

**ENIE 2003**

**Virtual LANs – Tipos, Aplicações, Vantagens e Tendências**

Marco A. Filippetti – Netceptions Consulting

## ÍNDICE

I - Introdução .....	3
1.1 Definição de LAN (Local Área Network) .....	3
1.2 Razões para o estabelecimento de VLANs .....	4
II – Tipos de VLANs .....	8
2.1 VLANs por associação de portas .....	8
2.2 VLANs por associação de endereços físicos .....	9
2.3 VLANs por associação de protocolos (Layer-3-based VLANs) .....	10
III – Configuração de VLANs .....	13
3.1 – Estabelecimento de uma VLAN .....	14
3.2 – Conexões Lógicas .....	15
IV – VLANs - Tendências .....	16
4.1 Comutação na camada 3 como base para a implementação eficiente de VLANs...	16
V – Bibliografia utilizada .....	18

## I - Introdução

Para iniciarmos uma discussão sobre VLANs (LANs virtuais), é preciso antes entender o que são LANs (Local Área Network)

### 1.1 Definição de LAN (Local Área Network)

“Uma LAN é uma rede de dados tolerante à 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 Internetworking Technologies Manual*)

A figura 1.1, é um exemplo simples de uma LAN:

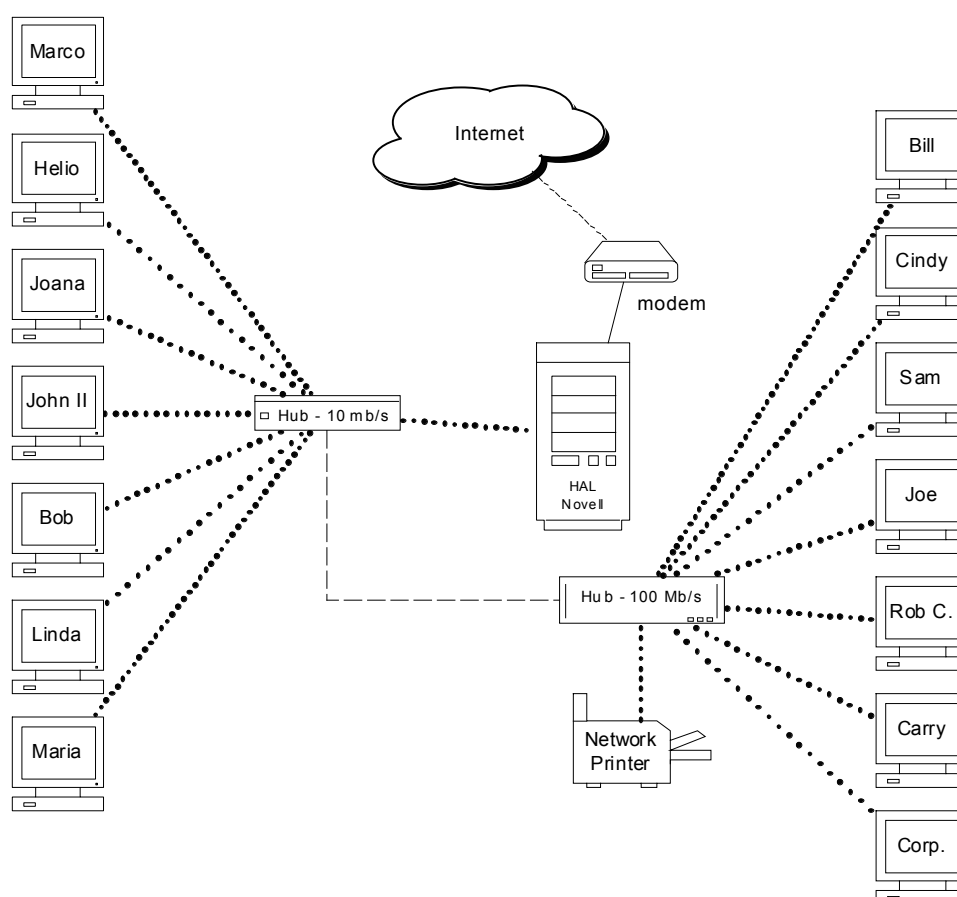


Figura 1.1 – exemplo de uma Local Área Network

Como podemos observar, temos um total de 14 máquinas “cliente” interconectadas dentro de um ambiente físico relativamente restrito, onde todas têm acesso a um servidor central Novell, e a uma única impressora de rede. O benefício-mor de criarmos uma estrutura como esta é o compartilhamento de recursos-chave entre os usuários, como o servidor e a impressora. Observe também que uma única conexão com a Internet é necessária para todos os membros da LAN criada. Todos os clientes membros podem acessá-la através do servidor Novell. Uma observação importante é que todos os recursos disponíveis ao grupo físico de usuário são compartilhados por

igual, ou seja, não há uma diferenciação feita por departamentos, tipos de usuários, projetos em andamento, grupos de interesse.

As LANs virtuais (VLANs) foram criadas para suprir esta limitação proporcionada pelas LANs, com uma série de vantagens.

Uma VLAN é uma rede que independe da localização física e que pode ser composta por diversos grupos espalhados por diferentes localidades tais como diferentes andares, prédios, ou mesmo cidades. Equipamentos de comutação de dados (*Switches*) são essenciais para a criação e o gerenciamento de VLANs.

### *1.2 Razões para o estabelecimento de VLANs*

#### *a) VLANs reduzem custos com o transporte de dados*

A criação de redes locais virtuais (VLANs) possibilita uma segregação total da estrutura física (como no exemplo da LAN, no diagrama 1.1) da estrutura lógica da rede. A partir do momento em que VLANs são definidas e implementadas, os participantes de uma determinada VLAN têm acesso apenas aos recursos alocados para aquela VLAN, e nada mais. Voltemos à ilustração apresentada anteriormente (fig. 1.1), onde uma LAN foi diagramada. Notem que os equipamentos usados para conexão entre os 2 principais segmentos de rede são “hubs”, ou repetidores. Isso garante o acesso a todos os recursos disponíveis na rede para todos os participantes da mesma.

Um repetidor não possui “inteligência”, ou seja, apenas recebe um sinal elétrico, o amplifica e o propaga por todas as portas disponíveis. Para a criação de VLANs, a substituição dos HUBS por SWITCHES é necessária, pois a implantação e o funcionamento de VLANs demandam um alto grau de inteligência na rede. Switches são capazes de fazer uma série de análises antes de encaminhar um determinado frame para uma determinada porta de saída. Assim que um equipamento destes recebe um frame em uma porta específica, ele faz uma análise do mesmo e, supondo que exista um caminho pré-determinado em sua tabela, ele enviará o frame recebido apenas para a porta destino, ou seja, nenhuma das outras portas tomará conhecimento do que está acontecendo.

