FACULDADE DE ADMINISTRAÇÃO E NEGÓCIOS DE SERGIPE – FANESE
NÚCLEO DE PÓS-GRADUAÇÃO E EXTENSÃO–NPGE
ESPECIALIZAÇÃO EM REDES DE COMPUTADORES

ZARATH MACHADO DA ROCHA

VLANS: segmentando e otimizando redes de computadores

Aracaju – SE
2010

ZARATH MACHADO DA ROCHA

VLANS: segmentando e otimizando redes de computadores

Trabalho de conclusão de Curso apresentado ao Núcleo de Pós-Graduação e Extensão da FANESE, como requisito para obtenção do título de Especialista em Redes de Computadores.

Orientador:

Aracaju – SE
2010

ZARATH MACHADO DA ROCHA

VLANS: segmentando e otimizando redes de computadores

Trabalho de Conclusão de Curso apresentado ao Núcleo de Pós-Graduação e Extensão – NPGE, da Faculdade de Administração de Negócios de Sergipe – FANESE, como requisito para a obtenção do título de Especialista em Redes de Computadores.

_____

Ricardo Torres

_____

Mário Andrade

_____

Zarath Machado da Rocha

Aprovado (a) com média: _____

Aracaju (SE), ____ de _____ de 2010.

RESUMO

A explosão do uso da Internet e seus serviços geraram, nos últimos anos, um grande impacto no fluxo de tráfego nas redes locais. O uso das Intranets corporativas e principalmente da Internet, tem como resultado uma grande quantidade de tráfego de informações trocadas com recursos remotos. Por possuírem a característica de crescimento acelerado, o impacto do fluxo de tráfego nas redes corporativas é mais drástico e, desta forma, a sua infra-estrutura não conseguirá suprir as necessidades computacionais de seus usuários em curto prazo.

Uma solução possível seria a segmentação da rede interna em redes virtuais, uma para cada departamento e/ou grupos de usuários. A utilização de VLANs em redes locais proporciona uma alta flexibilidade. Sendo ideal para ambientes dinâmicos, onde a todo o momento ocorrem mudanças de empregados, reestruturações internas, aumento do número de usuários, entre outras situações.

É objetivo deste artigo, a realização de uma revisão bibliográfica acerca da implantação de soluções de infra-estrutura lógica de redes que permitem otimizar os recursos físicos já existentes e proporcionam melhorias no desempenho da rede, além de possibilitar a aplicação de atividades gerenciais e rotinas de monitoramento.

Palavras-chave: segmentação, VLAN, otimização.

ABSTRACT

The explosion of Internet use and its services have generated in recente years, a great impact on the flow of traffic on local networks. The use of corporate intranets and especially the Internet, has resulted in a lot of traffic information exchanged with remote resources. Because they have the characteristic of rapid growth, the impact of traffic flow in corporate networks is sharper and thus its infrastructure can not meet the computing needs of its users in the short term.

One possible solution would be the internal network segmentation for virtual networks, one for eache department and/or groups of users. The use of VLANs in local networks provides a high flexibility. Ideal for dynamic enviroments where changes occur all the time of employees, internal restructuring, increasing the number of users, among other situations.

The aim of this paper, conducting a literature review on the implemetation of solutions to the logical infrastructure of networks to otimize the existing physical resources and provide improvements in network performance, and enable the implementation of management activities and routines monitoring.

Keywords: segmentation, VLANs, optimization.

Lista de Figura

Sumário

1 INTRODUÇÃO

A computação distribuída baseada em rede de computadores agora é aceita sem questionamento levando todos os setores das pequenas às grandes corporações a sofrer um acelerado processo de informatização.

A explosão do uso da Internet e seus serviços geraram, nos últimos anos, um grande impacto no fluxo de tráfego em redes locais. O uso das Intranets corporativas e principalmente da Internet, tem como resultado uma grande quantidade de trânsito de informações trocadas com recursos remotos. Por possuírem a característica de crescimento acelerado, o impacto do fluxo de tráfego nas redes corporativas é mais drástico e na maioria das vezes desordenado, desta forma, a sua infra-estrutura não conseguirá suprir as necessidades computacionais de seus usuários em curto prazo.

A transição das estruturas de rede tradicionais para um novo modelo que consiga suprir esta demanda é inevitável. Os altos custos decorrentes dessa re-estruturação, abre espaço para técnicas de otimização que procuram adequar as estruturas de rede legadas aos novos padrões de conectividade.

As corporações estão cada vez mais dependentes dos serviços informatizados e devido a este fato, é cada vez mais preocupante a idéia de se assegurar integridade aos dados bem como a constante melhoria na qualidade dos serviços de rede.

É neste sentido que a necessidade de reformulação do gerenciamento e da infra-estrutura lógica das redes é cada vez mais importante. Com a intenção de otimizar os recursos físicos já existentes, a utilização de VLANs aparece como uma boa solução, pois é capaz de melhorar o desempenho e facilitar a aplicação das atividades de gerência.

Como o tema é pouco conhecido e dificilmente aplicado, foi realizada uma revisão bibliográfica sobre VLANS, através de consulta a revistas e internet, tendo a fundamentação teórica sido feita por livros.

2 REDES DE COMPUTADORES

A redução de custos, a descentralização dos recursos computacionais e a facilidade de troca de informações, são algumas das razões do surgimento das redes de computadores. Redes de computadores são estruturas físicas e lógicas que permitem que dois ou mais computadores possam compartilhar suas informações entre si. Na sua forma mais simplória, uma rede é formada por duas estações interligadas entre si através de uma mídia de compartilhamento.

