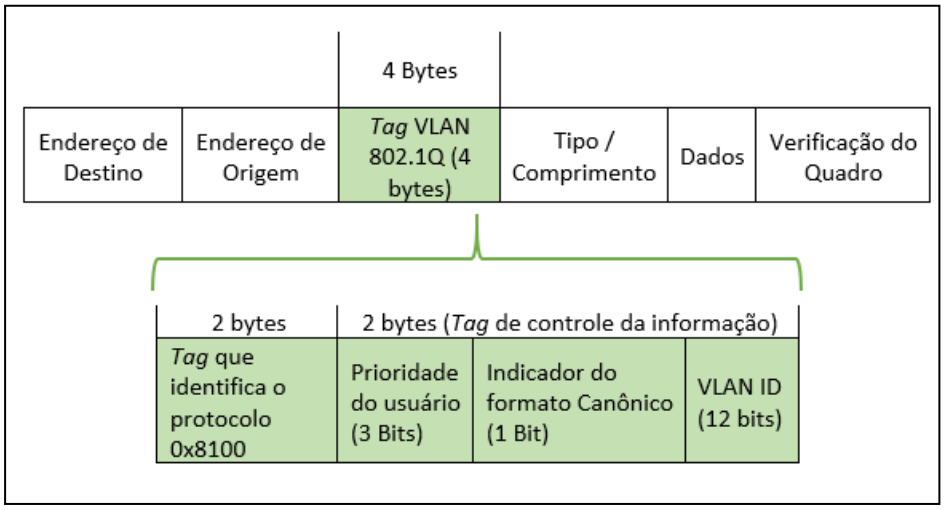
Figura 4: **Modelo OSI**

Fonte: próprio autor.

Para ter noção do que estamos falando veja onde fica localizada esta marcação, em relação ao modelo OSI (*Open System Interconnection*), como mostra a figura 4, que é dividido em sete camadas. Como afirma Júnior et. al (2017) “cada camada possui uma função específica para uma efetiva comunicação entre dois dispositivos” (JÚNIOR et. al, 2017, p. 3). O quadro *ethernet* está localizado na camada de enlace e quando o tipo do quadro (opção *Type*/*Len*) for igual a “0x8100” significa que este quadro está marcado com a *tag* de VLAN, ou seja, será um quadro do tipo VLAN, ver figura 5. Sendo assim será inserida a marcação com o cabeçalho de VLAN.

O protocolo da Cisco, *Inter-Switch Link - ISL*, é uma opção ao padrão IEEE 802.1q. A principal vantagem deste em relação àquele é o fato de não encapsular o cabeçalho, mas fazer a marcação (*tag*) interna no quadro, conforme apresentado na figura 5. Isso significa que quadros identificados também podem ser enviados através de ligações *ethernet* padrão.

Figura 5: **Estrutura do cabeçalho ethernet com marcação IEEE 802.1q**



Fonte: próprio autor (adaptado do padrão IEEE 802.1Q, p. 1269).

O padrão 802.1q também é suportado em dispositivos da Cisco, que está lançando seus novos *switches* com suporte apenas ao protocolo da IEEE, ver figura 6. O protocolo 802.1q insere 4 *bytes* no cabeçalho *ethernet* e recalcula o "*frame check"* do cabeçalho original. Dos quatro *bytes* que são inseridos, dois deles (16 *bits*) são para identificar o protocolo, exemplo 0x8100, 0x9100 ou 0x9200. Os outros dois *bytes* são divididos da seguinte forma: três bits para indicar o nível de prioridade, que vai de zero a sete. Um *bit* indica se o formato é "*Canonical*" (0 = *canonical* MAC e 1 = *non-canonical* MAC) e os outros doze *bits* são usados para o identificador único da VLAN (VLAN ID) que é representado por um número inteiro que vai de 0 a 4095, assim sendo são 4096 possibilidades de VLANs únicas. (IEEE, 2011)

Figura 6: **Modelos de switch da Cisco que suportam *trunking***

See this table for the current list of switch models that support trunking:

