UNIVERSIDADE TECNOLÓGICA FEDERAL DO PARANA
DEPARTAMENTO ACADÊMICO DE ELETRÔNICA
CURSO DE ESPECIALIZACÃO EM CONFIGURAÇÃO E GERENCIAMENTO DE SERVIDORES E EQUIPAMENTOS DE REDES

FABIAN MAURICE MALHEIROS FRANCO

PROJETO DE IMPLEMENTAÇÃO DE REDE LOCAL HIERÁRQUICA NO CÂMPUS PONTA GROSSA DA UNIVERSIDADE TECNOLOGICA FEDERAL DO PARANÁ

MONOGRAFIA

CURITIBA
2012

FABIAN MAURICE MALHEIROS FRANCO

PROJETO DE IMPLEMENTAÇÃO DE REDE LOCAL HIERÁRQUICA NO CÂMPUS PONTA GROSSA DA UNIVERSIDADE TECNOLOGICA FEDERAL DO PARANÁ

Monografia apresentada como requisito parcial para obtenção do grau de especialista em Configuração e Gerenciamento de Servidores e Equipamentos de Redes, do Departamento Acadêmico de Eletrônica da Universidade Tecnológica Federal do Paraná.
Orientador: Prof. MSc. Fabiano Scriptore de Carvalho

CURITIBA

2012

Dedico esta monografia à minha querida mãe Nadir Pereira Malheiros (In Memoriam) e à minha irmã Karla Adriana Malheiros Franco, minhas grandes motivadoras.

Agradecimentos

Agradeço a todos os professores do Curso de Especialização Semi Presencial em Configuração e Gerenciamento de Servidores e Equipamentos de Redes. Em especial aos professores Augusto Foronda e Kleber Kendy Horikawa Nabas.

Ao meu orientador Fabiano Scriptore de Carvalho pela dedicação, orientação e paciência.

Por apoio por parte do Câmpus Ponta Grossa da Universidade Tecnológica Federal do Paraná.

RESUMO

MALHEIROS FRANCO, Fabian Maurice. **Projeto de Implementação de Rede Local Hierárquica no Câmpus Ponta Grossa da Universidade Tecnológica Federal do Paraná**. 2012. 42 f. Monografia (Especialização em Gerenciamento de Redes) – Programa de Pós-Graduação em Tecnologia, Universidade Tecnológica Federal do Paraná. Curitiba, 2012.

Neste trabalho são tratados os principais conceitos teóricos envolvidos em redes de computadores e redes de computadores hierárquicas. São enumerados problemas encontrados em uma rede não segmentada, bem como o modo de funcionamento de uma rede segmentada por VLAN e suas vantagens. Os modos de configuração dos equipamentos envolvidos em um projeto real também são demonstrados. Como objetivo principal, o trabalho apresenta uma proposta de uma rede hierárquica para o ambiente de rede da Universidade Tecnológica Federal do Paraná, Câmpus Ponta Grossa. A proposta da rede é descrita em detalhes e envolve a criação de VLANs, roteamento, configurações de endereçamento e ACLs. Todos os comandos envolvidos na configuração são apresentados a partir de um ambiente simulado em Software.

Palavras-chave: VLAN. Segmentação de Rede. Domínio VTP. 802.1Q.

ABSTRACT

MALHEIROS FRANCO, Fabian Maurice Implementation Project of Hierarchical LAN for Câmpus Ponta Grossa of Federal Technological University of Paraná,. 42 f. Essay (Graduate Certificate in Networking and Systems Administration) - Graduate Programs in Technology, Federal Technological University of Paraná. Curitiba, 2012.

This paper addressed the main theoretical concepts involved in computer networks and computer hierarchical networks. Problems encountered are listed in a non-segmented network, as well as the mode of operation of a segmented network and VLAN by its advantages. The configuration modes of the equipment involved in a real project are also demonstrated. As a main objective, the paper presents a proposal of a hierarchical network to the network environment of Federal Technological University of Paraná, Campus Ponta Grossa. The proposed network is described in detail and involves creating VLANs, routing, addressing and settings ACLs. All configuration commands involved are presented from a simulated environment on Software.

Keywords: VLAN. Network Segmentation. VTP Domain. 802.1Q.

LISTA DE FIGURAS

LISTA DE TABELAS

LISTA DE SIGLAS E ACRÔNIMOS

ACL	Access Control List
Gbps	Gigabits per Second
IEEE	Institute of Electrical and Electronic Engineers
IP	Internet Protocol
ISO	International Organization for Standardization
LAN	Local Area Network
Mbps	Megabits per Second
OSI	Open Systems Interconnection
QoS	Quality of Service
TCP	Transmission Control Protocol
VLAN	Virtual Local Area Network
VOIP	Voice Over Internet Protocol
VTP	VLAN Trunk Protocol

SUMÁRIO

1 INTRODUÇÃO

Este primeiro capítulo abordará o tema, a delimitação da pesquisa, o problema objetivos, justificativa, procedimentos metodológicos, fundamentação teórica e estrutura completa do trabalho.

1.1 TEMA

O avanço dos recursos disponíveis na rede mundial de computadores e dentro das organizações conquistou um grande e crescente número de utilizadores. Da mesma forma as redes locais dentro das organizações se expandiram de forma muito rápida, e na maioria das vezes de forma não planejada.

Com mais utilizadores e dispositivos conectados em um mesmo domínio de difusão, a gerência da rede se torna muito mais complexa e problemática. Quando uma rede cresce de forma não planejada problemas como, por exemplo, de lentidão na rede e de segurança, podem aumentar tornando a experiência não muito agradável ao usuário final.

O desempenho da rede pode ser um fator na produtividade de uma organização. Uma das tecnologias que contribuem com a excelência do desempenho da rede é a separação dos grandes domínios de broadcast em domínios menores com a utilização de redes virtuais menores conhecidas como VLANs. Domínios de broadcast menores limitam o número de dispositivos que participam de broadcasts e permitem separar dispositivos em agrupamentos funcionais, como serviços de banco de dados para um departamento de contabilidade e de transferência de dados em alta velocidade para um departamento de engenharia (FILIPPETTI, 2008).

Este trabalho tem como objetivo apresentar e explorar os recursos disponíveis por meio da utilização do conceito de *Virtual Lan Area Network* (VLAN). Será proposto um modelo de implementação em uma rede já existente que apresenta os problemas de gerenciamento citados anteriormente.

O cenário utilizado será a rede local da Universidade Tecnológica Federal do Paraná – Câmpus Ponta Grossa. Como a unidade ainda não possui os equipamentos necessários para a aplicação da proposta, será utilizado um software de simulação de rede. Os comandos envolvendo as configurações necessárias também serão abordados.

1.2 **DELIMITAÇÃO DA PESQUISA**

A pesquisa, relacionada à segmentação de rede através do uso de VLANs, abrange os principais conceitos da tecnologia. São abordados os conceitos básicos sobre VLAN, protocolo 802.1q, roteamento entre VLANs, *Access Control List* (ACL) e sobre protocolo *VLAN Trunk Protocol* (VTP). Além dos conceitos, é apresentado um cenário de simulação com o modelo proposto, bem como os comandos necessários para a configuração dos equipamentos.

1.3 **PROBLEMA**

O rápido crescimento do câmpus Ponta Grossa, bem como de sua rede local, trouxe a necessidade de um estudo visando a melhoraria do desempenho e da segurança da *Local Area Network* (LAN).

A primeira questão observada na rede atual é a grande quantidade de dispositivos que pertencem ao mesmo domínio de *broadcast*. Os são pacotes de dados enviados a todos os nós de uma rede são chamados de *Broadcast* (KUROSE, 2006). O tráfego *broadcast* é necessário para o funcionamento da rede, entretanto limitar o tamanho do domínio de *broadcast* em uma LAN, trás benefícios de desempenho, segurança e privacidade (FILIPPETTI, 2008).

Para resolver as dificuldades encontradas em uma LAN muito grande são utilizados comutadores com suporte a VLANs. Dispositivos pertencentes a uma VLAN fazem parte do mesmo domínio de *broadcast*, ou seja, o trafego *broadcast* só pode alcançar dispositivos pertencentes associados à mesma VLAN (KUROSE, 2006).

1.4 **OBJETIVOS**

A seguir, serão apresentados os objetivos, geral e específicos, pretendidos com o presente projeto de pesquisa.