Tratando-se de tecnologia de transmissão podemos enumerar dois tipos, sendo elas as redes ponto a ponto e as redes de difusão. Redes ponto a ponto são tecnologias que utilizam uma mídia não compartilhada para conectar pares de computadores. Embora existam algumas exceções, as redes maiores (MAN's e WAN's) utilizam a tecnologia ponto a ponto e as redes menores (LAN's) tendem a usar o sistema de difusão.

As redes de difusão (*broadcasting*) têm apenas um canal de comunicação compartilhado por todas as máquinas. Os pacotes enviados por uma das estações são recebidos por todas as outras. Um campo dentro do pacote especifica o seu destinatário. Quando uma estação recebe um pacote, ela analisa o campo destinatário e se o pacote for endereçado para ela mesma ela o processará, ao passo que se for destinado a outra máquina ela o ignorará.

Existem diversas tecnologias de redes estando a Ethernet, FDDI, ATM e *Token Ring* dentre as mais populares. Cada tecnologia de Rede Local possui critérios distintos de projeto e desta forma várias topologias de rede estão atualmente em uso.

3 TOPOLOGIAS DE REDE

Podemos relacionar dois tipos de topologias utilizadas nas redes locais. A topologia lógica, também conhecida como método de acesso, refere-se à forma de funcionamento das redes, determina o modo como as mensagens são transmitidas no meio físico de um dispositivo para outro e a topologia física que se refere à forma física de interligar os computadores.

Quanto à topologia física podemos destacar três tipos mais comuns: barramento, estrela e anel; a partir dessas topologias surgiram topologias híbridas, sendo as mais conhecidas: estrela hierárquica, malha e árvore.

3.1 TOPOLOGIA EM BARRAMENTO

Em uma rede com esta configuração todas as estações se ligam ao mesmo meio de transmissão. A barra (um cabo central) é geralmente compartilhada em tempo e freqüência, permitindo transmissão de informação.

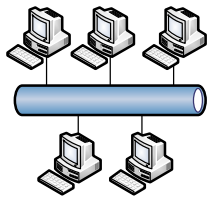

Figura 1: Tecnologia Barramento (BARRY,118, 1998)

Nas redes em barramento, cada nó conectado pode ouvir todas as informações transmitidas. Esta característica facilita as aplicações com mensagens do tipo difusão (para múltiplas estações).

Segundo [MUELLER, 2003] um barramento possui também características de topologia lógica, pois, do ponto de vista dos dispositivos, todas as outras estações se comunicam através do mesmo caminho compartilhado. Devido ao fato que esta é uma tecnologia de mídia compartilhada, mecanismos de arbitragem de tráfego precisam ser disponibilizados.

Existe uma variedade de mecanismos para o controle de acesso às redes em barramento que podem ser centralizados ou descentralizados. A técnica adotada para acesso à rede é a multiplexação no tempo. Em um ambiente de controle centralizado, o direito de acesso é determinado por uma estação especial da rede. Em um ambiente de controle descentralizado, a responsabilidade de acesso é distribuída entre todos os nodos.

Nesta topologia, quando acontece uma falha em um nó não causa a parada total do sistema. Relógios de prevenção (“watch-dos-timer”) em cada transmissor devem detectar e desconectar o nó que falha no momento da transmissão.

O desempenho de um sistema em barramento é determinado pelo meio de transmissão, número de nodos conectados, controle de acesso, tipo de tráfego entre outros fatores. O tempo de resposta pode ser altamente dependente do protocolo de acesso utilizado.

3.2 TOPOLOGIA EM ANEL

Uma rede em anel consiste em estações conectadas através de um loop fechado. Nesta configuração, muitas das estações remotas ao anel não se comunicam diretamente com o computador central.

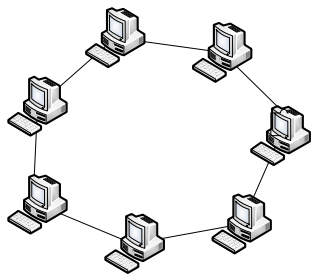

Figura 2: Tecnologia Anel (BARRY,119, 1998)

Esta topologia permite a transmissão e a recepção de dados em qualquer direção, apesar de as configurações mais usuais serem unidirecionais, de forma a

tornar menos sofisticado os protocolos de comunicação que asseguram a entrega da mensagem corretamente e em seqüência ao destino.

Quando uma mensagem é enviada para um nó, ela entra no anel e circula até ser retirada pelo nó destino, ou então até voltar ao nó fonte, dependendo do protocolo empregado. O último procedimento é mais desejável porque permite o envio simultâneo de um pacote para múltiplas estações. Outra vantagem é a de permitir a determinadas estações receber pacotes enviados por qualquer outra estação da rede, independentemente de qual seja o nó destino.

Os maiores problemas desta topologia são relativos à sua pouca tolerância a falhas. Havendo problema em um nó, é difícil determinar com exatidão se este controle foi realmente perdido e, em seguida, determinar qual nó deve recriá-lo, independente do controle de acesso empregado. Erros de transmissão e processamento podem fazer com que uma mensagem continue eternamente circulando no anel. A utilização de uma estação monitora pode contornar este tipo de problema. Outras funções desta estação seriam: iniciar o anel, enviar pacotes de teste e diagnóstico e outras tarefas de manutenção. A estação monitora pode ser dedicada ou não, podendo ser outra que assuma em determinado tempo essas funções.