Observemos a figura 1.2.

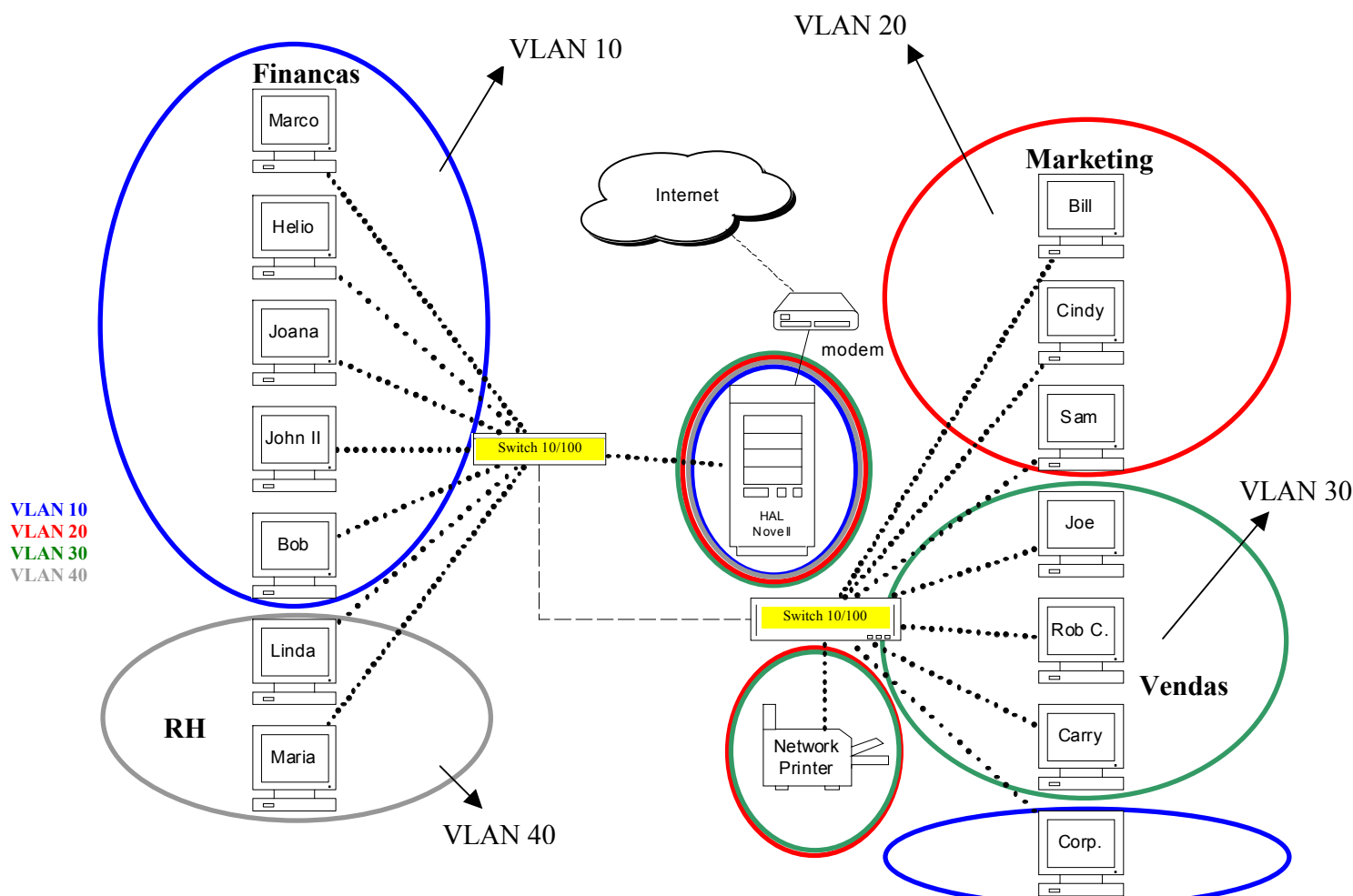


Figura 1.2 – LAN ilustrada anteriormente, com a implementação de VLANs

Notem que os hubs foram substituídos por switches (em amarelo). A razão disso é que, sem estes dispositivos, VLANs não podem ser criadas. Cada cor representa uma VLAN diferente. Cada departamento dentro desta corporação fictícia (Finanças, RH, Marketing e Vendas) é associado a uma VLAN específica (10, 20, 30 ou 40). Como podemos observar na ilustração, apenas as VLANs 20 (Marketing) e 30 (Vendas) possuem acesso à impressora de rede, pois a mesma encontra-se associada apenas a estas 2 VLANs. Já o servidor que gerencia, dentre outros serviços, o acesso a Internet, pode ser acessado por qualquer uma das 4 VLANs existentes.

Outro ponto: Os 2 usuários pertencentes ao departamento de RH (Linda e Maria) não têm nenhum tipo de acesso aos outros departamentos da empresa, não importando se o colega de Maria, Bob, do departamento Financeiro, senta-se à mesa exatamente ao seu lado. Isso ocorre porque as máquinas de Bob e Maria encontram-se associadas a VLANs diferentes (Bob: VLAN 10; Maria: VLAN 40), e podem apenas acessar recursos designados para suas respectivas VLANs. De modo análogo, suponhamos que os departamentos de Vendas e Marketing encontrem-se em outro prédio, dentro da corporação. Dentro do departamento de Vendas da empresa, uma máquina chamada “Corp” foi instalada para acessar alguns recursos do departamento financeiro. A máquina “Corp”, conforme a ilustração, apesar de encontrar-se fisicamente dentro do departamento de Vendas, faz parte da VLAN criada para o departamento financeiro, e como tal, terá acesso aos recursos disponibilizados pela mesma. Esta máquina, por exemplo, ficaria impossibilitada de

imprimir na impressora de rede, por fazer parte de outra VLAN (VLAN 10), que não se encontra associada as VLANs com permissão de impressão (VLANs 20 e 30, somente).

Uma das maiores vantagens em se adotar o esquema ilustrado na figura 1.2 em detrimento ao da figura 1.1 é o ganho de performance da rede como um todo. A começar pela substituição dos hubs por switches, os domínios de colisão são “quebrados”, aumentando muito a performance da rede. Indo além, com a criação de VLANs, conseguimos um aumento ainda maior, uma vez que conseguimos também a quebra dos domínios de broadcast, ou seja, um broadcast destinado a uma VLAN específica não é propagado para as demais, o que resulta em grande economia de largura de banda.

