UNIVERSIDADE ESTÁCIO DE SÁ

CURSO DE REDES DE COMPUTADORES
PROFESSOR MARCELO BERRÊDO REVISÃO 01/09/2000
NOTAS DE AULA – TECNOLOGIA DE SWITCHES

1. SWITCHES - DEFINIÇÃO:

Switches são dispositivos que filtram e encaminham pacotes entre segmentos (sub-redes) de redes locais. Operam na camada de enlace (camada 2) do modelo OSI, devendo ser independentes dos protocolos de camada superior.

LANs que usam switches para ligar segmentos são chamadas *switched LANs (LANs comutadas)* ou, no caso de redes Ethernet, *switched Ethernet LANs*.

Conceitualmente, switches poderiam ser consideradas bridges multi-portas. Tecnicamente, bridging é uma função da camada 2 do modelo OSI, e todos os padrões atuais de rede, como Ethernet, Token Ring e FDDI, podem ser conectados através de bridges ou switches.

Os switches aprendem quais estações estão conectadas a cada um dos segmentos de suas portas. Ele examina o tráfego de entrada, deduz endereços MAC de todas as estações conectadas a cada porta, e usa esta informação para construir uma tabela de endereçamento local.

Os quadros recebidos, em vez de serem propagados para todas as portas, são enviados apenas para a porta correspondente ao endereço de destino.

Muitos switches usam uma arquitetura baseada em ASIC (Application Specific Switching Circuits), ao invés dos microprocessadores tradicionais, permitindo com isto uma maior velocidade na comutação, e um barateamento do custo.

2. CLASSIFICAÇÃO DOS SWITCHES:

2.1. Quanto ao **método de encaminhamento dos pacotes** utilizado: ***store-and-forward***, ***cut-through*** ou ***adaptative cut through***.

- **Store-and-Forward**

Switches ***Store-and-Forward*** guardam cada quadro em um buffer antes de encaminhá-lo para a porta de saída. Enquanto o quadro está no buffer, o switch calcula o CRC e mede o tamanho do quadro. Se o CRC falha, ou o tamanho é muito pequeno ou muito grande (um quadro Ethernet tem de 64 bytes a 1518 bytes) o quadro é descartado. Se estiver tudo OK, o quadro é encaminhado para a porta de saída.
Esse método assegura operações sem erro e aumenta a confiabilidade da rede. Contudo, o tempo gasto para guardar e checar cada quadro adiciona um tempo de latência grande ao processamento dos quadros.
A latência total é proporcional ao tamanho dos pacotes: quanto maior o pacote, maior o delay.

- **Cut-Through**

Os Switches ***Cut-Through*** foram projetados para reduzir a essa latência. Esses switches minimizam o delay lendo apenas os 6 primeiros bytes de dados do pacote, que contém o endereço de destino, e logo encaminham o pacote.
Contudo, esse switch não detecta pacotes corrompidos causados por colisões (conhecidos como *runts*), nem erros de CRC. Quanto maior o número de colisões na rede, maior será a largura de banda gasta com o encaminho de pacotes corrompidos.
O segundo tipo de switch cut-through, ***fragment free***, foi projetado para eliminar esse problema. Nesse caso, o switch sempre lê os primeiros 64 bytes de cada pacote, assegurando que o quadro tem pelo menos o tamanho mínimo, evitando o encaminhamento de *runts* pela rede.

- **Adaptative Cut-Through**

Os switches que processam pacotes no ***modo adaptativo*** suportam tanto store-and-forward quanto cut-through. Qualquer dos modos pode ser ativado pelo gerente da rede, ou o switch pode ser inteligente o bastante para escolher entre os dois métodos, baseado no número de quadros com erro passando pelas portas.

Quando o número de quadros corrompidos atinge um certo nível, o switch pode mudar do modo cut-through para store-and-forward, voltando ao modo anterior quando a rede se normalizar.

Switches *cut-through* são melhor utilizados em pequenos grupos de trabalho e pequenos departamentos. Nessas aplicações é necessário um bom throughput, mas erros potenciais de rede ficam no nível do segmento, sem impactar a rede corporativa.

