VOLTAR

Interconexão de redes locais (LANs)

Descrever o método de funcionamento dos dispositivos bridge e switch, desenvolver os conceitos básicos de LANs intermediárias, do uso do protocolo STP e VLANs.

NESTE TÓPICO

Marcar tópico

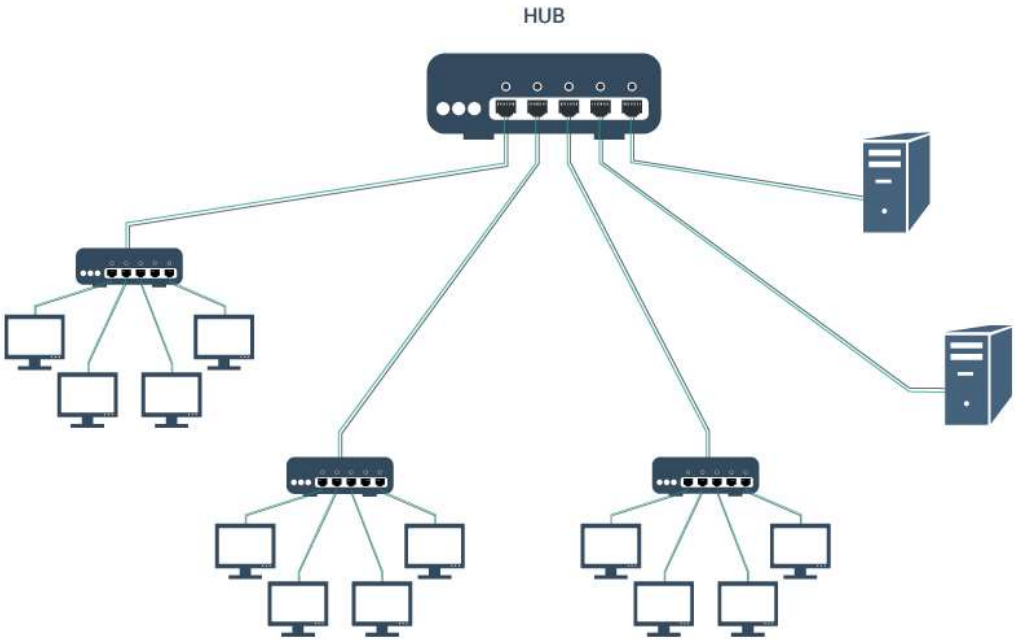
Com o método de acesso ao meio e as diferentes formas com que os equipamentos de conectividade têm para filtrar o tráfego na rede, as formas de transmissão de sinais do meio ficaram divididas em dois domínios. O primeiro deles, definido na camada de enlace, sub-camada MAC, é identificado como domínio de colisão.

O domínio de colisão é a área da rede em que os quadros são originados e colidem, ou seja, são áreas em que os quadros estão propensos a interferir uns nos outros. Esse conceito é aplicável aos segmentos de rede interligados às portas de uma bridge (Ponte) ou às portas de um switch da camada 2 (enlace – OSI).

Em um domínio de colisão temos o tráfego limitado, ou seja, nele, apenas uma máquina de cada vez pode iniciar uma transmissão. Caso duas máquinas tentem transmitir, haverá uma colisão.

Um segmento de rede é a área da rede eletricamente contínua, em que os hosts (máquinas) estão conectados e interligados a uma das portas de um switch ou bridge.

No caso de se ter um dispositivo Hub conectado a uma das portas de uma bridge ou switch, tem-se então configurado um único domínio de colisão, uma vez que dentro dele temos uma topologia física em barra na qual todas as máquinas nela conectadas disputam o meio de transmissão, quando apenas uma delas poderá transmitir por vez, (TANENBAUM, A. S. 2011).



Domínio de colisão com HUB

Segmentação

Como se pode ver, um segmento de rede é a parte que interliga um conjunto de hosts (máquinas) a uma das portas de uma bridge ou switch (dispositivos). O termo segmentação surge pelo fato de esses dispositivos terem a capacidade de segregar ou isolar o tráfego das máquinas no segmento, ou seja, se em um segmento estão conectadas quatro máquinas, “A”, “B”, “C” e “D”, e a máquina “A” deseja enviar um quadro de dados para a máquina “C”, o dispositivo irá restringir, “segmentar” o tráfego apenas nesse segmento (domínio de colisão), não propagando o quadro para outro segmento configurado em outra de suas portas.