Espero que este exercício tenha sido esclarecedor no que se refere a como a implantação de VLANs ajuda a reduzir custos com as operações de rede, ao mesmo tempo em que flexibilizar a expansão da mesma.

b) A implementação de VLANs agiliza o processo de mudanças na rede

Administradores de rede dedicam um precioso tempo cuidando da movimentação de usuários e estações de trabalho pela rede. Apesar de existirem hoje ferramentas que agilizam o gerenciamento da rede, o custo inerente a esta atividade ainda representa uma grande fatia do orçamento de TI alocado por uma empresa. O custo relacionado com o gerenciamento de rede cresce proporcionalmente a quantidade de usuários e recursos que a mesma tem de comportar. Cada usuário novo é um custo adicional, normalmente, alto.

Com a implementação de VLANs, estes custos podem ser dramaticamente reduzidos. Uma vez implementadas, quaisquer alterações na rede podem ser rapidamente gerenciadas e realizadas. O estabelecimento de grupos lógicos dentro de uma rede (uma das possibilidades com a implementação de VLANs) é efetuado através de funções de software (dentro do switch), enquanto que o endereçamento lógico (IP ou IPX) pré-estabelecido e suas respectivas sub-redes podem ser mantidos. Tudo o que o administrador tem de fazer é reconfigurar a nova porta (do switch) para que a mesma torne-se associada a VLAN desejada. Por exemplo, suponha que um vendedor foi deslocado de um prédio para outro, dentro de uma mesma organização. Este vendedor fazia parte da VLAN “Vendas”. Assim que ele chegar ao outro lado da empresa, tudo o que o administrador terá de fazer será configurar a porta do switch onde sua máquina será conectada para que a mesma participe da VLAN “Vendas”. Pronto. Ele continuará tendo acesso a todos os recursos a que tinha anteriormente.

c) A implementação de VLANs aumenta a segurança da(s) rede(s)

Em alguns casos, a comunicação entre determinadas máquinas deve ser restrita a um determinado nível. Sem a criação de VLANs, todas as máquinas em uma rede comutada encontram-se dentro de um grande domínio de broadcast, ou seja, se uma máquina “X” necessita localizar um determinado recurso dentro da rede, ele enviará uma solicitação em formato “broadcast”, que atravessará toda a rede e atingirá virtualmente todas as máquinas conectadas a mesma. Quando criamos VLANs, solicitações e mensagens de broadcast são propagadas apenas para máquinas que estejam associadas dentro da mesma VLAN de onde tal mensagem foi originada.

Outro ponto importante: Uma vez que VLANs estejam implementadas, máquinas que pertençam a VLANs distintas não podem se comunicar sem que um equipamento de camada 3 (ex. roteador) faça a ponte entre estas VLANs. Desta forma, políticas de acesso podem ser implementadas dentro do dispositivo de camada 3 visando restringir o nível de acesso até o ponto desejado.

d) A implementação de VLANs ajuda no controle de tráfego da rede

Como já foi dito, com VLANs implementadas, o tráfego de mensagens de broadcast é enormemente reduzido nos backbones e sub-redes para as quais não seja destinado.

Em uma rede baseada em VLANs:

- Cada pacote enviado por uma estação pode estar associado à exatamente 1 VLAN,
- Uma estação em uma determinada VLAN pode receber todas as mensagens e solicitações multicast ou broadcast, desde que originadas dentro da mesma VLAN

VLANs, portanto, dividem o tráfego, de modo similar aos roteadores, com a diferença que são criadas e agem em grande parte na camada 2 do modelo OSI de referência, e que a segmentação mencionada é atingida via software. VLANs, por este motivo, são também conhecidas por “Domínio de Broadcast”, onde cada VLAN representa seu próprio domínio.

## II – Tipos de VLANs

Em geral, existem 3 tipos básicos de VLANs:

- 1) VLANs por associação de portas (port-based VLANs)
- 2) VLANs por associação de endereços físicos (MAC address-based VLANs)
- 3) VLANs por associação de protocolos (Protocol-based ou Layer-3 VLANs)

### 2.1 VLANs por associação de portas

Em uma VLAN do tipo por associação de portas (port-based VLAN), cada porta de um determinado switch pode ser associada a uma VLAN específica.

Exemplo:

	VLAN 1	VLAN 2
Switch	Portas	Portas
1	2,3,7	-
2	2,3	1,5,8
3	1,2,3,6,7	-
4	2,3,7	4,5,8
5	-	1,2,5,7

A VLAN 1 é formada por associações de portas nos switches 1 (2,3 e 7), 2 (2,3), 3 (1,2,3,6, e 7), e 4 (2,3 e 7). O switch número 5 não possui portas associadas a VLAN 1.

Analogamente, a VLAN 2 é formada por associações de portas nos switches 2 (1,5 e 8), 4 (4,5 e 8), e 5 (1,2,5 e 7). Os switches 1 e 3 não possuem portas associadas a VLAN 2.

Quando uma estação é movida de uma porta de um switch para outra, por algum motivo, a nova porta deve ser configurada no switch para que seja associada a VLAN original da estação.