Já os switches *store-and-forward* são projetados para redes corporativas, onde check de erros e bom throughput são desejáveis.

Apenas os switches *store-and-forward*, ou Adaptative cut-through funcionando no modo *store-and-forward* possuem a capacidade de suportar mais de um tipo de LAN (como por exemplo Ethernet e Fast Ethernet), pois são os únicos com capacidade de bufferização dos quadros, condição necessária para a posterior conversão do formato do quadro MAC, ou do método de sinalização.

2.2. Quanto à **forma de segmentação das sub-redes,** podem ser classificados como **switches de camada 2 (Layer 2 Switches), switches de camada 3 (Layer 3 Switches), ou switches de camada 4 (Layer 4 switches).**

- **Layer 2 Switches**

São os switches tradicionais, que efetivamente funcionam como bridges multi-portas. Sua principal finalidade é de dividir uma LAN em múltiplos domínios de colisão, ou, nos casos das redes em anel, segmentar a LAN em diversos anéis.

Os switches de camada 2 possibilitam, portanto, múltiplas transmissões simultâneas, a transmissão de uma sub-rede não interferindo nas outras sub-redes. Os switches de camada 2 não conseguem, porém filtrar broadcasts, multicasts (no caso em mais de uma sub-rede contenham as estações pertencentes ao grupo multicast de destino), e quadros cujo destino ainda não tenha sido incluído na tabela de endereçamento.

- **Layer 3 Switches**

São os switches que, além das funções tradicionais da camada 2, incorporam algumas funções de roteamento, como por exemplo a determinação do caminho de repasse baseado em informações de camada de rede (camada 3), validação da integridade do cabeçalho da camada 3 por checksum, e suporte aos protocolos de roteamento tradicionais (RIP, OSPF, etc)

Os switches de camada 3 suportam também a definição de redes virtuais (VLAN's), e possibilitam a comunicação entre as diversas VLAN's, sem a necessidade de se utilizar um roteador externo.

Por permitir a interligação de segmentos de diferentes DOMÍNIOS DE BROADCAST, os switches de camada 3 são particularmente recomendados para a segmentação de LAN's muito grandes, onde a simples utilização de switches de camada 2 provocaria uma perda de performance e eficiência da LAN, devido à quantidade excessiva de broadcasts.

Apesar da semelhança entre os switches de camada 3 e os roteadores, existem algumas características que os distinguem, conforme podemos verificar na tabela comparativa abaixo:

Características	**Switch de Camada 3**	**Roteador Tradicional**
Roteamento IP, IPX, AppleTalk	Sim	Sim
Definição de sub-rede	Por porta ou Grupo de portas	Por Porta
Implementação do repasse	Hardware (ASIC)	Software / Microprocessadores
Suporte RMON	Sim	Não
Custo	+ Baixo	+ Alto
Suporte WAN	Não	Sim
Desempenho	Relativamente + alto	Relativamente + baixo
Escalabilidade	+ Escalável	- Escalável

Tabela 1 – Principais diferenças entre switches de camada 3 e roteadores:

Pode-se afirmar que a implementação típica de um switch de camada 3 é mais escalável que um roteador, pois este último utiliza as técnicas de roteamento a nível 3 e repasse a nível 2 como complementos, enquanto que os switches sobrepõem a função de roteamento em cima do switching, aplicando o roteamento aonde se mostrar necessário.

- **Layer 4 Switches**

Estão no mercado a pouco tempo, e geram uma controvérsia quanto à adequada classificação destes equipamentos. São muitas vezes chamados de Layer 3+ (Layer 3 Plus).

Basicamente incorpora às funcionalidades de um switch de camada 3, a habilidade de se implementar a aplicação de políticas e filtros a partir de informações de camada 4 ou superiores, como portas TCP e UDP, ou SNMP, FTP, etc.

