

## REDES LOCAIS VIRTUAIS

Rômulo Raimundo de Andrade Rotondaro<sup>1</sup>  
Matheus Guedes<sup>2</sup>

### RESUMO

O artigo tem como escopo principal a vantagem de uma Rede Local Virtual (VLAN), onde o mesmo destina-se a entender como é seu funcionamento, desde a sua configuração por software até a sua economia, reduzindo custo e tempo, como por exemplo, em uma migração de estações que são transferidas de um grupo para outro. Através de estudos podem-se comparar os tipos de VLANs, sendo elas de forma estática ou dinâmica, baseando-se no número de portas de Switches como uma característica para participação. Associados por endereços MACs, os dispositivos podem ser movidos para qualquer localização dentro da organização, que continuarão a fazer parte da mesma rede virtual. As VLANs agrupam protocolos diferentes em redes, além dos benefícios, que possibilitam a divisão da rede em vários segmentos, mesmo se a estrutura física for a mesma, os dispositivos de rede são separados logicamente. Em suma, têm-se as VLANs como uma rede local virtual que oferece inúmeras vantagens, desde a sua agilidade, fácil manuseio, baixo custo e alto desempenho.

**Palavras-chave:** Rede Local Virtual.VLAN.MAC.Software.

### 1 – INTRODUÇÃO

O presente trabalho é sobre VLANs, mais concretamente Virtual Local Area Network que é basicamente uma rede lógica onde podemos agrupar várias máquinas de acordo com vários critérios.

Objetivo deste artigo é através de apuramento aprofundar sobre as redes VLANs e apresentar as vantagens na rede tais como maior flexibilidade para a administração, ganho em segurança, redução da divulgação do tráfego sobre a rede.

A implantação de VLANs (Virtual Local Área Network) tem como foco principal aumentar o controle de tráfego da rede, diminuir o alcance disseminação de broadcast e de pragas virtuais, melhorando assim consideravelmente o desempenho e a segurança de uma determinada rede corporativa.

---

<sup>1</sup> Aluno pesquisador, pós-graduando em Tecnologia e Gerenciamento de Redes de Computadores pela UNIS-MG. rominho111@hotmail.com

<sup>2</sup> Professor orientador, especialista MBA em Gestão Estratégica e Inteligência em Negócios pelo Centro Universitário do Sul de Minas. orientadormatheus@unis.edu.br

Está organizado em cinco partes. Na primeira parte será abordado o que é VLAN e quais os tipos de VLAN na segunda parte serão abordados os benefícios e tipos de conexões dos dispositivos e na terceira parte os Padrões IEEE 802.1Q e identificação de quadros (frames), na quarta e última parte as Entradas dinâmicas.

A metodologia utilizada foi à pesquisa bibliográfica, enriquecida com artigos científicos.

## **2 - O QUE É VLAN E QUAIS OS TIPOS DE VLAN**

### **2.1 – VLAN**

Uma Virtual Local Area Network (VLAN) é uma rede local que agrupa um conjunto de máquinas de maneira lógica e não física. (PILLOU, 2014).

Uma estação é considerada parte de uma LAN se pertence fisicamente a ela. O critério de participação é geográfico. O que acontece se precisarmos de uma conexão virtual entre duas estações pertencentes a duas LANs físicas diferentes? Podemos definir de forma grosseira uma VLAN como uma rede local configurada por software em vez de fiação física. (FOROUZAN, 2010).

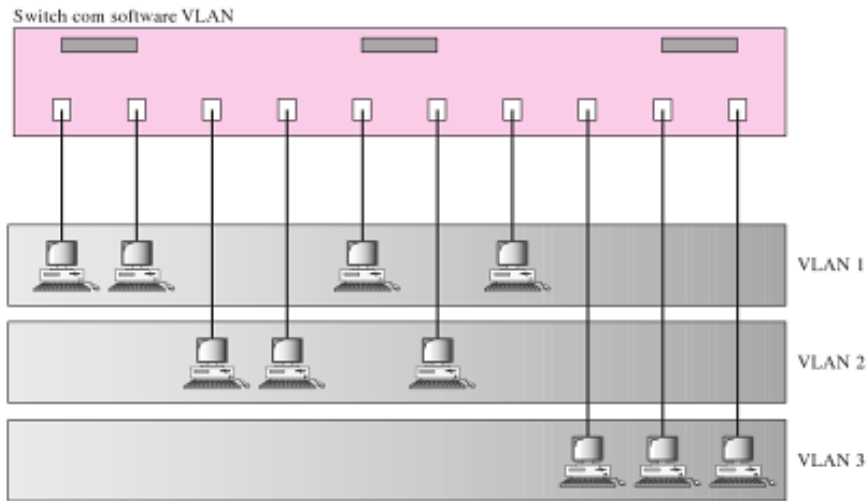
Segundo frinhani (2005, P.45): “Uma VLAN é a união de dispositivos de uma rede local em um agrupamento lógico que tem a intenção de segmentar a rede em pequenos domínios de difusão”.