1.4.1 OBJETIVO GERAL

Realizar um estudo sobre a atual estrutura lógica de rede da Universidade Tecnológica Federal do Paraná, Câmpus Ponta Grossa, e propor uma solução de segmentação de rede utilizando VLANs.

1.4.2 OBJETIVOS ESPECÍFICOS

Os objetivos específicos são:

- Compreender o funcionamento de uma rede segmentada por VLAN;
- Propor a criação de sub-redes.
- Propor a criação de VLANs conforme características da organização;
- Propor a criação de um domínio VTP;
- Relacionar Protocolos a serem utilizados;
- Criar um ambiente de simulação conforme a proposta apresentada;
- Apresentar os comandos e configurações necessárias para a implementação da proposta.

1.5 JUSTIFICATIVA

As organizações geralmente possuem um número significativo de computadores. A fim de compartilhar recursos esses computadores são interligados através de uma rede local. À medida que a rede cresce, ou seja, a quantidade de dispositivos interconectados aumenta, cresce de forma conjunta a disputa pela utilização do meio de transmissão. Quando isso ocorre, problemas de lentidão ou até mesmo de inoperabilidade na transmissão de dados são frequentemente observados.

Outro problema que ocorre em uma rede sem segmentação está relacionado à segurança. Como não existe uma divisão lógica delimitando a comunicação entre os dispositivos, vulnerabilidades na rede podem ser facilmente exploradas.

Para que a rede não entre em colapso, é necessário adotar algumas medidas. A subdivisão da rede local em redes locais menores é uma delas. De maneira eficaz, a segmentação com VLANs, aumenta o nível de segurança e elimina tráfegos desnecessários na rede, o que aumenta o desempenho da rede.

Nos últimos anos, a UTFPR Câmpus Ponta Grossa, passou por uma ampliação considerável. Além do espaço físico ampliado a quantidade de alunos e funcionários aumentou. Consequentemente, a quantidade dispositivos que utilizam a sua rede local também cresceu. Entretanto não houve um planejamento para dar suporte a todos esses dispositivos.

Ao notar momentos de lentidão ou até mesmo de indisponibilidade da rede, bem como a necessidade tornar o ambiente de rede mais seguro, justifica-se a proposta de seguimentação de rede para a unidade do câmpus Ponta Grossa.

1.6 **PROCEDIMENTOS METODOLÓGICOS**

Para o desenvolvimento deste projeto, foram utilizadas as seguintes metodologias:

- Pesquisa bibliográfica de referências clássicas sobre redes de computadores.
- Pesquisa bibliográfica em redes VLAN.
- Para a simulação do ambiente foi necessária a utilização de um software educacional, desenvolvido pela empresa Cisco, chamado *Packet Tracer* versão 5.3.2.

1.7 **FUNDAMENTAÇÃO TEÓRICA**

Os conceitos e protocolos, abordados e estudados no transcorrer desta monografia, são fundamentados na literatura relacionada à área de telecomunicações e redes de computadores.

1.8 **ESTRUTURA**

O presente trabalho esta dividido em 4 capítulos e 1 apêndice.

O capítulo 2 aborda conceitos básicos de redes de computadores, descrição de equipamentos e protocolos e os principais conceitos relacionados à segmentação de rede.

O capítulo 3 traz uma visão geral da infraestrutura de rede da Universidade Tecnológica Federal do Paraná – Câmpus Ponta Grossa, ao qual se propõe a adoção de uma rede segmentada. Neste capítulo também é apresentada a proposta de uma rede local hierárquica e segmentada para o Câmpus Ponta Grossa.

Finalmente o capítulo 4 apresenta as conclusões e considerações finais sobre o trabalho proposto.

Os comandos utilizados executados para a criação do cenário em simulador são relacionados e explicados no apêndice A.

2 REFERENCIAL TEÓRICO

Este capítulo abordará os conceitos necessários para a compreensão do funcionamento das redes locais virtuais (VLAN). Serão apresentadas ainda, as principais características das redes de computadores locais (LAN), os equipamentos essenciais utilizados em uma rede e seus meios de transmissão.

2.1 **REDES DE COMPUTADORES**

Pode-se definir as redes de computadores, de forma simplificada, como sendo um conjunto de máquinas, que por meio de estruturas físicas (cabos e equipamentos) e lógicas (protocolos e softwares), compartilham recursos entre si. Essas redes podem ser classificadas, dentre outras maneiras, de acordo com sua abrangência geográfica. Segundo Tanembaum (2003), uma rede privada, localizada dentro de um câmpus universitário, pode ser chamada de rede local ou *Local Area Network*.

Atualmente a tecnologia Ethernet é predominante em redes LAN (KUROSE, 2006), definida pelo padrão IEEE 802.3, opera entre 10 Mbps até 10 Gbps e utiliza cabo par

trançado, ou fibra óptica para transmissão de dados entre dois ou mais equipamentos (TANEMBAUM, 2003).

2.2 **MODELO DE REFERÊNCIA OSI**

O modelo Open System Interconnection (OSI), ou modelo interconexão de sistemas abertos, se baseia em uma proposta desenvolvida pela International Standards organization (ISO) e tem sete camadas. O modelo foi criado a partir dos seguintes princípios (TANEMBAUM, 2003):

- Cada camada foi criada quando houve necessidade de um novo grau de abstração.
- Cada camada executa uma função bem definida.
- As funções de cada camada foram escolhidas com base da definição de protocolos padronizados internacionalmente.
- Os limites de camadas foram escolhidos para minimizar o fluxo de informações nas interfaces.
- O número de camadas foi definido para que funções distintas não precisem ser colocadas em uma mesma camada e de forma que a arquitetura não se torne de difícil controle.

Apesar de ser um modelo completo e bem definido, o modelo é adotado apenas como referência para interconexão de redes, ou seja, não existe uma aplicação prática com as sete camadas sujeridas.

A tabela 1 apresenta as sete camadas definidas pelo modelo de referência OSI.

Tabela 1 – Modelo de Referência OSI

Camada	Identificação
7	APLICAÇÃO
6	APRESENTAÇÃO
5	SESSÃO
4	TRANSPORTE
3	REDE
2	ENLACE DE DADOS
1	CAMADA FÍSICA

Fonte: Autoria Própria.

A camada física trata da transmissão dos bits pelo canal de comunicação. Isso envolve a garantia correta de entrega dos bits do emissor ao receptor, as voltagens utilizadas para representar os bits, tempo de duração de um bit, a forma como a conexão inicial é estabelecida e como é encerrada. Nesta camada também são estabelecidas a quantidade de pinos que o conector de rede terá e qual a finalidade de cada um deles (TANEMBAUM, 2003).

A principal tarefa da camada de enlace é fazer com que o canal de transmissão pareça livre de erros. Para isso a camada de enlace de dados divide os dados em quadros e os transmite sequencialmente. Se o serviço for confiável o receptor enviará uma confirmação de cada quadro recebido corretamente. A camada de enlace também faz o controle de fluxo e controle de acesso a um canal compartilhado em redes de difusão (TANEMBAUM, 2003).

A camada de rede prove um mecanismo de endereçamento e foi projetada para possibilitar a interconexão entre redes heterogêneas. A camada 3 determina a maneira como os pacotes são roteados da origem até o destino. As rotas podem ser consultadas em tabelas estáticas ou em tabelas criadas dinamicamente (FILIPPETTI, 2008).

Essa camada é responsável pela transferência fim-a-fim dos dados de uma aplicação cliente servidor (TANEMBAUM, 2003). A camada de transporte determina que tipo de serviço deve ser fornecido à camada de sessão. Existem dois tipos de serviço de transporte, um deles orientado à conexão, que provê garantia de entrega sequencial de mensagens ou bytes, e é tolerante a erros. O outro serviço, não orientado à conexão não possui garantia de entrega, controle de erros e as mensagens não chegam ao destino de forma ordenada (FILIPPETTI, 2008).

A camada de sessão permite que usuários de diferentes computadores estabeleçam sessões entre si. A camada fornece o serviço de controle de diálogo, gerenciamento de símbolos e sincronização (TANEMBAUM, 2003).

A sintaxe e a semântica das informações transmitidas são tratadas pela camada de apresentação. Isso torna possível a comunicação entre computadores com diferentes representações de dados (TANEMBAUM, 2003).

A sintaxe e a semântica das informações transmitidas são tratadas pela camada de apresentação. Isso torna possível a comunicação entre computadores com diferentes representações de dados (FOROUZAN, 2008).