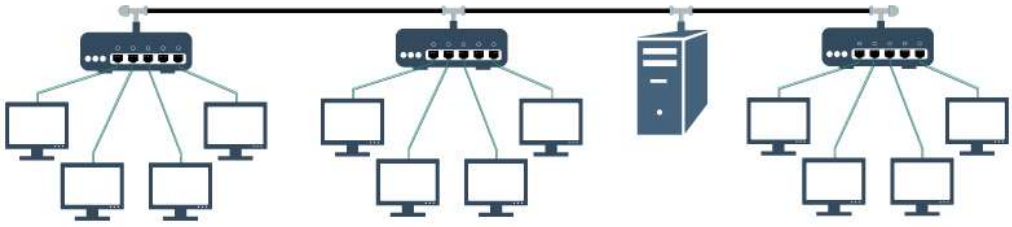
O quadro só será passado ou propagado, por difusão (broadcast), para outra porta/segmento (domínio de colisão) do dispositivo se for endereçado, por exemplo, para uma máquina “G” nele conectada.

A segmentação feita com bridges ou switches tem por objetivo reduzir a níveis mínimos o tráfego nos segmentos da rede.

Os dispositivos de camada 2 (enlace), bridge e switch, são capazes de definir os domínios de colisão (segmentação), porque são capazes de identificar as máquinas por meio de seus endereços físicos (Mac Address).

Eles então constroem suas tabelas de endereços identificando os endereços físicos das máquinas por portas, ou seja, a tabela lista o número da porta com endereço físico da máquina nela conectada. (TANENBAUM, A. S. 2011).

As bridges e switches têm a capacidade de segmentar a rede, para assim melhorar seu desempenho, fornecendo a cada uma de suas portas, que podem estar ligadas a uma ou mais estações, uma taxa de transmissão na rede igual à do seu enlace de entrada/saída.



Domínio de colisão com Switch

Modos de switching para encaminhamento de quadros

Store and forward (armazenar e encaminhar)

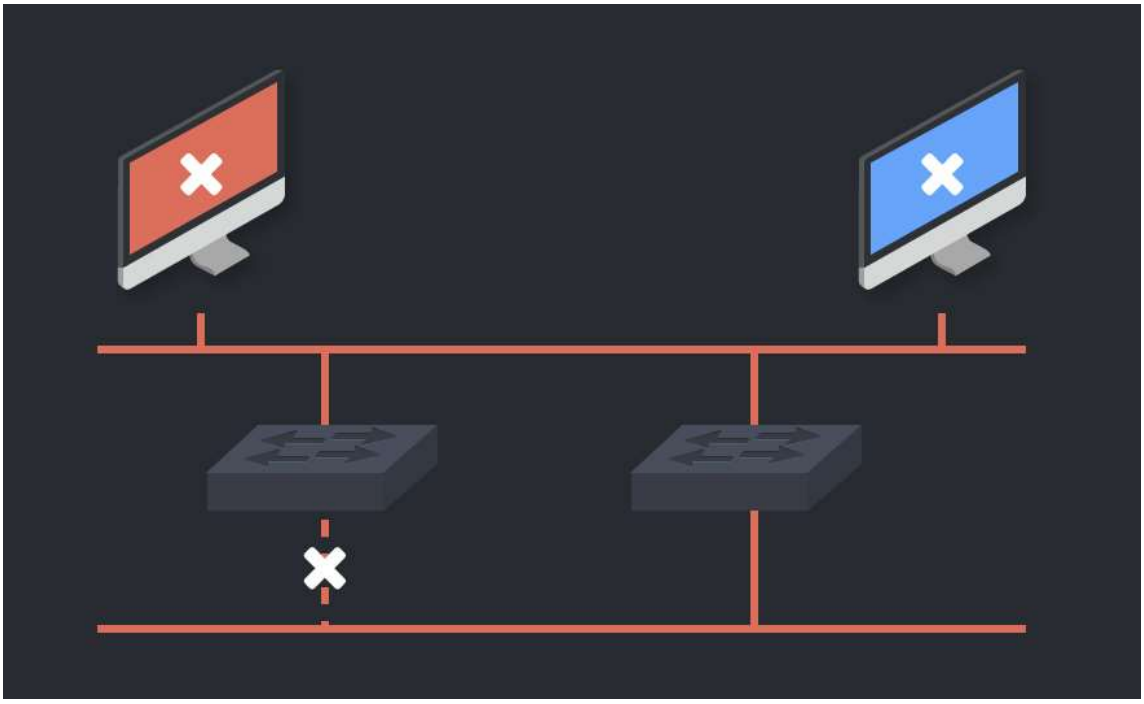
O switch recebe todos os bits do quadro no seu buffer (store), realiza a verificação da sua consistência por meio do FCS (Frame Check Sequence) e é encaminhado (forward) quando o endereço de destino é localizado.