As VLANs se baseiam em switches especialmente projetados para reconhecê-las. Para configurar uma rede baseada em VLANs, o administrador da rede decide quantas delas haverá, quais computadores estarão em qual VLAN e qual será o nome de cada uma. (TANEMBAUM, 2011).

A ideia central da tecnologia VLAN é dividir uma LAN em segmentos lógicos em vez de físicos. Uma LAN pode ser dividida em diversas LANs lógicas denominadas VLANs. Cada VLAN é um grupo de trabalho na organização. Se uma pessoa for transferida de um grupo para outro, não há nenhuma necessidade de alterar a configuração física. A participação em um grupo em VLANs é definida por software, não por hardware. Qualquer estação pode ser transferida logicamente para outra VLAN. Todos os membros pertencentes a uma VLAN podem receber mensagens de broadcast enviadas para essa VLAN em particular. (FOROUZAN, 2010).

A Figura 1 mostra a mesma LAN comutada subdividida em VLANs.

**Figura 1** – Um switch usando software VLAN



**Fonte:** adaptado de Forouzan, 2010.

## 2.2 Tipos de VLAN

As portas de um *switch* podem pertencer a uma ou mais VLANs. Para fazer parte de uma rede virtual, a porta de um *switch* deve ser associada à VLAN. Os métodos de associação de VLANs podem ser configurados para trabalhar de forma estática ou dinâmica (CISCO SYSTEMS, 2007).

Segundo Filippetti, (2008) o método de associação de VLAN estática é o mais comum e fácil de monitorar, desde que implantado em um ambiente de rede com poucos usuários.

Nas VLANs do tipo estática, uma ou mais portas do *switch* são designadas a uma determinada VLAN pertencendo a esta até que o administrador de rede altere estas configurações (FILIPPETTI, 2008).

Após a criação da rede lógica, um *range* de portas do *switch* são conferidas a VLAN. Os dispositivos conectados as portas irão pertencer as VLANs associadas. Caso o cliente mude de porta, pode ocorrer de este usuário trocar de VLAN. Por este motivo, este método requer maior controle por parte do administrador (CISCO SYSTEMS, 2007).

O método de atribuição de VLAN dinâmica funciona de maneira em que um dispositivo conectado a um segmento de rede receba uma atribuição de VLAN de forma automatizada. Utilizando aplicações que realizem este tipo de tarefa, é possível associar VLANs através de endereçamento de *hardware*, conhecido como endereço MAC, por protocolos ou de forma autenticada (FILIPPETTI, 2008).

### 2.2.1 - VLAN Baseada em Portas

Alguns fabricantes usam os números de portas de Switches como uma característica para participação. Por exemplo, o administrador pode definir que estações conectadas às portas 1, 2, 3 e 7 pertencem à VLAN 1; estações conectadas às portas 4, 4, 10 e 12 pertencem à VLAN 2 e assim por diante. (FOROUZAN, 2010).

No uso desta técnica, a porta é associada a uma determinada VLAN sem levar em conta o utilizador ou o sistema conectado á porta, mesmo que sejam oriundos de edifícios ou pisos diferentes. (BARROS, 2007).

**Tabela 1** – Atribuição das portas às VLANs

PORTAS	1	2	3	4	5	6	7	8	9
VLAN	1	1	1	2	2	2	1	2	1

Fonte – Próprio Autor.

Este método apresenta a desvantagem, quando se refere á conexão de um repetidor, um hub ou qualquer outro dispositivo de rede partilhado a uma porta pertencente a uma VLAN, todos os equipamentos conectados a este dispositivo passarão a fazer parte deste VLAN. Por outro lado, caso haja uma deslocação de uma porta para outra, ou da estação para um local diferente, fora do dispositivo ao qual se encontrava conectado, o administrador da rede terá de reconfigurar a VLAN associando esta á sua anterior VLAN. (BARROS, 2007).

### 2.2.2 - VLAN Associados por Endereço MAC

Outra forma de agrupamento de VLANs se faz através do endereço físico das interfaces de rede dos dispositivos (endereço MAC). Neste método, o administrador de redes associa um endereço MAC de um dispositivo a uma determinada VLAN no switch. Assim os dispositivos podem ser movidos para qualquer localização, dentro da organização, que continuarão a fazer parte da mesma rede virtual, sem qualquer reconfiguração posterior. (HAFFERMANN, 2009).

**Tabela 2** - Atribuição de MAC as VLANs

Endereço MAC	00239A738B11	00F42230BG23	00F4GG509NF1
VLAN	1	1	2

Fonte – Próprio Autor.