Esta configuração requer que cada nó seja capaz de remover seletivamente mensagens da rede ou passá-las adiante para o próximo nó. Nas redes unidirecionais, se uma linha entre dois nós cair, todo sistema sai do ar até que o problema seja resolvido. Se a rede for bidirecional, nenhum ficará inacessível, já que poderá ser atingido pelo outro lado.

3.3 TOPOLOGIA EM ESTRELA

Na topologia em estrela todas as mensagens passam por um nó principal que age como controlador central da rede ao qual estão interligados todos os outros nós, cada estação pode se comunicar com uma outra estação de cada vez. A comunicação simultânea é possível quando os nós envolvidos são diferentes.

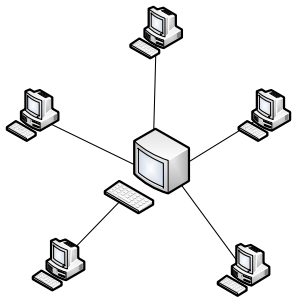

Figura 3: Tecnologia Estrela (BARRY,121, 1998)

Nas redes em estrela a gerência das informações é feita pelo nó central, podendo ser através do chaveamento de circuitos ou chaveamento de pacotes, não havendo a necessidade de roteamento, já que todas as mensagens passam por este nó. No chaveamento de pacotes, os pacotes são encaminhados do nó de origem para o nó central que reenvia ao destino final, no instante adequado. No chaveamento de circuitos, o nó central estabelece uma ligação elétrica ou através de software entre o nó de origem e o de destino que irá existir durante todo o diálogo entre os nós. No último caso, se já houver uma ligação entre duas estações, não será estabelecida nenhuma outra conexão entre estes nós.

A topologia em estrela se assemelha a topologia em barramento em determinados aspectos das suas configurações, porém os requisitos de comunicação são menos limitados, pois o sistema em estrela proporciona mais de uma conexão simultânea. A confiabilidade das ligações também é maior, pois uma falha na linha de comunicação em uma estrela só colocaria a estação escrava correspondente fora de operação. Por outro lado, o nó central é mais complexo, uma vez que deve controlar vários caminhos de comunicação concorrentemente.

A velocidade do processamento e encaminhamento das mensagens pelo nó central irá determinar o desempenho das redes em estrela, além, é claro, da carga de tráfego na conexão. Um crescimento modular visando o aumento do desempenho torna-se a partir de certo ponto impossível, tendo como única solução a substituição do nó central.

4 REDES LOCAIS

[JACK, 2003], de uma forma geral, define uma Rede Local ou LAN (Local Área Network) como sendo qualquer rede, que conecta dois ou mais computadores ou dispositivos relacionados, localizados dentro de uma área geograficamente limitada (até uns poucos quilômetros).

As redes locais nasceram nos ambientes de institutos de pesquisa e universidades. A perspectiva dos sistemas de computação que perduravam durante a década de 70, seguia em direção à repartição do poder computacional. Redes locais surgiram para tornar viável a troca e o compartilhamento de informações e dispositivos periféricos (recursos de hardware e software), resguardando a independência das várias estações de processamento e possibilitando a integração em ambientes de trabalho cooperativo.

Pode-se caracterizar uma rede local como sendo uma rede que permite a interconexão de equipamentos de comunicação de dados numa pequena região que possuem distâncias entre 25m e 100km, embora as limitações associadas às técnicas utilizadas em redes locais não imponham limites a essas distâncias. Além dessas características típicas, encontramos outras que são comumente associadas às redes locais são as altas taxas de transmissão (de 0,1 a 100Mbps) e baixas taxas de erro (1 bit em cada 108 a 1011 bits transmitidos).

5 PADRÃO ETHERNET

O padrão Ethernet é um dos mais populares protocolos e esquemas de cabeamento de rede utilizados atualmente. Sua arquitetura é baseada na mídia de comunicação compartilhada e seus elementos são provenientes dos estudos realizados em 1980, pelo consórcio das empresas Xerox, Intel e Digital Equipment Corporation que conceberam uma tecnologia de rede chamada DIX Ethernet. Em 1985 a IEEE[3] procurando desenvolver padrões de rede não proprietários, realizou algumas modificações no padrão DIX e criou o padrão 802.3 CSMA/CD mais conhecido como padrão Ethernet.

Na sua primeira versão (Ethernet 1.0 e 2.0) utilizava topologia em barramento onde os nós da rede eram conectados a um cabo coaxial grosso Thick Ethernet ou fino Thin Ethernet. A partir do padrão 802.3 esta tecnologia passou a utilizar além da topologia em barramento a topologia em estrela podendo utilizar o cabo par trançado ou a fibra óptica como mídia de comunicação.

A tecnologia Ethernet juntamente com suas variantes definidas no padrão IEEE 802.3, são atualmente as arquiteturas de redes locais mais utilizadas e suas vantagens incluem:

- Facilidade de instalação a um custo moderado;
- A tecnologia é muito bem conhecida e está disponível a partir de várias fontes;
- O padrão oferece grande diversidade de opções de cabeamento;
- Eficiente em redes que possuem altos níveis de tráfego que ocorrem em períodos não constantes.

