# Administração de Redes



## Introdução às VLAN

Este documento pretende dar uma breve introdução às *Virtual LAN* (VLAN), um conceito fundamental nas redes locais da actualidade.

### Conceito

Por razões de ordem diversa (organização da rede, desempenho, privacidade, segurança, etc.) é frequentemente necessário dividir a rede de uma organização em diversas "ilhas" sem ligação directa entre si (domínios de difusão). Tradicionalmente, essa divisão correspondia a uma separação física — numa rede *ethernet* comutada, cada domínio de difusão corresponde a um ou mais comutadores ligados entre si, funcionando como uma LAN independente. Dado não existir nenhuma ligação directa entre as LAN assim formadas (caso contrário a separação perder-se-ía), se houver necessidade de comunicação entre essas diferentes LAN, elas têm que ser interligadas através de um *router*.

Apesar de funcionar, este tipo de divisão da rede pode ser muito ineficiente ou inconveniente. É comum a divisão lógica que se quer fazer da rede não se mapear bem na divisão dos espaços físicos. Por exemplo, uma empresa instalada num edifício de vários pisos que tenha um departamento de desenvolvimento, outro de marketing e outro de serviços administrativos, e que queira separar as redes desses departamentos pode precisar de ter em cada piso o triplo dos comutadores de que necessitaria se as redes não estivessem isoladas. Pior, se num piso faltasse uma porta para ligar o computador do funcionário de um dado departamento seria necessário instalar mais um comutador, mesmo que sobrassem portas livres nos comutadores dos outros departamentos. A aquisição, renovação, manutenção e administração de todo o equipamento adicional tem, naturalmente, custos, pelo que se tornou necessário encontrar uma outra alternativa.

Para resolver estas questões, a maioria dos comutadores actuais (excepto os de muito pequena dimensão destinados a uso em *SOHO*) permite fazer a divisão de uma mesma rede física em diferentes domínios de difusão, designados VLAN (LAN virtuais). Do ponto de vista lógico, diferentes VLAN funcionam como se fossem redes independentes, com cablagem e equipamentos separados. Tal como no caso em que a separação era física, continua a não haver ligação directa entre máquinas pertencentes a diferentes VLAN, pelo que a comunicação entre elas tem que ser feita através de um *router*[1].

[1] Alguns comutadores são capazes de detectar os endereços IP em uso nas suas VLAN e encaminhar pacotes entre elas, prescindindo assim de um *router* (salvo para comunicação com o exterior).

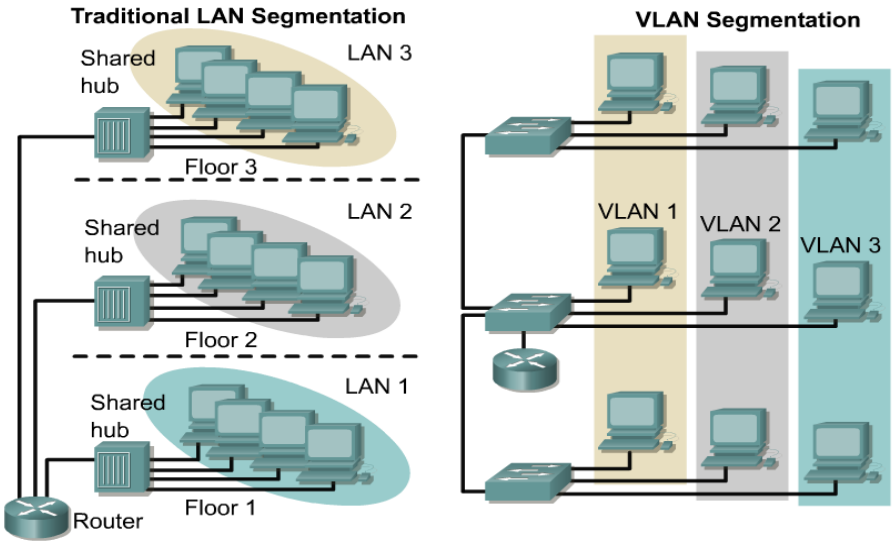


Figura 1 — Segmentação da rede com base na localização física (tradicional) ou em critérios lógicos (VLAN)

O mecanismo mais básico das VLAN consiste na atribuição de cada uma das portas do comutador a uma dada VLAN, de modo a que haja comunicação directa apenas entre portas pertencentes à mesma VLAN. Tramas recebidas pelo comutador numa porta pertencente a uma VLAN, mesmo que sejam de *broadcast*, nunca são retransmitidas para portas pertencentes a VLAN diferentes (ou seja, cada VLAN é um domínio de difusão independente). A atribuição de uma porta (física) do comutador a uma dada VLAN pode ser feita através de configuração (VLAN estáticas), ou então de forma automática (VLAN dinâmicas). No segundo caso, a atribuição de uma porta a uma VLAN pode fazer-se com base em critérios como o endereço MAC da máquina ligada nessa porta (critério de camada 2), do seu endereço IP (critério de camada 3), ou ainda por autenticação através do protocolo 802.1x.

