Redes e Conectividade

Operação e funcionamento de switch e bridge, conceitos básicos de LAN, VLAN e STP

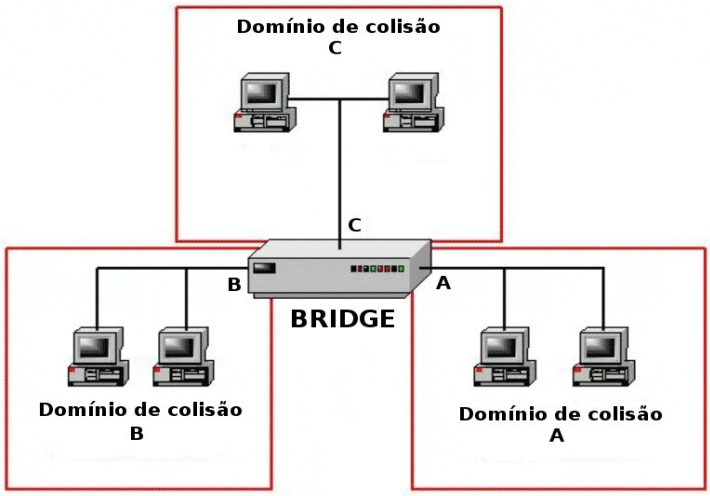
Versão 1.0
Setembro de 2016

Prof. Jairo

jairo@uni9.pro.br
professor@jairo.pro.br

http://www.jairo.pro.br/

Bridge (ou ponte) e switch (chaveador) são equipamentos que operam na camada 2 do RM-OSI, portanto trabalham encaminhado quadros para os endereços físicos dos nós que compõem a LAN.



Bridge segmentando a rede em 3 domínios de colisão.

O bridge é um equipamento simples que serve para conectar dois (ou mais) segmentos de rede sem aumentar o domínio de colisão, isso porque o bridge é capaz de analisar o endereço físico de destino no quadro e então encaminhar de um segmento para o outro apenas se o nó destino e de origem estão em segmentos distintos.

Os switches são comutadores de rede, e podem ser entendidos como bridges mais sofisticados. São equipamentos classificados como concentradores de rede, cuja função básica é o chaveamento de quadros. Normalmente numa LAN ethernet o switch é usado na topologia estrela, e nas suas portas vão ligados os equipamentos (nós) que compõem esta rede.


Switch de 48 portas.

1 – Funcionamento de switch e bridge

Tanto os switches quanto os bridges contêm portas onde conectam equipamentos (switches, hubs, roteadores) e computadores. Switches e bridges funcionam inspecionando os endereços físicos de destino dos quadros, e assim decidindo se devem ser internamente encaminhados ou não para determinada porta. As diferenças entre switches e bridges vão por conta da forma de uso e topologia da rede.

1.1 - Bridge

A bridge é um equipamento antigo, que era normalmente usada para conectar dois ou mais segmentos de rede que estavam em topologia difusão, como por exemplo, barramento.

Quanto ao funcionamento, uma vez recebido o quadro numa porta da bridge, esta inspeciona o endereço de destino e toma uma das seguintes decisões:

- se o endereço de destino está no mesmo segmento que originou o quadro, não encaminha;
- se o endereço de destino está num segmento diferente do que originou o quadro, encaminha o quadro. Por exemplo, se o segmento de origem está na porta 2 do bridge e o de destino na porta 3, internamente encaminha o quadro somente da porta 2 para a 3.

Para poder decidir se encaminha internamente o quadro, a bridge “aprende” os endereços físicos dos equipamentos e computadores de todos os segmentos conectados a ela, assim quando recebe um quadro numa porta tem como avaliar se deve encaminhar (ou não) o quadro.

```
# brctl  showmacs  br0
port no   mac addr          is local?    ageing timer
  1       00:11:3e:ad:bq:cc   no          1.01
  1       00:11:3e:af:bq:cc   no          20.17
  1       00:11:3e:ag:bq:cc   no          60.53
  2       fe:ff:ff:ff:ff:ff   yes         0.00
```

O princípio de funcionamento aqui é garantir a comunicação entre os dois ou mais segmentos de rede sem aumentar o domínio de colisão. Se fosse usado um hub ao invés do bridge, também funcionaria a comunicação entre os segmentos de rede, porém iria aumentar o domínio de colisão.