Segundo [FEIBEL, 1996] uma rede Ethernet possui as seguintes características:

• Trabalha diretamente nas duas camadas mais baixas do modelo de referência TCP/IP: As camadas Enlace e Rede;
• Utiliza topologia em barramento (padrões Ethernet 1.0 e 2.0). O padrão 802.3 utiliza topologia em barramento ou estrela;

• Pode operar nas seguintes velocidades:

– 10Mbps (10Base5, 10Base2, 10BaseT, 10BaseF);

– 100Mbps (100BaseT, 100BaseTX, 100BaseFX, 100BaseT2);

– 1000Mbps (1000BaseSX, 1000BaseLX, 1000BaseCX, 1000BaseT);

– 10Gbps (10GBaseX).

• Utiliza o método de acesso ao meio CSMA/CD *Carrier Sense Multiple Access with Collision Detection* baseado na detecção de colisão (especificado como parte do documento do padrão IEEE 802.3);

• Transmissões *Broadcast*;

• É uma tecnologia de rede do tipo banda base (indicada para transmissões a distâncias curtas) embora suas variantes suportarem redes de banda larga.

6 TCP/IP

O conjunto de protocolos TCP/IP permite que computadores de todos os tamanhos, dos mais diferentes fabricantes, executando sistemas operacionais totalmente diferentes, possam se comunicar entre si. Criado no final da década de 60 como um projeto de pesquisa financiado pelo governo para redes de comutação, foi na década de 90, transformado no protocolo de redes mais utilizado na comunicação entre computadores. O protocolo TCP/IP é essencialmente um sistema aberto na sua definição de conjunto de protocolos e muitas das suas implementações estão publicamente disponíveis [STEVENS, 1993].

Protocolos de rede são normalmente desenvolvidos em camadas, onde cada camada é responsável por facetas diferentes na comunicação. Uma suíte de protocolos ou um conjunto de protocolos, como o TCP/IP, é uma combinação de protocolos diferentes em cada camada. TCP/IP é normalmente considerado como um sistema de 4 camadas definidos como na figura 4.1 abaixo:

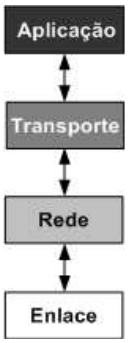

Figura 4. As quatro camadas da suíte de protocolos TCP/IP. (BARRY,127, 1998)

Cada camada possui uma responsabilidade diferente [STEVENS, 1993]:

1. A camada de **Enlace**, as vezes chamada Link de Dados (*Data Link*) ou simplesmente *Link*, normalmente inclui o *driver* de dispositivo no sistema operacional e a sua interface de rede correspondente no computador. Juntos eles tratam todos os detalhes de hardware, e a comunicação física com a mídia de transmissão utilizada;

2. A camada de **Rede** (ás vezes chamada de camada internet ou Inter-rede) trata do movimento dos pacotes (ou *datagramas*) na rede. O roteamento de pacotes ocorre nesta camada. IP (*Internet Protocol*), ICMP (*Internet Control Message Protocol*), e IGMP (*Internet Group Management Protocol*) fazem parte da camada de rede no suíte de protocolos TCP/IP;

3. A camada de **Transporte** determina o fluxo de dados entre os hosts, para a camada de aplicação localizada acima. Na suíte de protocolos TCP/IP existe dois protocolos de transporte diferentes: TCP (*Transmission Control Protocol*) e UDP (*User Datagram Protocol*).

• **TCP** cuida do fluxo de dados confiável entre dois hosts. Ele se preocupa com tarefas do tipo, repartir os dados que passam por ele vindos da camada de aplicação em pedaços de tamanho apropriado para a camada de rede, reconhecer pacotes recebidos ajustando *timeouts* para garantir o reconhecimento de pacotes que enviou, etc. Devido a este fluxo de dados confiável proporcionado pela camada de transporte, a camada de aplicação pode ignorar estes detalhes.

• **UDP**, por outro lado, fornece um serviço mais simples para a camada de aplicação. Ele apenas envia pacotes de dados de um host para outro, mas ele não garante que estes pacotes alcançarão o seu destino. Qualquer recurso de confiabilidade que seja desejado precisa ser adicionado à camada de aplicação.

4. A camada de **Aplicação** cuida dos detalhes de uma aplicação em particular.
Existem várias aplicações TCP/IP algumas delas estão listadas abaixo:

• Telnet, para conexão remota;
• FTP (*File Transfer Protocol*), protocolo de transferência de arquivo;
• SMTP (*Simple Mail Tranfer Protocol*), para correio eletrônico;
• SNMP (*Simple Network Management Protocol*), para gerenciamento de redes;

Cada camada possui um ou mais protocolos para comunicação com seu par, localizados na mesma camada no *host* origem e no *host* destino. Um protocolo, por

exemplo, permite que duas camadas TCP possam se comunicar, e outro protocolo permite que duas camadas IP possam se comunicar.

Normalmente a camada de Aplicação é um processo do usuário enquanto as outras três camadas são usualmente implementadas no *kernel* (o sistema operacional). Outra diferença entre a camada de Aplicação e as outras três camadas é que esta se preocupa com os detalhes da aplicação e não com o movimento dos dados através da rede. As outras três camadas não sabem nada a respeito da aplicação, mas cuidam de todos os detalhes de comunicação.

O propósito da camada de Rede e da camada de Aplicação são óbvios – o primeiro cuida dos detalhes da mídia de comunicação enquanto o segundo trata uma aplicação específica do usuário (FTP, Telnet, etc.).

