

Aula 6 - Camada de Enlace: VLANs

Diego Passos

Universidade Federal Fluminense

Redes de Computadores II

Na Última Aula (I)...

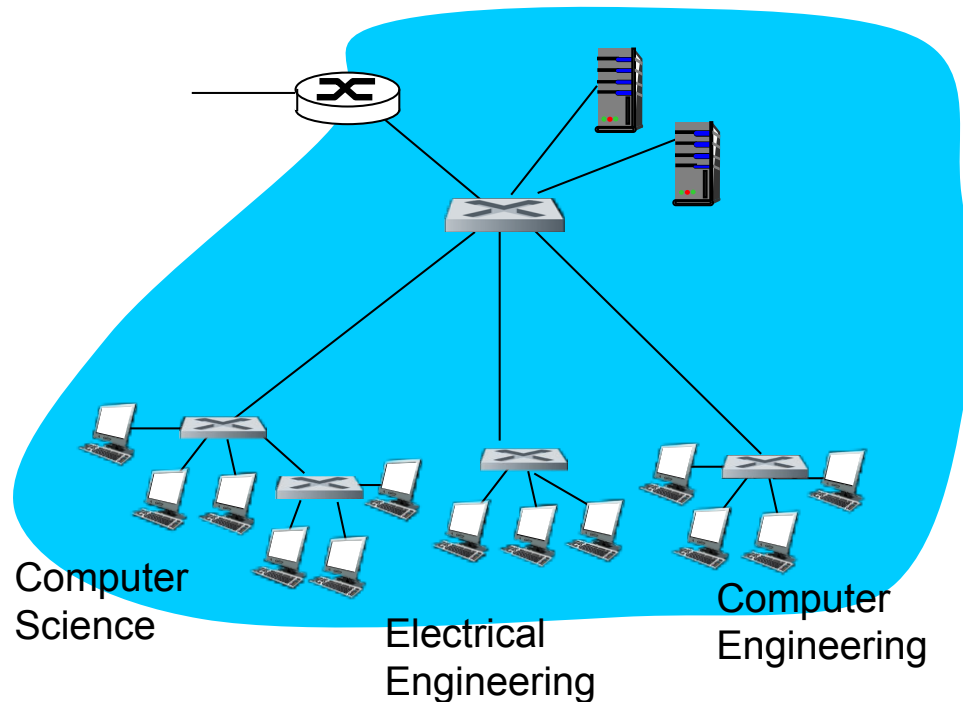
- **Switch**: dispositivo ativo, nível 2, intermediário.
 - **Enlaces dedicados** para cada dispositivo conectado.
 - Paradigma *store-and-forward*.
 - **Examina** quadros recebidos, **seleciona** porta de saída.
 - **Transparente** para os dispositivos.
 - Permite **transmissões simultâneas**.
- **Aprendizado automático**: descobre sozinho onde estão os dispositivos.
 - Monta uma **tabela de encaminhamento**.
 - Se não há entrada na tabela: **inundação**.
- **Switches em cascata**: podem ser interconectados para estender a rede.
 - Auto-aprendizado continua funcionando.
 - Potencialmente, **mais de um MAC associado a cada porta**.
 - Pode **esgotar a capacidade** da tabela de encaminhamento.
 - Mais inundações, pior desempenho.
- **Várias diferenças** em relação aos roteadores.
 - **Camada**.
 - Encaminhamento baseado em **endereços diferentes**.
 - Métodos de **construção** das tabelas.

Na Última Aula (II)...

- Vários potenciais problemas decorrentes de má configuração.
 - Erros de configuração física: *loops*.
 - Quadros em *broadcast* circulam pelos switches indefinidamente.
 - Erros de configuração lógica: conflitos de endereço.
 - Conflito de IP.
 - Conflito de MAC.
- Tempestade de *broadcast*.
 - Transmissões em *broadcast* (custosas) consomem muitos recursos da rede.
 - Muitas vezes decorrente de *loops*.

VLANs

VLANs: Motivação



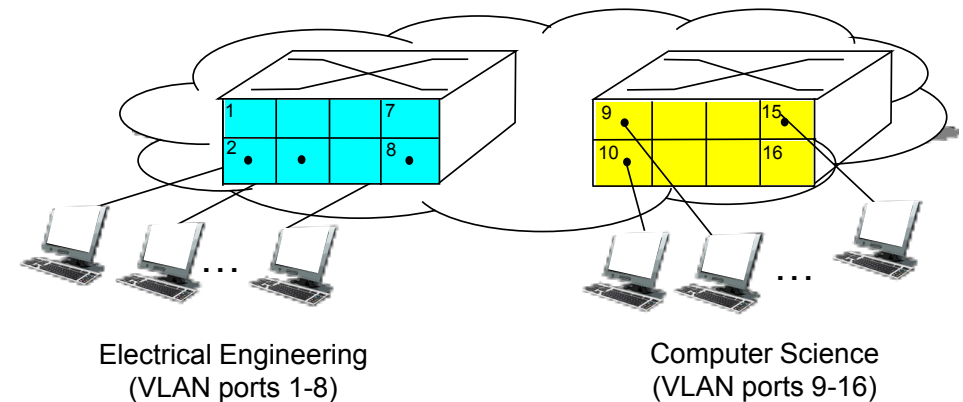
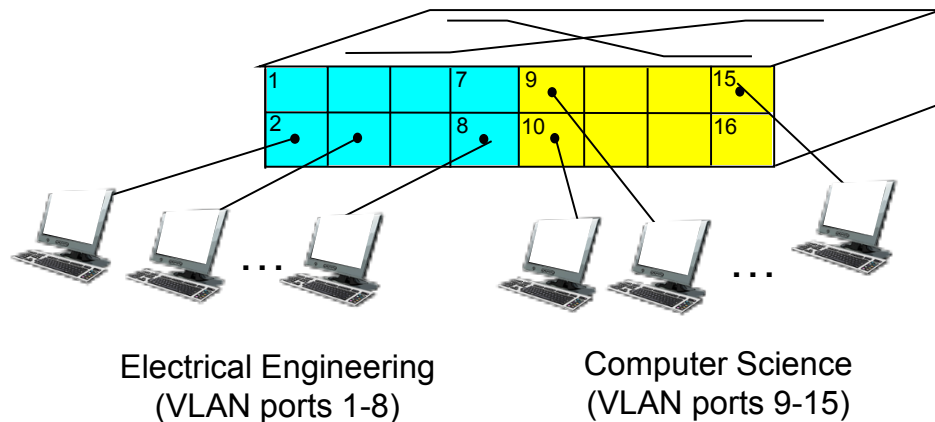
- Considere os seguintes aspectos:
 - Funcionário da CS muda para escritório na EE.
 - É possível mantê-lo “conectado” ao switch da CS?
 - Outra questão: único domínio de *broadcast*.
 - Todo tráfego de nível 2 (ARP, DHCP, inundações por falta de entrada nas tabelas de encaminhamento) atravessa toda a LAN.
 - Problemas de privacidade/segurança e eficiência.