2.3. Classificação dos Switches Layer 3:

Existem dois tipos básicos de Switches Layer 3: **Pacote-por-Pacote (Packet by Packet) e Layer-3 Cut-through.**

Basicamente um switch **Packet By Packet** é um caso especial de switch Store-and-Forward, pois como estes, bufferizam e examinam o pacote, calculando o CRC do quadro MAC, e além disto decodificam o cabeçalho da camada de rede para definir sua rota através do protocolo de roteamento adotado.

Um switch **Layer 3 Cut-Through** (não confundir com switch Cut-Through, assim classificado quanto ao método de encaminhamento dos pacotes), examinam os primeiros campos, determinam o endereço de destino (através das informações dos "headers" de camada 2 e 3), e, a partir deste instante, estabelecem uma conexão ponto a ponto (a nível 2), examinando apenas as informações de nível 2, para conseguir uma alta taxa de transferência de pacotes.

Cada fabricante tem o seu projeto próprio para possibilitar a identificação correta dos fluxos de dados a fim de possibilitar o repasse após os primeiros terem sido roteados. Como exemplo, temos o "IP Switching" da Ipsilon, o "SecureFast Virtual Networking da Cabletron", o "Fast IP" da 3Com.
O único projeto adotado como um padrão de fato, sendo portanto implementado por diversos fabricantes, é o MPOA (Multi Protocol Over ATM). O MPOA, a despeito de sua comprovada eficiência, é complexo e caro de se implementar, e é limitado a backbones ATM.

O switch **Layer 3 Cut-Through**, a partir do momento em que a conexão ponto a ponto for estabelecida, poderá funcionar no modo "Store-and-Forward" ou "Cut-Through"

3. CARACTERÍSTICAS A SE CONSIDERAR NA ESCOLHA DOS SWITCHES:

- Modo de operação (cut-through/Store-and-Forward);
- Suporte a VLAN's (Porta/Protocolo/Endereço MAC);
- Suporte a "VLAN Trunk" (IEEE 802.1Q);
- Modo de segmentação (Layer 2, Layer 3, etc);
- Número máximo de VLAN's que o equipamento suporta;
- Capacidade de implementar mais de uma VLAN em uma mesma porta;
- Capacidade do backplane;
- Capacidade de aprendizagem de Endereços MAC;
- Suporte à definição de Classes de Serviço (CoS) IEEE 802.1p;
- Suporte à configuração de "Link Agregation";
- Suporte à definição de Qualidade de Serviço (QoS) RSVP;
- Suporte ao protocolo Spanning Tree;
- Capacidade de definição de Links Resilientes;
- Capacidade de implementação de filtros de protocolo;
- Capacidade de implementação de controle de contenção de broadcast;
- Capacidade de implementação de filtros de multicast;
- Capacidade de implementação de controle de fluxo (congestão);
- Suporte a "DHCP Relay";
- Número de portas;
- Quantidade e tipo de portas "uplink";
- Implementação de tecnologia "auto-sensing";
- Implementação de Ethernet/Fast/Giga no modo "Full Duplex";
- Capacidade de empilhamento entre switches, sem adicionar níveis de repetição;

- Redundância de fontes, portas, módulos de rede, módulos de gerência e controle;
- Suporte ao gerenciamento SNMP, SNMP v2;
- Capacidade de implementar o espelhamento de tráfego em mais de uma porta;
- Suporte ao Gerenciamento RMON, para os 4 grupos básicos (Statistics, Events, Alarms, History);
- Suporte a RMON, para os demais Grupos (Hosts, HostsTopN, Matrix, Filter, Packet Capture).

4. ALGUMAS DAS CARACTERÍSTICAS DESEJÁVEIS:

4.1. Capacidade do *backplane*:

A capacidade de repasse de pacotes do *backplane* de um switch deverá ser de pelo menos a metade da soma das taxas máximas de transmissão de todas as portas do switch, se estas forem half duplex. Se as portas do switch puderem operar em full fuplex, a capacidade de repasse dos pacotes deverá ser igual ou maior à soma das taxas máximas de transmissão das portas do switch.