7 Segmentação

Projetistas de rede frequentemente se defrontam com a necessidade de estender o perímetro da rede, o número de usuários no sistema, ou a largura de banda disponível para os usuários.

Mudar a infra-estrutura da rede para que estas necessidades possam ser atendidas, não implica somente na substituição das interfaces de rede, mas principalmente na substituição dos equipamentos de interconexão. Embora eficiente, uma atualização na rede pode resultar em custos proibitivos.

A segmentação é uma técnica que procura disponibilizar aos usuários largura de banda adicional sem a necessidade de se substituir todos os seus equipamentos. Através da segmentação, pode-se quebrar uma rede em porções menores e conectar estar porções com o equipamento de interconexão apropriado [CLARK, *et.Al.*,1999].

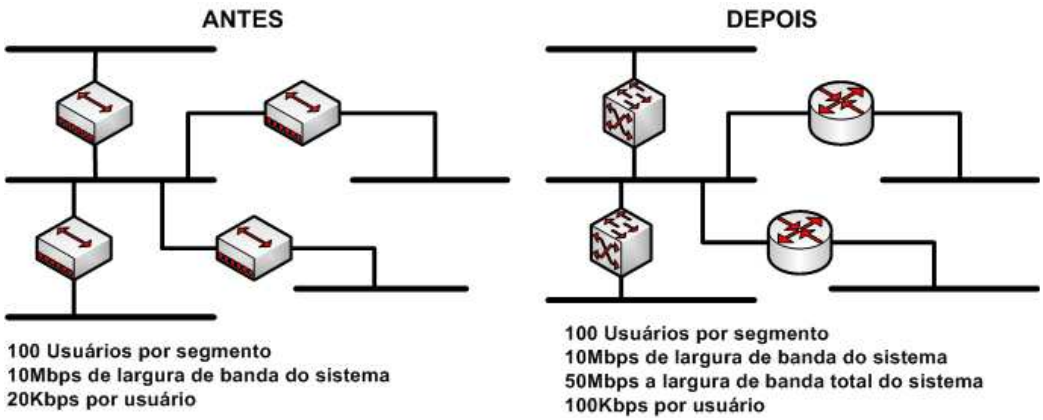

Figura 1: Exemplo de VLANS (BARRY,167, 1998)

No exemplo acima, antes da segmentação, todos os 500 usuários dividiam a banda de 10Mbps pelo fato dos segmentos estarem interconectados com repetidores. Após a substituição dos repetidores por comutadores e roteadores, os segmentos foram isolados e mais largura de banda pôde ser disponibilizada aos usuários. Comutadores e roteadores aumentam a largura de banda, pois criam novos domínios de colisão e difusão. Com a redução do número de usuários por segmento, mais largura de banda está disponível para cada um. O caso extremo,

dedica um usuário para cada segmento disponibilizando a total largura de banda da mídia de comunicação para cada usuário [CLARK, *et.Al.*,1999].

Repetidores não realizam a segmentação da rede e não criam mais largura de banda. Eles simplesmente permitem o aumento do diâmetro da rede. Comutadores e roteadores são os equipamentos mais adequados para a segmentação.

São diversos os motivos que levam a segmentação dos dispositivos em uma rede. Segundo [MUELLER, 2003] estes podem incluir:

• **Limitações topológicas:** Quando se deseja incluir mais nós em uma rede, mas a expansão é impedida devido a limitações de distância ou o número máximo de nós por segmento já foi atingido.

• **Limitações no protocolo de rede:** Quando o espaço de endereçamento é dividido e tem se a necessidade de conectar segmentos que possuem endereços de rede diferentes.

• **Limitações na largura de banda da rede:** Quando servidores de alto desempenho ou estações de trabalho consomem grande parte da banda do segmento.

• **Razões de segurança:** Quando se deseja limitar os acessos externos à rede interna (políticas de segurança) e acessos internos à rede externa (políticas de uso).

• **Conexões geograficamente distantes:** Quando se deseja assegurar que um tráfego desnecessário não alcance uma conexão remota o que de certa forma consumiria largura de banda.

8 VLAN (Virtual Local Área Network)

Uma VLAN (Virtual Local Area Network) 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 surgem como uma solução alternativa ao uso dos roteadores para a contenção de quadros de difusão, proporcionando aos comutadores a capacidade de contenção deste tipo de tráfego. São definidas pelo IEEE conforme o padrão 802.1Q (Virtual Bridged Local Area Networks).

Ao introduzirmos uma VLAN em uma porta de um comutador, é como se usássemos um roteador para conter os broadcasts em um segmento. Cada VLAN tornar-se um domínio de difusão individual. Quando um nó da rede envia um broadcast para os outros nós do seu segmento, somente os nós determinados pela VLAN possuem a capacidade de recebê-lo, ou seja, quadros de broadcast são transmitidos somente para as portas de um comutador localizadas na mesma VLAN [ODOM, 2001].

As VLANs não possuem limitações físicas e podem ser organizadas por localização de hosts, função, departamento, aplicações ou protocolos, sem se problemas quanto a localização de recursos ou usuários.

8.1 Características das VLANs

As VLANs solucionam alguns dos problemas de escalabilidade das grandes redes de topologia plana ao dividir um domínio de difusão em partes menores. Cada parte confere uma LAN virtual. Um ponto a ser considerado, é que cada LAN virtual possui as características de escalabilidade de uma LAN comum e desta forma, uma VLAN por si só não é suficiente na resolução dos problemas com quadros de broadcast herdados de uma rede que possui topologia plana. As VLANs sem roteadores não possuirão escala nas grandes redes. O roteamento neste ambiente é necessário para que se possa obter VLANs escaláveis, sendo esta a única forma de

se impor hierarquia em uma rede comutada que possua VLANs [MCGREGOR, 1998].