2.3 **PILHA DE PROTOCOLOS TCP/IP**

Em termos de software, os projetos de redes são organizados em camadas ou níveis, a fim de diminuir sua complexidade. O número de camadas, nomes, conteúdos e funções variam de uma rede para outra. Entretanto as camadas têm o mesmo propósito, oferecer serviços à sua camada superior, isolando-as dos detalhes de implementação desses recursos (TANEMBAUM, 2003).

O desenvolvimento da pilha de protocolos TCP/IP, teve inicio no final dos anos 60. Na década de 90, como um protocolo aberto que possibilita a comunicação entre computadores de diferentes capacidades e fabricantes. Assim tornou-se a forma mais utilizada para a organização de redes de computadores e a base para o que conhecemos como *Internet* (STEVENS, 1994). Normalmente o TCP/IP é considerado um sistema de quatro camadas como representado na tabela 2.

Tabela 2 - Pilha de Protocolos TCP/IP

Identificação da Camada	Principais Protocolos
Aplicação	HTTP, FTP, SMTP, etc.
Transporte	TCP, UDP
Rede	IP, ICMP, IGMP
Acesso ao Meio	Controlador da Placa de Rede

Fonte: Autoria Própria.

As camadas possuem funções diferentes entre si, essas funções são apresentadas de forma resumida logo abaixo (STEVENS, 1994).

- A camada de acesso ao meio, às vezes chamada de camada de enlace de dados, inclui o controlador da placa de rede e interface física com o cabo;
- A camada de rede ou camada de *Internet* é quem determina o encaminhamento de pacotes na rede. Nesta camada são estabelecidos detalhes de endereçamento IP e protocolos de roteamento;
- A Camada de transporte se responsabiliza pelo fluxo de dados entre dois hosts;

- Por fim, a camada de aplicação trata de detalhes de aplicações particulares, que por sua vez são de grande diversidade.

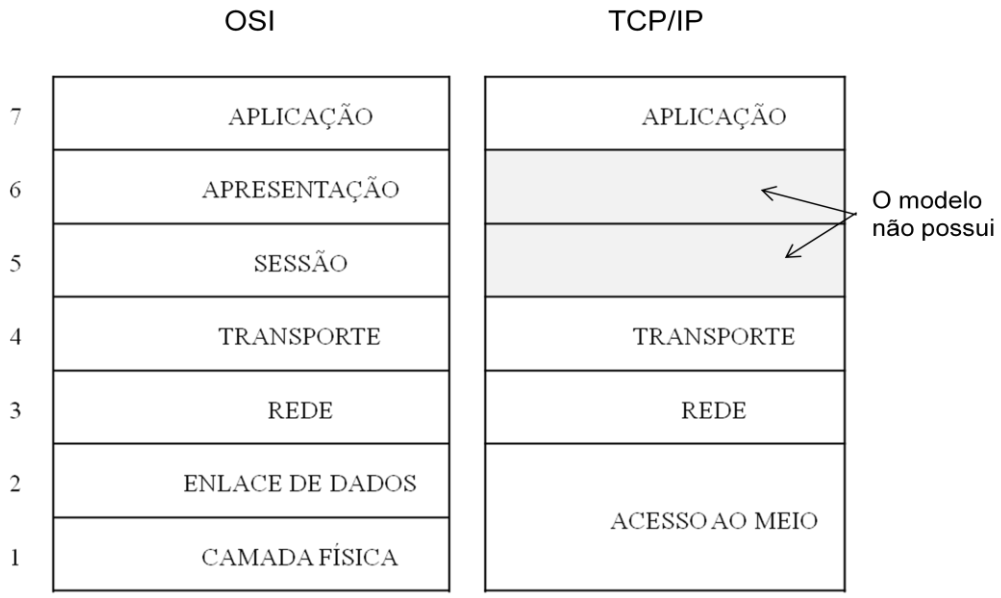

Figura 1 – Relação entre camadas do modelo OSI e Pilha TCP/IP.
Fonte: TANEMBAUM (2003).

2.4 **EQUIPAMENTOS DE REDES**

A Ethernet foi originalmente concebida como uma topologia de barramento, o que não era muito conveniente, já que todos os hosts eram conectados pelo mesmo cabeamento. Uma vez que houvesse um problema em um computador, toda rede poderia ser comprometida. Ao longo do tempo, o padrão Ethernet passou a operar por meio de cabos chamados de par trançado. Neste caso a topologia é chamada de estrela, onde todos os segmentos são interligados por um hub (PEARLMAN, 1999). A figura 2 demonstra a diferença entre as duas topologias.

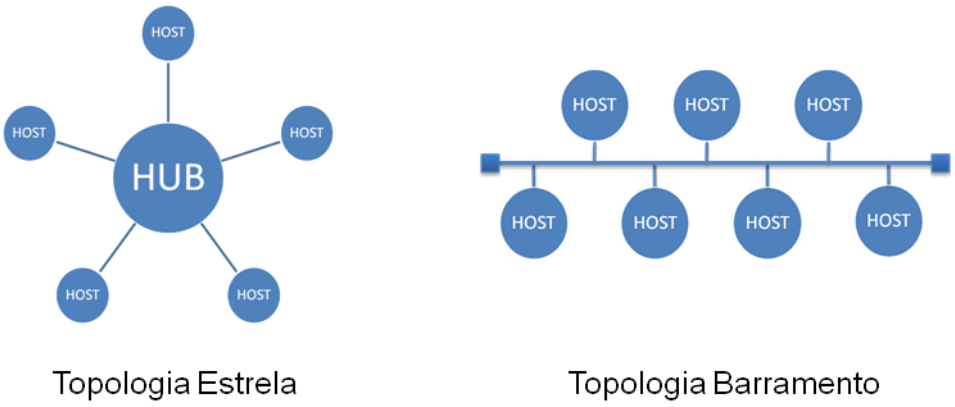

Figura 2 – Comparação entre as Topologias Estrela e Barramento.
Fonte: Autoria Própria.

Através da figura 2, é possível observar que a topologia estrela possui apenas um ponto de falha, o que é uma boa vantagem em relação à topologia barramento. Entretanto, nas duas topologias acima, caso dois hosts tentarem enviar dados pela rede ao mesmo tempo, haverá colisão e os dados serão perdidos.

2.5 **SWITCH**

O termo *switch* se dá ao dispositivo de rede encarregado de filtrar, encaminhar e preencher quadros, tomando como base o endereço de destino de cada quadro que recebe. Dessa forma podemos dizer ainda, que é um dispositivo operante na camada de enlace de dados do modelo OSI (FILIPPETTI, 2008), ou comutador de pacotes da camada de enlace (KUROSE, 2006).

Em relação a uma rede LAN, podemos observar algumas vantagens da utilização de um comutador ao invés de um enlace de broadcast em topologias estrela. Pode-se dizer que o *switch* obtém grande melhora com relação ao desempenho, já que nenhum quadro é transmitido ao mesmo tempo em um segmento. Dessa forma, colisões são evitadas e há um melhor aproveitamento de banda disponível (KUROSE, 2006).

2.6 **ROTEADOR**

O roteador é um equipamento capaz de conectar duas ou mais redes. É o roteador que permite a entrega de pacotes em redes diferentes. O destino de um pacote IP pode ser um sistema web na rede local ou um servidor de email em outro país. É responsabilidade dos roteadores a entrega desses pacotes, da maneira mais eficiente possível e em tempo hábil (FILIPPETTI, 2008).

Para atender às demandas das redes atuais os roteadores também prestam outros serviços além do encaminhamento de pacotes. Esses dispositivos podem oferecer priorização de Qualidade de Serviço (QoS, *Quality of Service*) dos pacotes IP. Assim é possível assegurar que tráfegos em tempo real, como voz, vídeo e dados críticos não sofram atrasos ou sejam descartados. Também podem atenuar o impacto de ataques na rede, permitindo ou negando o encaminhamento de pacotes (FILIPPETTI, 2008).

2.7 **MEIOS DE TRANSMISSÃO**

A troca de dados em redes de computadores passa pode passar por uma série de pares transmissor-receptor. Estes pares são interconectados por um meio físico heterogêneo. Existem duas categorias de meios físicos: os meios guiados e não guiados. Os meios guiados são aqueles onde os sinais são dirigidos ao longo de um meio sólido. Nos meios não guiados os sinais são propagados na atmosfera e no espaço (KUROSE, 2006).