Para a Cisco System (2003) uma das desvantagens da implementação de VLANs com base nos endereços MAC, é a exigência de que todos os utilizadores estejam configurados logo no início em pelo menos uma VLAN. Após a inicial configuração manual, os utilizadores poderão então ser encaminhados automaticamente, dependendo das soluções do fabricante.

Contudo, essa exigência de uma configuração prévia obrigatória, impede que utilizadores não autorizados se conectem á rede apresentando assim um acréscimo á

segurança, por outro lado, a atribuição inicial torna-se muito exigente quando se trata de uma rede ampla, ou seja, uma rede que dispõe de um elevado número de utilizadores, não é fácil de configurar, sendo que cada posto de trabalho requer uma “assinatura” explicitamente particular a uma VLAN, dificultando desta forma toda a tarefa de configuração, dificultando também na detecção e resolução de problemas. (BARROS, 2007).

### 2.2.3 - VLANS Baseado em Protocolos de Rede

Em redes onde são suportados protocolos diferentes (IP, IPX, NetBIOS, Apple Talk) este método pode ser usado para agrupar cada protocolo em uma VLAN diferente. Os comutadores verificam cada pacote para identificar a qual rede virtual o mesmo está associado por meio do tipo de protocolo usado. Apesar de se basear em endereçamento de 3º nível estes comutadores não realizam funções de roteamento, sendo restritamente usado para identificação e agrupamento das VLANs. (HAFFERMANN, 2009).

**Tabela 3** - Associação de protocolos de rede á VLAN

Protocolos	IP	IPX	NETBIOS	APPLE TALK
VLAN	1	2	3	1

Fonte – Próprio Autor.

Segundo Mollinari (1999), neste tipo de VLAN a identificação dos membros é feita com base em informações da camada de rede, mas ainda assim, não se deve confundir esta etapa com a função de routing geral da rede.

O particionamento por protocolo e a mobilidade física das estações de trabalho sem a necessidade de reconfiguração de endereços IP, estão dentre as vantagens de se utilizar este tipo de VALN. Uma das desvantagens deste tipo de VLAN sobre os dois tipos anteriores está relacionado ao desempenho. É necessário mais tempo para se inspecionar endereços IP em pacotes de transmissão do que endereços MAC em quadros. Além deste fato, as VLANs por agrupamento de protocolo possuem dificuldades ligadas aos protocolos não roteáveis como NetBIOS. (FRINHANI, 2005).

## 3- BENEFÍCIOS E TIPOS DE CONEXÕES DOS DISPOSITIVOS

Em muitas empresas, as mudanças organizacionais ocorrem o tempo todo; isso significa que os administradores de sistemas passam muito tempo retirando plugues e inserindo-os de novo em algum outro lugar. Além disso, em alguns casos, a mudança não pode ser feita de modo algum, porque o par trançado da máquina do usuário está longe demais do hub correto (por exemplo, em outro edifício). Em resposta à solicitação de usuários que desejam maior flexibilidade, os fornecedores de redes começaram a buscar um meio de recompor a fiação dos edifícios inteiramente em software. O conceito resultante é chamado

VLAN (Virtual LAN) e foi até mesmo padronizado pelo comitê 802. Atualmente, ele está sendo desenvolvido em muitas organizações. (TANEMBAUM, 2011).

A VLAN possibilita a divisão da rede em vários segmentos, apesar de a estrutura física ser a mesma, os dispositivos de rede presentes em uma VLAN são separados logicamente, por isso o nome de rede virtual (CISCO SYSTEMS, 2007).

### **3.1.1 - CONTROLE DO TRÁFEGO BROADCAST**

Da mesma maneira que os comutadores isolam domínios de colisão e repassam o tráfego para a porta apropriada, VLANs refinam este conceito provendo um isolamento completo entre as VLANs. Uma VLAN é um único domínio de difusão e todo o tráfego broadcast ou multicast é contido por ela. Diferente de um sistema que utiliza mídia compartilhada, onde somente uma estação poderá transmitir por vez, uma rede comutada permite que várias transmissões concorrentes possam acontecer sem afetar diretamente outras estações que estejam dentro ou fora do seu domínio de difusão. (FRINHANI, 2005).

### **3.1.2 - AUMENTO DE NÍVEL DE SEGURANÇA**

Um dos principais benefícios da utilização de VLANs para segmentação de redes é a segurança, visto que esta proporciona uma separação lógica do tráfego de uma rede virtual composta por servidores, por exemplo, da rede virtual dos usuários de uma corporação. Porém, o uso de algumas soluções complementares pode reforçar ainda mais a segurança de uma rede composta por VLANs. (HAFFERMANN, 2009).

As VLANs fornecem uma medida extra de segurança. Pessoas pertencentes ao mesmo grupo podem enviar mensagens de broadcast com absoluta garantia de que os usuários nos demais grupos não receberão essas mensagens. (FOROUZAN, 2010).

