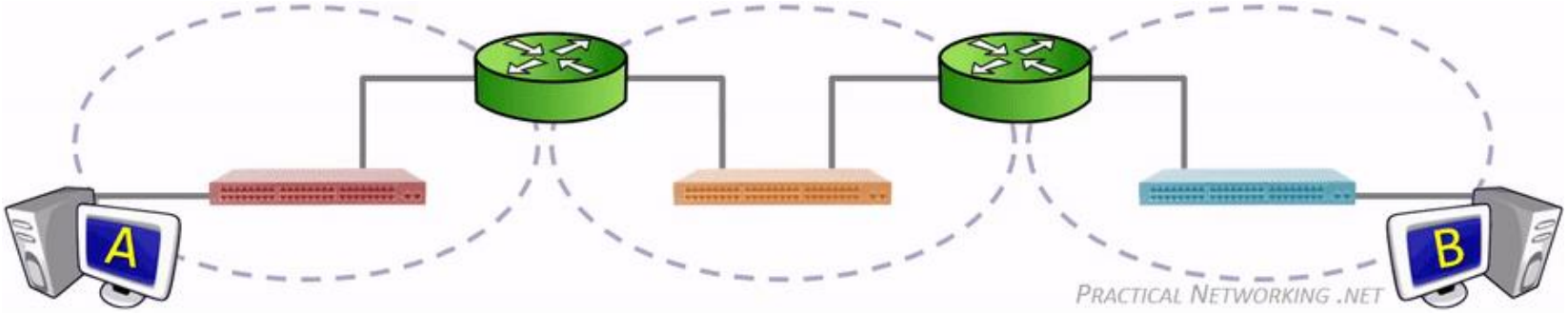
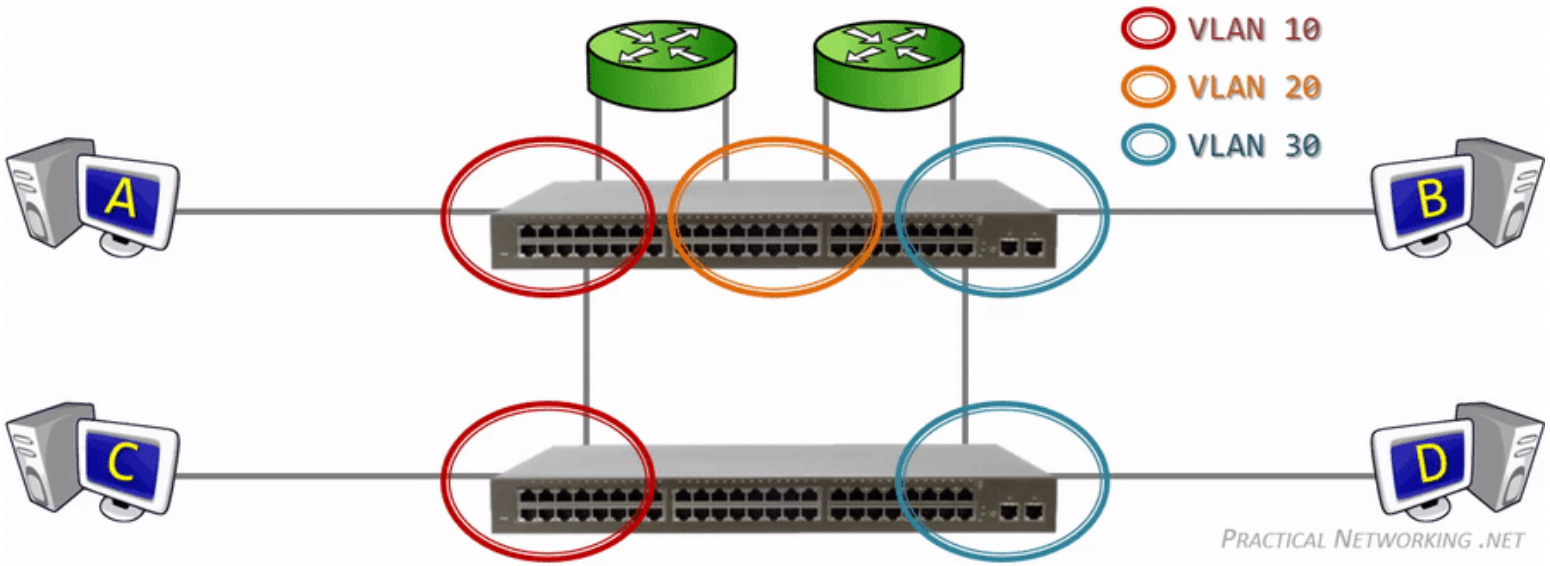
VLAN


A
B
PRACTICAL NETWORKING .NET


VLAN 10
VLAN 20
VLAN 30
A
B
C
D
PRACTICAL NETWORKING .NET

VLAN

LAN virtual (VLAN) é uma partição lógica de uma rede física (camada OSI 2). Podem ser criadas várias partições (vlan's) numa única rede física.

Cada VLAN é um domínio de Broadcast IP.

As VLAN's estão isoladas entre si, comunicando apenas através de um router, como se fossem redes diferentes.

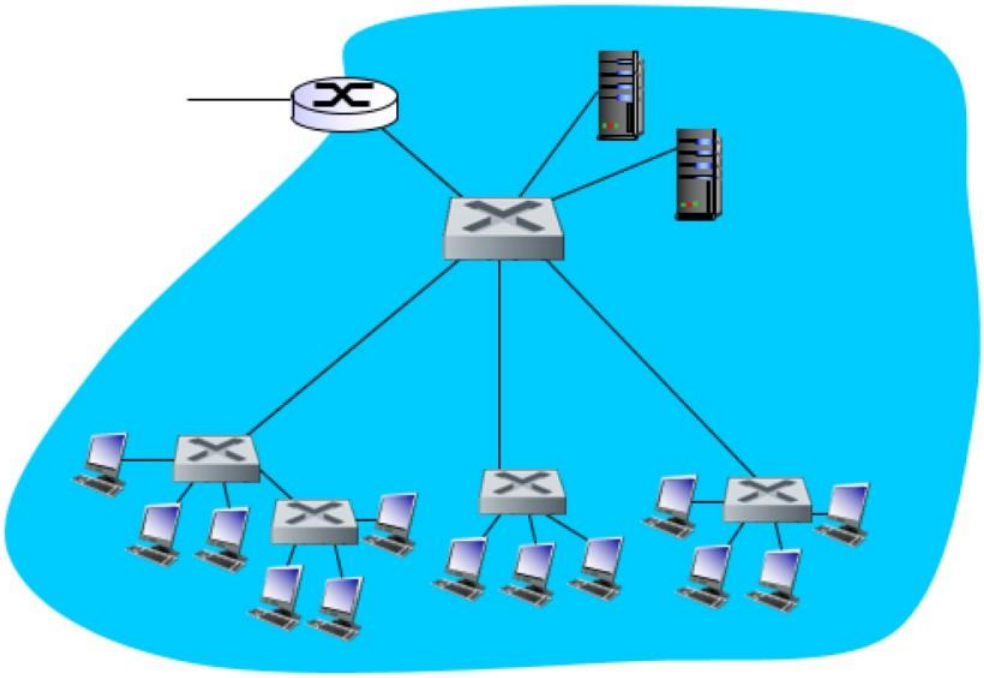
As VLAN's são criadas num dispositivo de nível 2, normalmente num switch.

Os postos da VLAN não têm conhecimento da existência da VLAN.

Benefícios das VLAN

- **Segurança** – dados sensíveis são separados do resto da rede, aumentando a confidencialidade.
- **Redução de custos** – melhor gestão da largura de banda da rede e equipamentos menos potentes.
- **Melhor desempenho** – menos utilizadores têm menos colisões.
- **Encolhe os domínios de broadcast** – minimiza o numero de dispositivos no domínio de broadcast.
- **Aumenta a eficiência da equipa de IT** – redes com requisitos semelhantes partilham a mesma VLAN.
- **Projecto mais simples e melhor gestão das aplicações** - VLANs agrega utilizadores e dispositivos de rede.