Switch Models	Minimum Cisco IOS Software Release Necessary for ISL Trunking	Minimum Cisco IOS Software Release Necessary for 802.1Q Trunking	Current Cisco IOS Software Release Necessary for Trunking (ISL/802.1Q)
WS-C3548-XL	Cisco IOS Software Release 12.0(5)XP, Enterprise Edition	Cisco IOS Software Release 12.0(5)XP, Enterprise Edition	Cisco IOS Software Release 12.0(5)WC(1) or later
WS-C3524-PWR-XL WS-C3524-PWR-XL	Cisco IOS Software Release 12.0(5)XU	Cisco IOS Software Release 12.0(5)XU	Cisco IOS Software Release 12.0(5)WC(1) or later
WS-C2940-8TF-S WS-C2940-8TT-S	No support for ISL	Cisco IOS Software Release 12.1(13)AY	Cisco IOS Software Release 12.1(13)AY or later for 802.1Q No support for ISL
WS-C2950-12 WS-C2950-24 WS-C2950C-24 WS-C2950T-24 WS-C2955T-12 WS-C2955C-12 WS-C2955S-12	No support for ISL	Cisco IOS Software Release 12.0(5)WC(1)	Cisco IOS Software Release 12.0(5)WC(1) or later for 802.1Q No support for ISL
WS-C2970G-24T-E	Cisco IOS Software Release 12.1(11)AX	Cisco IOS Software Release 12.1(11)AX	Cisco IOS Software Release 12.1(11)AX or later

Fonte: cisco.com

Fonte: cisco.com

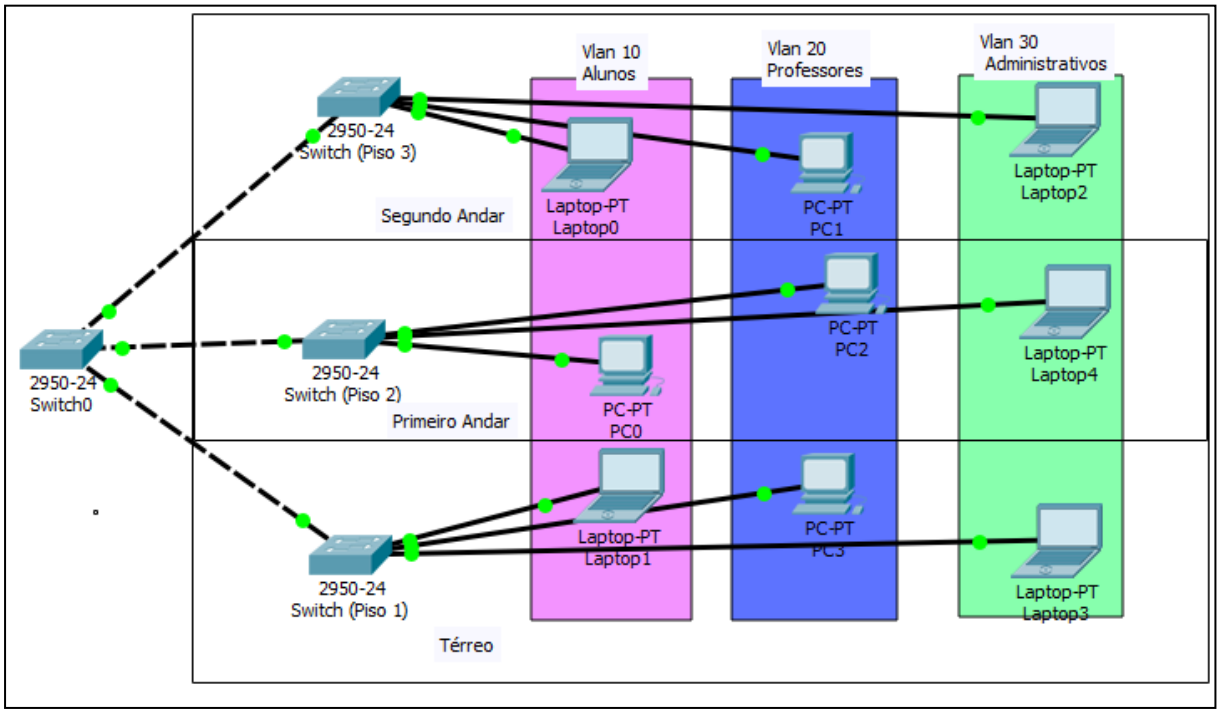
2.2.1 Tipos de Porta

Conforme IEEE (2011) são definidos dois principais tipos de portas nos *switches* para a efetivação da comunicação entre dois hosts. A porta *access*: porta comum que liga um dispositivo ao comutador (*switch*). É uma porta que tem tráfego comum sem a necessidade de marcação do quadro. O outro tipo é a porta *trunk* (tronco), que tem a função de enviar e receber quadros identificados em todas as VLANs, exceto na VLAN nativa. Ela é usada para ligar um *switch* ao outro ou o *switch* ao roteador. Por essa porta, há o tráfego de todas as "*tagged VLANs*", ou seja, todas as VLANs que estiverem associadas a este tronco com uma marcação. Este tronco lógico é composto por todas as portas *trunk* de todos os *switches* que estiverem interligados.