2.8 **CABO PAR TRANÇADO**

O meio de transmissão mais utilizado em redes locais é o cabo par trançado. Um par trançado consiste em dois fios de cobre encapados e enrolados de forma helicoidal. Em geral esses fios têm cerca de 1 mm de espessura. Quando trançados, as ondas de diferentes partes dos fios se cancelam. Isso faz com que o cabo sofra menor interferência, proporcionando assim melhor desempenho em termos de largura de banda e alcance (TANEMBAUM, 2003). Hoje, as taxas de transmissão de dados para redes LAN que utilizam par trançado atingem de 10Mbps a 1Gbps (KUROSE, 2006).

2.9 **FIBRA ÓPTICA**

A fibra óptica é um meio delgado e flexível capaz de conduzir pulsos de luz. Cada pulso representa um bit e uma única fibra pode suportar taxas de dezenas ou centenas de gigabits por segundo (KUROSE, 2006). As fibras podem ser confeccionadas em vidro ou plástico. O limite prático de transferência atual é de cerca de 10 Gbps, pois existe uma incapacidade em realizar a conversão entre sinais elétricos e ópticos com velocidade maior (TANEMBAUM, 2003). A fibra óptica possui grande largura de banda, baixa atenuação e não sofre interferência eletromagnética. Sua principal utilização é em *backbones* de redes de dados (FOROUZAN, 2008).

2.10 **SEM FIO**

A transmissão de dados sem fio ocorre por meio de ondas de rádio, seja em ambientes fechados ou abertos. Elas podem percorrer longas distâncias e atravessar barreiras como paredes por exemplo. As ondas de rádio são omnidirecionais, o que facilita muito sua utilização, já que os dispositivos transmissor e receptor não precisam estar fisicamente alinhados. É uma tecnologia que facilita, sobretudo, a utilização de dispositivos móveis. No entanto pode haver casos onde podemos usar a transmissão sem fio para estações fixas, como por exemplo, onde a instalação de uma estrutura com cabos seja inviável (TANEMBAUM, 2003).

2.11 **DOMÍNIOS DE BROADCAST**

A comunicação em uma rede local pode ser *unicast, multicast* ou *broadcast*. Dizemos que uma comunicação é *unicast* quando o quadro é enviado de um host e é endereçado a um destino específico. Na comunicação *multicast* a transmissão é feita para um grupo específico de dispositivos ou clientes. Quando o quadro é enviado para todos os outros receptores conectados a comunicação é classificada como *broadcast* (TANEMBAUM, 2003).

Todos os dispositivos conectados a um *switch* estão no mesmo domínio de *broadcast.* Assim, podemos dizer que, um conjunto de *switches* interconectados entre si

fazem parte do mesmo domínio *broadcast*. Em uma rede não segmentada, dispositivos como computadores e impressoras geram grande quantidade de pacotes de difusão, isso ocorre devido ao mau funcionamento de placas de rede, falhas em conexões do cabo de rede ou protocolos e aplicações que utilizam esse tipo de tráfego.

Quando um *switch* recebe um quadro *broadcast* ele é difundido para todos os dispositivos conectados. Isso diminui a eficiência da rede, pois a largura de banda é usada para propagar esses quadros. Para evitar domínios de *broadcast* muito grandes, são utilizados roteadores e ou LANs virtuais (VLANs) para criar vários subdomínios de difusão. Essa prática diminui o tráfego de mensagens *broadcast* no subdomínio e na rede como um todo (FILIPPETTI, 2008). A figura 2.1 demonstra da disseminação do tráfego de difusão em uma rede segmentada com a aplicação de VLANs.

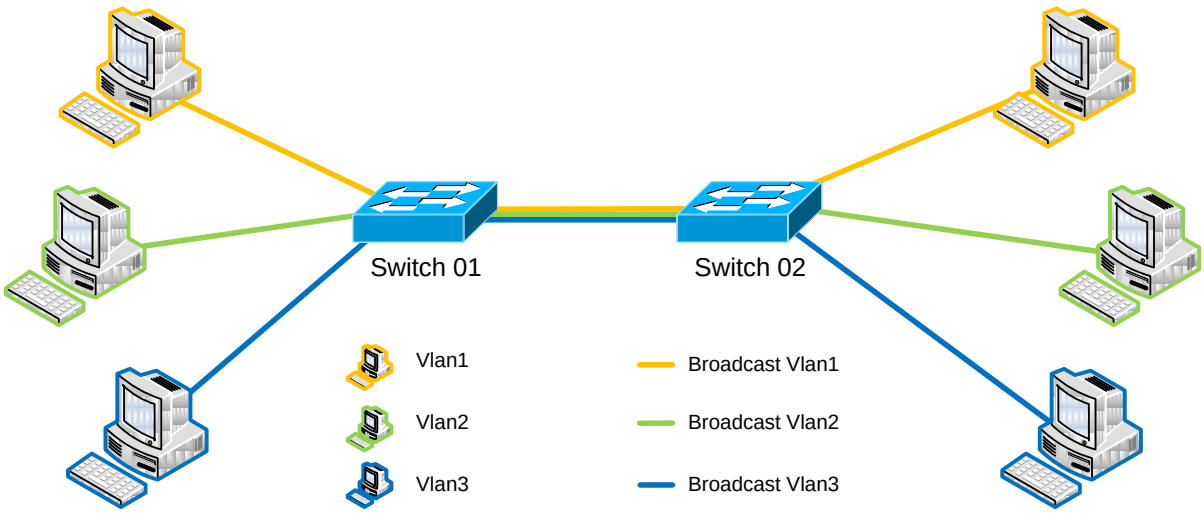

Figura 3 – Tráfego de difusão em rede segmentada por VLAN.
Fonte: Autoria Própria.

2.12 **LANS VIRTUAIS (VLANS)**

O conceito de rede local virtual diz respeito ao isolamento de duas ou mais LANs através da utilização de software, ou seja, as redes são isoladas logicamente. Fisicamente essas redes podem compartilhar o mesmo *switch*, mas com a vantagem de compreenderem domínios de broadcast diferentes. Em uma universidade podemos separar os computadores

dos alunos dos computadores da administração, mesmo que estes compartilhem a mesma infraestrutura. A figura 4 mostra uma rede LAN com três grupos de computadores compartilhando o mesmo *switch*. A figura 5 demonstra a segmentação de uma LAN em três redes locais virtuais.

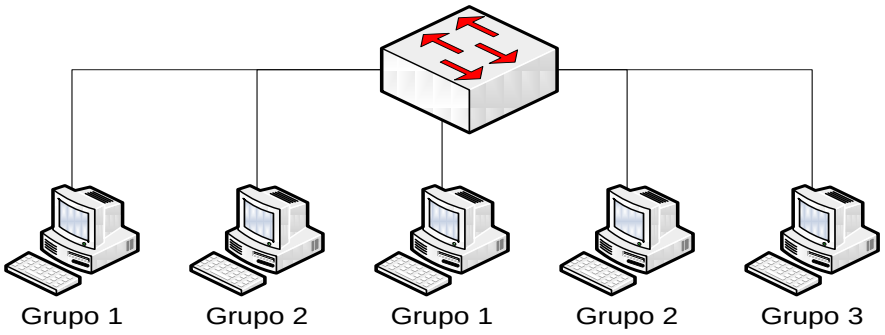

Figura 4 – Grupos de computadores em uma única rede local interligados por um *switch*.
Fonte: Autoria Própria

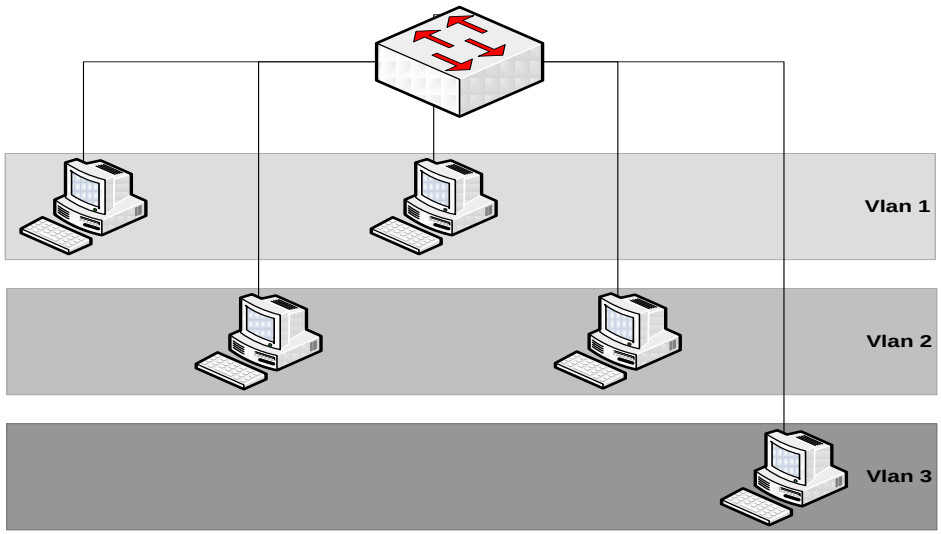

Figura 5 – Computadores isolados logicamente por meio de redes virtuais em um único *switch*.
Fonte: Autoria Própria

As VLANs se baseiam em *switches* especialmente projetados para oferecer este recurso. Para configurar uma rede com VLANs, o administrador de rede deve decidir a quantidade de VLANs, seus respectivos nomes e quais serão os computadores ligados a cada uma delas (TANEMBAUM, 2003). O agrupamento de computadores pode ser definido,

dependendo do fabricante do equipamento, empregando parâmetros como (FOROUZAN, 2008):

- Número de porta do *switch*;
- Endereço MAC do host;
- Endereço IP do host;
- Endereço *multicast*;
- Combinações dessas opções.