Embora os equipamentos bridge sejam antigos e não mais usados nas redes atuais, o conceito continua sendo usado internamente nos switches e em alguns softwares de virtualização.

1. 2 - Switch

Quanto à classificação, os switches são Layer 2 (L2, data-link layer), Layer 3 (L3, network layer) e Layer 4 (L4, transport ou application layer).

Os **switches L2** também são classificados como não gerenciáveis. Na prática, são bridges

com um maior número de portas, mas que, ao contrário das bridges, são capazes de processar quadros a nível de hardware. As bridges usam software para processar os quadros.

Os switches não gerenciáveis normalmente são usados nas redes pequenas em substituição aos hubs. Por serem mais simples, fazem chaveamento de quadros mais rapidamente que os L3 e L4.

Os **switches L3** são classificados como gerenciáveis e operam também em camada 3. Neste caso, conseguem fazer uso de endereços lógicos (IP) para identificar a localização do equipamento ou computador de destino. Incorporam funções de roteamento de pacotes, além de chaveamento de quadros.

Os **switches L4** operam também na camada de aplicação e funcionam determinando quais protocolos de aplicação estão incluídos em cada pacote. Estes switches tomam decisões de encaminhamento de pacotes baseados na aplicação ao qual o pacote pertence, e não apenas baseado em endereços físicos ou lógicos. Exemplos de protocolos de aplicação: HTTP, FTP, SMTP.

Inicialmente vieram como balanceadores de carga, mas recentemente surgiu uma nova geração de switches L4 classificados com Application Delivery Controller (ADC), isto devido a diversidade de características suportadas: balanceamento de carga, compressão de dados, SSL (Secure Sockets Layer), filtragem de tráfego, etc.

Switch L4 Big IP F5

Devido a todas estas características, os switches L4 são os de resposta mais lenta.

Pelas características da topologia estrela, o switch é o concentrador de rede e também um ponto único de falha: se ele parar, para toda a LAN. Devido a isso, nos casos onde o acesso não pode ser perdido precisa ser incluído redundância, e isso é conseguido com o uso de pelo menos dois switches. Envolve duplicar o cabeamento e também as interfaces de rede nos computadores.

Mas caminhos redundantes (duplicados) podem levar a loops no encaminhamento de quadros de um switch para o outro. Uma das maneiras de amenizar os loops é habilitar o STP (Spanning Tree Protocol) em todos os switches envolvidos nesta redundância de caminhos.

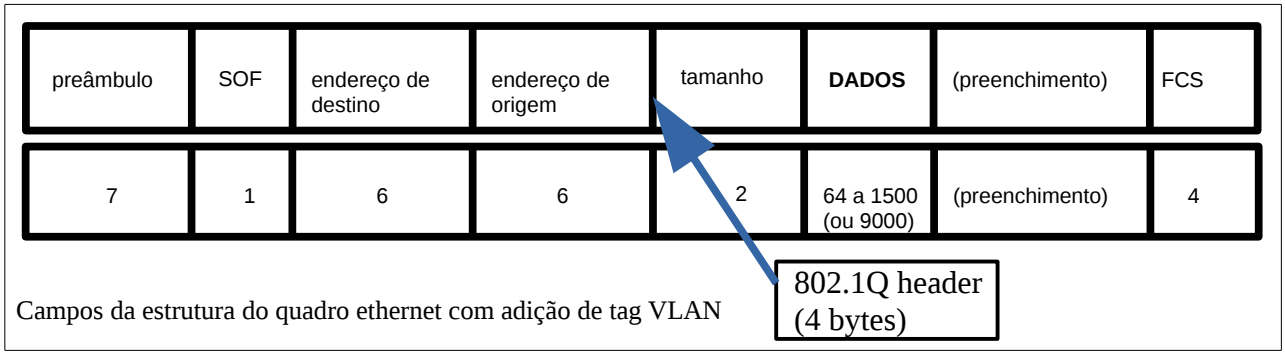
2 – VLAN

2.1 - VLAN

Uma LAN virtual (VLAN, Virtual LAN) é qualquer domínio de broadcast que, num switch, é particionado a nível de data link layer (camada 2). Por ser camada 2, um switch L2 pode criar VLANs, porém a falta de roteamento (L3) vai dificultar a comunicação entre estas diferentes VLANs assim formadas. Desse modo, normalmente são usados switches L3 para criar VLANs.