Cut through

O switch consulta a tabela de endereços tão logo o campo de endereço de destino contido no cabeçalho seja recebido. Os primeiros bits do quadro podem ser enviados por meio da porta de saída antes que os bits finais do próximo campo do quadro sejam recebidos. Isso não permite ao switch descartar quadros que falhem na verificação do FCS. É um modo otimizado, pois o switch encaminha o quadro assim que termina a leitura do seu endereço de destino.

Fragment free

Tem um funcionamento semelhante ao cut through, só que o switch espera o recebimento dos primeiros 64 bytes antes de encaminhar o quadro. Verificou-se que a possibilidade de haver erros no quadro acontecia durante o recebimento desses 64 bytes. Detalhe que a FCS ainda não pôde ser verificada.



Spanning Tree

Bridge e switch – funcionamento

Ao ligarmos um switch, nesse momento a sua tabela de endereços estará vazia e continuará assim até que a primeira máquina da rede transmita informações para um destino. Mas, se a tabela do switch está vazia, como ele vai direcionar o quadro para o computador de destino? Para iniciar, o switch terá que encaminhar o quadro para todos os segmentos conectados às suas portas (broadcast).

Nesse momento já foi armazenado o endereço de origem na tabela. O endereço de destino será armazenado logo em seguida, quando a máquina de destino responder à requisição feita. Com o passar do tempo, durante o encaminhamento de novos quadros, esse processo vai se repetindo e o switch consegue então montar sua tabela de endereços, ou seja, já é capaz de encaminhar um quadro ao seu destinatário, pois já tem a localização dos endereços de cada máquina em relação às suas portas.

Um switch Ethernet aprende o endereço de cada máquina no segmento lendo o endereço de origem no quadro transmitido e identificando a porta utilizada. O switch então guarda essas informações em sua tabela de endereços. Os endereços são aprendidos de forma dinâmica e armazenados na **CAM** (*Content-Addressable Memory*).

Toda vez que um endereço for armazenado, será registrada a hora, para ele ser mantido por um determinado período de tempo. Assim, quando um endereço for consultado na CAM, ele terá seu registro atualizado. Os endereços que não forem consultados por um determinado período de tempo serão descartados. Isso mantém a tabela da CAM sempre precisa e funcional.