### **3.1.3 - SEGMENTAÇÃO LÓGICA DA REDE**

A criação de VLAN pode ser baseada na própria estrutura organizacional da empresa. Por conseguinte, o administrador da rede consegue agrupar utilizadores pertencentes ao mesmo departamento ou grupo de trabalho, independente deles estarem no mesmo espaço físico ou não. Deste modo pode possibilitar assim uma segmentação lógica da rede. (BARROS, 2007).

Em determinadas organizações, alguns sectores devem pertencer a uma VLAN diferente das restantes. O propósito disso é proteger informações sigilosas, como é o caso do departamento financeiro (HAFFERMANN, 2009).

### **3.1.4 - REDUÇÃO DE TEMPO E CUSTOS**

As VLANs podem reduzir o custo de migração de estações que são transferidas de um grupo a outro. A reconfiguração física leva tempo e é dispendiosa. Em vez de transferir

fisicamente uma estação para outro segmento ou até mesmo para outro Switch, é muito mais fácil e rápido transferi-la via software. (FOROUZAN, 2010).

A utilização de uma VLAN conduz a uma solução de criação e gestão de rede, com um custo inferior do que as redes tradicionais. Não há necessidade da existência de um switch para cada domínio de broadcast, e de várias configurações de interfaces de ligação do router para o switch. Um só switch com VLAN consegue suportar múltiplos domínios de broadcasts e necessita só uma configuração de interface de ligação entre o switch e o router. (VÉSTIAS, 2005).

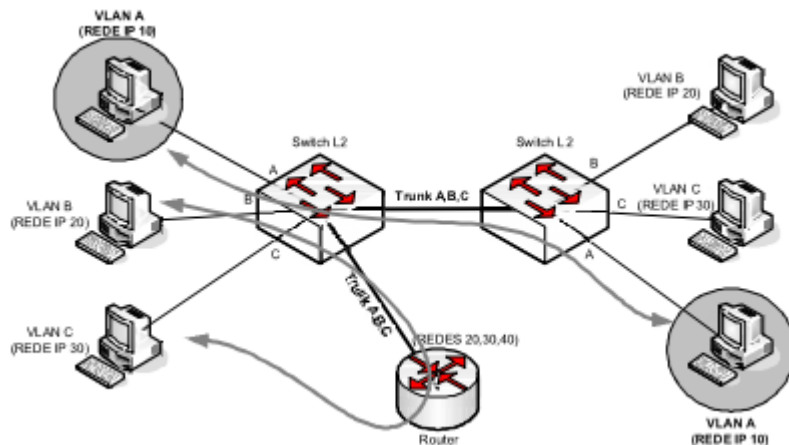
Moraes (2010) ressalta que a utilização do recurso de redes virtuais e demais mecanismos presentes nos switches são poucos exploradas pelas organizações, recursos estes que podem aprimorar o desempenho das redes dentro de um ambiente corporativo.

### 3.2 - TIPOS DE CONEXÕES DOS DISPOSITIVOS

Uma VLAN pode ser definida numa variedades de switches, e que estes processos de encaminhamentos de tramas são parecidos, como a de um só switch. Contudo apresentam problemas na necessidade de comunicar tramas de VLAN diferentes (VÉSTIAS, 2005).

Para que a comunicação na camada 3 entre os dispositivos aconteça, todos os dispositivos conectado à uma mesma VLAN devem estar inseridos em uma mesma rede IP. É importante ressaltar que é parte integrante de um bom projeto de redes colocar cada VLAN em uma rede IP diferente, pois desta forma, a comunicação inter-VLANs torna-se possível. Se duas VLANs distintas forem colocadas em uma mesma rede IP, a comunicação entre elas jamais será possível. Agindo de forma correta, cada VLAN fará parte de uma rede IP diferente e, desta forma, um router poderá permitia a comunicação inter-VLANs roteando os pacotes entre as diferentes redes IP. Observe a figura 2. (FILIPPETTI, 2008).

**Figura 2** – Comunicação inter-VLANs por intermédio de um router.



Fonte: adaptado de Filippetti, 2008.

Para melhor compreensão desse tipo de ligação existem dois tipos de ligação entre switches. (BRITO, 2011).

### **3.2.1 – LINKS DE ACESSO (ACCESS LINKS)**

Links que são apenas partes de uma VLAN e são tidos como a VLAN nativa da porta. Qualquer dispositivo conectado a uma porta ou link de acesso não sabe a qual VLAN pertence. Ele apenas assumirá que é parte de um domínio de broadcast, sem entender a real topologia da rede. Os switches removem qualquer informação referente às VLANs dos frames antes de enviá-los a um link acesso. Dispositivos conectados a links de acesso não podem se comunicar com dispositivos fora de sua própria VLAN, a não ser que um router faça o roteamento dos pacotes. (FILIPPETTI, 2008).