Motivação para VLANs



Computação

Engenharia Electrotécnica

Engenharia de Computadores

considerando:

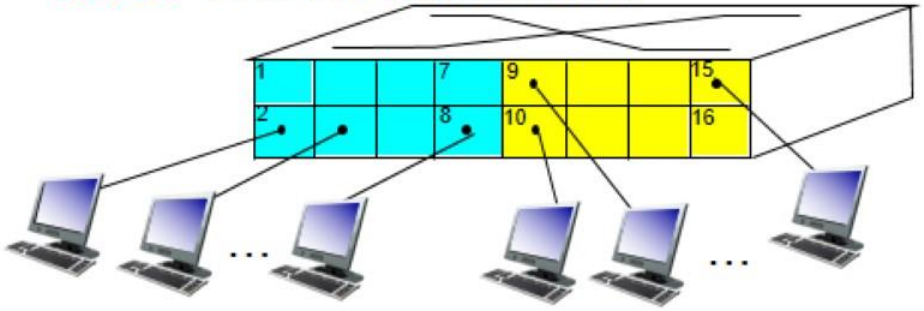
- Os alunos de Computação vão mudar para as instalações de EE, mas querem manter-se ligados ao mesmo switch
- Único domínio de broadcast:
  - Todo o tráfego broadcast de nível 2 (ARP, DHCP, endereço MAC desconhecido) têm de atravessar toda a rede
  - Problemas de segurança/privacidade e eficiência

VLANs

Virtual Local Area Network

switch(es) que suportam VLAN podem ser configurados para definir multiplas LANS ***virtuais*** sobre a única infraestrutura física.

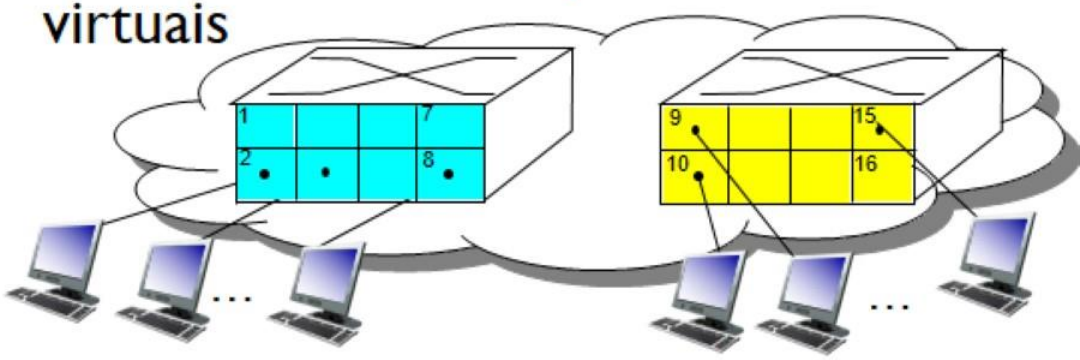
port-based VLAN: as portas do switch são agrupadas (por software de gestão do switch) tal que um *único* switch físico……



Engenharia Electrotécnica (VLAN ports 1-8)

Computação (VLAN ports 9-15)

… funciona como *multiplos* switches virtuais

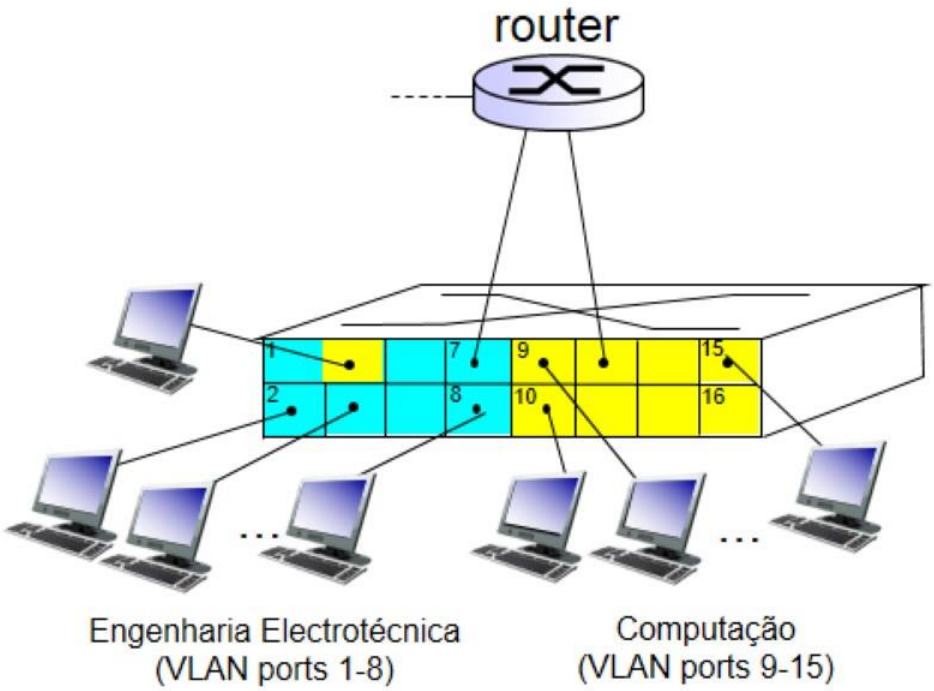


Engenharia Electrotécnica (VLAN ports 1-8)

Computação (VLAN ports 9-16)

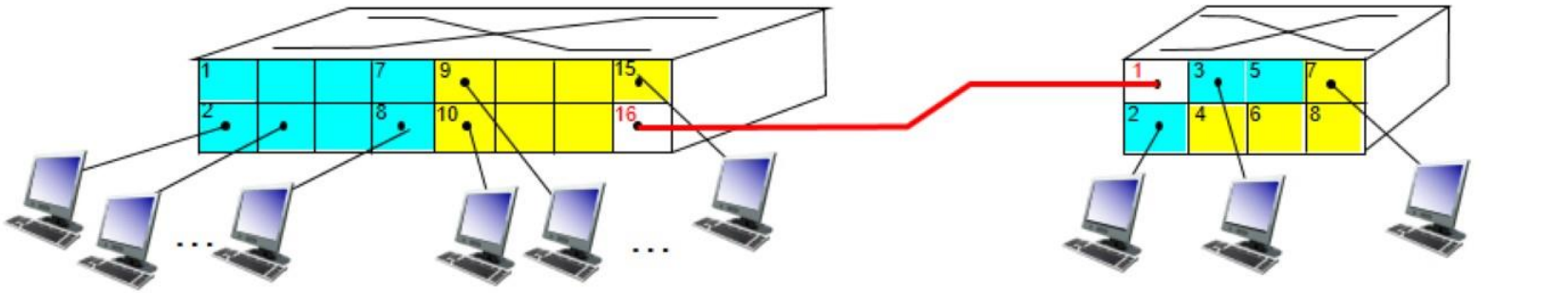
Vantagens VLAN

- *isolamento do tráfego:* frames de/para os ports 1-8 apenas podem chegar aos ports 1-8
  - Tambem se podem definer VLAN baseados em endereços MAC dos terminais, em vez das portas do switch
- *Agrupamento dinâmico:* ports podem ser dinamicamente assignados às VLANs



- *Encaminhamento entre VLANS:* feito via routing (como se fossem switches separados)
  - na prática, vendedores combinam switches e routers

VLANS abrangendo multiplos switches



Engenharia Electrotécnica
(VLAN ports 1-8)

Computação
(VLAN ports 9-15)

Ports 2,3,5 pertencem à EE VLAN EE
Ports 4,6,7,8 pertencem à VLAN Comp

- *trunk port:* transportam frames entre VLANS definidas nos multiplos switches físicos
  - frames enviadas numa VLAN entre switches não podem ser frames do tipo 802.1 (têm de transporter informação ID VLAN)
  - 802.1q protocol adiciona/remove campos de cabeçalho adicional das frames enviadas entre ports trunk

VLAN Trunk

Um trunk VLAN transporta mais de uma VLAN

Estabelece-se um VLAN trunk entre switches para que dispositivos na mesma VLAN possam comunicar entre si mesmo que estejam fisicamente ligados a switches diferentes.

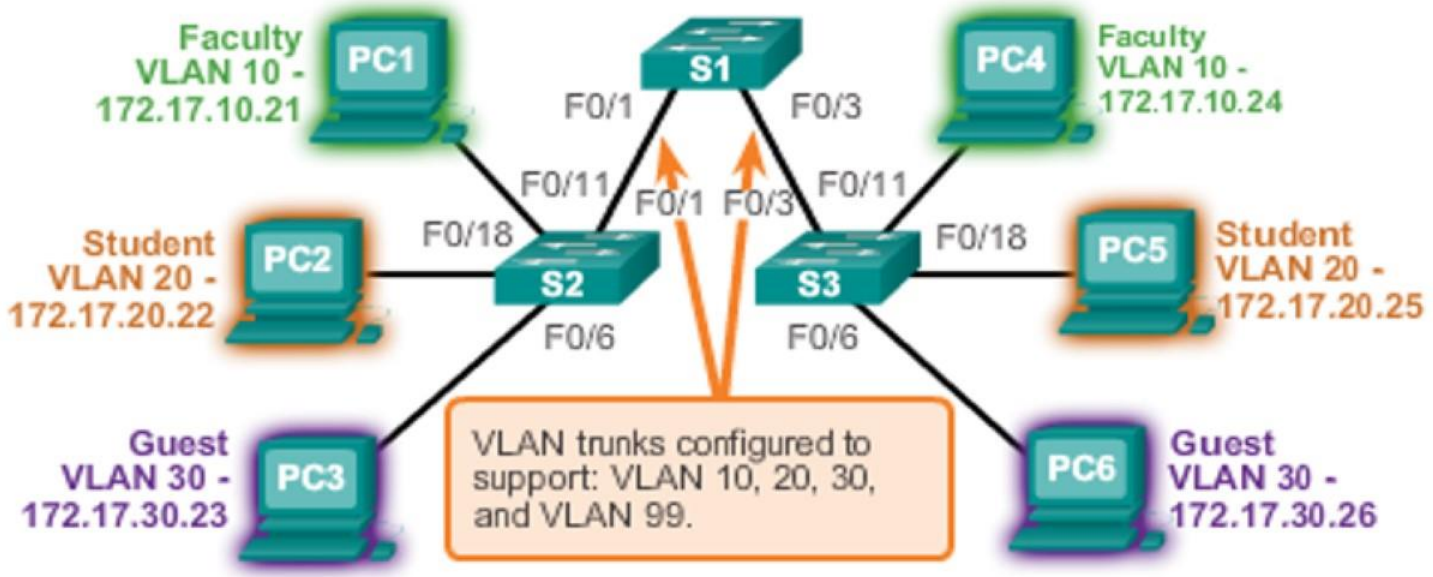
Nem o VLAN trunk nem as portas usadas para estabelecer a ligação trunk estão associados a nenhuma VLAN.