As VLANs possuem os seguintes benefícios:

1. Controle de Broadcast: Da mesma forma que os comutadores isolam domínios de colisão e retransmitem o tráfego para a porta adequada, 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. Que difere de um sistema que utiliza mídia compartilhada, onde somente uma estação poderá transmitir por vez. Uma rede comutada permite que várias transmissões que concorrem possam acontecer sem afetar diretamente outras estações que estejam dentro ou fora do seu domínio de difusão.

2. Segurança: A capacidade das VLANs para servirem como uma proteção adicional pode, inclusive, satisfazer as exigências mais severas de segurança e desta forma suprir muitas das funcionalidades dos roteadores nesta área. As VLANs podem garantir a segurança de duas formas:

• Usuários especiais, mesmo em locais diferentes, podem ser agrupados em uma VLAN e nenhum usuário fora da VLAN poderá se comunicar com este grupo.

• Por serem agrupamentos lógicos que se comportam como entidades fisicamente separadas a comunicação entre elas ocorre por um roteador. Quando a comunicação entre VLANs ocorre através de um roteador, todas as funcionalidades de segurança e filtragem que os roteadores tradicionalmente fornecem podem ser utilizadas. No caso de protocolos não roteáveis, toda a comunicação precisa ocorrer na mesma VLAN.

3. Desempenho: Quando usuários estão conectados no mesmo segmento, eles dividem a largura de banda total da mídia e desta forma, quanto mais usuários estão conectados no mesmo segmento menor será a quantidade de banda para cada um. Se o compartilhamento se torna muito grande há uma perda de desempenho nas aplicações compartilhadas. VLANs são geralmente criadas em equipamentos de comutação o que de certa forma garante mais largura de banda para cada usuário [CLARK, et.Al.,1999].

4. Alto desempenho e redução da latência de rede: Quando a rede se expande, mais e mais roteadores são necessários para dividir a rede em domínios de difusão. Quando o número de roteadores aumenta, a latência começa a degradar o desempenho da rede. Um alto grau de latência na rede é um problema para muitas aplicações legadas, mas isto é particularmente preocupante para aplicações novas com características de tempo real. Comutadores podem utilizar VLANs para realizar a divisão da rede em domínios de difusão, e de certa forma possuem tempos de latência muito menores quando comparados aos roteadores [PASSMORE, 1996].

5. Gerenciamento da Rede: O agrupamento lógico de usuários independente da sua localização física ou geográfica. Neste contexto, não há a necessidade de manejar cabos para que se possa mover um usuário de uma rede para outra. É possível realizar mudanças apenas inserindo uma porta do comutador na VLAN apropriada. O gerenciamento da rede pode ser através de atribuições lógicas de usuários, dessa forma os altos custos com a reestruturação do cabeamento não são mais necessários.

6. Custo: A interface de um roteador é mais cara que as de um comutador. Além disso, a utilização de comutadores e a implantação de VLANs permitem que uma rede seja segmentada a um custo mais baixo se comparado a segmentação da rede através de roteadores [PASSMORE, 1996].

8.2 Classificação das VLANs

As VLANs podem ser classificadas quanto a sua forma de agrupamento de elementos, sendo os quatro principais tipos:

- Agrupamento por portas;
- Agrupamento por endereços MAC;
- Agrupamento por protocolo;
- Agrupamento por IP multicast;

8.2.1 Agrupamento por portas

Uma VLAN com agrupamento por portas representa uma LAN virtual criada pelo agrupamento de portas de um comutador para formar um domínio de difusão [HELD, 2003]. As primeiras implementações determinavam o agrupamento de portas somente em um único comutador. A segunda geração de VLANs baseada em agrupamento de portas permitiu a configuração de portas de múltiplos comutadores na formação de uma VLAN.

As vantagens associadas com esta técnica incluem a habilidade de se usar as capacidades de comutação do equipamento de interconexão e a habilidade de suportar múltiplas estações por porta (cascateamento).

A principal desvantagem associada a esta técnica é que geralmente só pode ser atribuída uma VLAN por porta. O administrador precisará re-configurar o agrupamento caso necessite mover um usuário (ou grupo de usuários) de uma porta à outra.

Todo o tráfego dentro da VLAN é comutado e o tráfego entre VLANs deverá ser roteado. Este tipo de VLAN é também conhecido como VLAN baseada em segmento [PASSMORE, 1996].

8.2.2 Agrupamento por endereços MAC

VLANS baseadas em endereços MAC permitem que os administradores da rede movimentem uma estação de trabalho para diferentes localizações físicas na rede, porém a estação é automaticamente reagrupada à sua VLAN original.

Uma das desvantagens desta técnica é a necessidade de todos os usuários inicialmente estarem configurados em pelo menos uma VLAN. Após a configuração manual, o remanejamento automático de usuários é possível, contudo a desvantagem da configuração inicial pode ser percebida em redes muito grandes, nas quais centenas de usuários precisam ser expressamente “amarrados” a uma VLAN.

Quando membros de VLANs diversas coexistirem na mesma porta do comutador bem como em implementações que envolvam muitos usuários, as VLANs baseadas em endereçamento que são implementadas em mídias compartilhadas, sofrerão com a perda de desempenho.