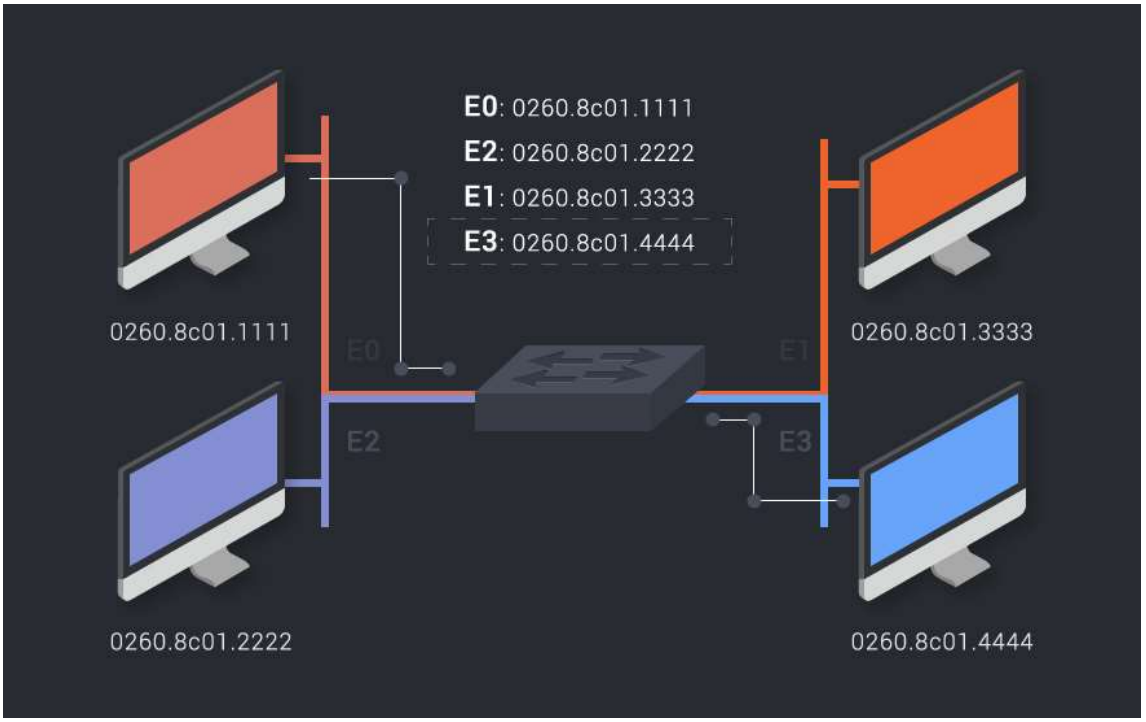
Os switches são mais funcionais que as bridges nas redes atuais porque operam em velocidades muito mais altas que as bridges e podem suportar novas funcionalidades, como as LANs virtuais (VLANs).

Uma bridge é capaz de transmitir quadros de uma máquina em um segmento a uma máquina de destino em outro segmento. Quando uma bridge é ativada e começar a operar, ela analisa os endereços MAC dos quadros de chegada e criará uma tabela de endereços conhecidos.

Se a bridge identificar que o destino de um quadro está no mesmo segmento da origem do quadro, ela irá descartá-lo, porque não existe a necessidade de encaminhá-lo. Se a bridge identificar que o destino está em outro segmento, então o quadro será encaminhado apenas para aquele segmento. Se ela não identificar o segmento de destino, então ela o encaminhará para todos os segmentos, exceto para o segmento de origem.

Apesar de uma bridge e um switch terem um funcionamento tão próximo, passam a impressão que utilizar um ou outro resulta na mesma operação, mas existem algumas diferenças marcantes entre eles.

Uma bridge faz a segmentação e encaminhamento dos quadros por meio de suas portas utilizando recursos de software, já um switch realiza a mesma tarefa via hardware (utiliza circuitos específicos chamados ASICs – Application-Specific Integrated Circuits). Uma bridge só pode configurar uma instância de Spanning Tree por bridge, enquanto que os switches podem ter mais de um.



Como os switches encaminham os frames por endereço MAC

Quiz

Exercício

Interconexão de redes locais (LANs)

INICIAR

Protocolo STP

As LANs atuais, quando são projetadas, tendo em vista seu tamanho, naturalmente contemplam arranjos de várias bridges e switches em enlaces redundantes. Assim, sem a utilização do protocolo STP (Spanning Tree Protocol), uma LAN com enlaces redundantes seria inutilizável. Logo, um bom projeto exige redundância física e o STP permite isso.

A solução adequada inclui redes com bridges e switches com redundância física, usando o STP para bloquear, de maneira dinâmica, algumas portas, para que haja apenas um caminho ativo em qualquer momento.

O protocolo STP é autoconfigurado, é responsável pela remoção de loops na rede e mantém a redundância de caminhos. Um loop pode ser formado quando existem duas ou mais bridges ou switches interligados configurando uma espécie de anel. Uma situação de loop pode parar por completo uma rede.

Está padronizado pelo IEEE 802.1d e apresenta as seguintes funcionalidades:

• Detecção e eliminação de loops;

• Habilidade automática de detectar falha nos caminhos ativos e utilizar os caminhos alternativos que estavam temporariamente desabilitados.