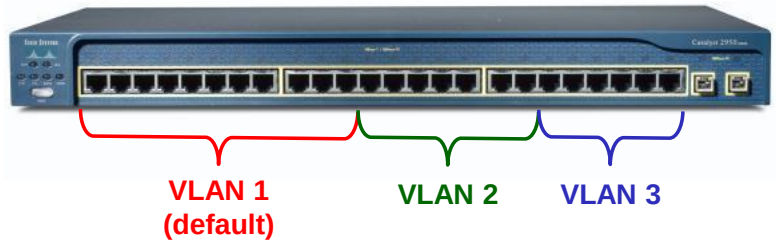


Figura 2 — Atribuição de portas físicas a diferentes VLAN

## VLAN *trunking*

Havendo uma ou mais VLAN que se estendem por vários comutadores surge outra questão: com cada porta atribuída a uma e uma só VLAN, para manter o seu funcionamento inalterado (podem trocar-se tramas entre quaisquer portas de uma mesma VLAN mas não entre portas de VLAN diferentes) seria necessário ter várias ligações físicas (i.e., vários cabos de rede) a interligar cada par de comutadores, um por VLAN. Quer o consumo excessivo de portas a que conduz, quer a necessidade de instalar cablagem adicional, tornariam esta solução indesejável, pelo que foi desenvolvida uma alternativa.

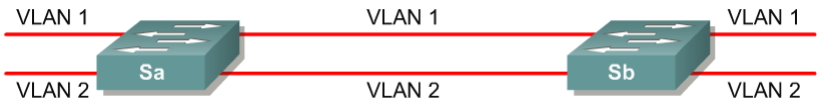


Figura 3 — Interligação entre comutadores apenas com uma VLAN por porta

De modo a poder fazer com apenas um cabo a interligação entre comutadores com VLAN, estes permitem configurar cada porta num de dois modos: acesso ou *trunk*. Enquanto uma porta de acesso está atribuída a uma única VLAN, nas portas de *trunking* circulam tramas de diferentes VLAN.

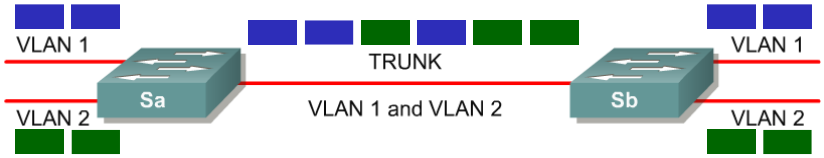


Figura 4 — Interligação entre comutadores com portas em modo *trunk*

Para que um comutador, quando recebe uma trama numa porta em modo *trunk*, possa saber a que VLAN pertence, as tramas enviadas em ligações em modo *trunk* precisam de transportar no cabeçalho uma etiqueta (VLAN *tag*) indicando a VLAN a que pertence. Infelizmente, não existe nenhum campo no cabeçalho das tramas *ethernet* normais onde a VLAN *tag* possa ser transportada, pelo que é necessário utilizar nas portas em modo *trunk* um encapsulamento diferente. O encapsulamento *standard* para tramas enviadas por portas em modo *trunk* está definido na norma 802.1Q. Existem encapsulamentos alternativos, como o Cisco Inter-Switch Link (ISL), mas por ser proprietários não são adequados para redes com equipamento de múltiplas marcas.