O padrão VLAN está definido no **IEEE802.1Q**, usado em rede ethernet, que também define procedimentos para os switches e bridges manusearem os quadros tagged (“tageados”) pelo uso de VLANs.

Convém notar quer a tag de VLAN não encapsula o quadro original, mas inclui uma marca ou etiqueta (tag) no seu interior:



Campos da estrutura do quadro ethernet com adição de tag VLAN

Este padrão define um sistema que usa tags (etiqueta ou marca) no quadro ethernet para indicar a qual VLAN o quadro se destina.

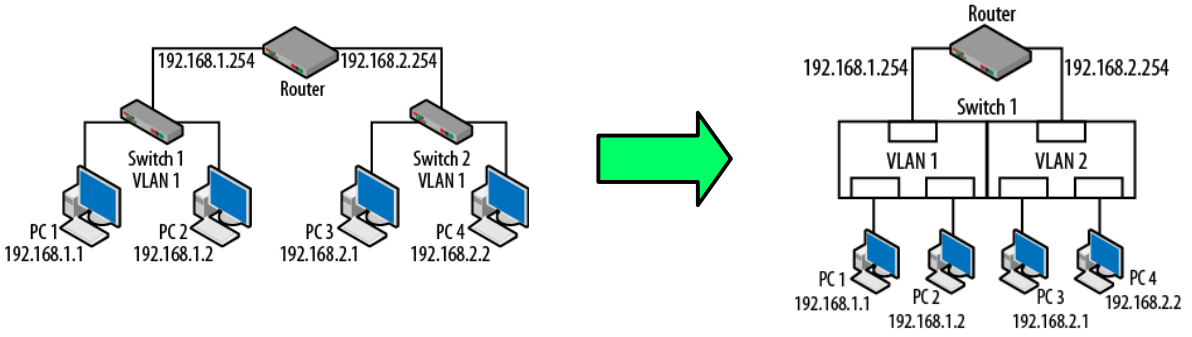
Naturalmente, a ideia de VLANs é para criar várias LANs segmentadas num mesmo switch. Mas se não for definido VLANs num switch, este vai tratar todos os equipamentos e computadores conectados nas suas portas como pertencentes à mesma LAN.

VLAN pode ser usado em outros casos, como por exemplo num ambiente de trabalho onde os funcionários de um mesmo grupo (por exemplo, contabilidade) estejam distribuídos em dois andares do prédio, desse modo as estações de trabalho do grupo estão cabeadas para dois (ou mais) switches. Nesse caso, as portas dos switches onde estão conectadas as estações de trabalho de todos eles devem ser marcadas com o mesmo número da VLAN (VLAN ID) da contabilidade, por exemplo 566. Isso vai colocá-los todos na mesma LAN, embora fisicamente falando eles estejam conectados em switches diferentes.

Uma outra definição é que VLAN seja um grupo lógico de portas de switches independente da localização. Outro aspecto é que os membros de um mesmo grupo não precisam estar limitados a

portas sequenciais do switch.

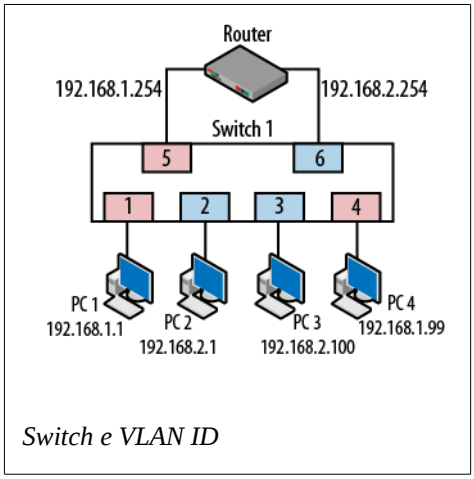
Nas figuras abaixo é mostrado à esquerda o esquema tradicional de LAN com switches e roteadores, e à direita o equivalente com o uso de VLAN.



LAN tradicional e equivalente com VLAN.

2.2 – VLAN ID

Para que duas portas de switch estejam na mesma VLAN, basta que se atribua a elas o mesmo VLAN ID, que é o número que identifica a VLAN.