### **3.2.2 - LINKS DE TRANSPORTE (TRUNK LINKS)**

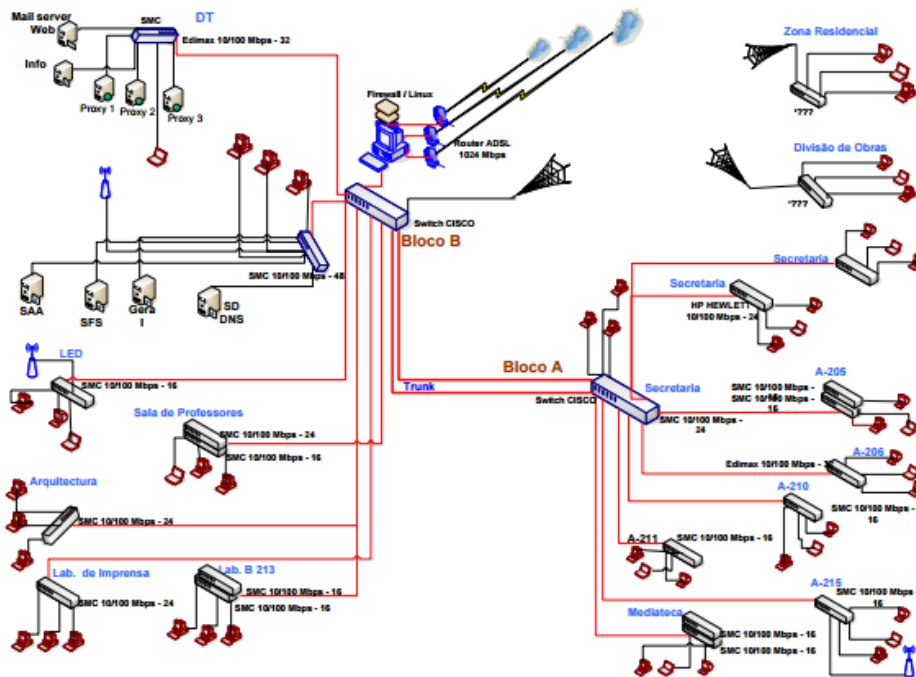
Inicialmente as VLANs apresentavam certas dificuldades na implementação através de redes, pelo que, cada VLAN era configurada manualmente em cada switch, dificultando desta forma a administração das mesmas em caso de rede extensa. Para piorar ainda mais a situação, cada fabricante de switch utilizava técnicas diferentes para implementar VLANs. Neste contexto surge o “VLAN trunking”, elaborado especificamente para resolver esses problemas. (BARROS, 2007).

O processo de "entroncamento" de links permite que você torne uma única interface (ou porta) de um switch ou servidor parte de múltiplas VLANs simultaneamente. O benefício disso é que um servidor, por exemplo, pode ser membro de duas ou mais VLANs de forma concomitante, o que evita que usuários de VLANs diferentes tenham de atravessar um router para poder ter acesso aos recursos desse servidor. (FILIPPETTI, 2008).

Mesmo estando em edifícios distantes à informação flui de VLAN a VLAN através do trunk link que permite controlar informações das VLANs entre switches. Como mostrado na figura 3. (BARROS, 2007).



**Figura 3** – Configuração das VLANs e Trunk Link



Fonte: adaptado de Barros, 2007.

#### 4- PADRÃO IEEE 802.1Q E IDENTIFICAÇÃO DE QUADROS (FRAMES)

Um pouco mais de reflexão sobre esse assunto revela que o importante é a VLAN do próprio quadro e não a VLAN da máquina transmissora. Se houvesse algum modo de identificar a VLAN no cabeçalho do quadro, a necessidade de inspecionar a carga útil desapareceria. No caso de nova LAN, como a 802.11 ou a 802.16, seria fácil simplesmente acrescentar um campo VLAN no cabeçalho. De fato, o campo Identificador de conexão no padrão 802.16 é de certa forma semelhante em espírito a um identificador de VLAN. No entanto, o que fazer no caso do padrão Ethernet, que é a LAN dominante e que não tem nenhum campo sobressalente que possa ser usado como identificador da VLAN? (TANEMBAUM, 2011).

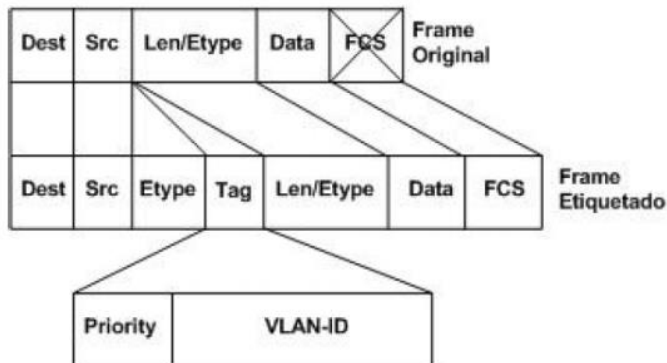
Em 1996, o subcomitê IEEE 802.1 aprovou um padrão denominado 802.1Q que define o formato para identificação de frames. O padrão também estabelece o formato a ser usado um backbones multicomutados e permite o uso de equipamentos de diferentes fornecedores em VLANs. O IEEE 802.1Q abriu caminho para padronização adicional em outras questões relacionadas a VLANs. (FOROUZAN, 2010).