O Cisco IOS suporta o protocolo de trunk de uso geral IEEE802.1q.

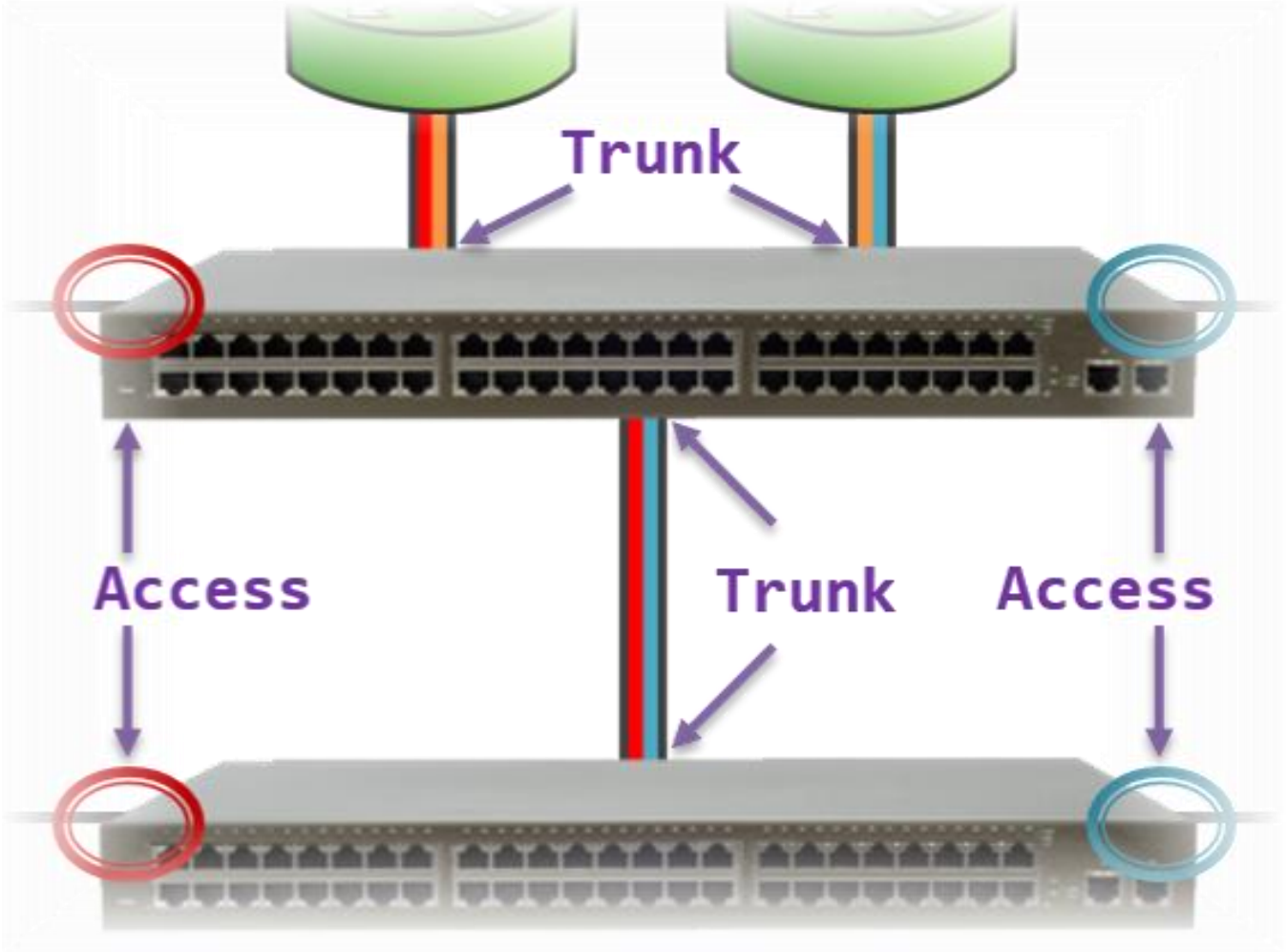
VLAN Trunks

VLAN 10 Faculty/Staff - 172.17.10.0/24
VLAN 20 Students - 172.17.20.0/24
VLAN 30 Guest - 172.17.30.0/24
VLAN 99 Management and Native - 172.17.99.0/24

F0/1-5 are 802.1Q trunk interfaces with native VLAN 99.
F0/11-17 are in VLAN 10.
F0/18-24 are in VLAN 20.
F0/6-10 are in VLAN 30.