Virtual Local Area Network

- Switches que possuem capacidades de VLAN podem definir **múltiplas LANs virtuais** usando uma única infraestrutura física.

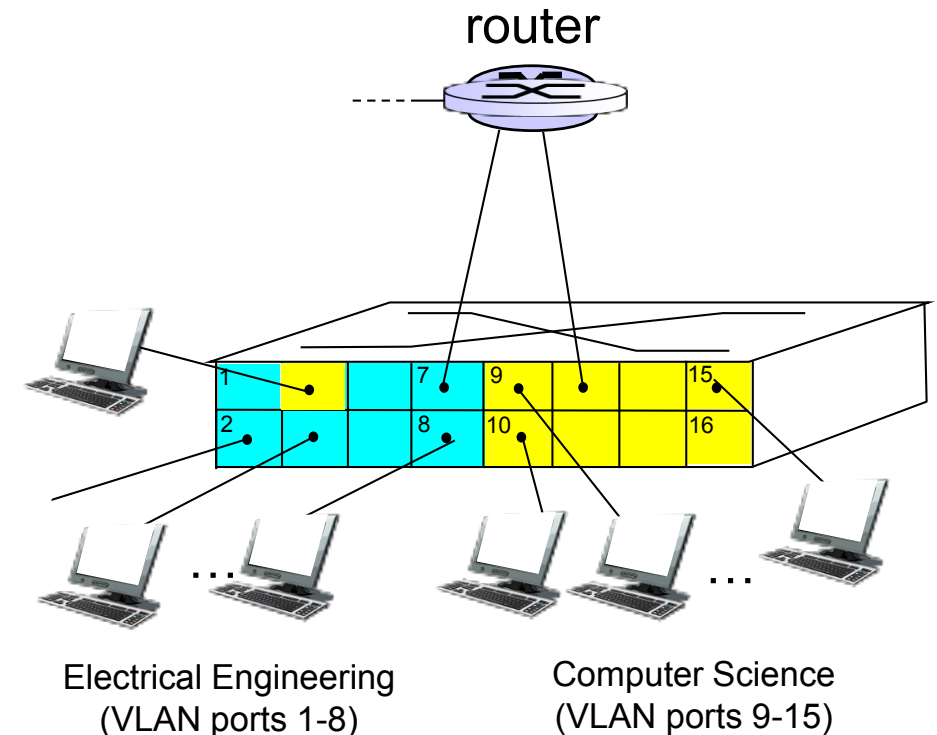
- VLAN baseada em porta:**

- Portas do switch agrupadas (pelo *software* de gerenciamento do switch).
- Um único switch físico...
- ... age como **múltiplos** switches virtuais.

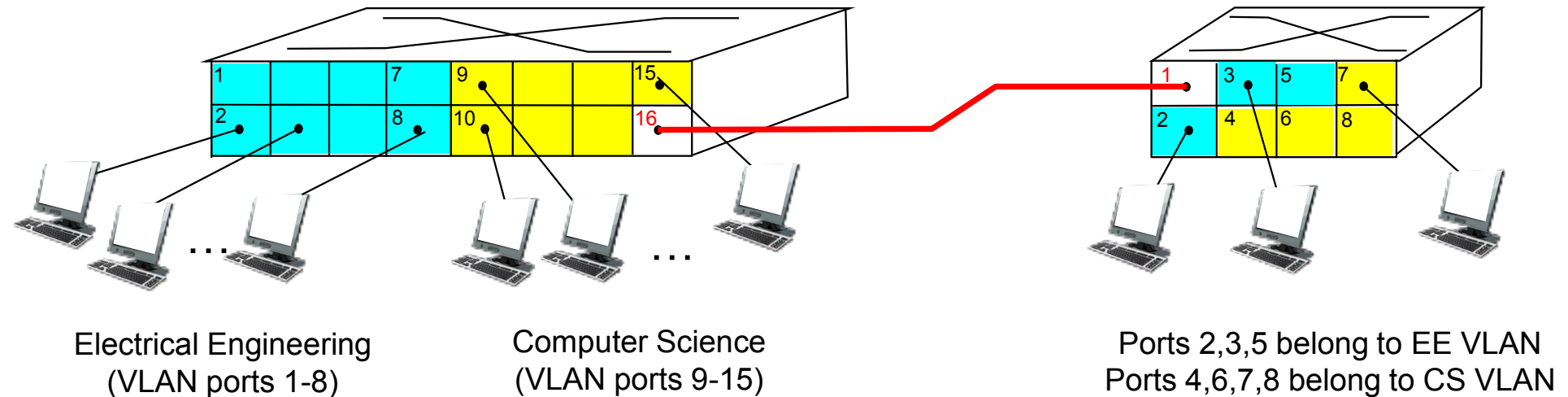


VLAN Baseada em Porta

- **Isolamento de tráfego:** quadros originários das portas 1–8 chegam **apenas** às portas 1–8.
- **Alocação dinâmica:** portas podem ser alocadas dinamicamente a VLANs.
 - É possível definir VLANs com base nos MACs dos dispositivos.
- **Encaminhamento entre VLANs:** feita via roteamento (nível 3).
 - Na prática, fabricantes vendem switches que são, também, roteadores.