O IEEE 802.1Q também como o do protocolo ISL é usada em interfaces FastEthernet e GigabitEthernet. A diferença é que, ela é usada quando pretendemos interligar equipamentos de fabricantes diferentes (Véstias, 2005).

O protocolo IEEE 802.1Q identifica quadros com o número de VLAN, usando um estilo de cabeçalho diferente do protocolo ISL. O protocolo IEEE 802.1Q simplesmente adiciona um cabeçalho de 4 bytes ao cabeçalho Ethernet original, que serve de identificador campo da VLAN. Contudo é necessário um novo cálculo de campo FCS original no Trailer Ethernet, porque o FCS é baseado no conteúdo do quadro inteiro. (Zacaron, 2007).

O mesmo pode ser conferido na figura 4.

**Figura 4** - Encapsulamento IEEE 802.1Q da trama



Fonte: adaptado de Zacaron, 2007.

## 4.2 - IDENTIFICAÇÃO DE QUADROS (FRAMES)

Um switch conectado a uma rede de grande porte necessita fazer um acompanhamento dos usuários e frames que atravessam o aglomerado de switches e VLANs. Uma "malha" de switches (também conhecida como switch fabric) é um grupo de switches que compartilham as mesmas informações de VLAN. O processo de identificação de frames (frame tagging) associa, de forma única, uma identificação a cada frame. Essa identificação é conhecida como VLAN ID ou VLAN color. (FILIPPETI, 2008)

A tecnologia de frame tagging foi criada pela Cisco para ser utilizada quando um frame Ethernet atravessasse um link de transporte (trunked link). A identificação (tag) da VLAN é removida do frame antes que ele deixe o link de transporte, tornando o processo totalmente transparente. Cada switch que o frame atravessa deve identificar o ID (tag) da VLAN a que ele pertence e, então, determinar o que fazer com ele baseado na tabela de filtragem (filter table). Caso o frame alcance um switch que possua outro link de transporte, ele será encaminhado através da porta onde esse link se encontra. Uma vez que o tframe alcance uma porta para um link de acesso, o switch remove a identificação da VLAN. O dispositivo final receberá os frames sem ter de entender à qual VLAN eles pertencem, garantindo a transparência do processo. (FILIPPETI, 2008).

Em um processo de comunicação, quando o tráfego de rede atravessa os comutadores, estes devem ser capazes de identificar as quais VLANs os pacotes fazem parte. Esta

identificação pode ser feita através do reconhecimento dos quadros que pode ser realizada pelos métodos implícito e explícito: (HAFFERMANN, 2009).

- Método implícito: ou marcação implícita (implicit tagging) caracteriza os quadros que não são rotulados. Os comutadores identificam a VLAN a que este quadro pertence através de informações contidas em seus cabeçalhos como, por exemplo, a porta por onde o quadro chegou ou cruzando o endereço MAC com a tabela de associação das VLANs, para assim encaminhar os pacotes para o destino correto. Neste método os dispositivos da rede não necessariamente precisam saber que existe VLANs, pois o quadro permanece inalterado;
- Método explícito: ou marcação explícita (explicit tagging) ocorre quando um dispositivo de rede marca (tagg) o quadro com um identificador de VLAN acusando a qual rede virtual este quadro pertence. Neste método os dispositivos precisam saber da existência das VLANs, pois são inseridas informações referentes a esta identificação no cabeçalho do quadro, alterando seu tamanho, e caso um dispositivo que não suporte VLAN receba o quadro, este será descartado. Os dispositivos na rede devem também possuir uma base de dados, igual para todos, com informações de identificação de cada VLAN e onde encontrar estas informações nos quadros. Os dispositivos adicionam, ou não, a tagg de VLAN dependendo se o dispositivo de destino possui suporte, ou não, ao protocolo de VLAN (IEEE 802.1Q).

#### **4.2.1 CLASSIFICAÇÃO DE FRAMES**

A construção de quadros relacionados à VLANs são definidos pelas normas IEEE 802.3ac e IEEE 802.1Q e podem ser classificados como Untagged frames; Priority tagged frames e Tagged frames: (HAFFERMANN, 2009).