Por exemplo, um switch de 12 portas fast ethernet half duplex deverá possuir um *backplane* com a capacidade de efetuar o repasse dos quadros a uma velocidade mínima de 600 Mbps, o que corresponde à situação crítica de haver 6 portas recebendo quadros, e estes sendo redirecionados às outras 6 portas. Se o *backplane* não suporta o fluxo agregado de 600 Mbps está recebendo, terá que guardar em memória alguns dos quadros, a fim de evitar o seu descarte. Neste caso o *backplane* torna-se o gargalo da rede.

Um switch que, por maior que seja o tráfego recebido, o *backplane* nunca será o gargalo da rede é chamado ***Non Blocking.***

4.2. Capacidade da aprendizagem dos endereços MAC:

Os switches possuem tabelas onde armazenam os endereços MAC "conhecidos" da rede, e sua correspondente porta de origem, chamadas de *source address tables* (SAT). Estes endereços MAC são das estações de trabalhos, hubs "inteligentes", outros switches, bridges ou roteadores. Os switches implementam o repasse dos quadros de acordo com a informação do endereço de destino nos mesmos e na porta de saída correspondente ao endereço MAC nas tabelas.

Toda vez que chega um quadro cujo endereço MAC não consta nas tabelas, é necessário que o quadro seja enviado a todas as portas do switch, como se fosse um *broadcast*. Esta ação acentua drasticamente o tráfego na rede, e pode provocar um número considerável de colisões. Uma vez que a estação de destino responde à transmissão, seu endereço MAC é "aprendido" e armazenado nas SAT.

Porém, se as tabelas dos *switches* possuírem uma capacidade de aprendizagem de endereços MAC inferior ao número de dispositivos da rede, é possível que estas já estejam cheias. Neste caso uma das entradas da SAT deverá ser descartada para a armazenagem do novo endereço aprendido.

O critério para descarte do endereço na tabela varia de fabricante ou modelo, sendo mais comuns o uso de uma fila FIFO, onde se descarta o que não se anuncia a mais tempo, ou um critério estatístico em que se descarta aqueles que em uma média temporal geraram um menor tráfego. De qualquer modo, a necessidade de se descartar entradas na tabela acabará por acarretar no aumento do tráfego "broadcast" da rede, o que é altamente indesejável.

Por esta razão, ao se escolher um switch para sua rede, recomenda-se dimensionar o tamanho da rede e escolher um modelo cuja capacidade de armazenagem de endereços seja igual ao maior ao número de dispositivos da mesma.

4.3. Protocolo IEEE 802.1D Spanning Tree

O Spanning Tree é um protocolo para sistemas baseados em bridges/switches, que permite a implementação de caminhos paralelos para o tráfego de rede, e utiliza um processo de detecção de "loops" para:

- Encontrar e desabilitar os caminhos menos eficientes (os com menores largura de banda);
- Habilitar um dos caminhos menos eficientes, se o mais eficiente falhar.

A figura abaixo mostra uma rede contendo três sub-redes, separadas por 3 bridges/switches. Com esta configuração, cada segmento pode comunicar com os outros utilizando dois caminhos distintos. Sem o STP ("Spanning Tree Protocol"), esta configuração cria loops que provocarão uma sobrecarga na rede. O Spanning Tree possibilita esta configuração, porque seu algoritmo detecta caminhos duplicados, e bloqueará o repasse de pacotes em um deles.

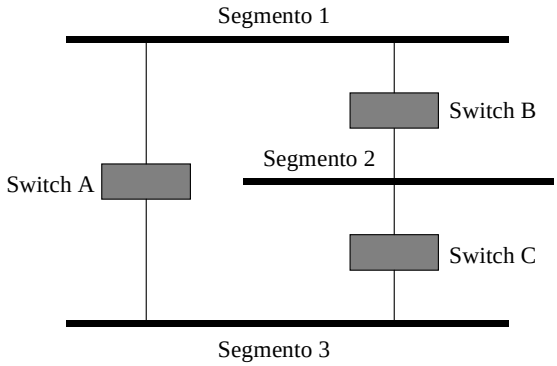

Figura 1 – Spanning Tree

No diagrama abaixo, temos um exemplo do protocolo Spanning Tree decidindo que o tráfego entre o segmento 2 e o segmento 1 somente poderá ocorrer através dos switches C e A. Caso ocorra um problema neste link através dos switches C e A, o link entre B e A será automaticamente habilitado, e o tráfego entre os segmentos 1 e 2 fluirá través do switch B.