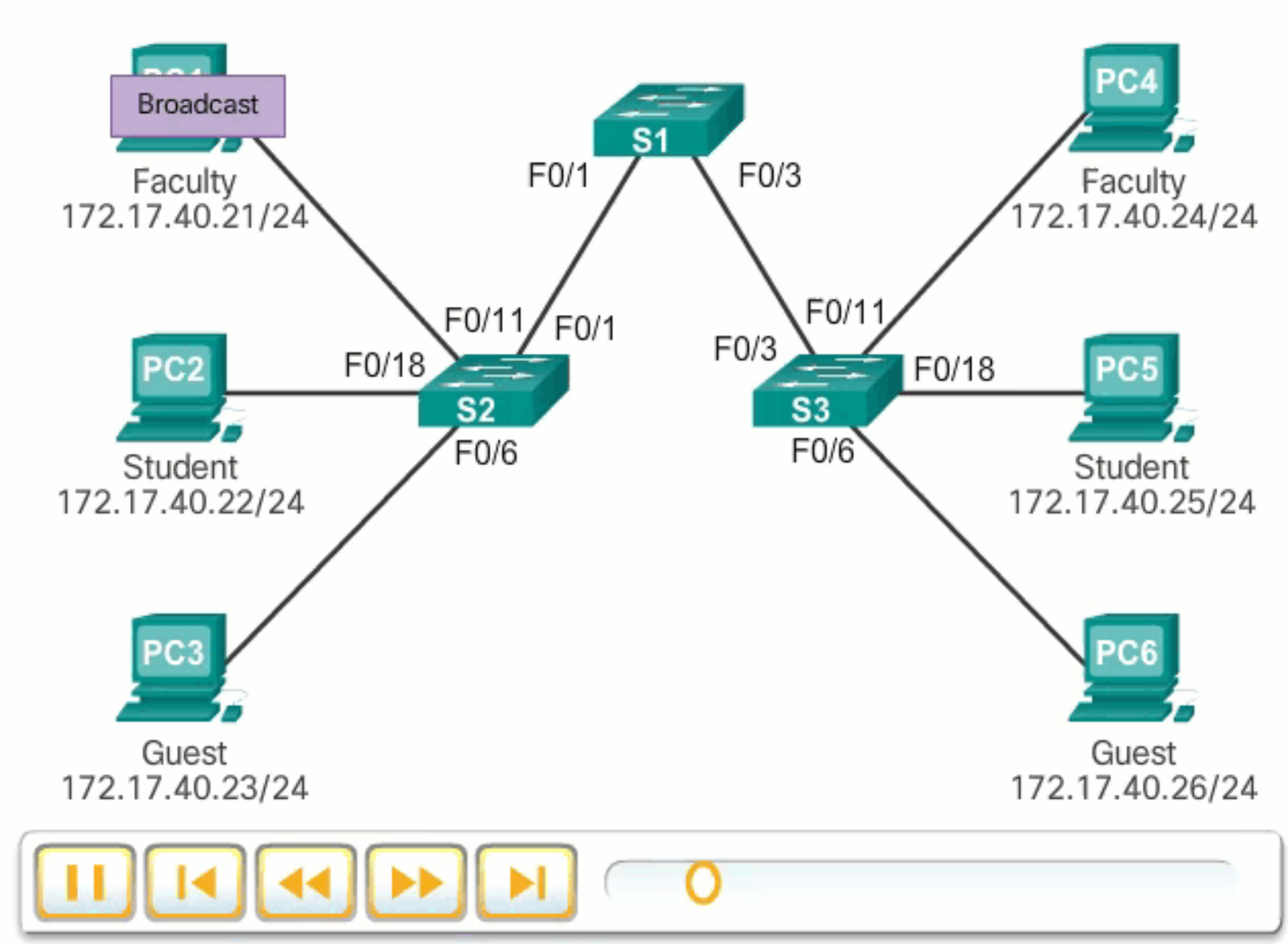


VLAN Trunks



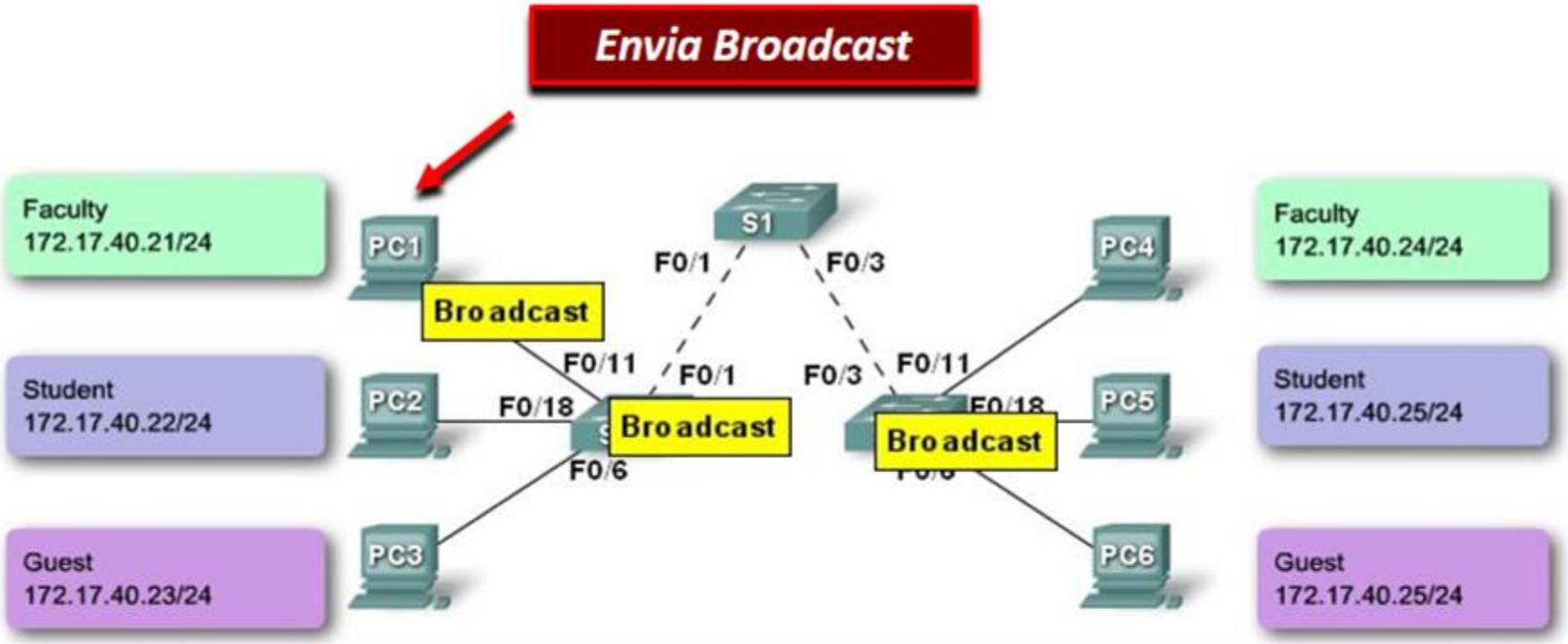
Rede sem VLAN

inundação em cada switch



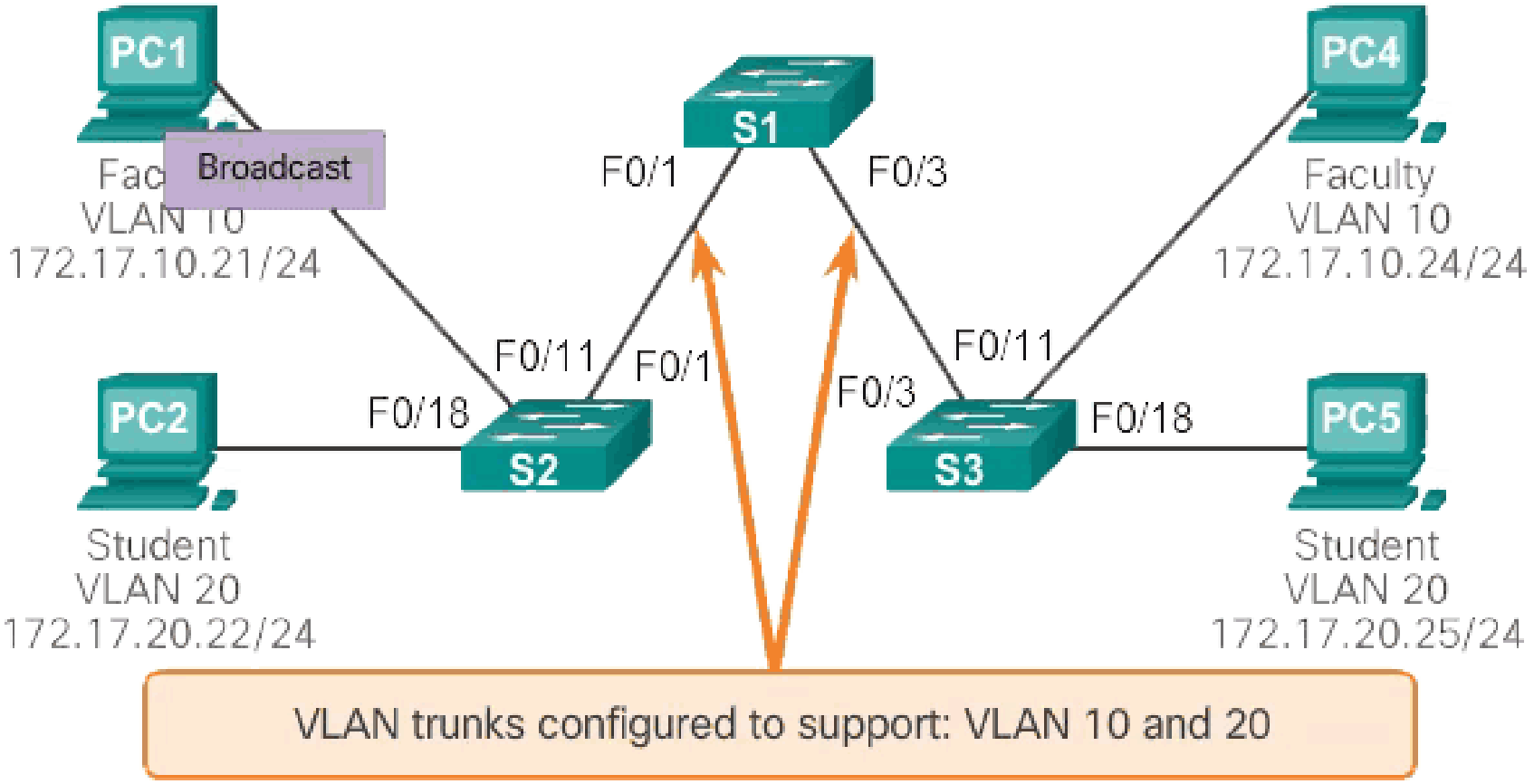
Controlo de Domínio de Broadcast

- Rede sem VLANs:



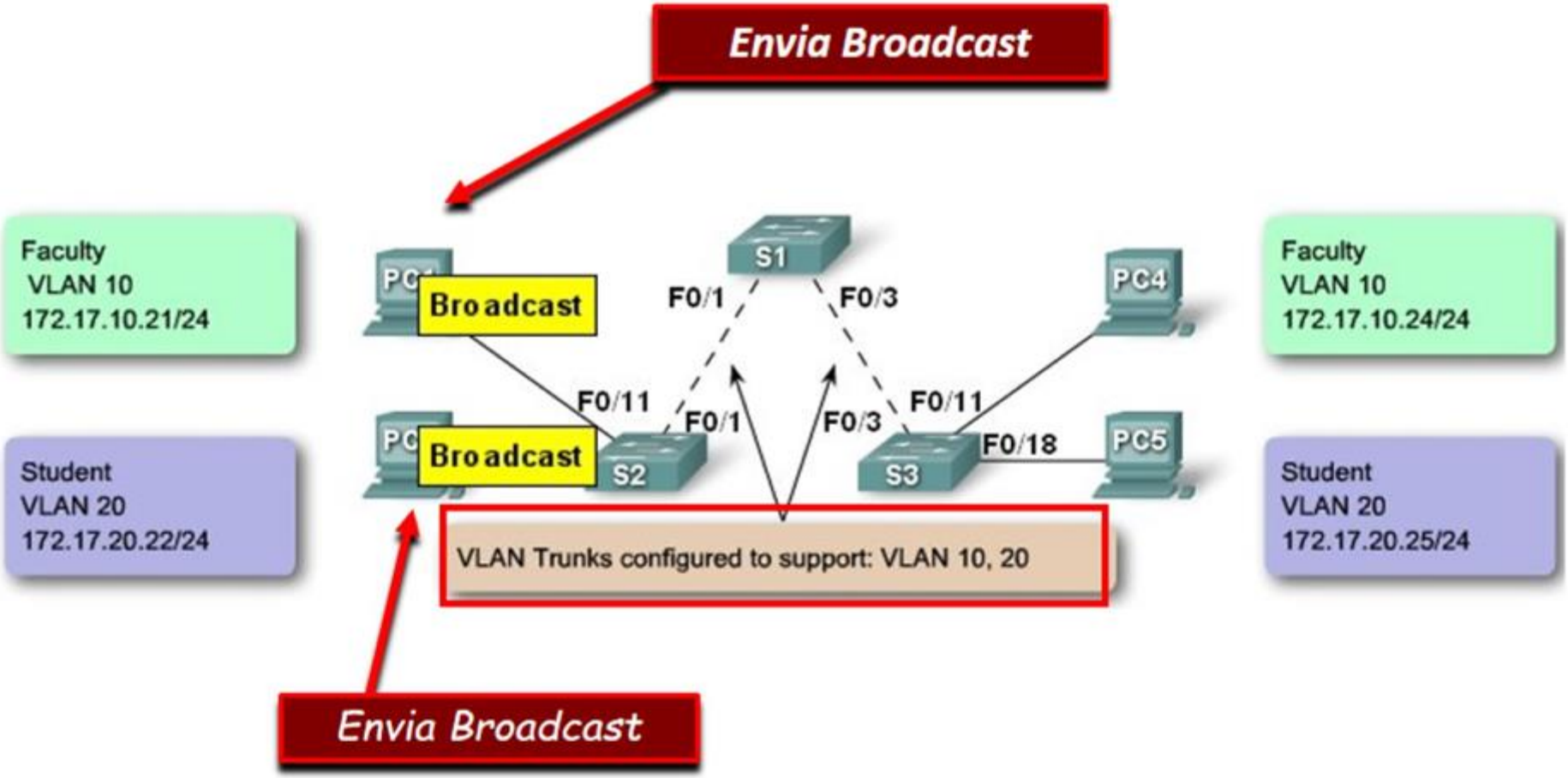
Rede com VLAN

Isolamento de broadcast



Controlo de Domínio de Broadcast

- Rede com VLANs:



Marcação das frames VLAN

A marcação das frames (tagging) é o processo de adicionar a identificação da VLAN no cabeçalho da frame.

A marcação é usada para transmitir frames de múltiplas VLANs numa ligação de trunk.

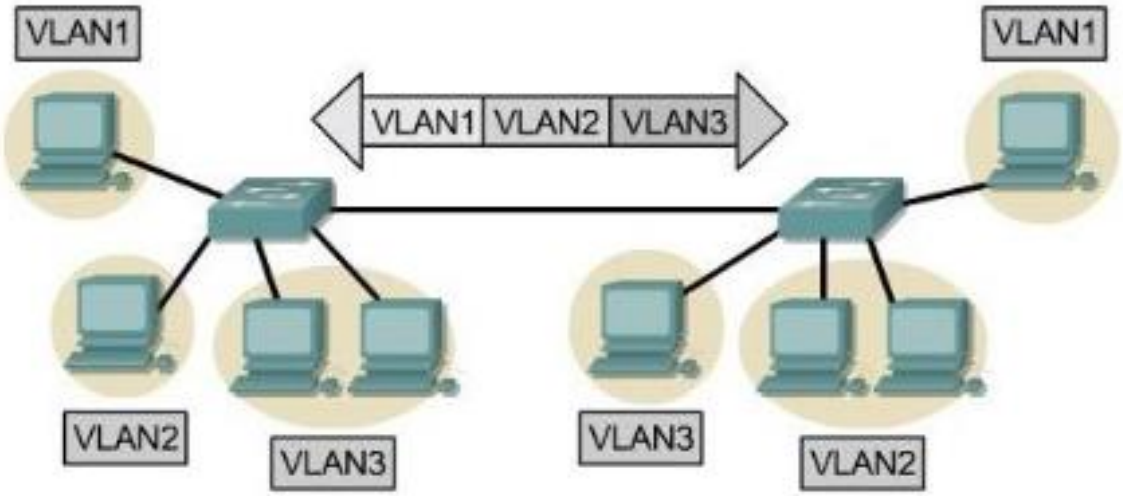
Os switches marcam as frames para identificar a VLAN a que pertencem. Existem diferentes protocolos de tagging, sendo o IEEE 802.1q o mais popular.

O protocolo define a estrutura da marca (tag) adicionada no cabeçalho da frame.

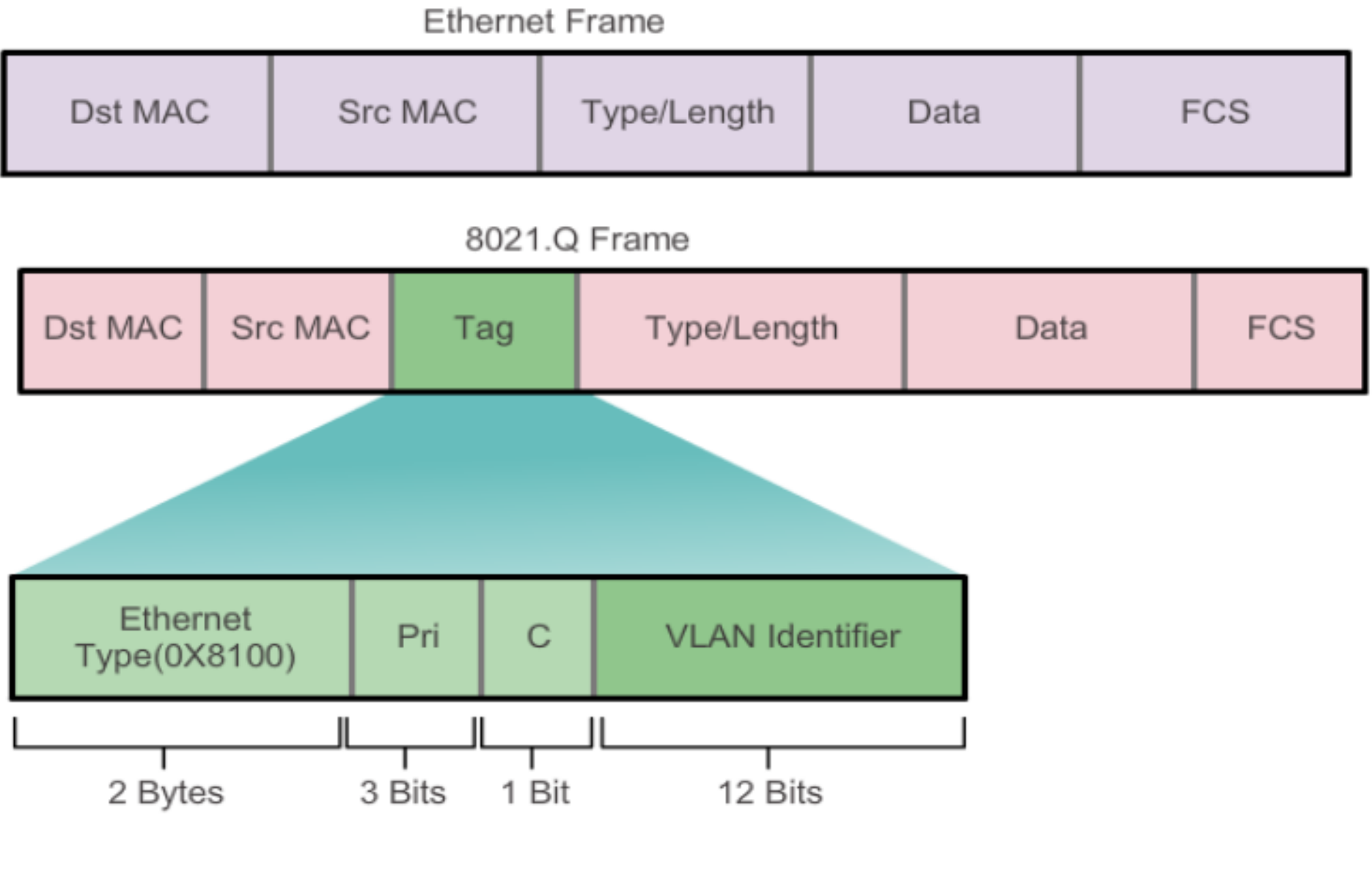
Marcação das frames VLAN

Os switches adicionam a marca da VLAN às frames antes de as colocar nas ligações de trunke e retiram as marcas antes das enviarem para as portas nontrunk.