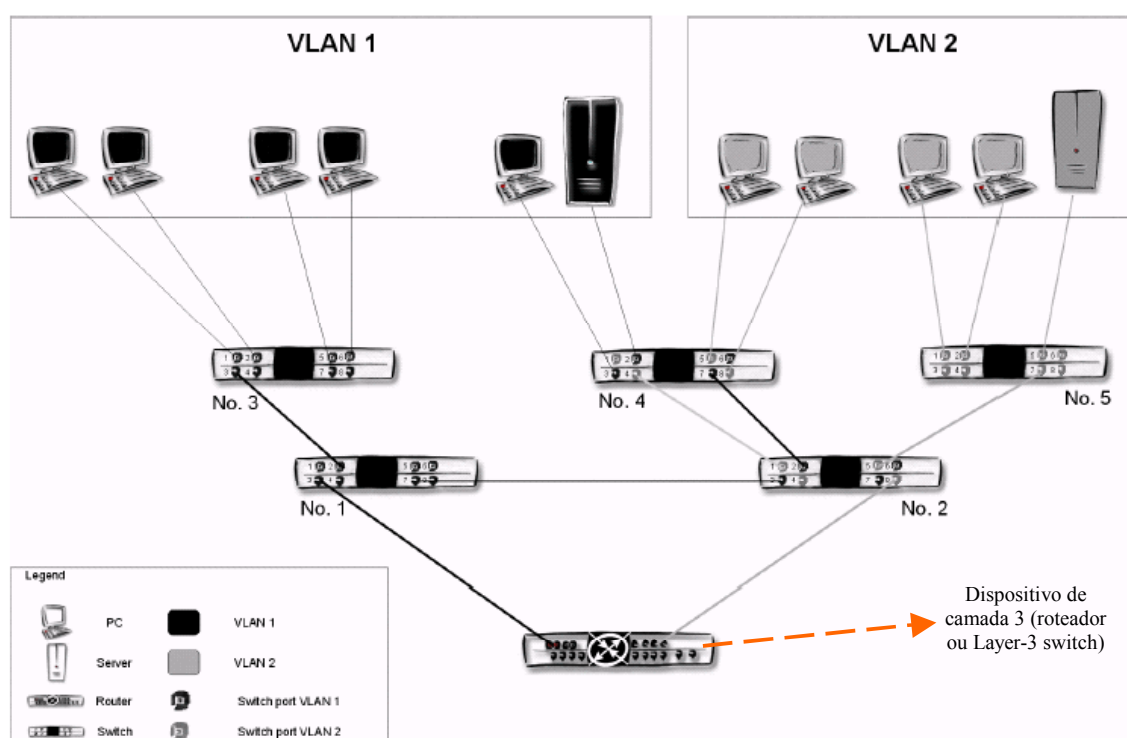


Figura 2.1 – VLANs baseadas em associações de portas no switch

Este tipo de VLAN é bastante comum, porém, exige um pouco do administrador para sua implementação, dependendo do número de switches envolvidos. A detecção de problemas neste tipo de VLAN é facilitada, uma vez que – teoricamente – se tem conhecimento da associação de cada porta para cada VLAN, em cada switch.

Note que, neste modelo, se um hub encontrar-se conectado a uma porta de um switch que participe de uma determinada VLAN, todos os dispositivos conectados a este hub farão parte desta mesma VLAN, obrigatoriamente.

## 2.2 VLANs por associação de endereços físicos

Em uma VLAN do tipo por associação de endereços físicos (MAC addresses), o endereço físico de uma estação ou dispositivo é associado a uma determinada VLAN. Todos os dispositivos de rede possuem um endereço identificador único associado à interface que conecta os mesmos a rede. Ou seja, PCs possuem estes endereços gravados em suas placas de rede, roteadores os possuem em cada uma de suas interfaces, e switches e hubs o possuem gravados em suas placas internas (diferentemente dos roteadores, apenas 1 único MAC address identifica um switch, um hub ou uma bridge, independente do número de portas que os mesmos disponibilizem).

Cada switch deve manter uma base de dados que associa todos os endereços MAC disponíveis na rede as suas respectivas VLANs. Outra possibilidade, que pode resultar em economia de memória nos switches, é a configuração de uma base de dados centralizada que mantém estas associações. Desta forma, os switches são configurados para buscarem esta informação nesta base de dados, tornando desnecessário que cada switch mantenha uma cópia desta base dentro de si. Outra vantagem de se manter uma base de dados centralizada é a facilidade de gerenciamento. Para adicionar um endereço MAC a uma determinada VLAN, mudar a associação de um endereço MAC de uma VLAN para outra, expurgar um determinado endereço MAC da base de dados, basta acessar a base central e fazer esta mudança uma única vez.

Exemplo:

	VLAN 1	VLAN 2
Switch	MAC address	MAC address
1	-	-
2	-	-
3	MAC_01, MAC_02, MAC_03, MAC_04	-
4	MAC_05, MAC_06	MAC_07, MAC_08
5	-	MAC_09, MAC_10, MAC_11

A VLAN 1 é formada pelos endereços MAC MAC\_01, MAC\_02, MAC\_03 e MAC\_04 no switch 3, e pelos endereços MAC MAC\_05 e MAC\_06 (servidor) no switch 4. Os switches 1, 2 e 5 não possuem endereços MAC associados a VLAN 1.

Analogamente, a VLAN 2 é formada pelos endereços MAC MAC\_07 e MAC\_08, no switch 4, e pelos endereços MAC MAC\_09, MAC\_10 e MAC\_11 no switch 5. Os switches 1, 2 e 3 não possuem endereços MAC associados a VLAN 2.

Quando uma estação é transferida dentro de uma mesma VLAN, nenhuma configuração adicional é necessária. Apenas se uma estação for transferida para uma VLAN diferente, seu endereço MAC deve ser remapeado para a nova VLAN.

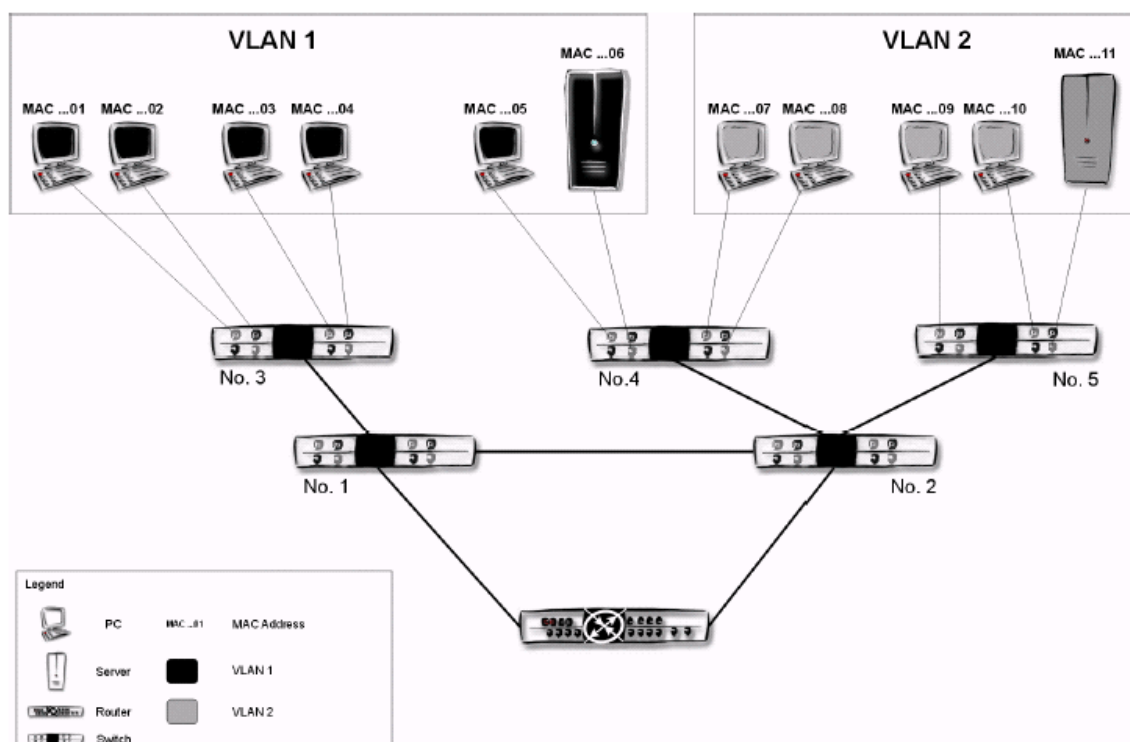


Figura 2.2 – VLANs baseadas em associações de endereços de hardware (MAC address)