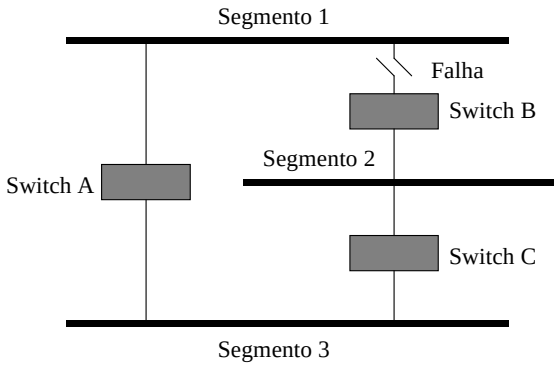

Figura 2 – Spanning Tree

O algoritmo de Spanning Tree determina qual é o caminho mais eficiente entre cada segmento separado por bridges ou switches. Caso ocorra um problema nesta caminho, o algoritmo irá recalcular, entre os existentes, o novo caminho mais eficiente, habilitando-o automaticamente.

As especificações do protocolo Spanning Tree são padronizadas pelo IEEE, dentro do conjunto das normas IEEE 802.1D.

4.4. Links Resilientes

Além da redundância automática implementada pelo protocolo Spanning Tree, totalmente padronizado pelo IEEE, os fabricantes de switches costumam implementar um nível de redundância de links, chamado de resiliência. Cada implementação é proprietária, não sendo garantida a interoperabilidade entre switches de fabricantes diferentes, quando se aplica a resiliência.

Ao contrário do Spanning Tree, em que a definição do link ativo e dos links de standbye é feita por algoritmo próprio, através da determinação do melhor caminho, a escolha do par de links resilientes é a cargo do administrador da rede, desta forma é possível "forçar" um determinado link a ficar ativo, mesmo que este não seja o caminho que proporcione a maior largura de banda.

Ao se definir duas portas de um switch como resiliente, isto é, uma sendo ativa e outra standbye, é necessário que se utilize a mesma configuração nas outras pontas definindo uma porta como ativa e a outra standbye.

As aplicações do protocolo Spanning Tree e da definição de Links Resilientes não podem ser aplicadas conjuntamente em um switch, ou seja, se for desejo do administrador da rede configurar links resilientes, a função de spanning tree deverá estar desabilitada no equipamento.

4.5. "Link Agregation" (IEEE 802.3ad):

Link Agregation é um tipo de conexão especial que possibilita aos dispositivos comunicarem-se utilizando mais de um link em paralelo. Estes links em paralelo produzem os seguintes benefícios:

- podem multiplicar a largura de banda da conexão, dependendo da quantidade de links que comporão o "tronco" de portas ("Port Trunk")

- podem prover um nível de redundância. Se um link quebrar, os outros links dividirão entre si o tráfego que se destinaria ao link defeituoso.

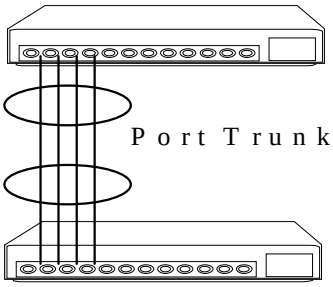

Figura 3 – Link Agregation

Observações:

- As portas nos dois lados da conexão deverão estar configuradas como "port trunk";
- Uma porta não pode pertencer ao mesmo tempo a mais de um "tronco";
- Não é possível mesclar portas de mais de um switch em um mesmo "tronco";
- É possível haver portas de mídia diferentes, como fibra e par trançado, em um mesmo "tronco".
- É possível haver portas de velocidades diferentes, como 10 e 100 Mbps, em um mesmo "tronco". Neste caso somente as portas de maior velocidade ficarão ativas. As de menor velocidade ficarão em standbye;
- As estatísticas em um port trunk são medidas em separado para cada link, e depois somadas. Não é possível coletar estatísticas do "tronco", de outra maneira.
- Antes de se desabilitar um port trunk, é recomendável desconectar todos os links, ou desabilitar todas as portas, senão poderá ser criado um loop, caso o protocolo spanning tree não estiver habilitado.