2.3 VLAN *Trunking*

O padrão 802.1q especifica encapsulamento para multiplexação de VLAN em um único link e os quadros podem ser identificados ou não. Na figura 7, observamos um *trunk* entre várias VLANs. Neste exemplo, pode-se perceber que dispositivos em que estão localizados desde o primeiro piso até o terceiro piso podem se comunica normalmente entre si, desde que estejam na mesma VLAN. Do contrário, só poderiam se comunicar se houvesse uma regra de roteamento entre as VLANs diretamente nos *switches* ou com uma configuração no *firewall* para este fim. Apesar de estes dispositivos estarem conectados fisicamente no mesmo concentrador, estes *hosts* estão segmentados em "*VLAN ID*" diferentes e cada uma delas identifica uma rede em que os dispositivos, por padrão, só se "falam" entre si.

Figura 7: **Exemplo de "*trunk*" entre redes virtuais**



Fonte: Próprio Autor

Se um host quer se comunicar com o outro em uma VLAN distinta, sem a configuração de *trunk* e com as redes virtuais no mesmo *switch,* deve-se usar a função de roteador no switch para rotear os pacotes de uma rede (VLAN 10) para a outra (VLAN 20) como mostra a figura 2. Do contrário, seria necessário que liguasse um cabo fisicamente de uma interface que está na VLAN 10 para uma interface que

se encontra na VLAN 20, para que dispositivos de ambas as VLANs pudessem se comunicar.

Diante do exposto, os *hosts* se comunicariam e o tráfego *broadcast* das duas redes seria compartilhado. Mas para o caso de haver várias redes virtuais e vários concentradores, esta solução ficaria inviável, porque para cada rede virtual que fosse se comunicar com outra, seriam necessárias duas interfaces: uma em cada *switch* e um cabo interligando as duas redes.

Como solução intermediária, poderia ser instalado apenas um *switch* para interligar as duas sub-redes. E, caso a configuração da VLAN abrangesse faixa de endereço IP (*Internet Protocol*) diferente, os computadores compartilhariam o mesmo domínio broadcast, mesmo assim não se comunicariam. Seriam necessários roteadores entre os *switches,* o que aumenta o custo-benefício.

A solução definitiva, para resolver os problemas elencados acima, foi criar um modo de comunicação com *hosts* de VLANs distintas de forma lógica. Surge então a necessidade de simular também estes cabos que ligam todas as redes. Para resolver isto, utiliza-se um *trunk* entre os *switches* para a comunicação, como pode ser observado na figura 7.

Na figura 7, observamos um dispositivo “PC2” que está no “andar 2” e associado à “*VLAN* 20” se comunica com o dispositivo “PC1” do andar 3 da mesma VLAN. Sabe-se que ambos estão conectados em uma porta *access* (porta de acesso ou porta comum) de *switches* diferentes, mas ambos pertencem a mesma VLAN, o que faz com que a comunicação aconteça.

2.4 A configuração prática

Esta configuração se dá em um ambiente em que há uma possibilidade frequente de haver grande quantidade de *hosts* conectados nessa mesma rede. E os *hosts* produzem tráfego de vários tipos, como tráfego de voz, vídeo ou dados.

Nessa rede também há vários tipos de usuários com funções distintas. Como ela é uma rede corporativa universitária, possui usuários do tipo: alunos, professores, administrativos, e usuários ainda mais críticos em relação à segurança, como setor de gestão de pessoas, contabilidade e o gabinete da administração geral. Surge a necessidade de segmentar as redes em VLAN pelo fato de ser mais

seguro e de alocar cada tipo de dispositivo em uma rede com usuário que tenha interesses afins.