A principal vantagem deste modelo é que o switch não necessita ser reconfigurado se uma estação vier a mudar de porta. Outra grande vantagem: em um hub conectado a uma porta de um switch, cada dispositivo conectado ao mesmo (hub) pode pertencer a uma VLAN diferente, uma vez que a associação é feita através do endereço MAC, e não da porta.

Uma desvantagem: a base de dados que mapeia os endereços MAC para as respectivas VLANs deve ser manualmente configurada pelo administrador se não houver nenhuma ferramenta disponível para tal procedimento, o que leva algum tempo. Outra grande desvantagem: um usuário mais experiente pode reconfigurar o endereço MAC de sua máquina para, assim, obter acesso aos recursos destinados à outra VLAN. Finalmente, neste modelo o domínio de broadcast não é efetivamente segmentado, como ocorre no modelo de associação por portas, o que pode sobrecarregar a rede se a mesma não for bem planejada e dimensionada para este modelo.

### 2.3 VLANs por associação de protocolos (Layer-3-based VLANs)

Este modelo associa a distribuição dos pacotes na rede aos protocolos (IP, IPX, Appletalk, etc.) e endereços de camada 3. É sem dúvida o mais flexível dos modelos, proporcionando o mais lógico agrupamento de usuários e recursos.

Uma subrede IP, ou uma rede IPX pode ser associada a uma VLAN própria. Protocolos não-roteáveis por definição, como DECnet, e NetBIOS também podem ser utilizados neste modelo, permitindo a utilização dos mesmos em grandes VLANs, o que seria extremamente difícil com protocolos roteáveis como o IP ou o IPX. Isso aumenta enormemente a eficiência da rede como um todo. Outra grande diferença deste para outros modelos de implementação de VLANs é a técnica desenvolvida e utilizada para identificar a associação de um determinado pacote quando este atravessa uma “malha” de switches interconectados até o seu destino final. Basicamente, existem 2 técnicas de identificação: implícita e explícita.

Na primeira, a associação entre o pacote e a VLAN é realizada pelo endereço MAC. Neste caso, todos os switches que suportam determinada VLAN devem compartilhar uma base de dados comum, contendo os endereços MAC, e suas associações VLAN.

Já na segunda (explícita), a identificação de qual VLAN determinado pacote pertence é realizada por uma “etiqueta” (*tag*) que é adicionada ao cabeçalho do pacote. Esta técnica, bastante utilizada, é definida pela norma IEEE 802.1Q (dot-1q). Basicamente, quando um pacote de dados é transferido de um switch para outro, a identificação da VLAN a qual o mesmo pertence é feita implícita (através do endereço MAC) ou explicitamente (através de uma etiqueta adicionada ao pacote de dados assim que o mesmo sai do primeiro switch). Os tipos de VLAN baseados em portas e baseados em protocolos, normalmente utilizam a técnica explícita. Já o tipo baseado em endereçamento MAC, utiliza a técnica implícita de identificação.

Exemplo:

	VLAN 1	VLAN 2
Switch	Endereço IP	Endereço IP
1	-	-
2	-	-
3	129.0.1.10 129.0.1.11 129.0.1.12 129.0.1.13	-
4	129.0.1.14 129.0.1.15	129.0.2.10 129.0.2.11
5	-	129.0.2.12 129.0.2.13 129.0.2.14

A VLAN 1 é formada pelo intervalo de endereços IP de 129.0.1.10 a 129.0.1.13 no switch 3, e pelos endereços IP 129.0.1.14 e 129.0.1.15 no switch 4. Os switches 1, 2 e 5 não possuem endereços IP associados a VLAN 1.

Analogamente, a VLAN 2 é formada pelos endereços IP 129.0.2.10 e 129.0.2.11 no switch 4, e pelos endereços IP 129.0.2.12, 129.0.2.13 e 129.0.2.14 no switch 5. Os switches 1, 2 e 3 não possuem endereços IP associados a VLAN 2.

Quando uma estação é realocada dentro de uma mesma VLAN, ela não necessita ser reconfigurada. Apenas se a estação for realocada em uma VLAN diferente é que o endereço IP da mesma deve ser reconfigurado para a mesma subrede da nova VLAN.