4.6. Espelhamento de Tráfego

Esta característica é desejável se o administrador da rede pretende conectar um analisador de protocolo diretamente à uma porta do switch, e monitorar o tráfego de outras portas do equipamento.

Deve-se definir uma porta que será monitorada, e o seu "espelho", a porta em que o analisador de protocolo será conectado. Uma vez que esta funcionalidade for ativada, todo o tráfego oriundo ou destinado à porta monitorada será espelhado na porta "espelho"

O Espelhamento de Tráfego torna-se necessário se o administrador de rede não quiser monitorar o tráfego de um determinado segmento, sem modificar as características físicas do segmento monitorado, ao se conectar um analisador de protocolo ao segmento.

4.7. Controle de Fluxo (IEEE 802.3x):

O padrão IEEE 802.3x – Full Duplex e Controle de Fluxo – foi completado em 1997. O padrão Full Duplex já foi apresentado e bastante estudado. Vamos, portanto, enfocar a capacidade de controle de fluxo em switches:
Quando se trabalha com duas ou mais tecnologias de comunicação com diferentes taxas de transmissão, Poderá ocorrer um gargalo devido aos pacotes que chegam dos links de maior capacidade, e ainda não conseguiram ser retransmitidos nos links de menor capacidade. Eventualmente, se um servidor a 100 Mbps, por exemplo, estiver se comunicando simultaneamente com um número grande de estações a 10 Mbps, o gargalo pode ocorrer no link de maior velocidade (100 Mbps).

Nos dois casos, o switch deverá possuir capacidade de bufferização dos pacotes que não puderam ser reenviados no momento em que chegaram ao equipamento, devido ao gargalo.
O problema é que a capacidade de bufferização será limitada pela quantidade de memória disponível no equipamento, que, por maior que seja , sempre poderá ocorrer um "estouro" nos buffers, com o conseqüente descarte de pacotes.

Para que seja evitada a situação crítica em que os buffers fiquem cheios, é desejável que os switches implementem a capacidade de controle de fluxo, padronizada pela norma IEEE 802.3x.

Existem dois tipos básicos de controle de fluxo: o "Controle de Fluxo Half Duplex" e o Controle de Fluxo Full Duplex":

- **Controle de Fluxo Half Duplex ("Backpressure"):**

Em conexões Half Duplex, os switches utilizam um método chamado "Backpressure". Por exemplo, consideremos um servidor a 100 Mbps enviando pacotes a uma estação de trabalho a 10 Mbps. Será necessário bufferizar os pacotes no switch que não puderem ser transmitidos imediatamente pelo link de 10 Mbps. Caso os buffers do switch fiquem cheios, o switch necessita sinalizar ao servidor que pare temporariamente de transmitir. Isto é feito através do envio de um pacote gerado pela camada MAC do switch, forçando uma colisão no link de 100 Mbps. Serão geradas tantas colisões quanto forem necessárias para que se esvazie os buffers dos switches.

- **Controle de Fluxo Full Duplex:**

Para conexões Full Duplex, não é possível conter uma transmissão forçando colisões, uma vez que neste tipo de tecnologia é possível a transmissão de pacotes nos dois sentidos, sem que ocorra colisão.

O padrão IEEE 802.3x define um esquema diferente de controle de fluxo para ambientes full duplex, utilizando um quadro especial conhecido como quadro "PAUSE". O quadro PAUSE utiliza um endereço de destino de multicast especial, que não é repassado pelos switches, não gerando desta forma tráfego adicional desnecessário, nem interferindo com funções de controle de fluxo em outras partes da rede.