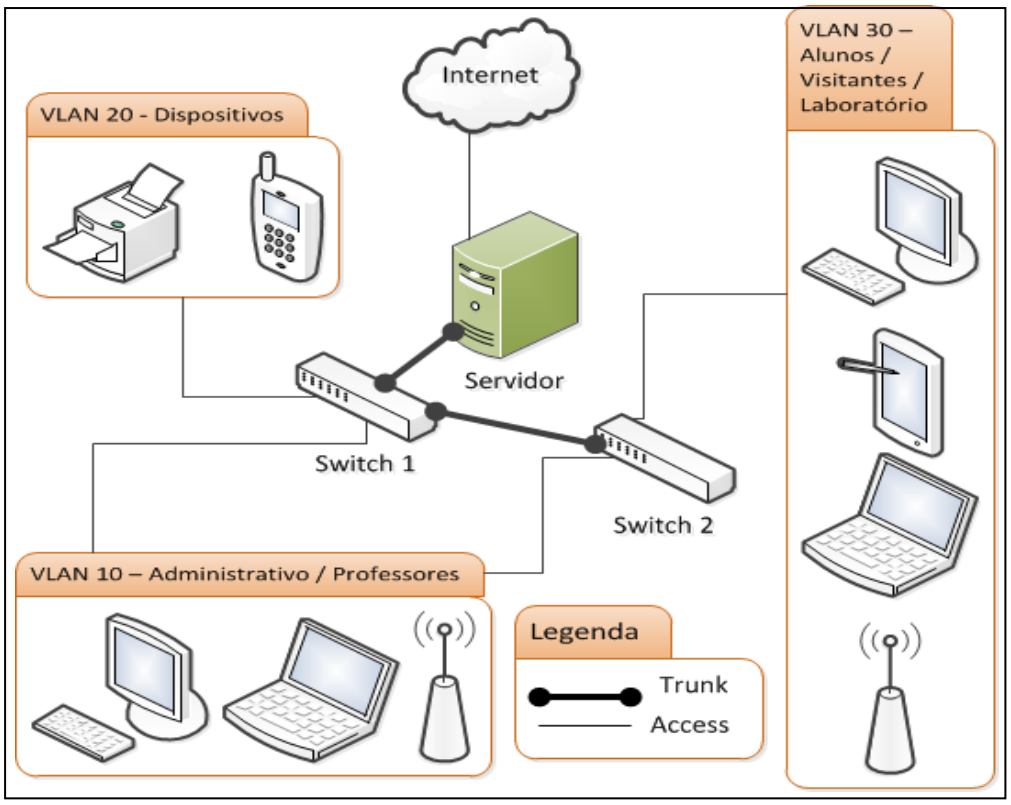
A rede antes de ser configurada VLAN, onde todos os computadores compartilham o mesmo domínio de *broadcast,* está representada na figura 1. Enquanto que a rede com VLAN pode ser representada nas Figuras 2 e 7. Com as redes virtuais, cada equipamento só se comunica com os demais que estão associados à mesma VLAN por padrão ou com outras redes virtuais ao utilizar as devidas configurações. Nesta configuração usa-se também um servidor Linux com vários serviços configurados: DNS, DHCP, Firewall e Proxy.

3. METODOLOGIA

O método desta pesquisa consta da utilização de uma topologia de rede com algumas VLANs. Os testes foram executados no mês de março de 2013. Com uma estação de trabalho, duas redes virtuais, dois switches e um tronco entre ambos. Utilizou-se também um servidor de rede, com sistema operacional Linux, configurado os serviços de DNS, DHCP, Roteamento, Firewall e Proxy.

Foram utilizadas também as ferramentas Wireshark e LibreOffice Calc. A primeira para capturar o tráfego da rede em tempo real e organizá-lo por protocolos assim como salvar estes dados em formato CSV (*comma-separated values* ou valores separados por vírgula). Já a segunda foi utilizada para segmentar os dados em colunas e para remover os valores duplicados na coluna “IP de origem”, para descobrir quantos computadores participaram desse teste e também para tabular os dados. Foram feitas cinco capturas de dados: três delas usando a estação de trabalho e duas delas direto no servidor.