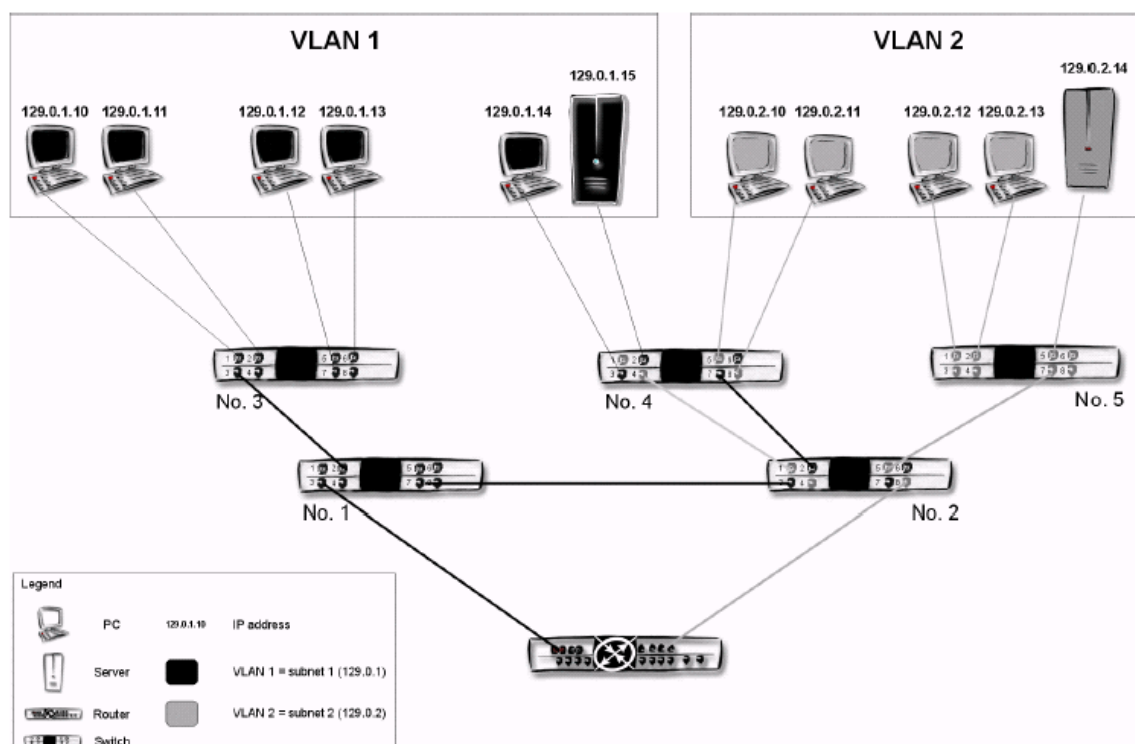


Figura 2.3 – VLANs baseadas em associações de endereços de camada 3

Uma das vantagens de VLANs baseadas em protocolos é que este método permite um excelente controle sobre o fluxo de dados. Qualquer tipo de broadcast pode ser segmentado de acordo com o tipo de protocolo usado. Mesmo estações com diferentes tipos de protocolos simultaneamente ativos podem ser suportadas por este modelo.

Uma desvantagem é o alto grau de complexidade gerado por este tipo de VLAN, o que demanda mais da administração da rede. O administrador de rede deve ter um conhecimento detalhado de todos os protocolos ativos na rede, bem como dos esquemas de endereçamento utilizados. Outro problema é que métodos de designação dinâmica de endereços, como o DHCP, não são compatíveis com este modelo de VLAN.

Quanto à técnica de identificação de frames (*frame-tagging*), uma das desvantagens é que, uma vez que há adição de informação sobre qual VLAN determinado frame pertence à medida que o mesmo atravessa os chamados “trunks”, ou “links de transporte”, o tamanho do frame Ethernet aumenta em relação ao frame padrão. Se os dispositivos receptores deste frame modificado não estiverem preparados para “entendê-lo”, pode ocorrer o descarte do mesmo. Para encerrar, além dos switches, todos os roteadores e servidores devem ser capazes de identificar frames modificados pelas especificações do IEEE 802.1Q.

### III – Configuração de VLANs

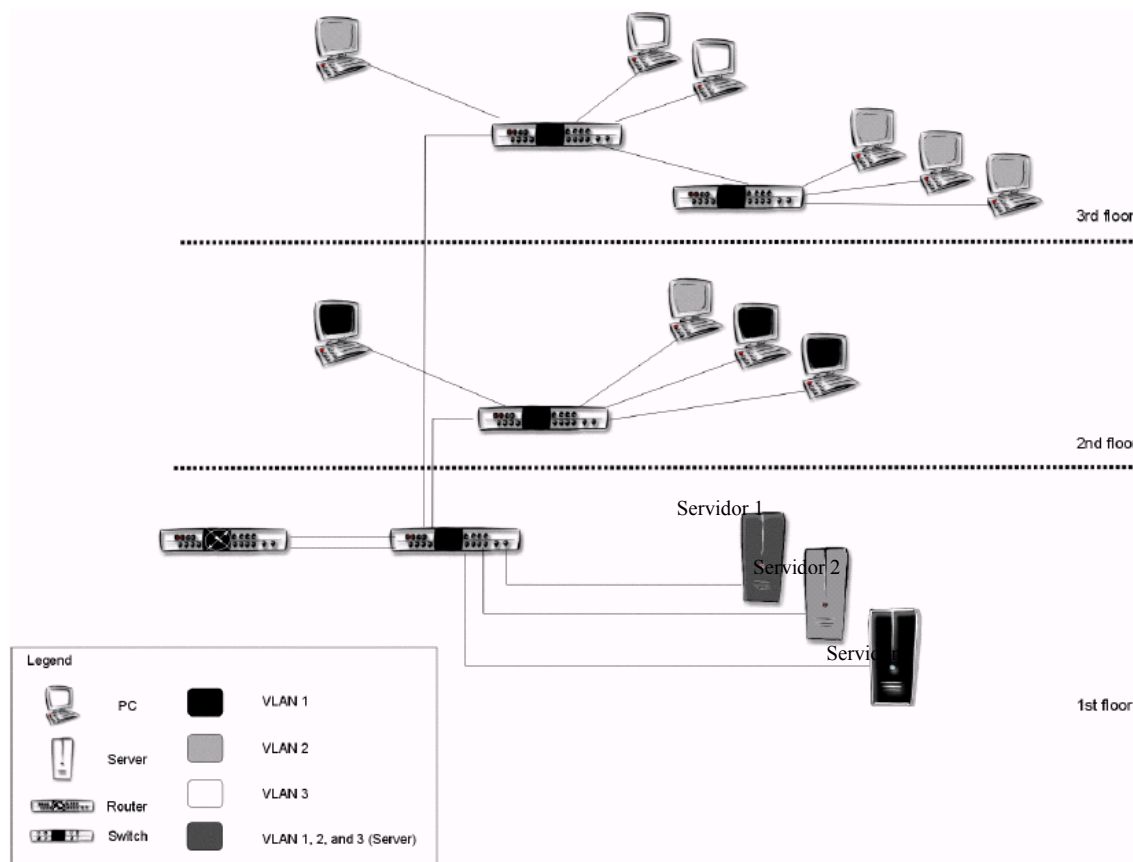


Figura 3.1 – Outro exemplo de uma rede com implementação de VLANs

O exemplo acima trata de uma LAN composta por um “server-farm” (primeiro andar), e diversos dispositivos e estações distribuídas entre os diversos andares. Neste exemplo, os switches empregados para a conectividade entre os elementos da rede e os servidores localizados no primeiro andar trabalham na camada 2, somente. Dispositivos pertencentes a uma determinada VLAN podem apenas acessar recursos associados a esta mesma VLAN. Para acessar recursos de outras VLANs, um roteador é necessário.

Se observarmos a figura, os servidores existentes no primeiro andar possuem algumas características próprias: o servidor 1 participa, simultaneamente, de todas as VLANs criadas, uma vez que encontra-se conectado ao switch por um “trunk”. Este servidor deve possuir uma placa especial de rede, que “entenda” o formato dos frames com o cabeçalho adicional proporcionado pelo padrão IEEE 802.1Q. Os outros 2 servidores se comunicarão apenas com as respectivas VLANs as quais pertencem. Resumindo: O servidor 1 encontra-se acessível para todas as VLANs, sem a necessidade de que o roteador tenha de interferir no fluxo de dados. Já os servidores 2 e 3 podem apenas ser acessados pelas respectivas VLANs as quais encontram-se associados: 2 e 1. Para uma estação pertencente a VLAN 3 acessar o servidor 2, por exemplo, o fluxo de dados deve passar pelo roteador.