Se um cliente a 10 Mbps estiver recebendo um tráfego muito intenso de um servidor, por exemplo, o cliente enviará quadros PAUSE ao switch, reduzindo o throughput pelo link. Isto não é comum acontecer, pois a interface do cliente está preparada para suportar tráfego intenso a 10 Mbps. Porém pode ocorrer, por exemplo, uma situação em que o cliente temporariamente não pode receber dados devido ao seu disco rígido estar cheio. O cliente enviará quadros PAUSE ao switch até que se apague arquivos e obtenha espaço no disco rígido, e a transmissão do switch irá ser reiniciada.

Da mesma forma, se um switch estiver recebendo quadros por um link e os buffers ficarem cheios, o switch passará a enviar quadros PAUSE pelo link, e a estação transmissora interromperá temporariamente a transmissão de pacotes.

A maioria dos switches e placas Fast Ethernet e Gigabit Ethernet fabricados atualmente já suportam IEEE 802.3x. Os equipamentos mais antigos que implementam Full Duplex, lançados antes do padrão muitas vezes utilizam métodos para controle de fluxo em links Full Duplex.

4.8. Classes de Serviço – IEEE 802.1p

- Recentemente ratificado pelo IEEE;
- Norma que visa estabelecer priorização de tráfego, de acordo com a definição de classes de serviço. A priorização de tráfego permite respostas quase instantâneas para aplicações críticas.
- Define oito níveis de prioridade, em que os quadros da rede carregarão a informação de prioridade do pacote, desde o nível 7 (maior prioridade) até o nível 0 (menor prioridade).
- Os equipamentos de infra-estrutura de rede, como switches e roteadores, construídos para serem compatíveis com o protocolo IEEE 802.1p, devem priorizar a entrega dos pacotes de acordo com a configuração de prioridade, dando maior preferência aos quadros de mais alta prioridade.
- Pode-se desta forma dar um tratamento preferencial a "dados críticos", e aplicações que necessitam tempo de resposta imediato, como sistemas em "real time".

- **Implementação:**

- Um novo campo é inserido no pacote Ethernet, entre os campos Source Address e Lenght: É o Campo Tag Control Info (TCI) de 4 bytes:

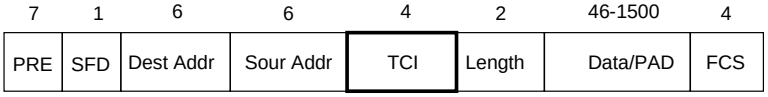

Figura 4 – Formato do quadro Ethernet com o campo TCI definido pela norma IEEE 802.1p

Os 3 bits de prioridade são lidos pelos dispositivos de infra-estrutura de rede suportam IEEE 802.1p, e o frame é roteado para um buffer interno (com estruturas em fila - FIFO). Sua posição de entrada será correspondente à prioridade do pacote.

Os quadros de maior prioridade serão entregues antes dos quadros de mais baixa prioridade. Quadros sem prioridade e quadros setados com prioridade 0 ficarão na fila de mais baixa prioridade.

Como a estrutura (e o tamanho máximo do pacote, que neste caso é de 1522 bytes, 4 bytes maior do que o Ethernet tradicional) mudou, Além dos switches e roteadores, as placas de rede deverão ser também compatíveis com a priorização de classes de serviço IEEE 802.1p.

Os hubs, switches e roteadores que não suportam 802.1p poderão descartar o pacote caso ele esteja no seu tamanho máximo (1522 bytes), pois está com um tamanho maior que eles reconhecem como o tamanho do frame Ethernet. Mesmo que não ocorra o descarte de pacote, este será tratado como um pacote Ethernet tradicional (sem prioridade).