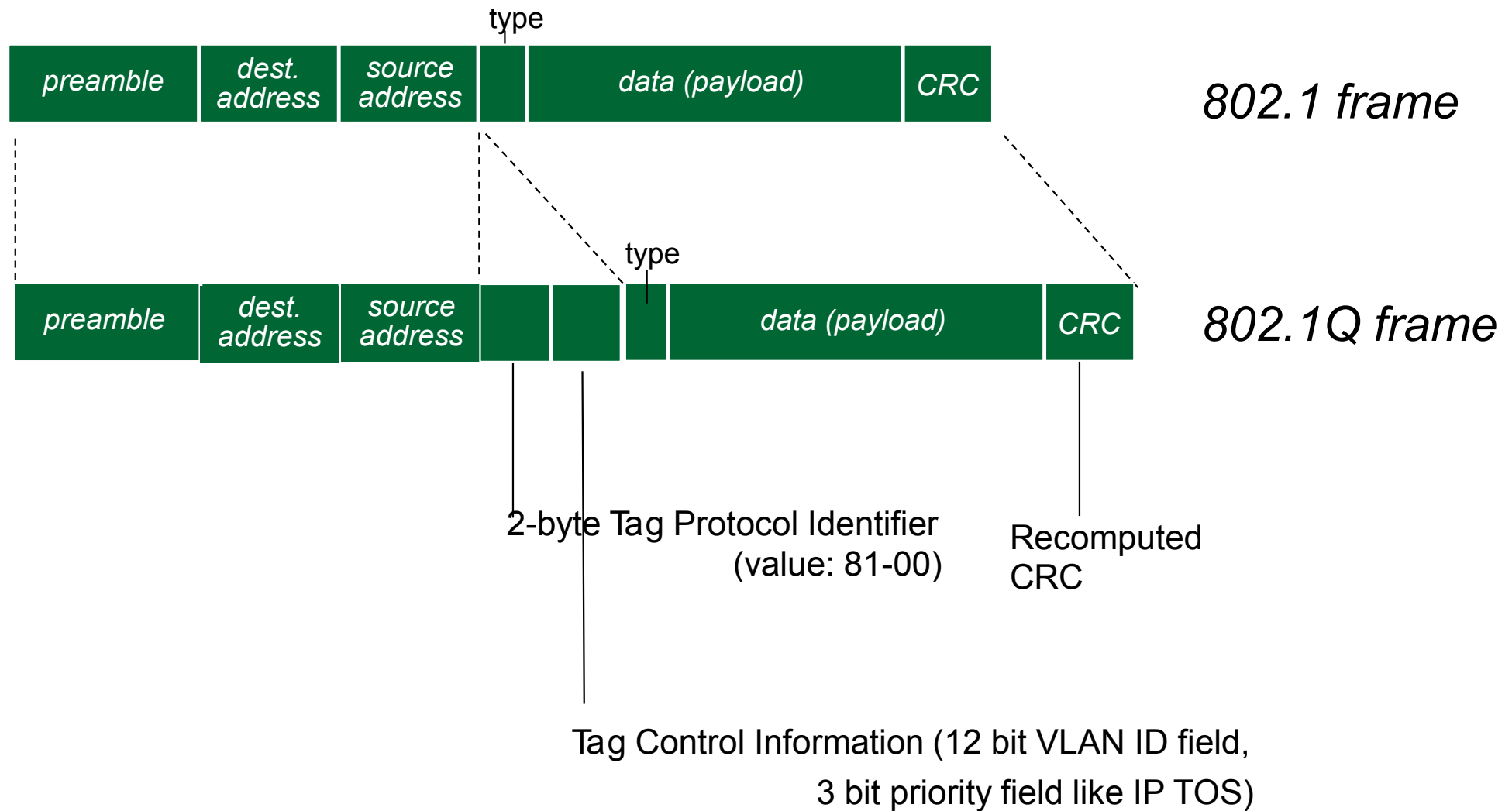


VLANs Formadas por Múltiplos Switches Físicos



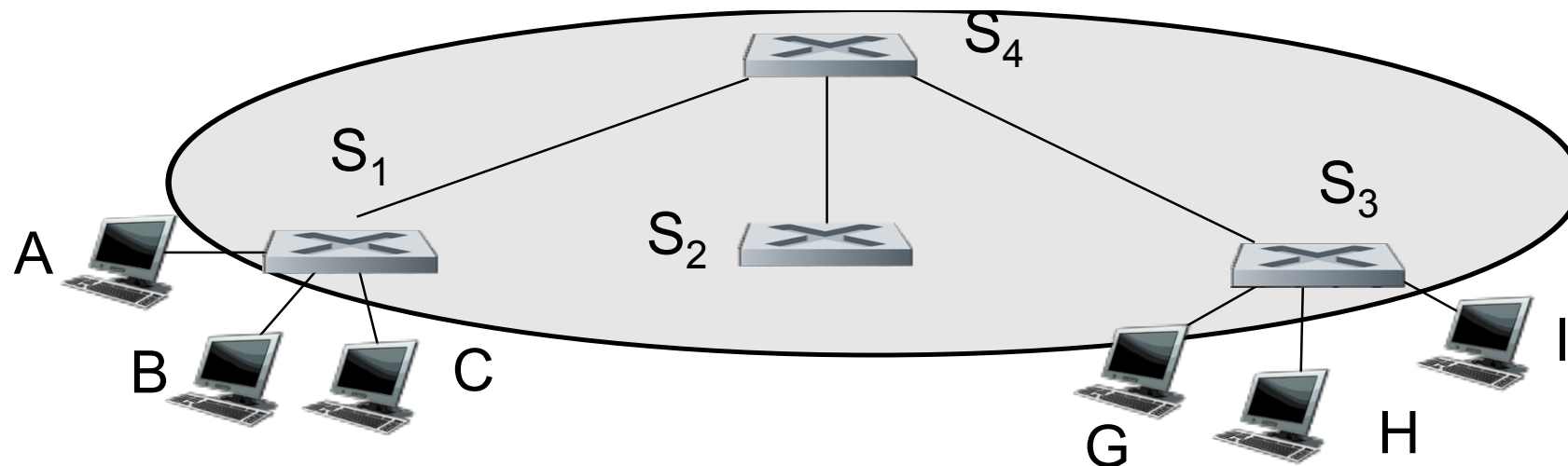
- **Porta trunk:** transportam quadros entre VLANs definidas sobre múltiplos switches físicos.
 - Quadros encaminhados dentro da mesma VLAN entre switches diferentes não podem ser quadros Ethernet “normais”.
 - Precisam armazenar identificador da VLAN.
 - Protocolo 802.1Q adiciona/remove campos adicionais de cabeçalho para quadros transmitidos entre portas *trunk*.