Switch e VLAN ID

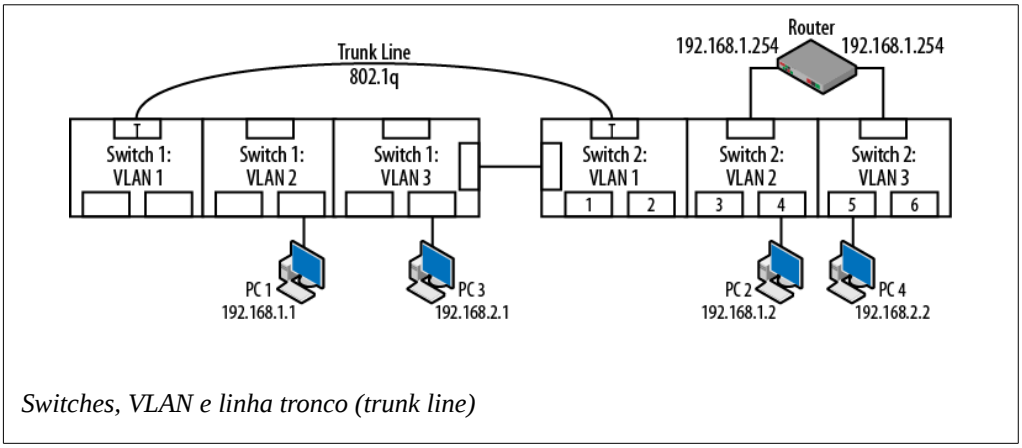
Um VLAN ID é um número que vai de 1 a 4095. Se não for definido VLAN na porta, este é assumido como o número 1.

Quanto aos tipos, as VLANs são estáticas ou dinâmicas. Na maior parte do caso são estáticas, que é o caso do administrador de redes configurar as portas do switch para determinado VLAN ID.

Numa VLAN dinâmica, o VLAN ID é atribuído automaticamente à porta quando o equipamento é conectado à qualquer porta do switch, e isto é possível devido a uma pré-configuração que atribuiu àquele MacAddress a uma determinada VLAN.

No caso de uma VLAN se estender por mais de um switch, é necessário também definir uma linha tronco (trunk) para conectar o tráfego da VLAN entre os switches.

Por padrão, todas as portas do switch são chamadas de “portas de acesso” (access ports), porém quando a porta é configurada como trunk ela não pertence a nenhuma VLAN.



Switches, VLAN e linha tronco (trunk line)

A virtualização de LAN continua sendo desenvolvida, agora com foco no cloud computing. Virtual Extensible LAN (VXLAN) é uma tecnologia de virtualização de redes que visa aprimorar problemas de escalabilidade em grandes implantações de cloud computing.

À semelhança do que ocorreu com os computadores, que passaram a virtualizar máquinas, agora é a vez dos equipamentos de rede também passarem a apresentar recursos virtualizados: ao invés de esparramar toda a infraestrutura de redes em vários switches com muito cabeamento, agora um único grande switch pode ser virtualizado e passar a apresentar várias LANs virtuais.

3 - STP

STP (Spanning Tree Protocol, árvore de espalhamento) roda em switches e bridges que são compatíveis com o protocolo **IEEE802.1D**.

Um switch L2 pertence a um único domínio de broadcast, e encaminha tanto broadcast quanto multicast para todas as portas, exceto a porta de origem.

O protocolo STP, trabalha na camada 2, e tem como objetivo impedir loops no encaminhamento de quadro entre switches (ou bridges), isso quando existe mais de uma caminho possível. Mais de um caminho possível é para ter redundância e não parar a rede inteira caso um switch falhe.

Mas caso exista um loop na rede redundante, um broadcast storm (tempestade de broadcast) vai se desenvolver em questão de segundos. A tempestade ocorre quando os broadcasts são direcionados para o loop e causa um estrangulamento no tráfego de dados nesta rede.

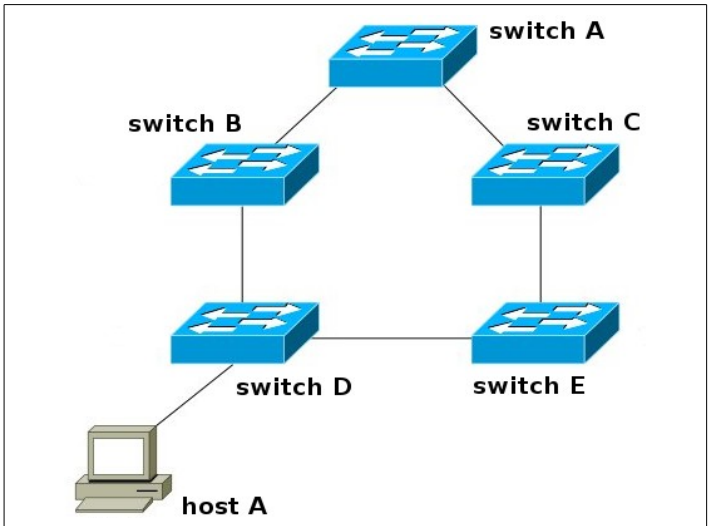
O STP é usado nas situações em que se quer linques redundantes, mas não loops.