Figura 9: Topologia da Rede com VLAN



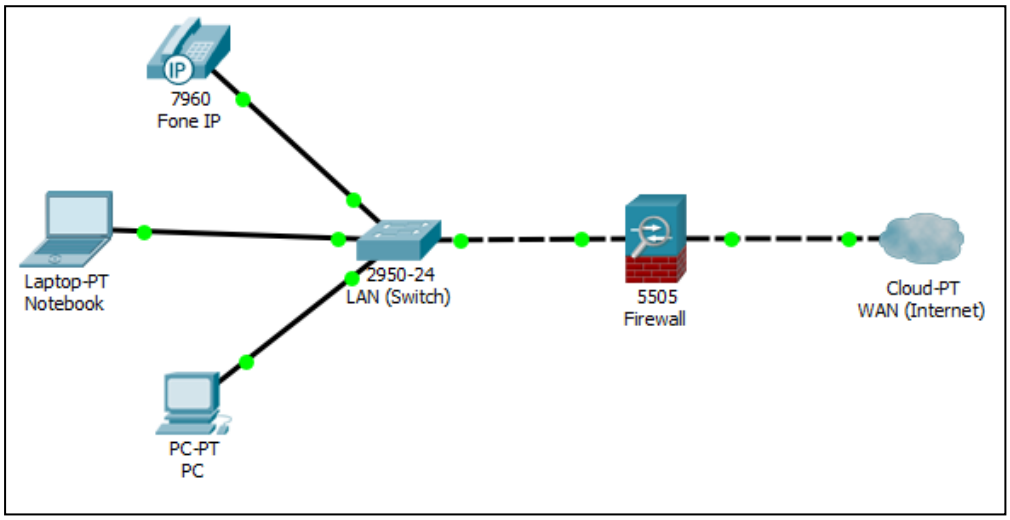
Fonte: próprio autor

Para desenhar a topologia da rede foram usadas as ferramentas Microsoft Visio e Cisco Packet Tracer Student. Os *switches* são da marca 3Com, modelo "3Com Switch 5500G-EI 48-Port", configurados via interface web. No computador "Servidor" foram instalados o Sistema Operacional Linux Debian e os serviços de DNS, respondendo consultas nas redes virtuais, e DHCP para distribuir a configuração automática em todas as redes virtuais locais. Também configurado o roteamento e o encaminhamento de pacotes entre as redes. Um *proxy* para filtrar os acessos à internet e o firewall, peça fundamental para a segurança desta topologia e que pode ser visto na Figura 10.

Para Tanenbaum (2003), os *firewalls* são apenas uma adaptação moderna de uma antiga forma de segurança medieval: cavar um fosso profundo em torno do castelo. Este recurso forçava todos aqueles que quisessem entrar ou sair do castelo a passar por uma ponte levadiça, onde poderiam ser revistados por guardas. Nas redes é possível usar o mesmo artificio: uma empresa pode ter muitas LANs conectadas de forma arbitrária, mas todo o tráfego de saída ou entrada da empresa

é feito através de uma ponte levadiça eletrônica (*firewall*). (TANENBAUM, 2003, p. 825).

Figura 10: **Topologia da Rede com *Firewall***



Fonte: próprio autor.

É no firewall, Figura 10, onde foram configuradas as rotas e as regras de acesso entre as redes. Por exemplo, a regra que diz que a rede dos “Alunos” acessa apenas a internet, mas não dá acesso aos compartilhamentos da rede “Administrativo”.

Recomenda-se que os dispositivos como impressoras e telefones IP fiquem em uma VLAN separada. Pois uma ligação de voz sobre IP pode ser interceptada facilmente usando um *sniffer* (analisador de rede, como o *Wireshark*) e decodificada em tempo real, ou gravar para possível utilização maliciosa. O acesso a estes dispositivos é liberado ou bloqueado por meio de regras no *firewall*.

4. RESULTADOS

Os resultados serão exibidos em forma de gráficos e tabelas para facilitar o entendimento. Este trabalho relata sobre melhoria da rede em desempenho e segurança, e apresenta a segmentação da rede como uma possível solução que poderia ser realizada por equipamentos físicos, como roteador, switch dentre outros. Mas como foco principal, esta segmentação foi disposta de forma lógica com redes virtuais locais.

As tabelas 1 e 2, mostram que foram feitas cinco capturas de pacotes na rede. (duas no servidor e três no cliente). Foram realizadas as capturas em dois modos de configuração: utilizando uma LAN (Tabela 2) e posteriormente em uma VLAN (Tabela 1).

Tabela 1: Quantidade de pacotes capturados na rede com VLAN

#	Local da Captura	Máquinas	Tempo (minutos)	Total pacotes	Destinado ao Computador
1	Servidor	16	2	38.393	0 (0%)
2	Cliente	11	2	11.762	7.740 (66%)

Fonte: próprio autor.

A tabela 2 representa as capturas de dados realizadas no servidor e no cliente, ambas na VLAN “Alunos” e com duração de dois minutos. Deve-se atentar que a quantidade de pacotes capturados no computador cliente foi de 11.762 pacotes e, neste momento haviam 11 dispositivos na rede. Já no momento em que foi feito a captura por diretamente no servidor, haviam 16 máquinas na rede e foram capturados 38.393 pacotes, sendo que estes pacotes não possuíam como destino final o próprio Servidor, mas sim outros computadores na rede.

Tabela 2: Quantidade de pacotes capturados na rede sem VLAN

#	Local da Captura	Máquinas	Tempo (min)	Total pacotes	Destinado ao Computador
3	Cliente (Stand by)	184	3	10.650	82 (1%)
4	Servidor	400	2	427.870	0 (0%)
5	Cliente	103	4	12.174	2.143 (18%)

Fonte: próprio autor.