Para que essas funções sejam atendidas, existem três parâmetros importantes que influenciam como o STP vai dividir a rede, são eles:

• Bridge Protocol Data Unit ou BPDU: é um quadro de multicast que as bridges periodicamente geram para compartilhar informações da rede e para eleger a chamada “Bridge Raiz”, que vai construir o STP e impedir o surgimento dos loops, ativando os enlaces quando for necessário.

• Bridge identifiers: cada bridge tem um identificador único, que é usado quando é feito um multicast BPDU.

• Path costs: é definido um custo para cada porta da bridge. Geralmente é o valor inverso da velocidade de transmissão da porta (por exemplo: uma porta de 100 Mbps com custo 1 e uma porta com 10 Mbps tem custo 100). A

porta com menor custo é utilizada quando duas portas existem para a mesma máquina.

• Port priority: cada porta tem uma prioridade padrão. Se dois caminhos que levam a um destino existirem e o acumulado do custo por porta for o mesmo, a porta com maior prioridade é preferencial, o menor valor tem maior prioridade. Se as duas prioridades forem a mesma, o número físico da porta com menor valor é escolhido.

Quando é aplicado o protocolo STP, rede que dispõe de enlaces redundantes, como um simples arranjo de duas bridges conectadas em um anel, o STP fará a varredura da rede em busca dos enlaces redundantes e irá desabilitá-los com o intuito de prevenir a ocorrência dos loops na rede. Para isso, é estabelecida a chamada bridge raiz, com suas portas designadas. Essas portas operam no modo de porta de encaminhamento de estado e são elas que enviam e recebem o tráfego, sendo selecionadas pelo valor de seu custo, TANENBAUM, A. S. (2011).

VLAN

No funcionamento normal de um switch de nível 2, coloca cada segmento com seu próprio domínio de colisão e todos os segmentos estão em um único domínio de broadcast.

Em uma rede com esse formato existem algumas deficiências que podem ser consideradas críticas para alguns ambientes, principalmente quando se trata de segurança. Um dos principais motivos é o fato de todas as máquinas poderem ter acesso a todos os dispositivos que estão no domínio de broadcast.

Por meio do uso de VLANs é possível criar segmentos logicamente separados que irão filtrar esse tipo de tráfego. Suas características são:

? Controle sobre o Broadcast: fornece isolamento completo entre as VLANs.

? Performance: segmenta o tráfego, diminuindo-o e incrementando a performance em um todo.

? Melhor gerência da rede: o agrupamento lógico de usuários não está vinculado à localização física ou geográfica, o que torna a adição ou remoção de máquinas mais flexível.

Uma LAN virtual é fundamentalmente uma ferramenta para estabelecer uma rede hierárquica. Quando se tem uma VLAN na rede é possível criar grupos de Broadcast. Dessa forma estarão vinculadas as portas com um determinado grupo.

Existem três formas de configuração de uma VLAN:

• Por porta: em que cada porta do switch pode suportar somente uma VLAN.

• Por protocolo: VLANs feitas a partir de endereçamento lógico (IP), por meio de switch de nível 3.

• VLAN definida por usuário: agrupa usuários pelos seus endereços MAC.

As VLANs são geralmente criadas pelo administrador da rede de acordo com necessidades específicas do ambiente, o que pode fazer com que se criem duas ou mais VLANs. Nesse processo de criação pode se especificar quais portas do switch estarão vinculadas a qual VLAN, ainda dentro desse aspecto, que tipo de VLAN, estática ou dinâmica.

Estática: definida pelo administrador, vincula uma determinada porta do switch à VLAN.

Dinâmica: nesse modo a porta e as máquinas da VLAN são atribuídas automaticamente por um software de gerenciamento inteligente.

Quiz

Exercício Final

Interconexão de redes locais (LANs)

INICIAR

Referências

TANENBAUM, A. S. Redes de computadores. 5. ed. Rio de Janeiro: Campus, 2011.

Avalie este tópico

ANTERIOR
Protocolo wireless Ethernet

Índice

PRÓXIMO
Sinais digitais e analógicos