Para facilitar o entendimento da rede, os layouts físico e lógico são representados em um único diagrama onde os membros das VLANs são identificados por cores (TANEMBAUM, 2003).

Entre os benefícios da utilização de VLANs estão os seguintes (FILIPPETTI, 2008):

- Segurança – Grupos com dados confidenciais podem ser separados do restante da rede.
- Redução de custo – Uso mais eficiente da largura de banda e dos *uplinks* existentes.
- Desempenho mais alto – Dividir a rede em vários grupos de trabalho lógicos (domínios de broadcast), reduz um tráfego desnecessário e assim aumenta o desempenho.
- Atenuação da tempestade de broadcast – Dividir a rede em VLANs reduz o número de dispositivos que podem participar de uma situação de descontrole por excesso de broadcast.
- Simplificação do gerenciamento – Usuários com requisitos de rede semelhantes compartilham uma mesma VLAN.

2.13 **PROTOCOLO IEEE 802.1Q**

O padrão denominado IEEE 802.1Q, define o formato do quadro ethernet para utilização de VLANs e o padrão a ser utilizado nos *backbones multi-switches* e regulamenta o uso de equipamentos de fabricantes diferentes (FOROUZAN, 2008). O campo de informações de controle do padrão 802.1Q possui dois bytes. Os três primeiros bits definem a prioridade do usuário. Possui um bit para identificação de formato canônico (CFI) permitindo o

transporte de quadros *Token Ring* em links ethernet. Outros doze bits são utilizados para identificar 4096 IDs de VLAN (TANEMBAUM, 2003).

2.14 INTERFACE DE ACESSO E INTERFACE DE TRONCO

Os *switches* que fornecem suporte à utilização de VLANs possuem todas as portas configuradas em uma VLAN padrão, geralmente VLAN 1. Quando apenas uma VLAN é atribuída a uma porta, dizemos que essa é uma interface ou porta de acesso. Ao configurar uma porta de acesso com uma determinada VLAN, essa porta passa a difundir apenas quadros da mesma VLAN a que pertence.

Diferentemente da interface de acesso, uma interface em modo tronco pode transportar quadros de mais de uma VLAN. Ao configurar um tronco é possível estender as VLANs por toda a rede através de enlaces ponto a ponto entre dispositivos (FILIPPETTI, 2008). Geralmente esses dispositivos são *switchs* e os enlaces são chamados de enlaces de tronco ou *trunk link.* Para que a comunicação funcione entre esses equipamentos é necessário que ambas as portas estejam configuradas no modo tronco. Também devemos indicar quais VLANS o enlace de tronco deve encaminhar.

A figura 6 demonstra a utilização de portas de acesso e tronco em uma rede. As portas de acesso são usadas para conectar computadores de diferentes VLANs, enquanto as portas de tronco interligam dois *switches*.

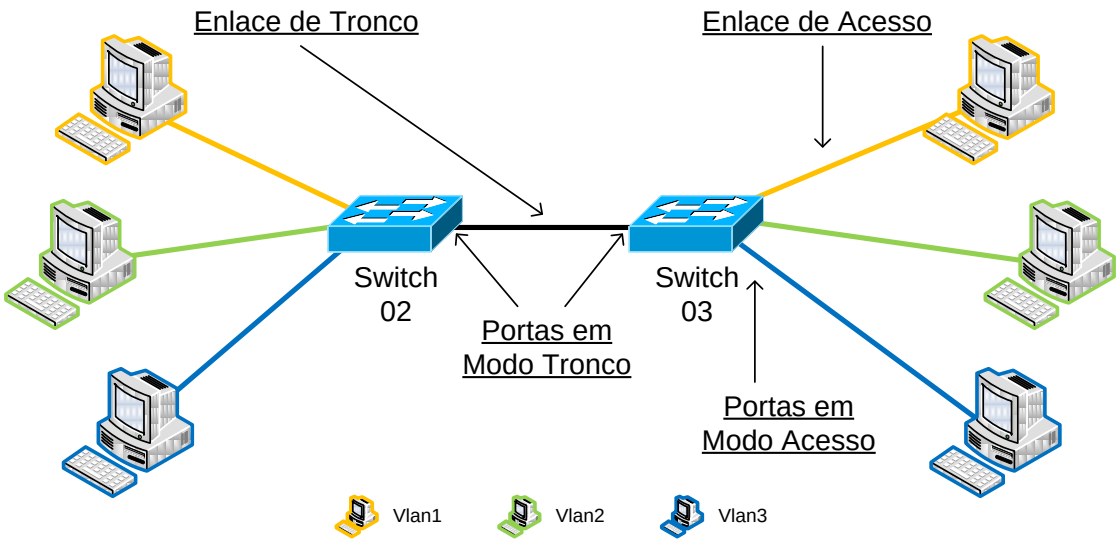

Figura 6 – Exemplo de aplicação de portas de tronco e portas de acesso.

Fonte: Autoria Própria

2.15 **PROTOCOLO VTP**

O protocolo de entroncamento de VLAN, VLAN *Trunking Protocol* (VTP), é um protocolo proprietário Cisco, que usa quadros de entroncamento para comunicar informações de VLAN entre um grupo de *switches*. O protocolo VTP permite que um gerente de rede configure um *switch* para que ele propague as configurações de VLAN aos outros *switches* da mesma rede. Através do VTP é possível gerenciar operações de adição, exclusão e renomeação de VLANs pela rede a partir de um *switch* configurado como servidor VTP. Para que os *switches* recebam as informações do servidor VTP é necessário que estejam configurados como clientes VTP (FILIPPETTI, 2008).

Os principais componentes do VTP são:

Domínio de VTP - Consiste em um ou mais *switches* interconectados. Todos os *switches* em um domínio compartilham os detalhes de configuração de VLAN utilizando anúncios VTP.

Anúncios de VTP - O VTP utiliza uma hierarquia de anúncios para distribuir e sincronizar configurações de VLAN pela rede.

Modos de VTP - Um *switch* pode ser configurado de três modos: servidor, cliente ou transparente.

Servidor de VTP - Os servidores VTP anunciam as informações de VLAN do domínio VTP para outros *switches* habilitados para VTP nesse mesmo domínio. Os servidores

de VTP armazenam as informações de VLAN para o todo o domínio em NVRAM (Non-Volatile RAM, RAM não-volátil).

Cliente de VTP - Os clientes VTP funcionam do mesmo modo que os servidores VTP, mas você não pode criar, alterar ou excluir as VLANs em um cliente VTP. Um cliente VTP somente armazena as informações de VLAN para o todo o domínio enquanto o *switch* estiver ativo.

VTP Transparente - *Switches* no modo transparente encaminham anúncios VTP para clientes VTP e servidores VTP. *Switches* no modo transparente não participam do VTP.

Corte de VTP - O corte de VTP aumenta a largura de banda disponível na rede restringindo o tráfego inundado aos links tronco que o tráfego deve utilizar para alcançar os dispositivos de destino.

2.16 **ROTEAMENTO DE VLANS**

O roteamento entre VLANs pode ser definido como um processo de encaminhamento do tráfego de rede de uma VLAN para outra. Esse processo de encaminhamento é feito por meio de um equipamento que atua na camada de rede do modelo OSI, já que cada VLAN é associada a uma sub-rede IP distinta (FILIPPETTI, 2008). Em um ambiente com muitas VLANs pode-se utilizar um *switch* de camada 3 ao invés de um roteador. Isso facilita o gerenciamento e reduz custos.