Quando marcadas adequadamente, as frames podem atravessar qualquer número de switches via ligações de trunk e continuarem a ser encaminhadas dentro da mesma VLAN.



Marcação das frames VLAN



VLAN nativa e tagging 802.1q

As frames que pertencem à VLAN nativa não são marcadas.

Se as frames recebidas não estiverem marcadas (untagged), mantêm-se untagged e são encaminhadas na VLAN nativa.

Se não existirem portas associadas à VLAN nativa e não existirem outras ligações de trunk, as frames untagged são descartadas.

Nos switches Cisco, a VLAN nativa por omissão é a VLAN 1

VLAN de voz

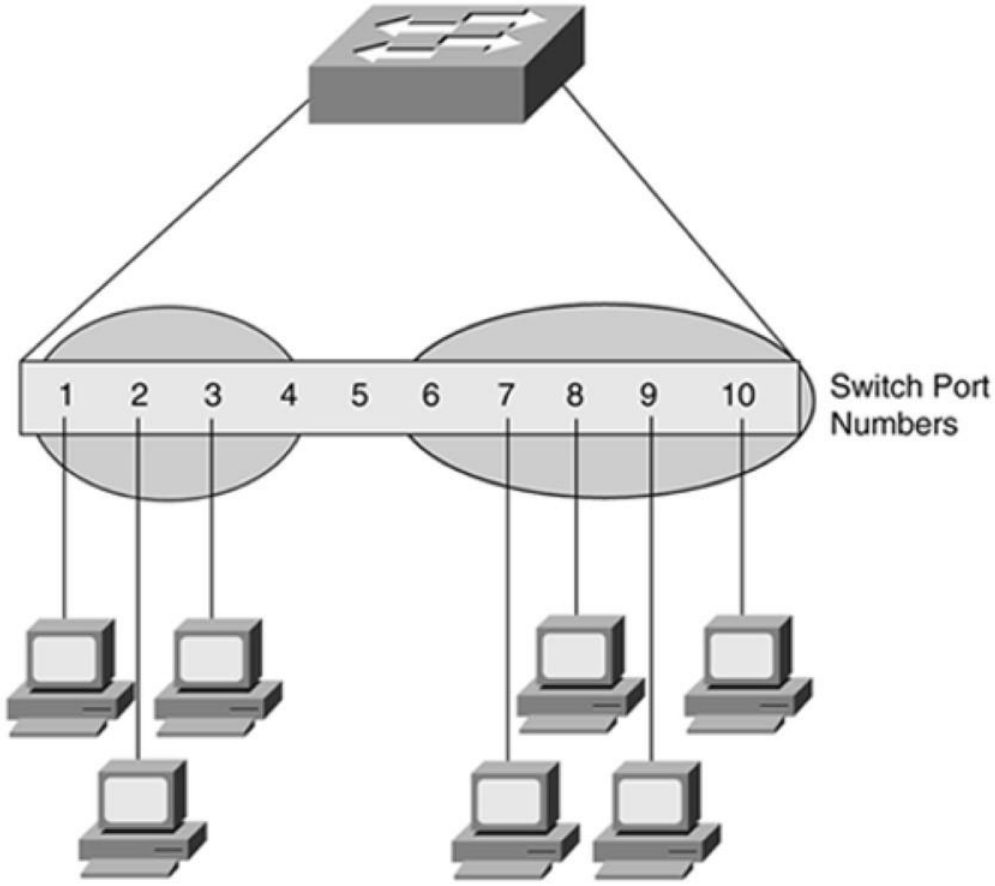
- O tráfego VoIP é time-sensitive e tem os seguintes requisitos:
  - Largura de banda garantida para assegurar qualidade de voz.
  - Prioridade na transmissão em relação a outro tipo de tráfego de rede.
  - Capacidade para se encaminhado por fora de áreas congestionadas da rede.
  - Atraso inferior a 150 ms na rede.

- A VLAN de voz permite que as portas de acesso transportem tráfego de voz sobre IP a partir de um telefone IP.

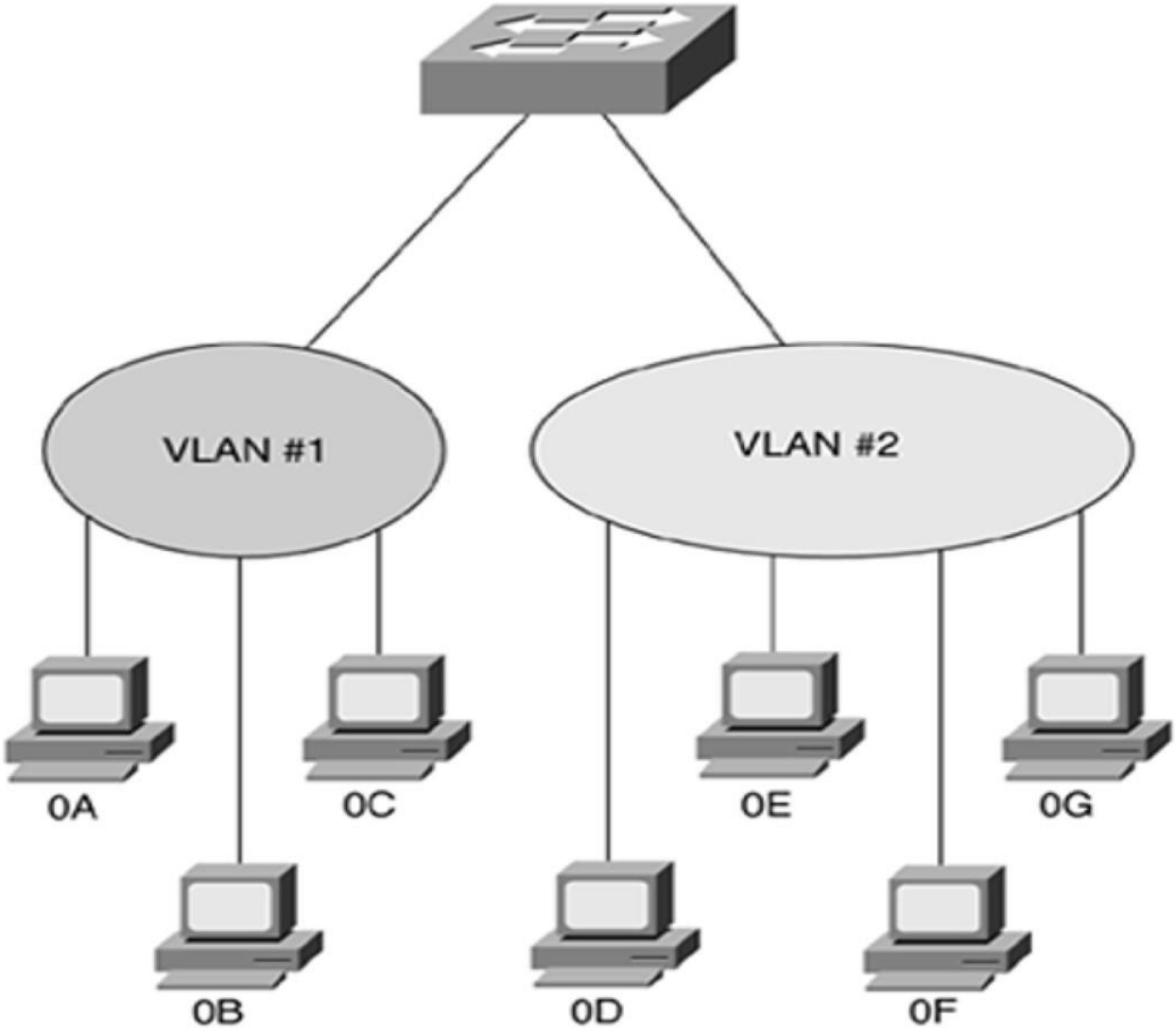
- O switch suporta qualidade de serviço (QoS)

- A qualidade do som de uma chamada de voz sobre IP pode deteriorar-se se os pacotes não forem enviados regularmente.