8.2.3 Agrupamento por protocolo

As VLANs que utilizam esta técnica levam em consideração o tipo do protocolo (se múltiplos protocolos são suportados) ou endereços de rede (endereços de sub-rede para redes TCP/IP) no momento de determinar os membros da VLAN. O fato destas VLANs serem baseadas em endereçamento de alto nível não constitui, necessariamente, em roteamento de pacotes. Ainda que o comutador examine o endereço IP do pacote para definir a sua VLAN, não existe cálculo de rotas e nem protocolos de roteamento que realizam o transporte dos quadros, sendo assim, o roteamento entre as VLANs que utilizam esta técnica ainda se faz necessário.

O particionamento por protocolo e a mobilidade física das estações de trabalho sem a necessidade de re-configuração de endereços IP, estão dentre as vantagens de se utilizar este tipo de VLAN. Uma das desvantagens deste tipo de VLAN sobre os dois tipos anteriores está relacionada ao desempenho. E 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.

8.2.4 Agrupamento por IP multicast

Grupos de endereço IP multicast representam uma abordagem diferente na definição de VLAN, embora os conceitos fundamentais de VLAN, como domínios de difusão, continua sendo aplicado. Quando um pacote IP é enviado por multicast, ele é enviado a um endereço que serve de procurador para um grupo de endereços IP explicitamente definidos e que são estabelecidos dinamicamente. A cada estação de trabalho, é dada a oportunidade de entrar em um grupo de IP multicast quando esta confirma uma notificação broadcast que declara a existência do grupo.

Todas as estações de trabalho que adentram em um grupo de IP multicast podem se tornar membros da mesma LAN virtual. Entretanto elas são somente membros de um grupo multicast durante certo período de tempo. Desta forma, a natureza dinâmica das VLANs definidas por este agrupamento permite um alto grau de flexibilidade. Além disso, VLANs deste tipo estão hábeis a transpor roteadores e desta forma estabelecer conexões WAN.

8.3 Formas de Configuração de VLANs

Outra classificação utilizada na concepção de VLANs está relacionada ao seu grau de configuração automatizado. Existem três níveis de automação utilizados na configuração de uma VLAN [PASSMORE, 1996]:

• Manual: Com uma configuração puramente manual, os ajustes iniciais e todos os movimentos e mudanças subseqüentes na rede são controlados pelo administrador. Uma configuração manual permite um alto grau de controle. Entretanto, em redes de grande porte, este tipo de configuração não é prático. Fora este fato, a configuração manual não concede um dos principais benefícios das VLANs que é a eliminação do tempo gasto pelo administrador na implantação de mudanças e movimentação de usuários na rede.

• Semi-automática: A configuração semi-automática refere-se à opção de automatização das configurações iniciais, e re-configurações subseqüentes (movimentações/mudanças). A configuração inicial automatizada é normalmente efetuada com um conjunto de ferramentas que mapeiam as VLANS em sub-redes existentes ou outro critério qualquer. A configuração semi-automática pode também se referir a situações onde VLANs são configuradas inicialmente de forma manual e todos os movimentos subseqüentes são rastreados automaticamente.

• Totalmente automática: Um sistema que automatiza totalmente as configurações de VLAN implica na agregação das estações de trabalho automaticamente e dinâmicamente, dependendo da aplicação, ID do usuário, política ou outro critério definido pelo administrador.

8.4 Comunicação entre membros de uma VLAN

Os comutadores devem possuir uma forma de reconhecer os membros de cada VLAN quando o tráfego da rede chega até ele oriundo de outros comutadores ou, de outra forma, as VLANs podem estar limitadas a um único comutador.

Geralmente VLANs baseadas na camada de rede (definidas por porta ou endereço MAC), devem se comunicar de forma implícita (implicity tagging - marcação implícita), enquanto membros de VLAN baseados em IP (protocolo ou multicast) comunicam-se explicitamente (explicity tagging - marcação explícita).

A marcação implícita é aquela onde a decisão é baseada nos dados que realmente já estão presentes no formato do quadro existente e o comutador precisa apenas examinar os dados no cabeçalho do quadro e implicitamente decidir qual VLAN ele pertence. Quando este tipo de marcação é utilizado, nenhuma espécie de informação adicional precisa ser adicionada ao quadro pela estação transmissora, e desta forma, os dispositivos da rede não tem consciência da existência da VLAN [MUELLER, 2003].

A marcação explicita requer a adição de um campo dentro do cabeçalho do quadro ou pacote para que se possa especificar a VLAN associada [HELD, 2003]. Geralmente é utilizada em aplicações de alto nível e em WANs de grande porte. Para este método a estação precisa saber da existência da VLAN. O comutador precisa entender o método e saber onde localizar a informação de marcação no quadro de dados e desta forma, determinar qual VLAN o quadro pertence.

8.5 Roteamento entre VLANs

VLANs podem ser utilizadas para definir domínios de difusão de uma rede da mesma forma que roteadores, mas elas não possuem a capacidade de repassar o tráfego de uma VLAN a outra. O roteamento ainda se faz necessário para o estabelecimento de tráfego entre VLANs.