As interfaces de um *switch* 2 podem ser configuradas em VLANs diferentes assim como os *switches* de camada 3. Entretanto apenas um *switch* de camada 3 ou um roteador permitem a comunicação de dispositivos que não pertençam à mesma VLAN. A comunicação entre VLANs também pode ser restrita pelo mesmo equipamento. Por exemplo, se em uma universidade criamos uma VLAN para alunos e não queremos que estes usuários acessem dados da VLAN destinada aos professores, podemos realizar uma configuração bloqueando tal acesso. Essa possibilidade se dá através da utilização de listas de controle de acesso.

2.17 **LISTAS DE CONTROLE DE ACESSO (ACL)**

Uma Access Control List (ACL) é uma lista sequencial de instruções de permissão ou negação que se aplicam a endereços e ou protocolos. É possível utilizar ACLs de forma eficiente para controlar o acesso, dentro e fora da rede, para qualquer protocolo que seja roteado. De forma geral as listas de controle de acesso são utilizadas como parte de uma solução de segurança para a rede (FILIPPETTI, 2008).

A filtragem através de ACL em uma rede com VLANs pode definir, por exemplo, que a VLAN A só terá acesso ao serviço de e-mail da VLAN B. Na medida em que os pacotes passam por uma interface com uma ACL associada, esta é consultada para em busca de um padrão correspondente ao pacote de entrada. Em seguida são aplicadas as regras de permissão ou negação, determinando assim o destino do pacote, que pode ser encaminhado ou descartado (FILIPPETTI, 2008).

3 PROJETO DE IMPLEMENTAÇÃO DE UMA REDE HIERARQUICA

Este capítulo pretende dar ao leitor uma visão geral da infraestrutura de rede da Universidade Tecnológica Federal do Paraná, Câmpus Ponta Grossa. Serão abordados meios de transmissão utilizados, equipamentos e uma breve identificação dos grupos de usuários que utilizam a rede local. Será apresentada ainda, uma proposta para implementação de VLAN no Câmpus como forma de solução aos problemas encontrados. A proposta prevê a utilização futura de tecnologias como VOIP, e equipamentos de monitoramento via IP.

3.1 MEIOS DE TRANSMISSÃO UTILIZADOS NO CÂMPUS

O Câmpus da UTFPR em Ponta Grossa é composto, atualmente, por 13 blocos. Cada bloco é conectado por meio de fibra óptica até ao *datacenter*, onde estão localizados os servidores e enlace de acesso à *Internet*. A distribuição da rede nos blocos se dá através de cabeamento metálico de par trançado. Cada bloco também possui pontos de acesso sem fio, visando facilitar a utilização de dispositivos móveis.

3.2 EQUIPAMENTOS E CONFIGURAÇÕES

A infraestrutura de rede do Câmpus não possui um padrão de implementação, assim os equipamentos atuais são bastante heterogêneos. Os comutadores de camada 2 existentes, em sua grande maioria, não possuem interfaces de gerenciamento ou suporte à VLAN. Sendo assim todos os dispositivos conectados compartilham o mesmo domínio de broadcast. A rede não possui roteadores, esse papel é assumido por servidores.

Os pontos de acesso distribuídos pela Universidade propagam dois SSIDs (Service Set Identifier), são eles UTFPRADM e UTFPRWEB. Apenas professores e técnicos administrativos tem acesso à rede UTFPRADM, a qual dá acesso a recursos locais como, por exemplo, impressoras de rede. O outro SSID permite apenas acesso à *Internet*.

A configuração IP da rede está na faixa de endereços privativos 172.25.0.0/16. Porém apenas o range 172.25.3.0-172.25.7.255 é distribuído dinamicamente aos usuários que conectam através rede de cabeamento metálico, ou da rede sem fio pelo SSID UTFPRADM. A propagação da rede UTFPRWEB é feita por um equipamento localizado na reitoria da universidade na cidade de Curitiba.

Não há um número exato de dispositivos que se conectam à rede diariamente, mas estima-se que este número esteja em torno de 500 dispositivos, considerando computadores de laboratório, setores administrativos e dispositivos móveis.

3.3 GRUPOS DE ACESSO À REDE

O Câmpus Ponta Grossa possui quatro grupos principais de acesso à rede. Não necessariamente esses grupos possuem níveis de acesso diferenciados na rede. Abaixo são identificadas as formas pelas quais esses usuários podem se conectar à rede local:

Visitantes – São usuários externos à universidade e podem se conectar à rede através do cabeamento metálico ou por meio da rede sem fio. Para acesso sem fio é necessário que usuário requisite um usuário temporário.

Alunos – Os alunos da instituição podem acessar a rede via cabeamento metálico, ou rede sem fio. Para acessar a rede sem fio o usuário utiliza seu código de registro acadêmico e sua senha pessoal.

Técnicos Administrativos – Os técnicos administrativos possuem computadores pessoais disponibilizados pela instituição conectados em cabeamento metálico. Em casos

onde se faz necessária a utilização da rede sem fio os funcionários podem utilizar os dados da conta de e-mail institucional.

Professores – Os professores geralmente fazem uso de dispositivos móveis e podem acessar a rede sem fio com as credenciais do e-mail institucional. O acesso também pode ser feito via rede de cabo metálico.

3.4 **PROBLEMAS ENCONTRADOS**

Tendo em vista o grande número de dispositivos que se conectam a uma rede com apenas um domínio de broadcast, podemos relacionar os seguintes problemas:

- Existe um grande número de mensagens broadcast gerando tráfego desnecessário na rede.
- Existem situações onde o envio descontrolado de mensagens broadcast torna a rede intrafegável para todos os dispositivos conectados.
- Encontra-se grande dificuldade no gerenciamento e identificação de dispositivos com problemas na rede, uma vez que os equipamentos de comutação não são gerenciáveis.
- Uma vez que todos os dispositivos estão em um único domínio de broadcast, é possível que um dispositivo se conecte e explore vulnerabilidades na rede.

3.5 **PROPOSTA DE SEGMENTAÇÃO DE REDE**

Uma visão geral da proposta pode ser consultada através do diagrama de rede representado na figura 7.