Formato de um Quadro 802.1Q



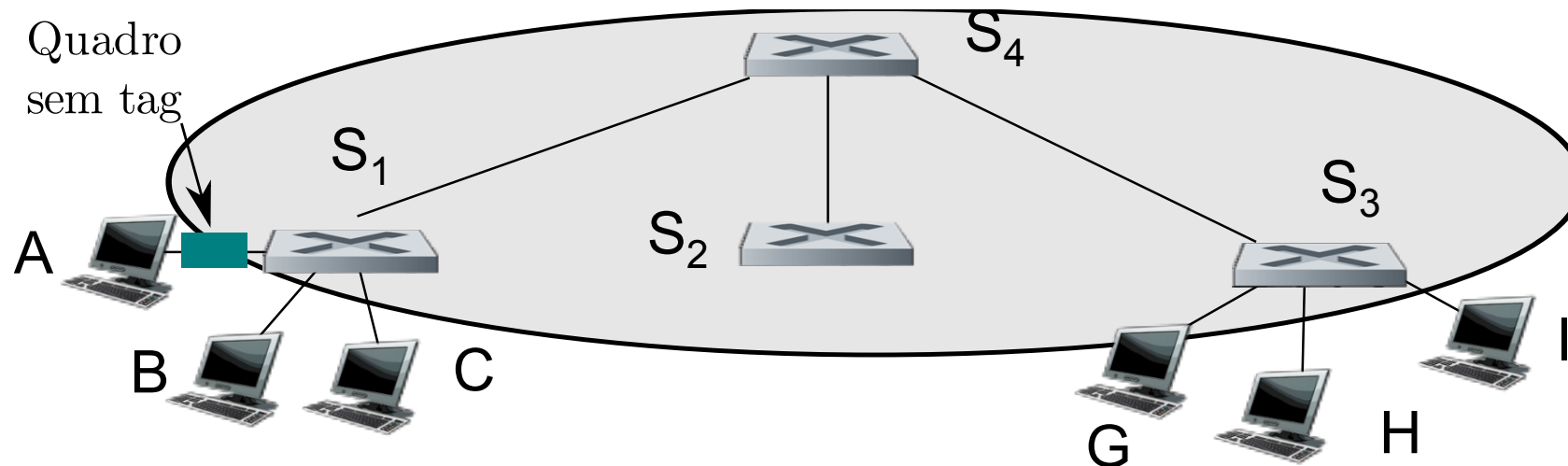
IEEE 802.1Q: Adição e Remoção de *tags* (I)

- Dispositivos como *switches* gerenciáveis normalmente são “cientes” da existência das VLANs de uma rede.
- Já dispositivos como *hosts* comumente não tem este conhecimento.
- É possível dividir a rede em duas porções:
 - Porção ciente das VLANs.
 - Resto da rede.



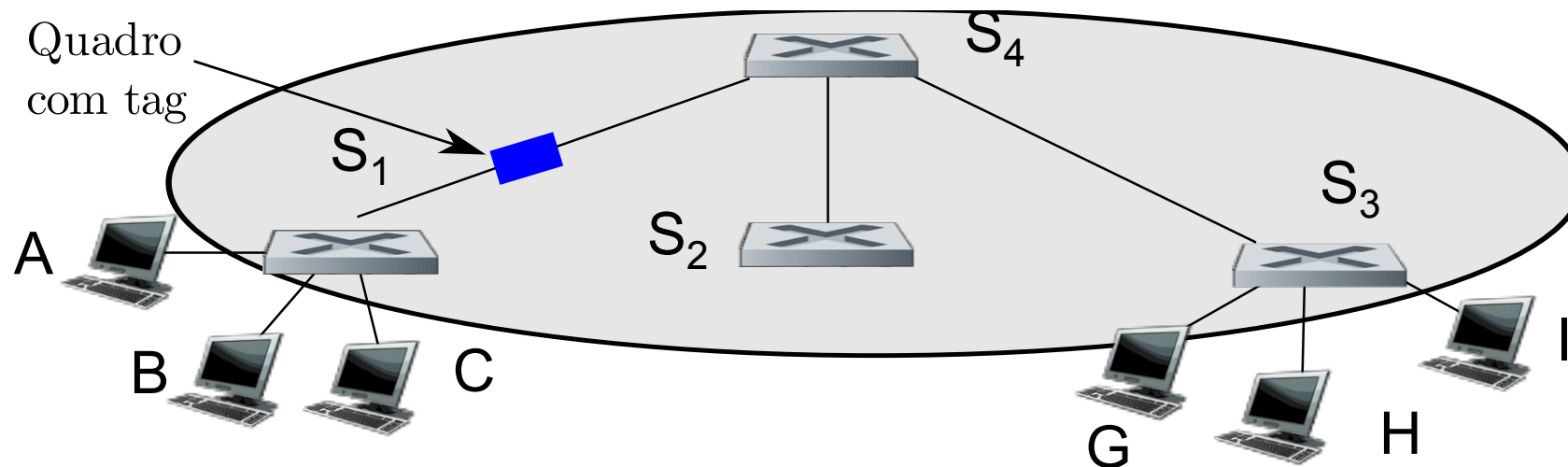
IEEE 802.1Q: Adição e Remoção de *tags* (II)

- Quando quadro entra na porção ciente da rede, não possui uma *tag* especificada.
 - Switch associa quadro a uma VLAN padrão (para a porta de entrada ou para a rede).
 - *Tag* correspondente é adicionada usando o cabeçalho IEEE 802.1Q.