São três as opções de roteamento [JACK, 2003]:

- Roteamento através de Múltiplos Enlaces;
- Roteamento por Trunking em um Enlace Único;
- Roteamento por Processador de Rotas Interno;

8.5.1 Roteamento através de Múltiplos Enlaces

Este modelo é também chamado "Roteamento por Roteador Externo". Neste tipo de roteamento, cada interface do roteador está ligada a uma porta do comutador que faz parte de uma VLAN. Cada estação de trabalho em uma VLAN deve possuir um endereço gateway padrão que geralmente é o endereço IP da interface do roteador, ligada a sua VLAN correspondente.

Esta é uma solução prática para redes pequenas, mas não possui escala em ambientes com muitas VLANs. A principal desvantagem deste tipo de técnica é o desperdício de portas do comutador e interfaces no roteador. Quanto maior o número de interfaces ativas no roteador, maior deve ser a sua capacidade de processamento o que do contrário fatalmente geraria um gargalo.

Neste tipo de roteamento, a utilização de roteadores de grande porte (que geralmente possuem um custo proibitivo) se faz necessário.

8.5.2 Roteamento por Trunking em um Enlace Único

É o modelo mais prático e econômico utilizado na comunicação entre duas ou mais VLANs, em um ou mais comutadores. A tecnologia para que este processo seja possível é conhecido como Trunking. Nesta tecnologia, a determinação do tráfego de cada VLAN é realizada através da análise das tags contidas nos pacotes de dados. As tags indicam a VLAN a qual o pacote em questão está relacionado.

Para que este processo possa ser realizado, uma das portas do comutador deve ser configurada com um protocolo de trunking e, desta forma, todo tráfego oriundo das múltiplas VLANs será encaminhado para esta porta. A mesma configuração deverá ser efetuada na interface do roteador onde será criada uma sub-interface para cada VLAN e será atribuído o número de cada VLAN para as sub-interfaces correspondentes.

Toda vez que uma estação de trabalho conectada em uma das VLANs desejar se comunicar com outra estação conectada em outra VLAN, o pacote percorrerá o trunk entre o comutador e o roteador. Ao chegar ao roteador, o pacote é modificado e encaminhando para a VLAN correspondente.

Este é provavelmente o esquema mais simples para que se possa realizar a comunicação entre VLANs, além de não consumir muitos componentes.

8.5.3 Roteamento por Processador Interno de Rotas

Modelo também chamado "Roteamento com auxílio de comutador de nível 3". Neste cenário temos um multilayer switch que é um equipamento de comutação capaz de manipular dados da terceira camada (transporte) e desta forma possui as mesmas características de um roteador externo com as vantagens de um roteamento interno (tabelas de roteamento em memória cache, sistemas operacionais específicos etc).

O tráfego entre as VLANs não é realizado por agentes externos, sendo o próprio comutador responsável pelo roteamento. Este modelo de roteamento entre VLANs é considerado o mais eficiente, embora os custos iniciais desta solução sejam bastante elevados.

9 CONCLUSÃO

A implementação de VLANs é uma prática pouco usada, apesar do grande potencial de utilização. Sua utilização, acrescida de algumas melhorias como a utilização de roteador com regras de firewall, adiciona mais segurança e controle no acesso às sub-redes. Contudo, a depender da natureza da rede e do volume de dados, poderá ser necessária uma infra-estrutura mais robusta.

O uso ou não atualmente está mais condicionado a falta de conhecimento técnico do que a tecnologia propriamente dita.

É interessante observar, após a revisão feita no artigo, que a implantação de VLANs é uma técnica que reduz custos, sendo, na maioria das vezes, a solução mais indicada pela eficácia da segmentação como técnica de otimização do tráfego nas redes. Porém, o seu uso ou não está mais condicionado a falta de conhecimento técnico do que a tecnologia propriamente dita.

É imprescindível ressaltar que o aprimoramento dos recursos já disponíveis nas redes ainda é considerado a forma mais racional para solucionar os possíveis problemas. A configuração dos equipamentos muitas vezes já existentes pode contribuir para que os objetivos sejam atingidos a um custo irrisório.

REFERÊNCIAS

[CLARK, *et.Al.*,1999] CLARK, Kennedy; HAMILTON, Kevin; ***CCIE Professional Development: Cisco LAN Switching*** - 1st Edition Copyrightc 1999 by Cisco Press.

[FEIBEL, 1996] FEIBEL, Werner; ***Encyclopedia of Networking*** - 2nd Edition Copyright c 1996 by SYBEX Inc.

[HELD, 2003] HELD, Gilbert; ***Ethernet Networks: Design, Implementation, Operation, Management*** - 4th Edition Copyrightc 2003 by John Wiley & Sons Ltda.

[JACK, 2003] JACK, Terry; ***CCNP: Building Cisco Multilayer Switched Networks*** Copyrightc 2003 SYBEX Inc.

[MCGREGOR, 1998] MCGREGOR, Mark; ***Cisco CCIE Fundamentals: Network Design & Case Studies*** - 2nd Edition Copyrightc 1998 by Macmillan Technical Pub.

[MUELLER, 2003] MUELLER´s, Scott; ***Upgrading and Reparing Networks*** - 4th Edition Copyrightc 2003 by QueR Publishing.

[ODOM, 2001] ODOM, Sean; NOTTINGHAN, Hanson ***Cisco Switching Black Book*** - Copyrightc 2001 by Coriolis Group.

[PASSMORE, 1996] PASSMORE, David; ***The virtual LAN technology report*** Copyrightc 1996 by Decisys.

[STEVENS, 1993] STEVENS, W. Richard; ***TCP/IP Illustrated Vol.1 – Protocols*** - Copyrightc 1993 by Addison-Wesley.