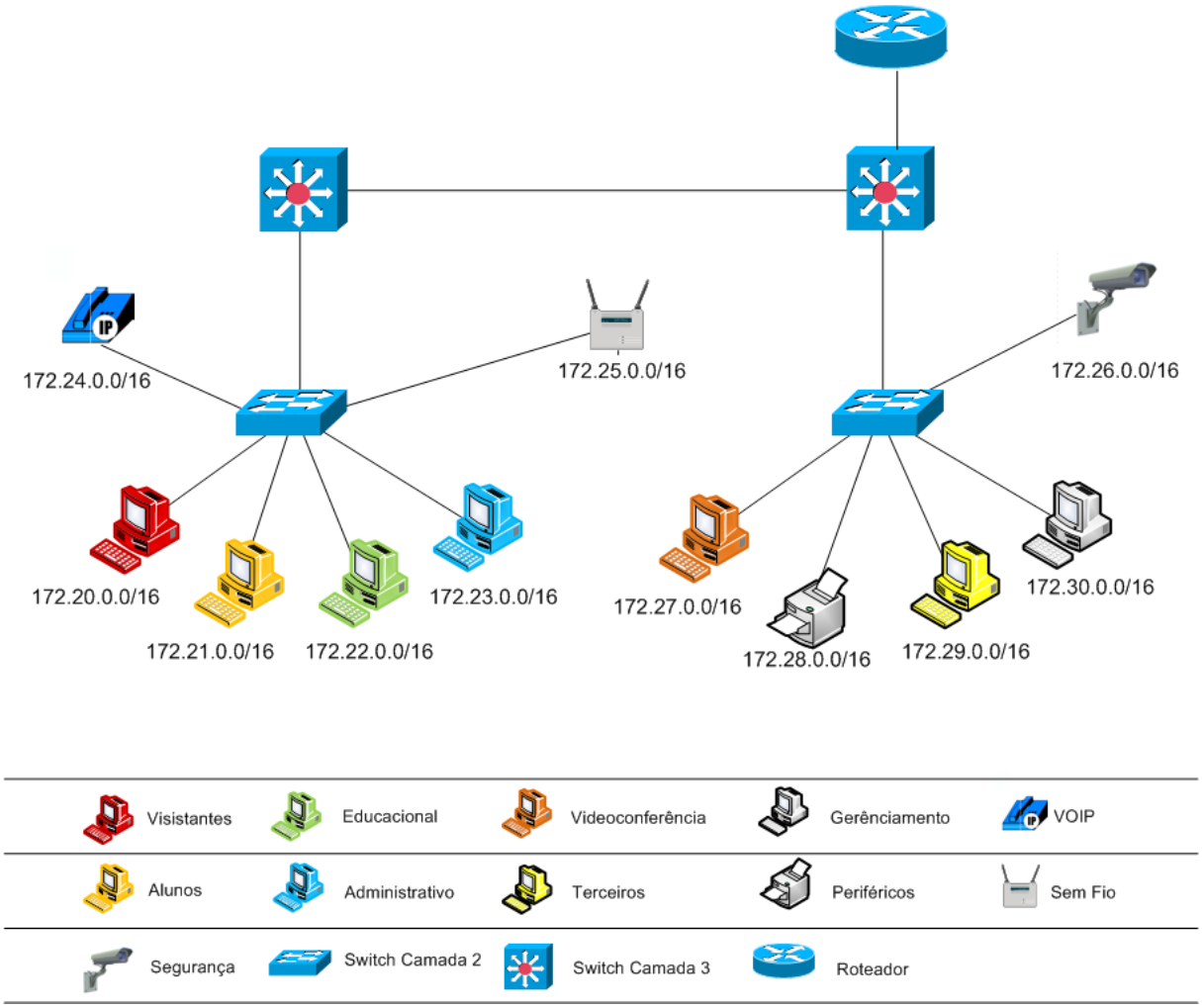

Figura 7 – Diagrama lógico de rede segmentada por VLANs.

Fonte: Autoria própria.

O diagrama da figura 7 não representa a disposição física de todos os equipamentos do câmpus, mas a partir dele é possível compreender a proposta de divisões lógicas para a rede. No cenário real existirão dois *switches* de camada 3 e vários outros de camada dois. As VLANs serão configuradas de acordo com as necessidades de cada ambiente pela configuração manual de portas do *switch*. Os *switches* terão conexão remota habilitada a fim de facilitar o gerenciamento e suas configurações. Abaixo são descritas onze VLANs como sugestão de implementação no câmpus Ponta Grossa da UTFPR.

3.6 **VLANS PROPOSTAS**

A seguir serão apresentadas e classificadas algumas VLANs propostas para aumentar o nível de segurança e eficiência bem como facilitar o gerenciamento da rede do Câmpus Ponta Grossa. As restrições de acesso sugeridas configurados por ACLs.

3.6.1 VLAN VISITANTES

A VLAN visitantes como o próprio nome sugere é destinada à usuários que visitam o câmpus, mas não possuem vínculo com a instituição. Poderá ser utilizada em semanas acadêmicas, simpósios ou congressos e eventos externos realizados no câmpus. O cliente conectado a esta VLAN não terá acesso a nenhum recurso local da rede, como por exemplo, servidores e impressoras. A VLAN visitantes dará acesso exclusivamente à *Internet*.

3.6.2 VLAN ALUNOS

A VLAN de alunos será utilizada para todos os dispositivos fixos utilizados por alunos, como por exemplo, os computadores dos laboratórios de informática. Esses usuários poderão ter acesso a alguns servidores e podem conectar-se à *Internet* por meio de suas credenciais de aluno.

3.6.3 VLAN EDUCACIONAL

Os funcionários alocados em setores e departamentos envolvidos diretamente com a educação, farão uso da VLAN educacional. A VLAN dará acesso a servidores e impressoras conectados a rede e que pertençam a este grupo. Também fornecerá acesso à *Internet* por meio das credenciais do e-mail institucional do usuário.

3.6.4 VLAN ADMINISTRATIVO

Os computadores presentes nos setores e departamentos que fazem parte da administração do câmpus farão parte da VLAN administrativa. Os clientes desta VLAN terão

acesso a servidores e periféricos do mesmo grupo. Assim como a VLAN educacional, o acesso à *Internet* será feito por meio das credenciais do e-mail institucional.

3.6.5 VLAN TELEFONIA

A VLAN em questão servirá para prover suporte a uma futura utilização da tecnologia de voz sobre IP (VOIP – *Voice Over Internet Protocol*), ou seja será destinada apenas ao tráfego de voz.

3.6.6 VLAN SEM-FIO

O câmpus possui equipamentos de transmissão sem fio espalhados por toda a unidade. Esses equipamentos serão atribuídos à VLAN rede sem fio.

3.6.7 VLAN SEGURANÇA

Esta VLAN de segurança será utilizada para o monitoramento do câmpus por intermédio de câmeras IP. A VLAN em questão deverá ser utilizada apenas pelos equipamentos e computadores de monitoramento.

3.6.8 VLAN VIDEOCONFERÊNCIA

A VLAN será utilizada para tornar possível a realização de videoconferências em qualquer ponto do Câmpus. Os equipamentos de videoconferência necessitam de um IP Público viabilizar seu funcionamento, sendo assim essa rede será conectada diretamente ao *switch* de acesso à *Internet*.

3.6.9 VLAN PERIFÉRICOS

Os periféricos que não estiverem contidos em nenhuma das VLANs relacionadas acima farão parte desta VLAN. Por exemplo, algumas salas de aula possuem equipamentos de projeção que podem ser conectados a rede local, esses equipamentos farão parte da VLAN de

periféricos. Apenas usuários das VLANs administrativa e educacional poderão utilizar estes equipamentos via rede.

3.6.10 VLAN TERCEIROS

Esta VLAN é destinada às empresas que utilizam a rede do câmpus mas não fazem parte da instituição. Empresas encubadas no Hotel Tecnológico utilizarão tal VLAN que fornecerá acesso apenas a serviços de e-mail e web.

3.6.11 VLAN GERENCIAMENTO

A VLAN de gerenciamento será utilizada para administração e configuração remota dos equipamentos de rede. Apenas os administradores da rede terão acesso a ela.

3.7 CRIAÇÃO DE DOMÍNIO VTP

A utilização de um domínio VTP é proposta a fim de facilitar a administração e configuração do ambiente segmentado. Entretanto este é um protocolo proprietário Cisco e funciona apenas para *switches* do fabricante. As configurações básicas do protocolo são:

VTP domain name – define o nome do domínio.

VTP mode – define se o *switch* será um servidor, cliente ou apenas encaminhará de forma transparente as atualizações do domínio.

VTP version – define a versão de utilização (todos os *switches* devem ser configurados com a mesma versão).

VTP password – define uma senha para o domínio.

VTP pruning – elimina tráfego desnecessário.

Caso sejam utilizados equipamentos Cisco para a implementação da proposta de segmentação, o nome do domínio que será criado receberá o nome de “UTFPR-PG”, onde dois *switches* serão configurados como servidor e os demais como clientes. A versão utilizada será a mais atual possível e a senha do domínio será definida segundo os padrões de segurança adotados pelo setor responsável.

3.8 **CONFIGURAÇÃO DE ENDEREÇAMENTO**

Ao adotarmos a utilização de VLANs em uma rede, devemos também criar suas respectivas sub-redes de endereçamento IP. A configuração de endereço IP será feita de forma manual e automática. A atribuição automática de IPs é realizada por um servidor através do protocolo DHCP (*Dynamic Host Configuration Protocol*), enquanto a configuração manual será realizada diretamente no equipamento. Na tabela 1 estão relacionadas as faixas de IP a serem utilizadas por cada VLAN bem como a forma como serão atribuídos os IPs.

Tabela 3 – Endereçamento de Vlans

VLAN	Identificação da VLAN	Faixa de Endereçamento IP	Atribuição de Endereçamento
VLAN 20	VISITANTES	172.20.0.1 – 172.20.3.254	Automático
VLAN 21	ALUNOS	172.21.0.1 – 172.21.3.254	Automático
VLAN 22	EDUCACIONAL	172.22.0.1 – 172.22.3.254	Automático
VLAN 23	ADMINISTRATIVO	172.23.0.1 – 172.23.3.254	Automático
VLAN 24	TELEFONIA	172.24.0.1 – 172.24.3.254	Manual
VLAN 25	SEM-FIO	172.25.0.1 – 172.25.3.254	Automático
VLAN 26	SEGURANÇA	172.26.0.1 – 172.26.3.254	Automático
VLAN 27	VIDEOCONFERÊNCIA	200.134.81.17-200.134.81.30	Manual
VLAN 28	PERIFÉRICOS	172.28.0.1 – 172.28.3.254	Manual
VLAN 29	TERCEIROS	172.29.0.1 – 172.29.3.254	Automático
VLAN 30	GERÊNCIAMENTO	172.30.0.1 – 172.30.3.254	Manual

Fonte: Autoria Própria.