Na tabela 2 percebemos algo similar à tabela 1. Mas como não havia uma segmentação por VLAN, o item 4 (quatro) demonstra que, no momento em que a captura foi efetuada a partir do servidor, haviam 400 máquinas na rede interagindo com o mesmo e foram 427.870 pacotes capturados. Já os itens 3 e 5 representam capturas feitas nos computadores clientes onde haviam 184 e 103 máquinas, respectivamente, que capturaram 10.650 e 12.174 pacotes respectivamente.

Tabela 3: Quantidade de pacotes em porcentagem de *broadcast*

#	**Broadcast**	**%**	**ARP**	**%**	**255.255.255.255**	**%**	**Total**	**%**
1	15	0,04%	115	0,30%	2	0,01 %	132	0,34%
2	92	0,78%	83	0,71%	2	0,02 %	177	1,50%
3	2.596	24,38 %	6.062	56,92 %	344	3,23 %	9.002	84,53 %
4	1.842	0,43%	5.326	1,24%	212	0,05 %	7.380	1,72%
5	1.490	12,24 %	5.934	48,74 %	257	2,11 %	7.681	63,09 %

Fonte: próprio autor.

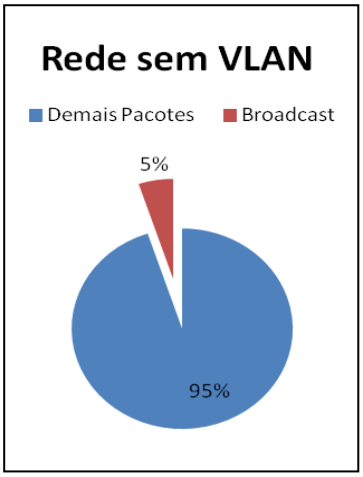
Na tabela 3 são apresentados os pacotes que foram destinados ao domínio de *broadcast* da rede. O domínio de broadcast da rede é representado pelo endereço IP 10.0.255.255 e o endereço da rede é 10.0.0.0/16. São apresentados também os pacotes do protocolo ARP (*Andress Resolution Protocol* - Protocolo de Resolução de Endereço) e os pacotes destinados para o IP 255.255.255.255 (*broadcast* geral).

A tabela 3 complementa as tabelas 1 e 2 e representa a quantidade de pacotes de *broadcast* em cada um dos itens relacionados nas tabelas 1 e 2. Nos itens 1 e 2 da tabela 3, vemos que totalizaram 132 e 177 pacotes de *broadcast* respectivamente, ou seja, pacotes que chegam sem ser solicitados por essas máquinas. Já nos itens de 3 a 5 da tabela 3, onde não há segmentação por VLAN, eles chegam, em média, a mais de sete mil pacotes em cada computador. Esses pacotes são enviados a todos os computadores do segmento físico, independente

de pertencerem a mesma faixa de rede. Isto posto, percebemos que quando a quantidade de *hosts* na rede aumenta, a quantidade de pacotes de *broadcast* tem aumento exponencial. Prejudicando assim o desempenho.

No gráfico 1, observa-se que em uma rede sem VLAN a quantidade de broadcast é de 5% (24.063 pacotes) do total de pacotes que chegam na máquina. Parece pouco quando se fala em porcentagem, mas isso é o total de pacotes que chega em cada dispositivo da rede e gera em cada máquina mais de 24 mil interrupções, que são tratadas uma a uma e pode acarretar na redução do desempenho do dispositivo.

Gráfico 1: Rede sem utilizar VLAN

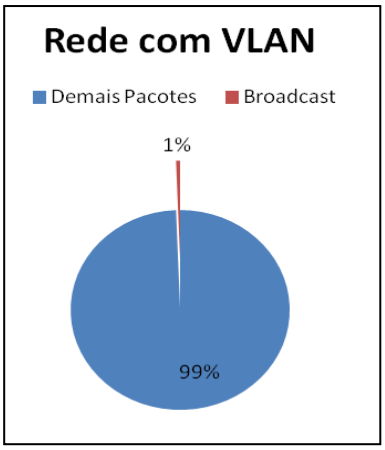


Fonte: próprio autor.

Em linhas gerais, percebe-se que quanto menor a quantidade de *hosts* em uma rede local, menor serão as colisões (caso utilize um *hub*), e menor ainda será a quantidade de pacotes não solicitados, mas que serão tratados por cada máquina.