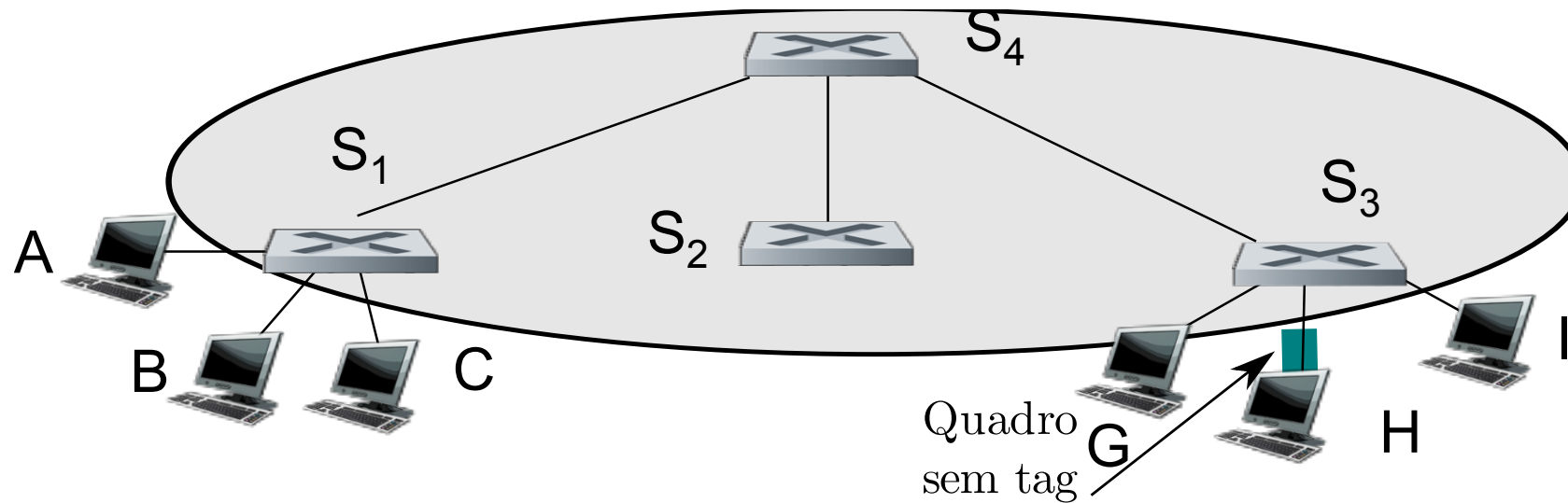
IEEE 802.1Q: Adição e Remoção de *tags* (III)

- Comunicações internas à porção ciente mantém a *tag* no quadro.
 - Permite que dispositivo que recebe o quadro identifique a VLAN.



IEEE 802.1Q: Adição e Remoção de *tags* (III)

- Quando quadro deixa a porção ciente, *tag* precisa ser removida.



Spanning Tree Protocol

STP: Introdução

- Protocolo executado na camada de enlace.
- Criado por Radia Perlman, padronizado no IEEE 802.1D.
- Objetiva evitar *loops* lógicos, ainda que existam *loops* físicos.
- Como funciona:
 - Dispositivos (*e.g.*, switches) criam uma árvore geradora (mínima) da topologia física.
 - Enlaces/portas que causariam *loops* são desativados para dados.

Algorhyme

I think that I shall never see
a graph more lovely than a tree.
A tree whose crucial property
is loop-free connectivity.
A tree that must be sure to span
so packet can reach every LAN.
First, the root must be selected.
By ID, it is elected.
Least-cost paths from root are traced.
In the tree, these paths are placed.
A mesh is made by folks like me,
then bridges find a spanning tree.

Radia Perlman

STP: Operação Básica

- Protocolo dividido nos seguintes passos:
 1. Escolha de uma raiz para a árvore geradora.
 - Algoritmo distribuído de eleição de líder.
 - Eleição se dá de acordo com identificador de cada dispositivo.
 2. Determinação do caminho mais curto entre cada dispositivo e a raiz.
 - Similar ao funcionamento de um algoritmo de roteamento de vetor de distâncias.
 - Mas apenas uma distância importa: até a raiz.
 3. Configuração das portas.
 - Porta que leva à raiz só é deixada ativa se pertence à árvore geradora.
 - Portas que não levam à raiz (e.g., interconectam *hosts*) são deixadas ativas.