Pode-se observar que todas as faixas criadas diferem entre si apenas no segundo octeto, essa configuração foi definida a fim de facilitar identificação das diferentes VLANs. Consultando o IP atribuído a um dispositivo é possível saber a qual VLAN ele pertence de forma rápida prática. Não é necessário saber onde começa e onde termina uma sub-rede, nem saber à qual porta e a qual *switch* o dispositivo está conectado. Por exemplo, se no segundo octeto temos o valor decimal igual a 20 o dispositivo pertence à VLAN visitantes, se esse valor for igual a 25 então pertence à VLAN de segurança.

4 CONCLUSÃO

As redes locais são hoje, elementos essenciais para uma organização. Entretanto seu desempenho deve ser satisfatório, pois essa interfere diretamente em questões de produtividade. Geralmente, problemas de desempenho são observados em casos onde houve um crescimento não planejado da rede local. Quando há o aumento de dispositivos conectados a um mesmo domínio de *broadcast*, aumentam também as chances de se ter um colapso geral na rede. Isso pode durar segundos, minutos ou horas, até que a raiz do problema seja encontrada e a rede volte ao normal.

Este trabalho traz uma proposta de segmentação para a rede local da Universidade Tecnológica Federal do Paraná, Câmpus Ponta Grossa, e tem como objetivo principal, tornar a rede mais robusta, segura e eficiente. Apesar de ter sido pensada para atender uma rede específica, pode ser facilmente adaptada à outras realidades. Para a criação da proposta foram relacionados os perfis de acesso existentes no câmpus, bem como possíveis perfis que possam vir a coexistir em um futuro breve.

Além dos conceitos primordiais de VLANs, foram apresentadas soluções para facilitar o gerenciamento e aumento da segurança da rede seguimentada. Pode-se verificar que, a criação de um domínio VTP torna mais fácil a administração das VLANs disponíveis em uma rede. Uma vez que as VLANs são criadas a partir de um *switch* configurado como VTP Server, essas são propagadas através dos enlaces tronco para todos os *switches* conectados em modo cliente. Da mesma maneira a aplicação de ACLs permite um controle justo na filtragem do encaminhamento de pacotes entre VLANs diferentes.

5 REFERÊNCIAS

FILIPPETTI, Marco Aurélio., **CCNA 4.1 (Exame 640-802): Guia Completo de Estudo**. Florianópolis: Editora Visual Books, 2008. 478 p.

FOROUZAN, Behrouz A., **Comunicação de Dados e Redes de Computadores**. 3ªEd. Porto Alegre: Bookman, 2006. 840 p.

KUROSE, James F., ROSS, Keith W., **Redes decomputadores e a *Internet*: Uma abordagem top-down**. São Paulo: Pearson Addison Wesley, 2006. 634 p.

PERLMAN, R., **Interconnections: Bridges, Routers, Switches, and Internetworking Protocols.** 2ªEd. Addison-Wesley, 1999.

STEVENS, W.R., **TCP/IP Illustrated, Volume 1: The Protocols**. Addison-Wesley, 1994. 519p.

STALLINGS, W., **Redes e Sistemas de Comunicação de Dados** 5ªEd., Editora Campus Elsevier, 2005.

TANENBAUM, A. C., **Redes de Computadores**. 4ªEd. Rio de Janeiro: Campus, 2003.

APÊNDICE A

Comandos para a criação das VLANs no *switch* de camada 3.

Todas as VLANs foram criadas no *switch* de camada 3 e posteriormente serão distribuídas aos demais através do protocolo VTP.

```
Switch-Layer3(config)#vlan 20
Switch-Layer3(config-vlan)#name visitantes
Switch-Layer3(config-vlan)#vlan 21
Switch-Layer3(config-vlan)#name alunos
Switch-Layer3(config-vlan)#vlan 22
Switch-Layer3(config-vlan)#name educacional
Switch-Layer3(config-vlan)#vlan 23
Switch-Layer3(config-vlan)#name administrativo
Switch-Layer3(config-vlan)#vlan 24
Switch-Layer3(config-vlan)#name telefonia
Switch-Layer3(config-vlan)#vlan 25
Switch-Layer3(config-vlan)#name sem-fio
Switch-Layer3(config-vlan)#vlan 26
Switch-Layer3(config-vlan)#name seguranca
Switch-Layer3(config-vlan)#vlan 27
Switch-Layer3(config-vlan)#name videoconferencia
Switch-Layer3(config-vlan)#vlan 28
Switch-Layer3(config-vlan)#name perifericos
Switch-Layer3(config-vlan)#vlan 29
Switch-Layer3(config-vlan)#name terceiros
Switch-Layer3(config-vlan)#vlan 30
Switch-Layer3(config-vlan)#name gerenciamento
```

Configuração de portas

As portas do switch camada 3 foram configuradas em modo conforme o exemplo e permitem o trafego de todas as VLANs criadas no projeto.

```
Switch-Layer3(config)#interface f0/0
Switch-Layer3(config)#no shutdown
Switch-Layer3(config)# interface f0/0.20
Switch-Layer3(config-subif)# encapsulation dot1Q 20
Switch-Layer3(config)# interface f0/0.21
Switch-Layer3(config-subif)# encapsulation dot1Q 21
Switch-Layer3(config)# interface f0/0.22
Switch-Layer3(config-subif)# encapsulation dot1Q 22
Switch-Layer3(config)# interface f0/0.23
Switch-Layer3(config-subif)# encapsulation dot1Q 23
Switch-Layer3(config)# interface f0/0.24
Switch-Layer3(config-subif)# encapsulation dot1Q 24
Switch-Layer3(config)# interface f0/0.25
Switch-Layer3(config-subif)# encapsulation dot1Q 25
Switch-Layer3(config)# interface f0/0.26
Switch-Layer3(config-subif)# encapsulation dot1Q 26
Switch-Layer3(config)# interface f0/0.27
Switch-Layer3(config-subif)# encapsulation dot1Q 27
Switch-Layer3(config)# interface f0/0.28
Switch-Layer3(config-subif)# encapsulation dot1Q 28
Switch-Layer3(config)# interface f0/0.29
Switch-Layer3(config-subif)# encapsulation dot1Q 29
Switch-Layer3(config)# interface f0/0.30
Switch-Layer3(config-subif)# encapsulation dot1Q 30
```

O exemplo apresentado configura subinterfaces para a porta f0/0. Através do protocolo 802.1q é possível a comunicação com as Vlans criadas.

Os switches de camada 2 terão suas portas configuradas manualmente conforme a necessidade de cada ambiente, sendo que a porta mais alta, neste caso f0/24, será configurada em modo de entroncamento. A porta configurada em modo tronco será conectada diretamente ao switch principal.

Configuração switch camada 2:

```
Switch-Layer2(config)#interface f0/1
Switch-Layer2(config-if)#switchport mode access
Switch-Layer2(config-if)#switchport access vlan20
Switch-Layer2(config)#interface f0/24
Switch-Layer2(config-if)#switchport mode trunk
Switch-Layer2(config-if)# switchport trunk allowed vlan 20-30
```

Configuração do domínio VTP

Abaixo seguem as configuração necessárias para tornar o switch camada 3 em um servidor VTP e os demais switches em clientes VTP.

Configuração VTP Server:

```
Switch-Layer3(config)#vtp mode server
Switch-Layer3(config)#vtp domain UTFPR-PG
Switch-Layer3(config)#vtp password utfpr
Switch-Layer3(config)#vtp version 2
```

Configuração VTP Cliente:

```
switch(config)#vtp mode client
Switch(config)#vtp password utfpr
```

Configuração do serviço de DHCP

As configurações do servidor DHCP devem ser feitas para todas as Vlans conforme demonstrado abaixo a partir da Vlan 20. O primeiro comando exclui o IP que servirá de Gateway da Vlan, pois este será configurado manualmente.

```
Switch-Layer3(config)#ip dhcp excluded-address 172.20.0.1
Switch-Layer3(config)#ip dhcp pool vlan20
Switch-Layer3(dhcp-config)#network 172.20.0.0 255.255.0.0
Switch-Layer3(dhcp-config)#default-router 172.20.0.1
Switch-Layer3(dhcp-config)#dns-server 8.8.8.8
```