- Untagged frames: são frames ethernet comuns, sem qualquer marcação adicional;
- Priority Tagged frames: são frames que possuem a informação de classe de prioridade (IEEE 802.1p), porém sem nenhuma informação sobre identificação da VLAN. A tagg de prioridade possui 3 bits de tamanho e permite oito valores possíveis, podendo variar de zero a sete;
- Tagged frames: são frames que possuem a identificação da VLAN a que pertence no campo VID (Vlan Identifier) de oito bits. Os frames Untagged e Priority Tagged realizam a identificação das VLANs a que pertencem por meio da associação de portas, endereços MAC, protocolos entre outros. Já os frames Tagged não necessitam

d tal associação pois, como explicado anteriormente, já possuem a identificação da VLAN inclusa no cabeçalho.

## **5 - BASE DE DADOS DE FILTRAGEM (FILTERING DATABASE)**

Uma estrutura de banco de dados dentro do 'switch' que contém a relação das associações entre endereços MAC, escolhas das VLAN, e números das interfaces (portas). O 'Filtering Database' é encaminhado para quando uma VLAN contida no 'switch' produz uma decisão de envio em um 'frame'. (BOTH, 2000).

As informações dos membros de uma VLAN são armazenadas em uma base de dados de filtragem (Filtering Database) que consiste de dois tipos de entrada: estáticas e dinâmicas. (MORAES, 2002).

### **5.1.1 - ENTRADAS ESTÁTICAS**

Uma entrada estática é adicionada, modificada ou removida apenas por gerenciamento, ou seja, não são tratadas automaticamente. Existem dois tipos de entradas estáticas:

- Entrada Estáticas de Filtragem, que especificam para cada porta, se quadros devem ser enviados para um dado endereço MAC específico ou grupo de endereços e, em uma VLAN específica, devem ser encaminhados ou descartados, ou deve seguir a entrada dinâmica.
- Entrada Estáticas de Registro, que especificam se quadros a serem enviados para uma determinada VLAN serão rotulados ou não e quais portas são registradas para esta VLAN.

### **5.1.2 - ENTRADAS DINÂMICAS**

As entradas dinâmicas são aprendidas pelo dispositivo de rede e não podem ser criadas ou atualizadas por gerenciamento. O processo de aprendizagem (treinamento) observa a porta de onde o quadro, com um dado endereço fonte e um identificador VLAN (VID), foi recebido e atualiza a base de dados de filtragem (filtering database). A entrada só é atualizada se todas as seguintes condições forem satisfeitas:

- Esta porta permite aprendizado
- O endereço fonte (source address) é uma estação de trabalho válida e não um endereço de grupo (group address)
- Há espaço disponível na base de dados

As entradas são removidas da base de dados de acordo com o processo de "saída por envelhecimento" (ageing out process). Neste processo, depois de um certo tempo especificado

por gerenciamento, as entradas permitem a reconfiguração automática da base de dados de filtragem, em caso de mudança na topologia da rede. (MORAES, 2002).

Existem três tipos de entradas dinâmicas:

- Entradas Dinâmicas de Filtragem, que especificam se quadros devem ser enviados para um endereço MAC específico e se devem ser encaminhados ou descartados em uma certa VLAN.
- Entradas de Registro de Grupo, que indicam, para cada porta, se quadros devem ser enviados para um endereço MAC de grupo e se devem ser encaminhados ou descartados em uma certa VLAN. Estas entradas são adicionadas e removidas mediante a utilização do Protocolo de Registro de Grupo Multidestinatário (GMRP - Group Multicast Registration Protocol). Isto permite que quadros multidestinatários (multicast) possam ser enviados em uma única VLAN sem afetar as demais.
- Entradas Dinâmicas de Registro, que especificam quais portas são registradas para uma VLAN específica. Estas entradas são adicionadas e removidas utilizando o Protocolo de Registro GARP VLAN (GVRP - GARP VLAN Registration Protocol), em que a sigla GARP significa Protocolo de Registro de Atributos Genéricos (Generic Attribute Registration Protocol).

O protocolo GVRP também é utilizado na comunicação entre pontes com suporte ao padrão IEEE 802.1Q.

Para que as redes locais virtuais encaminhem os pacotes para o destino correto, todas as pontes pertencentes a esta devem conter a mesma informação em suas respectivas base de dados. O protocolo GVRP permite que estações e pontes com suporte ao IEEE 802.1Q editem e revoguem membros de uma VLAN. As pontes também são responsáveis por registrar e propagar os membros de uma VLAN para todas as portas que participam da atual topologia desta. A topologia de uma rede é determinada quando as pontes são ligadas ou quando uma modificação no estado na topologia corrente é percebida. (MORAES, 2002).

A atual topologia da rede é determinada utilizando um algoritmo "varredura" de árvore (spanning tree algorithm), o qual impede a formação de laços na rede desativando as portas necessárias. (MORAES, 2002).

Uma vez obtida a atual topologia da rede, a qual contém diferentes VLANs, as pontes determinam a topologia corrente de cada rede virtual. Isto pode resultar em uma topologia diferente para cada VLAN ou uma comum para diversas destas. Em cada caso, a topologia da VLAN será um sub-conjunto da atual topologia da rede. (MORAES, 2002).