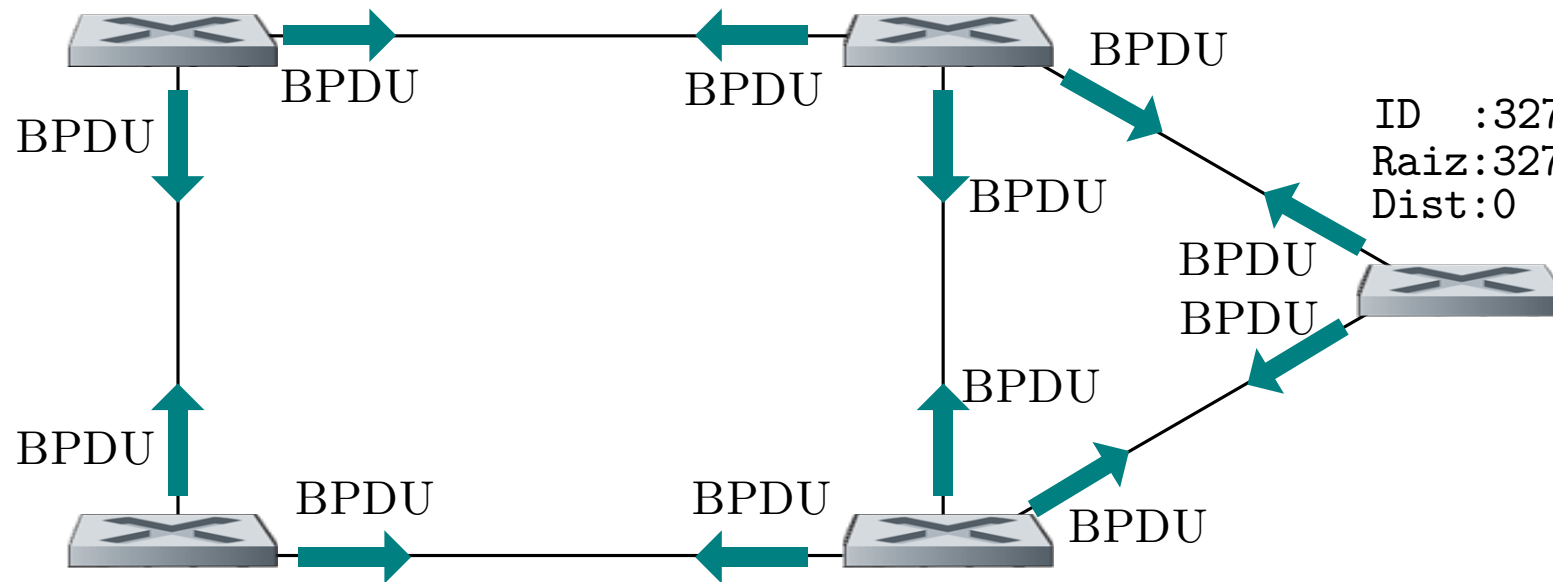
STP: Mais (Alguns Poucos) Detalhes

- Cada switch envia periodicamente BPDUs (*Bridge Protocol Data Units*).
 - Quadro de controle do protocolo.
 - Informa (entre outras coisas):
 - Identificador do switch.
 - Raiz da árvore.
 - Distância para a raiz.
 - Normalmente, a cada 2 segundos.
 - Enviado para o endereço MAC multicast **01:80:C2:00:00:00**.
- Identificador: prioridade, concatenada com MAC.
 - Prioridade é configurável.
 - Switch com menor identificador é eleito raiz.
- Inicialmente:
 - Switches não sabem nada sobre a topologia.
 - Cada switch **assume ser a raiz**.
 - Envia BPDUs com a tupla <ID, ID, 0> para todas as portas.
- Ao receber um BPDUs por uma porta:
 - Verifica se ID da raiz reportada é menor que a da raiz atualmente conhecida.
 - Se sim: atualiza raiz, distância.
 - Se não: ainda pode atualizar distância se menor.

STP: Exemplo (I)

ID :32768.06:00:00:00:00:01
Raiz:32768.06:00:00:00:00:01
Dist:0

ID :4096.06:00:00:00:00:04
Raiz:4096.06:00:00:00:00:04
Dist:0



ID :32768.06:00:00:00:00:05
Raiz:32768.06:00:00:00:00:05
Dist:0

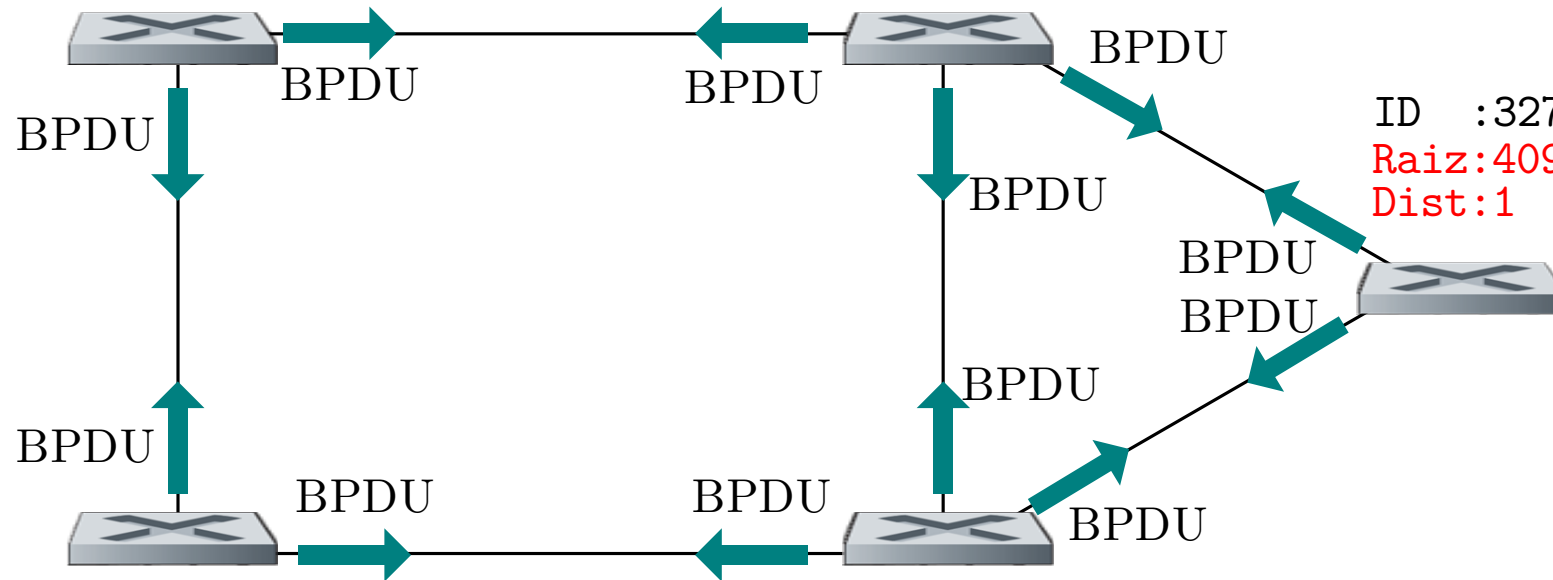
ID :32768.06:00:00:00:00:02
Raiz:32768.06:00:00:00:00:02
Dist:0

ID :32768.06:00:00:00:00:03
Raiz:32768.06:00:00:00:00:03
Dist:0

STP: Exemplo (II)