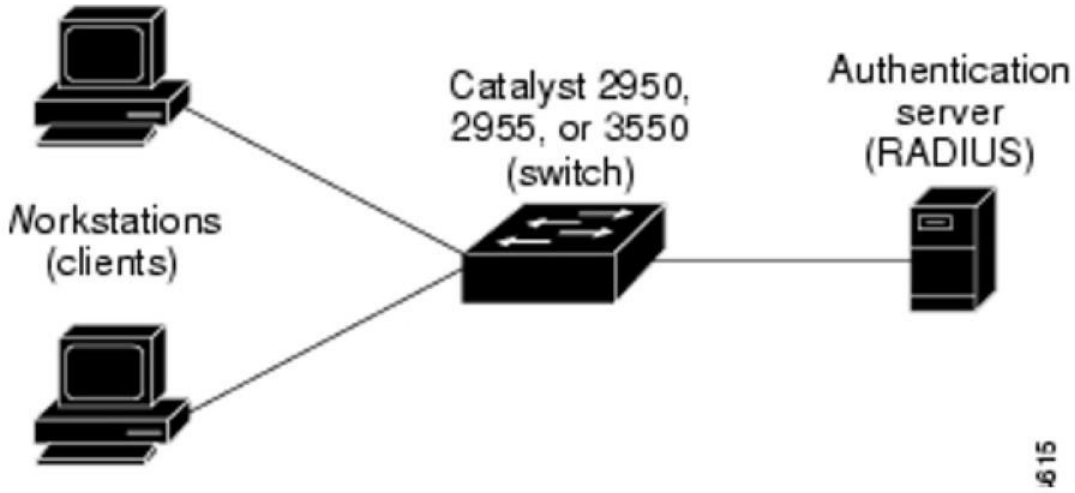
Port-Based VLAN



MAC Address-Based VLAN



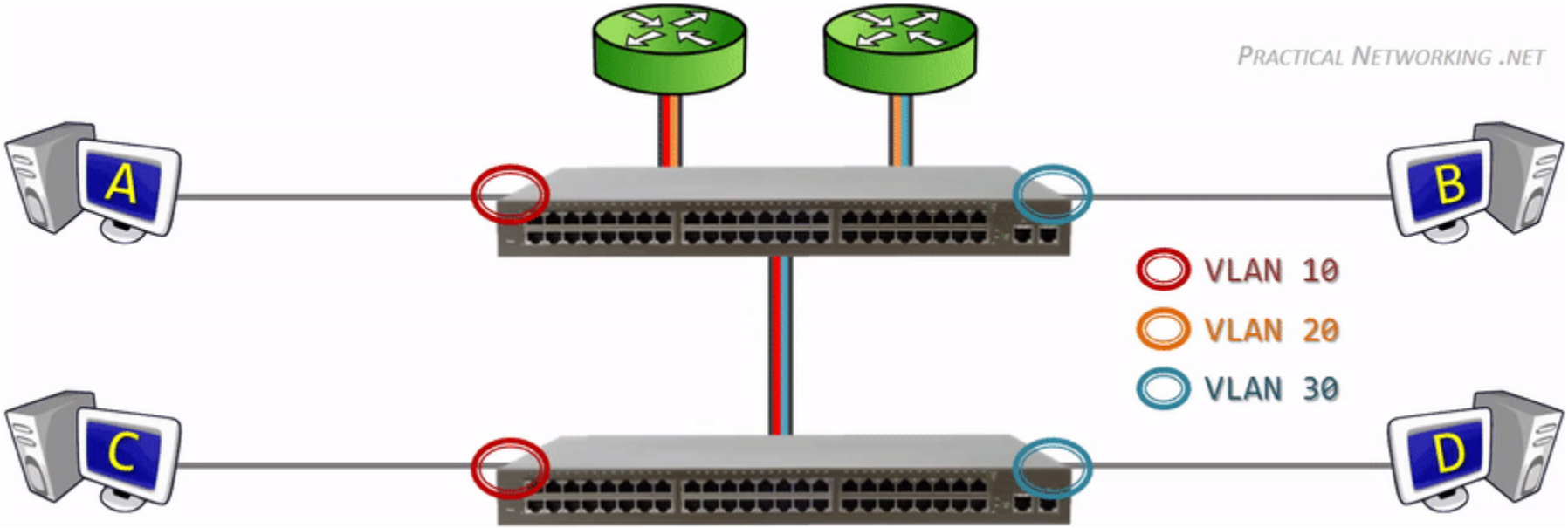
Dynamic VLAN Assignment



A autenticação e atribuição de VLAN é feita por um servidor RADIUS (norma IEEE 802.1x 2001)

Tráfego inter VLAN

Passagem obrigatória por router



Configuração por omissão nos switches

```
Switch# show vlan brief

VLAN Name                Status    Ports
---- ------------------- --------- -------------------------
1    default             active    Fa0/1,  Fa0/2,  Fa0/3,  Fa0/4
                                   Fa0/5,  Fa0/6,  Fa0/7,  Fa0/8
                                   Fa0/9,  Fa0/10, Fa0/11, Fa0/12
                                   Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                   Fa0/17, Fa0/18, Fa0/19, Fa0/20
                                   Fa0/21, Fa0/22, Fa0/23, Fa0/24
                                   Gi0/1,  Gi0/2
1002 fddi-default        act/unsup
1003 token-ring-default  act/unsup
1004 fddinet-default     act/unsup
1005 trnet-default       act/unsup
```

- *Por omissão, todas as portas de um Switch estão na VLAN 1.*
- *A VLAN 1 não pode ser apagada ou renomeada.*

Portas e vlan's no Switch

Um switch poderá ter até 4094 VLAN's configuradas, tantas quanto as necessárias para o funcionamento da rede.

Cada VLAN tem uma numeração, de 1 a 4094

A VLAN 1 (VLAN nativa) não pode ser apagada.

Portas de acesso – portas que ligam aos equipamentos terminais –tem assignada a VLAN atribuída ao posto

Portas trunk – portas que ligam a outros equipamentos de rede – transportam várias VLAN's

VLANs Nativas e *Tagging* 802.1q

- As *frames* que pertencem à VLAN nativa não são marcadas.
- Se as *frames* recebidas não estiverem marcadas (*untagged*), mantêm-se *untagged* e são encaminhadas na VLAN nativa.
- Se não existirem portas associadas à VLAN nativa e não existirem outras ligações de trunk, as *frames untagged* são descartadas.
- Nos switches Cisco, a VLAN nativa por omissão é a VLAN 1.

Redes de Datacenter

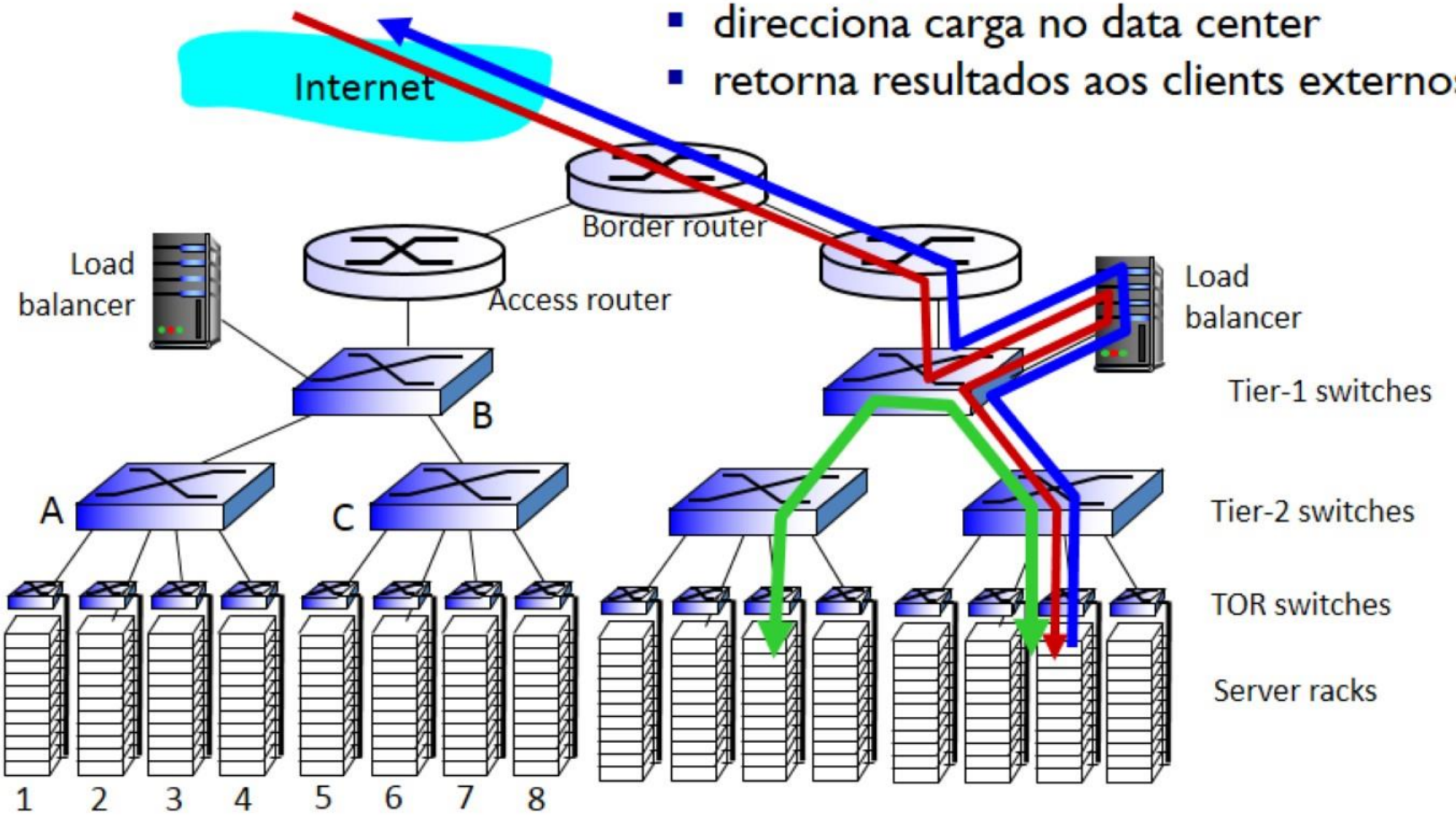
- Centenas a milhares de servidores, em fiadas de racks contínuos:
  - e-business (e.g. Amazon)
  - Servidores de conteúdos (e.g., YouTube, Akamai, Apple, Microsoft)
  - Motores de busca, data mining
  - (e.g., Google)
- desafio:
  - multiplas aplicações, cada uma servindo um número massivo de clientes
  - Gestão/balanceamento de carga, evitando estrangulamentos de processamento, de rede e de dados