No gráfico 2, percebe-se que apenas 1% (309 pacotes) é direcionado a todas as máquinas na rede. Assim, cada máquina gera menos interrupções e trata menos pacotes que não são direcionados diretamente a essa máquina. Isso melhora a rede em performance e os dados podem ser transferidos com uma menor quantidade de interrupções possíveis. Para o usuário “leigo”, isso se traduz em maior velocidade de *download* ou da Internet.

Gráfico 2: Rede que utiliza VLAN



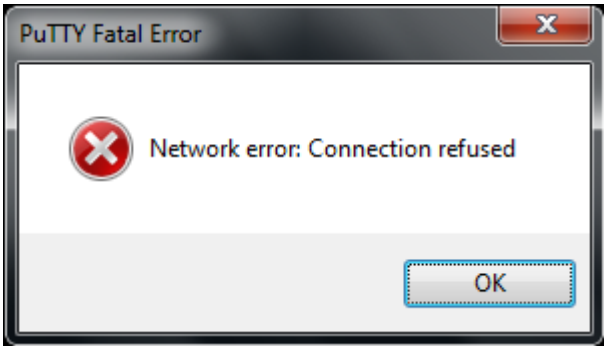
Fonte: próprio autor.

Cada pacote que chega à placa de rede gera uma interrupção e o mesmo deverá ser tratado pelo sistema operacional, mesmo que o pacote não seja destinado ao computador. Ou seja, o computador para de trabalhar para tratar o pacote. Quanto mais máquinas na rede, maior será o número de pacotes de *broadcast*, e quanto mais pacotes, mais interrupções, quanto mais interrupções, menor desempenho a rede terá.

Ao observar as tabelas 1 e 2, percebe-se que quanto menor a rede (menos dispositivos por segmento), menor será a quantidade de interrupções. Assim percebemos a ideia central da VLAN: segmentar a rede para melhorar o desempenho e a segurança.

Com base na topologia da rede apresentada na figura 9, percebe-se que há apenas um servidor. Neste servidor estão configurados os vários serviços citados. Um destes serviços é o de firewall, que complementará a segurança entre as redes. Por padrão os *hosts* das redes virtuais diferentes não comunicam entre si. Mas como todas as VLANs da topologia da figura 9 estão interligadas através do servidor, então será nele onde as regras de segurança serão implementadas.

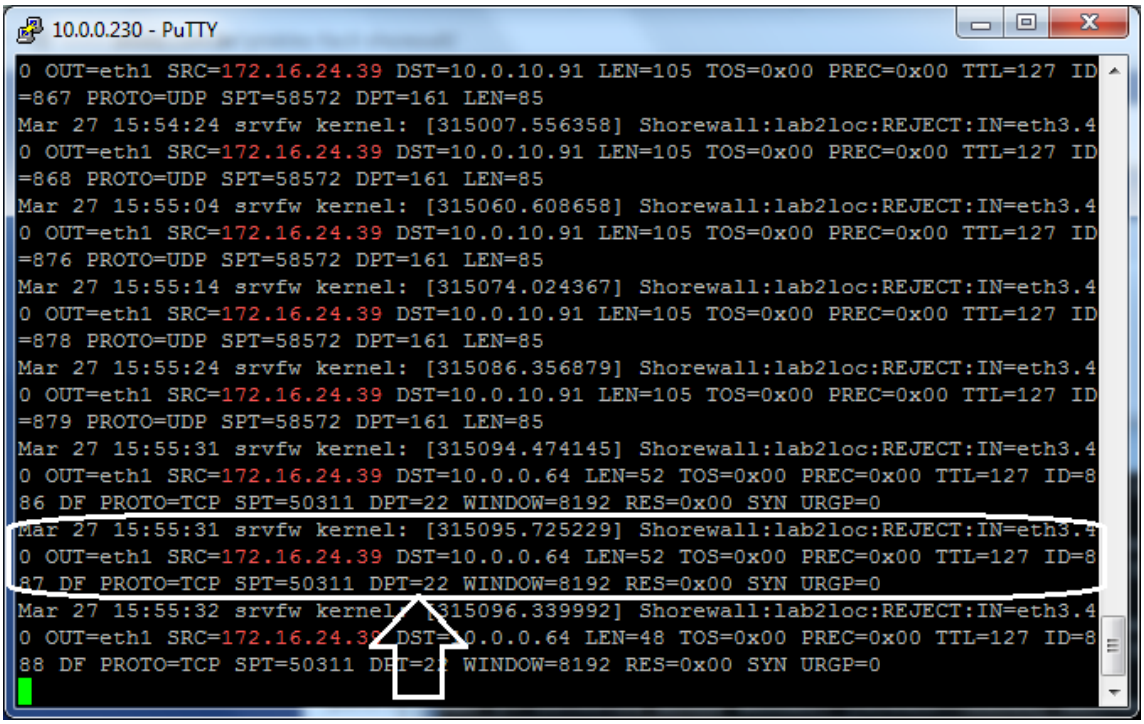
Figura 11: Erro, conexão recusada pelo firewall na porta 22, visão do Cliente



Fonte: próprio autor.