### 3.1 – Estabelecimento de uma VLAN

Assim que todas as associações entre usuários/estações – VLANs tenham sido criados, as respectivas VLANs devem ser designadas às portas desejadas através da configuração dos switches. Cada porta em um switch recebe a associação de uma única VLAN. Finalmente, os switches são conectados por cabos e colocados em ambiente de produção.

Uma das maiores características de VLANs é que elas podem se espalhar por múltiplos switches se conectadas através de 1 ou mais link de transporte, ou “trunk”. Com o uso das técnicas de identificação de frames (frame-tagging), múltiplas VLANs podem ser conectadas através de 2 switches através de um único “trunk”.

A possibilidade de se associar uma única porta a múltiplas VLANs simultaneamente (quando fazemos isso, dizemos que a porta encontra-se “truncada”) é umas das maiores vantagens das VLANs identificadas explicitamente (*tagged*). Isso é especialmente útil quando desejamos que um único servidor possa ser simultaneamente acessado por diversas VLANs, pois dispensa a obrigatoriedade do uso de um roteador. Neste caso, o servidor deve possuir uma placa de rede que “entenda” o método de identificação de frames em atividade (ex. IEEE 802.1Q). O exemplo é ilustrado abaixo:

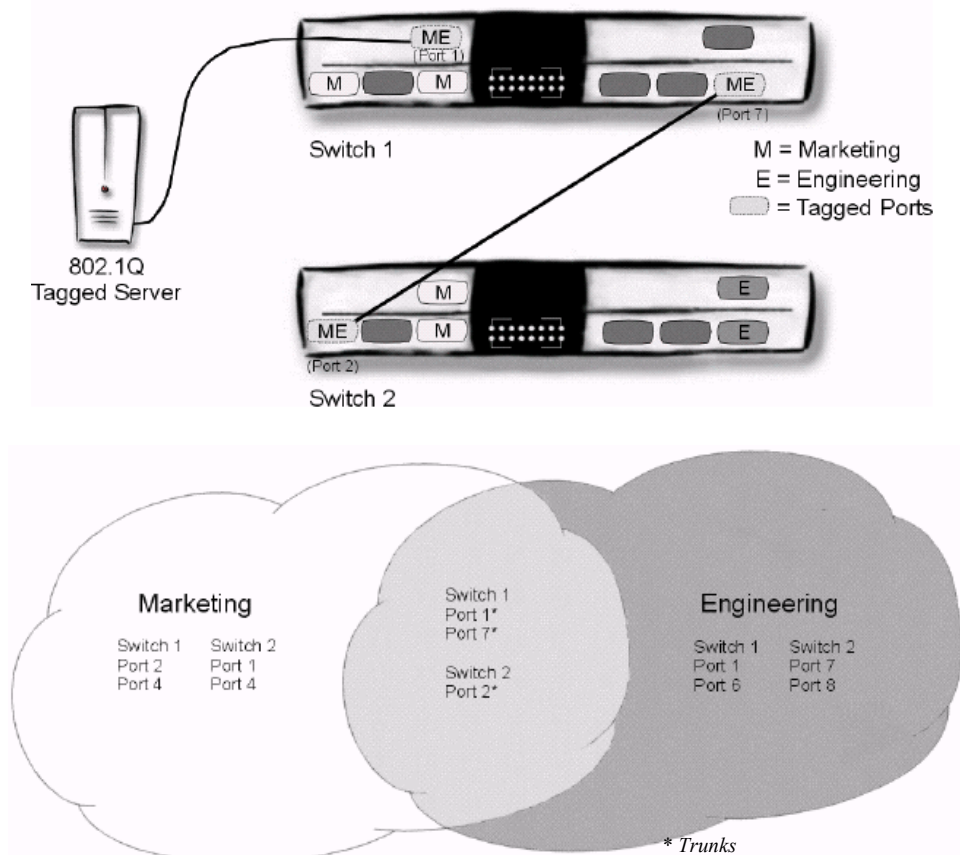


Figura 3.2 – Frame tagging em “ação”

### **3.2 – Conexões Lógicas**

Uma única porta pode pertencer a uma única VLAN baseada em portas. Caso a porta em questão precise ser associada a múltiplas VLANs, ela deve ser configurada de acordo para cada VLAN adicional (dependendo de o fabricante disponibilizar ou não esta função).

Durante a associação de portas para VLANs, o administrador decide se determinada porta deve ou não usar algum método de identificação de frames (tagging). Nem todas as portas precisam deste método habilitado. Portas com suporte a identificação de frames são especialmente úteis na comunicação inter-switches, ou entre switches e servidores. Estas portas são chamadas portas de transporte, ou “trunks”. Portas comuns, que possuem associação com apenas 1 VLAN, são chamadas de portas de acesso. Assim que um frame atravessa uma porta de transporte ele recebe a identificação sobre qual VLAN o mesmo pertence. Esta informação é retirada do frame assim que o mesmo alcança uma porta de acesso. Resumindo: A comunicação entre dispositivos conectados a portas de acesso de um switch ocorre de maneira transparente, ou seja, o dispositivo não faz a menor idéia sobre qual VLAN o mesmo faz parte. Tudo isso é gerenciado exclusivamente pelo switch.

## IV – VLANs - Tendências

### 4.1 Comutação na camada 3 como base para a implementação eficiente de VLANs

Os benefícios claros proporcionados pela implementação de VLANs – a independência da associação entre pessoas e recursos, da localização física dos mesmos – normalmente leva a criação de grupos isolados, o que pode ser prejudicial a um fluxo de dados favorável.

Exemplo:

Imaginemos que 4 estações encontrem-se associadas a diferentes VLANs: A, B, C e D. Se a estação pertencente a VLAN A desejasse se comunicar com a estação pertencente a VLAN D, todo o fluxo de dados deveria atravessar um roteador, uma vez que cada estação encontra-se em VLANs/subredes IP diferentes. Lembremo-nos que não importa onde estejam localizadas, fisicamente, estas estações, por exemplo, Se a estação que faz parte da VLAN A encontra-se fisicamente ao lado da estação associada a VLAN D, para que a comunicação entre uma e outra aconteça, o fluxo de dados irá seguir do switch até o router mais próximo, para depois retornar ao switch de partida. Ou seja, cada pacote trafega pelo link duas vezes antes de chegar ao destino, e, ainda, existe o processamento realizado por um router para que o processo tenha sucesso. Isso tudo gera uma grande latência na rede, afetando diretamente a performance da mesma.