ID :32768.06:00:00:00:00:01
Raiz:4096.06:00:00:00:00:04
Dist:1

ID :4096.06:00:00:00:00:04
Raiz:4096.06:00:00:00:00:04
Dist:0



ID :32768.06:00:00:00:00:05
Raiz:4096.06:00:00:00:00:04
Dist:1

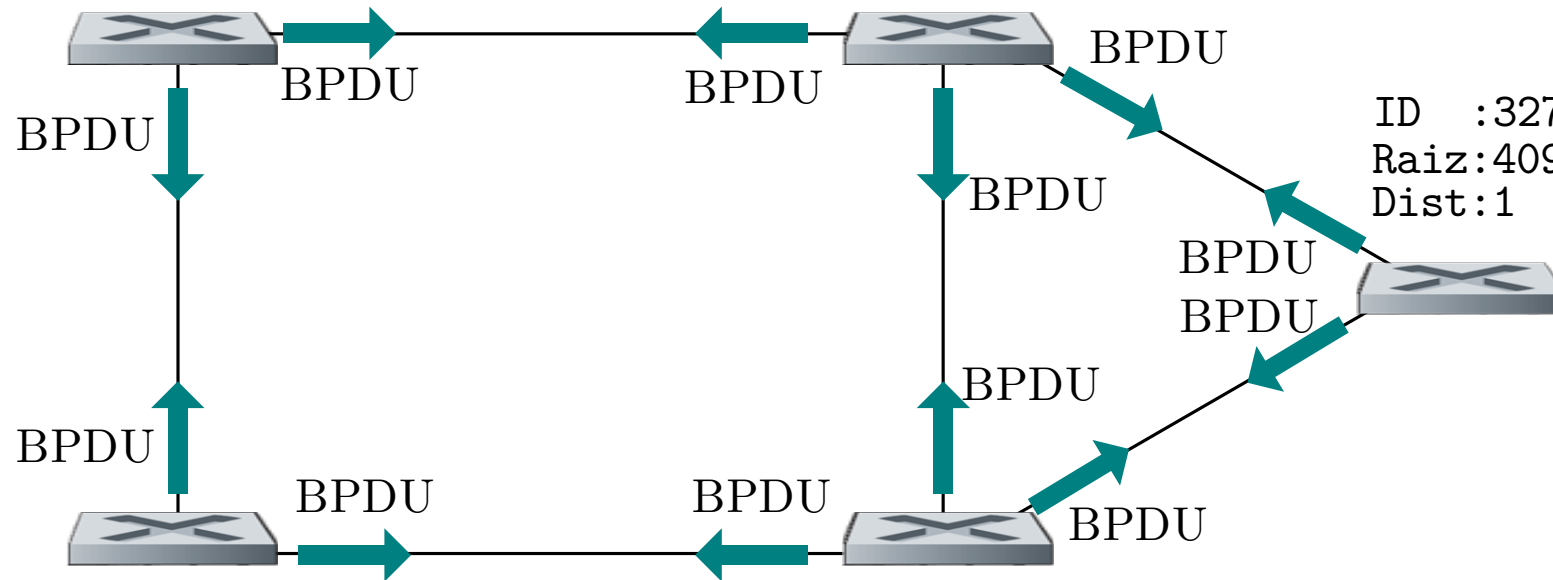
ID :32768.06:00:00:00:00:02
Raiz:32768.06:00:00:00:00:01
Dist:1

ID :32768.06:00:00:00:00:03
Raiz:4096.06:00:00:00:00:04
Dist:1

STP: Exemplo (III)

ID :32768.06:00:00:00:00:01
Raiz:4096.06:00:00:00:00:04
Dist:1

ID :4096.06:00:00:00:00:04
Raiz:4096.06:00:00:00:00:04
Dist:0



ID :32768.06:00:00:00:00:05
Raiz:4096.06:00:00:00:00:04
Dist:1

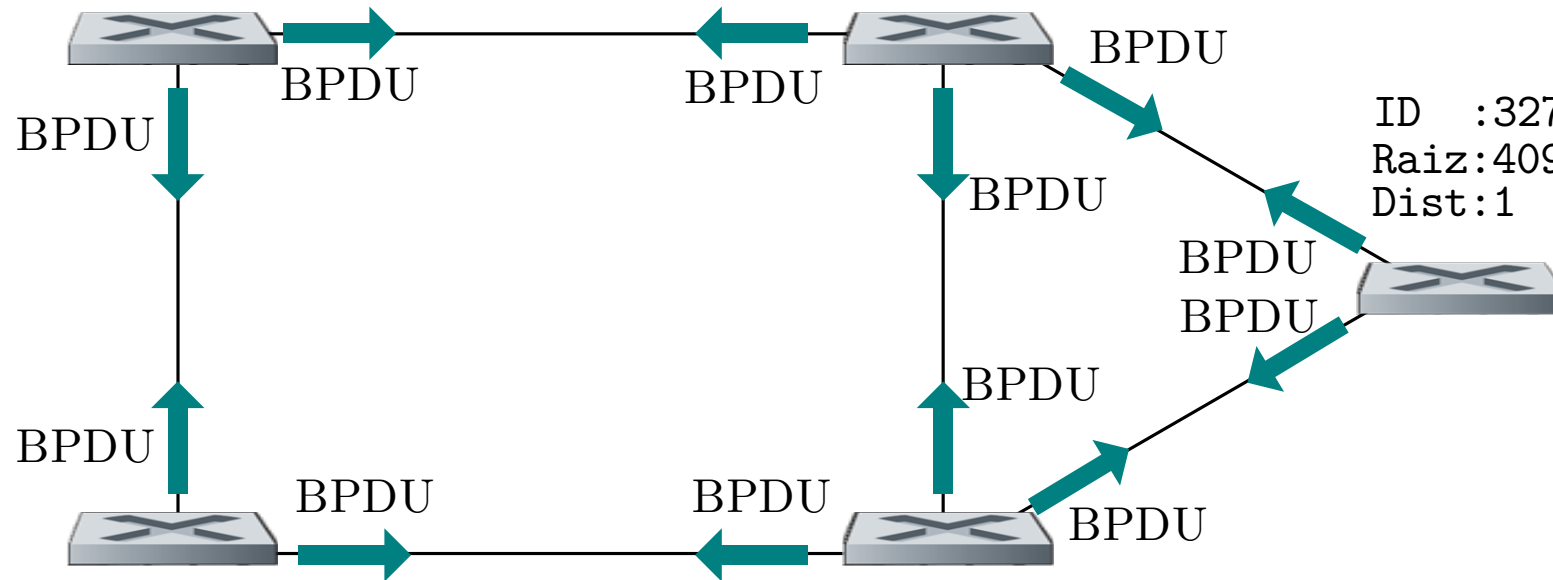
ID :32768.06:00:00:00:00:02
Raiz:4096.06:00:00:00:00:04
Dist:2