O roteamento entre as redes virtuais está habilitado, assim uma rede pode comunicar-se com a outra, inclusive acessar a Internet. Para demonstrar uma das regras do firewall funcionando, foi bloqueado o acesso via SSH (*Secure Shell*), que faz o acesso remoto ao terminal de servidores e dispositivos. A figura 11 mostra a visão do cliente, localizado na rede “Laboratório”, denominada “lab”, que tenta acessar um servidor na rede local, denominada “loc” por meio da ferramenta PuTTY. Já a figura 12 mostra a visão por parte do servidor, apresentando o log (registro de eventos relevantes) do firewall.

Figura 12: Erro, conexão recusada pelo firewall, visão do Servidor



Fonte: próprio autor.

A figura 12 mostra a porta 22, que é a porta padrão referente ao protocolo SSH, bloqueada para os *hosts* da VLAN ‘lab’ em direção à VLAN ‘loc’ [lab2loc:REJECT]. Assim o servidor rejeita toda solicitação que vier da rede ‘lab’ para a rede ‘loc’, se a porta de destino for igual a 22.

5. CONSIDERAÇÕES FINAIS

Diante dos resultados obtidos, pode-se inferir que o uso das técnicas de VLAN em redes universitárias ou corporativas pode impactar significativamente em uma melhoria de desempenho e de segurança em uma infraestrutura de rede de computadores. Com a segmentação da rede, problemas como infecção por vírus em um dispositivo podem ficar restritos apenas a uma parte da rede (VLAN), deixando todas as outras redes virtuais funcionando plenamente. Por exemplo, a rede “Alunos” e a Rede “Financeiro”. O mesmo vale para problemas de *loop* e ataques de negação de serviço. Já com as regras de *firewall*, como bloqueios e filtros, podem ser permitidos somente tráfegos autorizados de uma rede virtual para outra. Pode-se também limitar o que cada rede virtual acessa na Internet, como serviços ou portas. Outro motivo para usar as redes virtuais em detrimento as redes tradicionais é a economia em quantidade de equipamentos e uma melhora do gerenciamento da rede, uma vez que serão menos equipamentos para comprar e gerenciar. Tem-se como vantagem, se comparando a utilização de VLAN em detrimento da rede tradicional, que praticamente toda a estrutura ficará com uma administração centralizada. Nota-se também que o nível de capacitação do pessoal técnico necessariamente deverá ser maior para se ter uma estrutura de redes virtual em pleno funcionamento e com qualidade ao utilizar as técnicas de VLAN definidas no protocolo 802.1q.

REFERÊNCIAS

BIRKNER, Matthew H. **Projeto de Interconexão de Redes – Cisco Internetwork Design – CID**. São Paulo: Pearson Education do Brasil, 2003.

KUROSE, James F., ROSS, Keith W. **Redes de Computadores e a Internet: uma abordagem top-down.** 3. Ed. São Paulo: Pearson Addison Wesley, 2006.

SISTEMS, Cisco. **Internetworking Technology Handbook**. Disponível em: < http://docwiki.cisco.com/wiki/Internetworking_Technology_Handbook>. Acesso em: 22 dez. 2012.

SISTEMS, Cisco. **Virtual LANs/VLAN Trunking Protocol (VLANs/VTP)**. Disponível em: < http://www.cisco.com/en/US/tech/tk389/tk689/technologies_configuration_example09186a008009441a.shtml>. Acesso em: 15 fev. 2013.

IEEE, Computer Society. **IEEE Std 802.1Q: Media Access Control (MAC) Bridges and Virtual Bridge Local Area Networks**. New York: IEEE Standards, 2011. 1375p.

TANENBAUM, Andrew S. **Redes de Computadores.** 4. Ed. Rio de Janeiro: Elsevier, 2003.

JUNIOR, Ciro F. C.; ARRAIS, Ciro M. C.; CARVALHO, Kely R. S. A.; RIBEIRO, Antônio J. M. **A evolução da internet: uma visão geral.** JICE: Jornada de Iniciação Científica e Extensão, 2017.