Uma solução para este problema é a implantação de switches de camada 3, ou seja, switches com capacidade de roteamento. Com a aplicação de tais dispositivos, o encaminhamento de pacotes é executado o mais próximo possível ao destino, minimizando a latência e poupando recursos da rede.

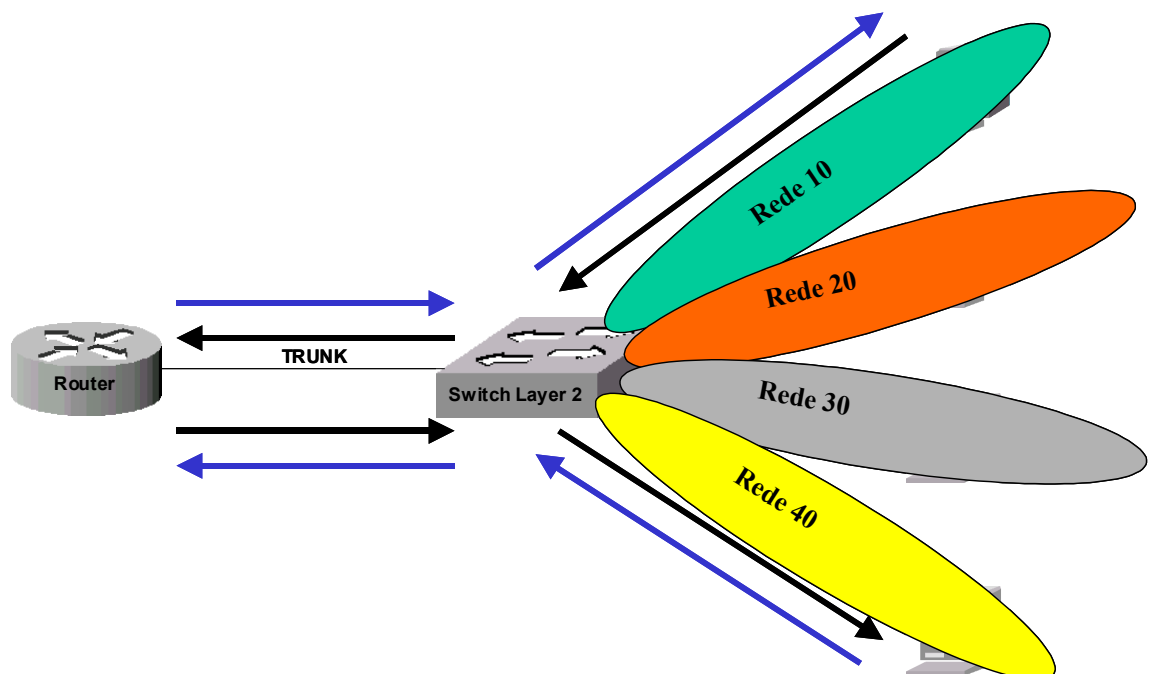


Figura 4.1 – Fluxo de dados gerado em uma VLAN Layer 2

Uma das premissas mais aceitas quando o assunto é VLANs é a seguinte:

“Comute sempre que possível, roteie sempre que preciso” (autor desconhecido)

É exatamente esta a premissa base para a substituição da comutação na camada 2 pela comutação na camada 3, ou *Layer-3 switching*.

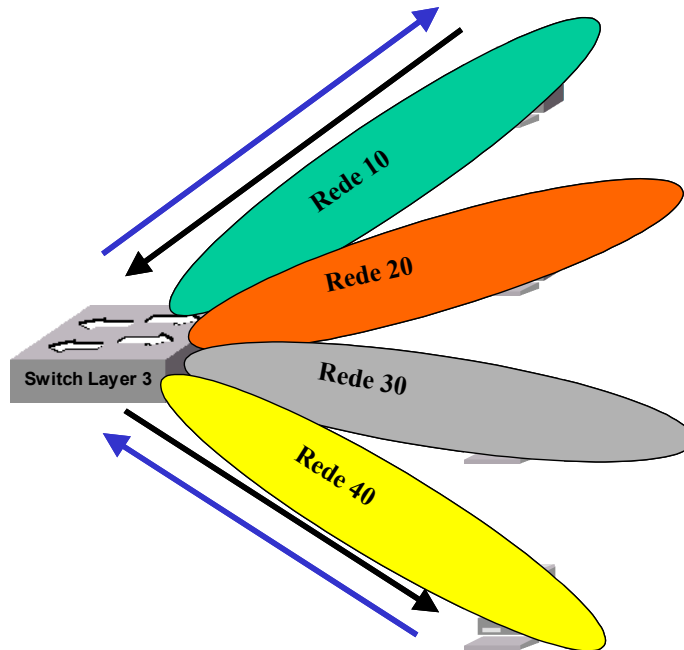


Figura 4.2 – O fluxo de dados é otimizado com a implementação de Layer-3 switching

Com a implementação de um switch capaz de realizar operações de camada 3, como roteamento inter-VLANs, o fluxo de dados já não precisa mais atravessar um roteador sempre que uma estação de uma VLAN tiver que acessar recursos de outra VLAN. Todas as decisões de encaminhamento, assim como o próprio roteamento será assumido pelo switch de camada 3. Existem diversas vantagens em se implementar este modelo:

- 1) **Custo:** O custo dos switches de camada 3 é muito inferior ao de roteadores capazes de suportar a identificação de VLANs (frame tagging IEEE 802.1Q);
- 2) **Performance:** Switches camada 3 efetuam todo o processo de decisão, encaminhamento e roteamento em hardware específico (ASICs), a maioria dos roteadores o fazem via software. Uma vez que switches que operam na camada 3 possuem hardware dedicado para este tipo de operação, sua performance é muito maior.
- 3) **Minimização do tráfego na rede:** Uma vez que pacotes não mais precisam atravessar a rede inteira para chegar a um roteador que faça o roteamento inter-VLANs, grande parte do fluxo fica restrita, o que também influencia diretamente na performance da rede como um todo.

## **V– Bibliografia utilizada**

White Paper – Virtual Networks – SysKonnnect (2001)

Cisco CCNA 3.0 – Guia Completo de Estudo – Marco Filippetti – Ed. Visual Books (2002)

Layer 3 Switching – 3Com

Manual de Tecnologias – Cisco Systems – Cisco Press