Tag Control Ïnfo Field	**Descrição**
Tagged Frame Type Interpretation	8100h para frames Ethernet. Reservado para outros frames
3-bit priority field	De "0" a "7" – 7 é a maior prioridade
Canonical	Setado para "0"
12-bit 802.1Q VLAN Identifier	Número de Identificação de VLAN

Tabela 2 – Campo "Tag Control Info

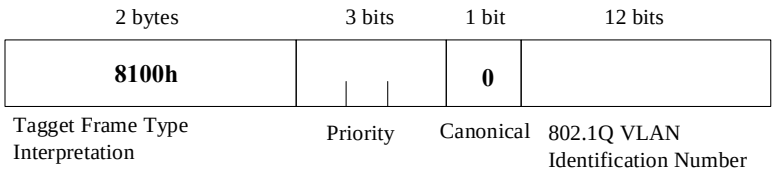

Figura 2 – Estrutura do campo "Tag Control Info"

- **Atribuição de Prioridades:**

Os fabricantes de hardware compatível (placas de rede) implementam "filtros" de prioridade, em que o usuário, por software, pode atribuir determinada prioridade a um serviço, endereço ou protocolo.

Por exemplo pode-se atribuir determinada prioridade a SNMP, SMTP, HTTP, TCP/UDP, endereços IP ou MAC, Sockets IPX, endereços IPX.

A atribuição de prioridade pode ser realizada por software, na montagem das informações de camada MAC do pacote (driver MAC da placa de rede).

É importante que seja feito um planejamento antes de atribuir um grau de prioridade a determinado serviço. Se todos os serviços da rede possuem o mais alto grau de prioridade, por exemplo, então a rede se comportará como uma rede em que não se aplicam níveis de prioridade. A aplicação deste recurso demanda então uma definição de políticas de priorização de tráfego.

5. CONSIDERAÇÕES SOBRE A UTILIZAÇÃO DE SWITCHES:

Os Switches podem ser usados em nível de grupos de trabalho, departamentos e backbone. São especialmente recomendados nas situações de congestionamento de tráfego, que pode ocorrer no acesso a um servidor de uma rede departamental ou a um backbone corporativo de uma LAN

compartilhada. A troca do hub por um switch irá expandir a largura de banda da LAN, enquanto segmenta o tráfego ponto-a-ponto entre clientes e servidores.

Para grupos de trabalho, configurações escaláveis podem ser as melhores soluções. À medida em que a demanda cresce, a largura de banda pode ser aumentada, dimuindo-se o número de usuários por hub e dedicando-se alguns portas do switch a estações individuais ou servidores. Cada estação conectada diretamente ao switch terá 10Mbps dedicados a ela.

A nível departamental, switches podem ser usados para segmentar a LAN, melhorando o acesso ao servidor, e interligando workgroups.

Gargalos podem ser aliviados economicamente instalando-se um switch ***dual-speed***, com a porta *high-speed* conectada ao backbone e as *lower-speeds* conectadas aos desktops de usuários.

Pode ser interessante também implementar redes virtuais (VLAN's) a fim de isolar tráfegos indesejáveis entre grupos de trabalho, proporcionando uma maior segurança no acesso às informações, e aliviando o tráfego na sub-rede.

No backbone corporativo, onde o tráfego vem de todos os segmentos de LAN, um switch pode aliviar a largura de banda substituindo um bridge/router utilizado para suportar um collapsed backbone, desde que políticas de roteamento e filtragem de pacotes não seja requeridas.

Nessas aplicações, switches tipicamente suportam características avançadas de bridges, que permitem aos administradores configurar parâmetros de filtragem de multicasts e limitar encaminhamentos de broadcasts, com a vantagem de que as funções de comutação são inteiramente implementadas em hardware, ao contrário das bridges e roteadores, sendo, portanto, muito mais rápidas.

Originalmente projetados para conectar servidores e workstations em LANs, os roteadores atualmente são mais utilizados para prover conectividade com WAN's, e links entre sites remotos e a LAN corporativa.

BIBLIOGRAFIA:

- Tanembaum, Andrew S. – REDES DE COMPUTADORES (3ª Edição)
  Editora Campus, 1997
- Soares, Luiz F. G. – REDES DE COMPUTADORES - DAS LANs, MANs, e WANs às REDES ATM (2ª Edição)
  Editora Campus, 1995
- Breyer, Robert – SWITCHED, FAST , AND GIGABIT ETHERNET (3ª Edição)
  Mcmillan Techincal Publishing, 1999