## **6- CONSIDERAÇÕES FINAIS**

Ao final deste artigo pode-se concluir que, um projeto eficiente, seguro e prático de uma estrutura VLAN, podem resultar em uma obtenção de excelentes resultados e desempenho para uma rede corporativa. Porém cada cenário requer o uso de diferentes tecnologias que focam a solução de determinadas necessidades. O conceito mais importante de uma implantação de um projeto VLAN é uma boa análise das tecnologias disponíveis para complementar as necessidades da organização.

Contudo, ficam eminentes os benefícios quando se trata das mudanças realizadas dentro de uma organização, pois quando os administradores de rede perdem muito tempo trocando conectores, numa VLAN isso é uma solução e a ganha de tempo considerável, além disso, em algumas ocasiões fica fisicamente inviável essa troca de plugues. Outras melhorias que uma VLAN oferece é um controle de tráfego broadcast robusto e eficaz, um aumento extra do nível de segurança para segmentação de uma rede, o administrador da rede consegue agrupar utilizadores pertencentes ao mesmo departamento ou grupo de trabalho, independente deles estarem no mesmo espaço físico ou não. Deste modo pode possibilitar assim uma segmentação lógica da rede, e como as migrações de estações e feitas via software a redução de custo e tempo fica nítido numa rede virtual.

Concluiu-se as VLANs, são uma ferramenta poderosa que bem implementada, traz uma gama de benefícios e uma redução de custo e gasto numa organização já que a configuração da rede é realizada através de software e não por hardware. Também fica visível que não existe um modelo a ser seguido ou um manual de melhores práticas para a obtenção de uma estrutura de VLAN eficiente, segura e prática.

### **VIRTUAL LOCAL AREA NETWORK**

#### **ABSTRACT**

This article has main scope the advantage of the Virtual Local Area Network (VLAN), it is intended to understand how it works, since its configuration by software until its economy, reducing cost and time, how for example, in one stations migration that are transferred from a group to another. Through of studies the VLANs could be compared, being them in static or dynamic form, based in the numbers of Switches doors as feature for participation. Associated by MAC address the devices can be moved to any location inside the organization that will still making part of same virtual network. The VLANs group together different protocols in networks, beyond the benefits that allows the network division in various segments, even if

the structure is the same the devices are separated logically. In short, it has the VLANs as a local virtual network that offer a lot of advantages, since the its agility, easy handling, low cost and high performance.

**Key-Words:** Virtual Local Area Network.VLAN.MAC.Software.

## REFERÊNCIAS

- TANENBAUM, Andrew S. "**Redes de Computadores**", 5a. edição. Editora Campus, 2011.
- BARROS, Odair Soares. **Segurança de redes locais com a implementação de VLANs**. Universidade Jean Piaget de Cabo Verde, 2007.
- HAFFERMANN, Leonardo. **Segmentação de Redes com VLAN**. Universidade Católica do Paraná, 2009.
- FRINHANI, Rafael de Magalhães Dias. **Projeto de re-estruturação do gerenciamento e otimização da rede computacional da Universidade Federal de Lavras**. Universidade Federal de Lavras, 2005.
- PILLOU, Jean François. **VLAN - Redes Virtuais**. kioskea.net, 2014.
- FOROUZAN, Behrouz A. **Comunicação de dados e redes de computadores**. 4ª, edição. Editora Bookman, 2010.
- FILIPPETI, Marco A. **CCNA 4.1: guia completo de estudo**. Visual Books, 2008.
- CISCO SYSTEMS. **Comutação de rede local e sem fio: VLANS**. 2007.
- CISCO SYSTEMS INC. **Cisco Networking Academy Program CCNA 3 and 4 Companion Guide**, Third Edition. Hardcover, 2003.
- MOLINARI, Marcelo. **Redes Virtuais**. Tecnologias Actuais, 1999.
- MORAES, Alexandre F. **Redes de computadores: fundamentos**. 7.ed. São Paulo: Érica, 2010.
- VÉSTIAS, M.. **Redes Cisco para Profissionais**. R. D. Estefânia, 183, R/C Dto., 1049-057 LISBOA: FCA - Editora de informática, Lda, 2005.
- BRITO, Pedro do Rosário de. **Implementação de uma VLAN, o caso da Universidade Jean Piaget de Cabo Verde**. Universidade Jean Piaget de Cabo Verde, 2011.
- ZACARON, M. A.. **Utilizando Recursos de Switching STG e Vlan**. Universidade Estadual de Londrina, 2007.
- MORAES, Igor Monteiro. **VLANs - Redes Locais Virtuais**. Universidade Federal do Rio de Janeiro, 2002.
- BOTH, José Luiz. **Excerto da Pré-Norma IEEE 802.1Q**. UFRGS - Universidade Federal do Rio Grande do Sul, 2000.