No exemplo abaixo, se o host A enviar um broadcast, o switch D irá encaminhar para todas as suas portas, inclusive as portas trunk (tronco) conectadas aos switch B e switch E. Neste caso, o broadcast vai permanecer em loop para sempre, em duas tempestades distintas circulando em

direções opostas através dos switches que compõem este loop.

Para prevenir esta tempestade de broadcast, os switches que rodam STP vão construir um mapa com a topologia da rede inteira para identificar se existe algum loop. Encontrado um ou mais loops na topologia, o STP desabilita ou bloqueia as portas redundantes que criam as condições para existência destes loops.

Mas o fato de ter bloqueado alguma porta não significa que ela permaneça bloqueada para sempre, pois em caso de perda de um caminho, por exemplo se um switch cair, o STP habilita a porta que leva pelo outro caminho. O STP mantém a redundância e a tolerância a faltas da rede.



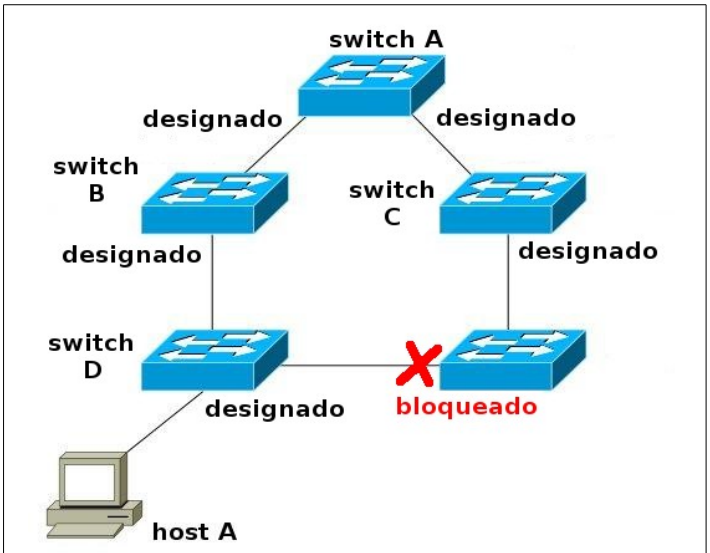
Topologia redundante com loop

Convém notar que neste exemplo STP não suporta balanceamento de carga, pois simplesmente impede o tráfego para caminhos alternativos.

Para construir um database com a topologia da rede, STP usa multicast de Bridge Protocol Data Unit (BPDU), que é enviado a cada dois segundos para toda a rede.

A construção da topologia é um processo de convergência que envolve:

- eleição de uma root bridge (raiz da árvore de espalhamento) pela atribuição de um bridge ID a cada switch: o de menor ID será a root bridge;
- identificação de root ports (portas raiz);
- identificação de portas designadas;
- bloqueio de portas conforme requerido para eliminar os loops.



Topologia redundante sem loop

A root bridge é o ponto central de referência para a topologia STP, e deve ser atribuído ao switch mais centralizado na topologia STP. Por default, qualquer switch acredita ser a root bridge, mas o recebimento de um BPDU oriundo de um switch com bridge ID menor reposiciona esta bridge na hierarquia. O processo é dinâmico, a inclusão ou retirada de switches causa nova eleição.

À exceção do root bridge, cada

switch tem apenas uma root port. A root port é escolhida por ter o menor custo de caminho para atingir a root bridge. Quanto maior a largura de banda, menor o custo de caminho. O menor custo é o preferido.

As portas designadas são as identificadas para encaminhar BPDU e quadros entre os segmentos da rede. As portas bloqueadas impedem a ocorrência de loop.

Para funcionar, exige que todos os switches estejam com o STP habilitado. Por default (padrão) todos os switches da Cisco já vem habilitados para STP em todas as VLANs.