Inside a 40-ft Microsoft container, Chicago data center

Redes de Datacenter

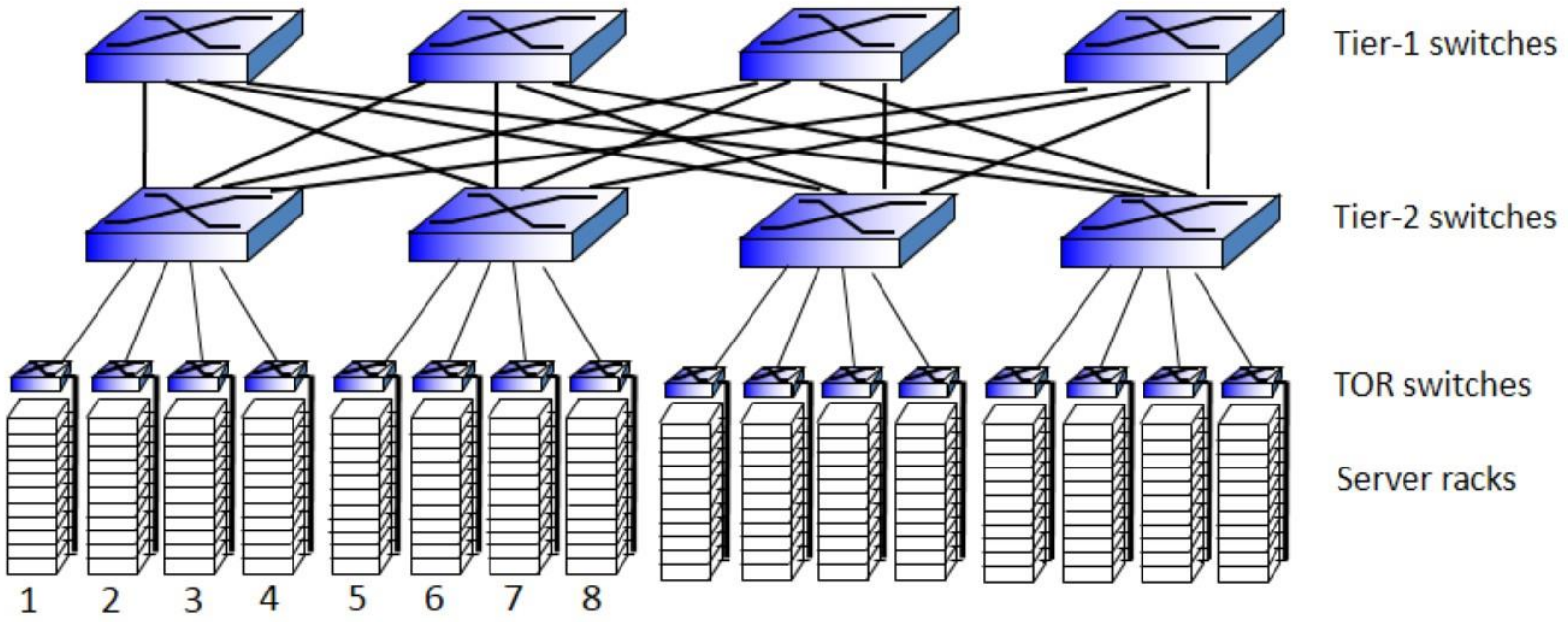
Balanceamento de carga: routing nível de aplicação

- Recebe pedidos dos clients externos
- direcciona carga no data center
- retorna resultados aos clients externos



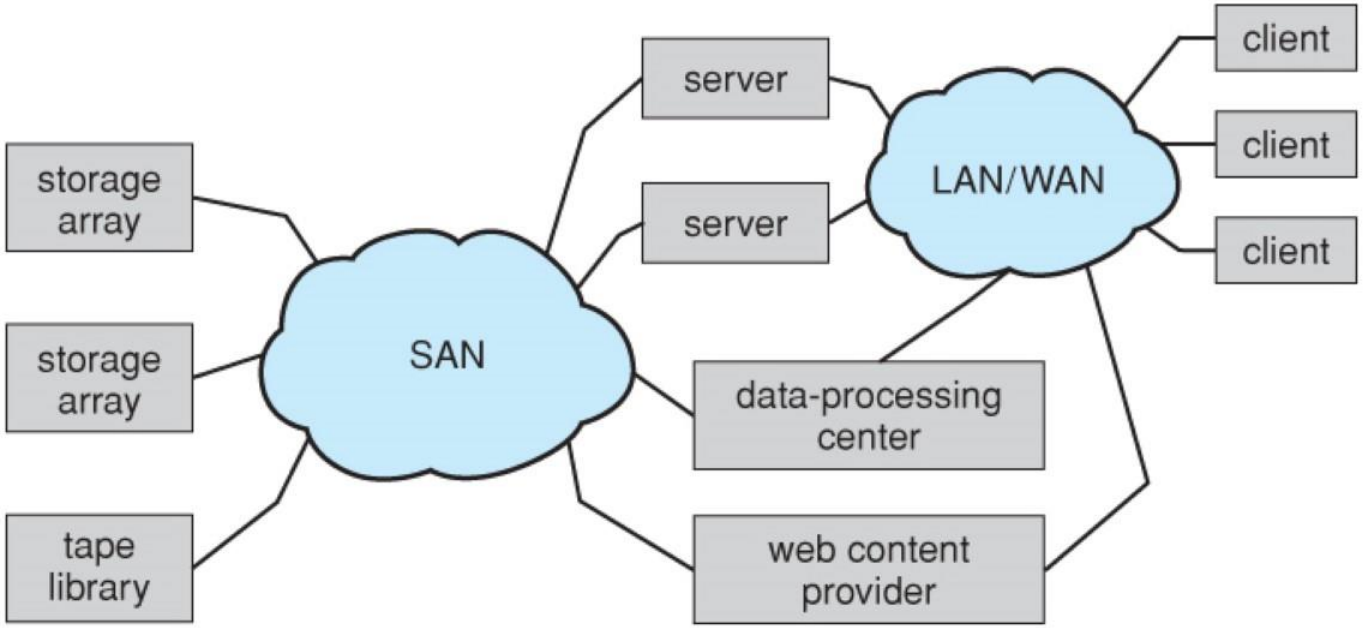
Rede de Datacenter

- Interligação rica entre switches e racks:
  - Aumenta desempenho entre racks (multiplos caminhos de routing)
  - Aumenta confiabilidade via redundância



Rede de Data center - SAN

- Interligação entre servidores e armazenamento de dados:
  - Switches de fibra entre servidores e discos
  - Aumenta redundância e segurança do armazenamento de dados
  - Aumenta confiabilidade via redundância



Rede de Data center - SAN

O armazenamento partilhado simplifica a gestão dos dispositivos de armazenamento. Atribuição dinâmica de "storage"

SANs aumenta a disponibilidade da informação em caso de acidentes (disaster recovery) . A SAN pode replica a informação noutras localidades através de armazenamento secundário (storage replication).