ID :32768.06:00:00:00:00:03
Raiz:4096.06:00:00:00:00:04
Dist:1

STP: Exemplo (IV)

ID :32768.06:00:00:00:00:01
Raiz:4096.06:00:00:00:00:04
Dist:1

ID :4096.06:00:00:00:00:04
Raiz:4096.06:00:00:00:00:04
Dist:0



ID :32768.06:00:00:00:00:05
Raiz:4096.06:00:00:00:00:04
Dist:1

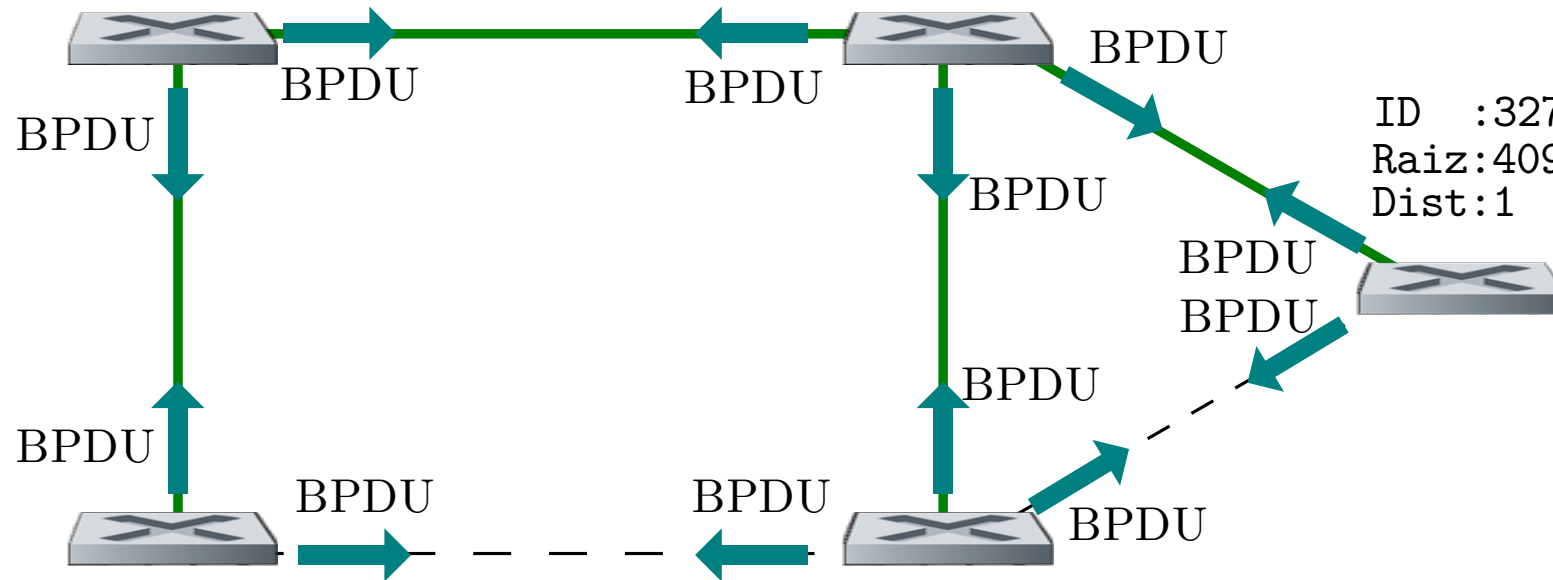
ID :32768.06:00:00:00:00:02
Raiz:4096.06:00:00:00:00:04
Dist:2

ID :32768.06:00:00:00:00:03
Raiz:4096.06:00:00:00:00:04
Dist:1

STP: Exemplo (V)

ID :32768.06:00:00:00:00:01
Raiz:4096.06:00:00:00:00:04
Dist:1

ID :4096.06:00:00:00:00:04
Raiz:4096.06:00:00:00:00:04
Dist:0



ID :32768.06:00:00:00:00:05
Raiz:4096.06:00:00:00:00:04
Dist:1

ID :32768.06:00:00:00:00:02
Raiz:4096.06:00:00:00:00:04
Dist:2

ID :32768.06:00:00:00:00:03
Raiz:4096.06:00:00:00:00:04
Dist:1

Resumo da Aula...

- VLANs:
 - Solução para “**separar**” **redes em nível 2**, compartilhando mesma infraestrutura física.
 - Separação **puramente lógica**.
 - Define **domínios de broadcast** distintos.
 - Motivações: **segurança, desempenho**.
- Podem ser definidas com base em:
 - Portas específicas.
 - Tags informadas em cabeçalhos específicos.
- VLANs podem se estender por **vários switches físicos diferentes**.
- STP:
 - **Protocolo** da camada de enlace.
 - Constrói **topologia lógica em árvore**.
 - Evita problemas causados por loops.
 - Permite estabelecimento (físico) de **enlaces redundantes**.
- Algoritmo distribuído:
 - Similar a roteamento em vetor de distância.
 - Switches **anunciam periodicamente** raiz, melhor distância conhecida.
 - **Conhecimento atualizado**, se informações mais corretas/caminhos melhores são recebidos.

Leitura e Exercícios Sugeridos

- VLANs:
 - Páginas 355 a 358 do Kurose (Subseção 5.6.5).
 - Exercícios de fixação 16 e 17 do capítulo 5 do Kurose.
- STP:
 - Páginas 208 a 212 do Tanenbaum (Seção 4.8 até 4.8.3).

Próxima Aula...

- Discutiremos uma tecnologia que atua entre as camadas 2 e 3 da pilha TCP/IP.
- MPLS:
 - O que é.
 - Como funciona.
 - Objetivos e aplicações.