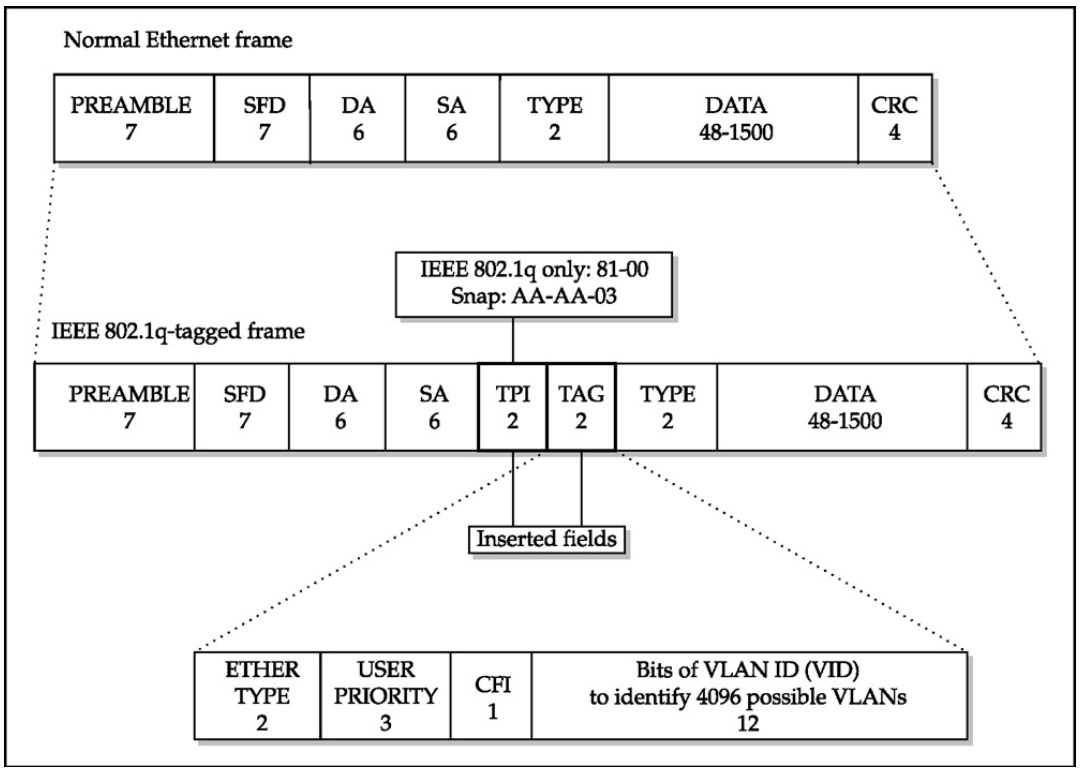


Figura 5 — Encapsulamento 802.11Q vs. *ethernet* normal

Uma porta em modo *trunk* pode ter configurada uma VLAN nativa. Nesse caso, uma trama com encapsulamento *ethernet* normal recebida nessa porta assume-se pertencente à VLAN nativa. Nos comutadores Cisco IOS, todas as portas *trunk* têm uma VLAN nativa (embora possa ser filtrada removendo-a das VLAN permitidas), mas outros fabricantes permitem configurar portas de *trunk* para descartar as tramas recebidas sem etiqueta VLAN.

## Encaminhamento entre diferentes VLAN

A nível de ligação lógica, as diferentes VLAN comportam-se como redes independentes, não havendo possibilidade de comunicação entre elas nessa camada. A existir necessidade de comunicação entre máquinas em diferentes VLAN, ela terá que efectuar-se na camada de rede, ou seja, através de um *router*. Este pode ligar-se ao(s) comutador(es) através de múltiplas portas físicas ou através de uma única porta em modo *trunk*. Alguns *routers* modulares permitem a instalação de módulos de comutação, constituindo um 2-em-1 de *router* e comutador.

## Configuração básica de VLAN

### Cisco IOS

#### *Criação de VLANs*

Criação da VLAN 5 para a rede do departamento de marketing (modo config):

```
vtp mode transparent
vlan 5
 name Marketing
```

NOTAS

1. A primeira linha indica que a configuração de VLANs é local (o protocolo VTP permite a configuração centralizada de VLANs).
2. A atribuição de nome à VLAN é opcional; sem ela, o próprio sistema atribuiria automaticamente o nome VLAN0005.
3. É possível criar uma série de VLANs duma só vez. Por exemplo, o comando `vlan 5,7-9,12` cria duma só vez as VLANs 5, 7, 8, 9 e 12. Não é possível, contudo, atribuir nomes personalizados às VLANs criadas desta forma.
4. A VLAN 1 (default) já vem pré-configurada, e é usada por todas as portas em que não seja explicitamente configurada uma VLAN diferente.
5. Pode verificar as VLAN existentes usando o comando `show vlan-switch brief`

#### *Configuração das portas (físicas)*

Configuração de f1/0 como porta de acesso na VLAN 5:

```
interface FastEthernet 1/0
 switchport mode access
 switchport access vlan 5
```

Configuração de f1/0 como porta de *trunking* com encapsulamento 802.1Q:

```
interface FastEthernet 1/0
 switchport trunk encapsulation dot1q
 switchport mode trunk
```

### *Configuração do endereço IP do comutador em cada uma das VLAN*

A configuração do endereço IP do *router* numa VLAN faz-se da mesma forma que a configuração do endereço IP de uma qualquer interface:

```
interface vlan 5
 ip address 192.168.1.1 255.255.255.0
 no shutdown
```

## Linux

O *kernel* Linux também permite configurar interfaces de rede com VLAN em modo *trunk* (encapsulamento 802.1Q). Exemplo de procedimento para configuração da porta `eth0` em modo *trunk*:

1. Adicionar a(s) VLAN desejada(s) — VLAN 5, neste caso. Por cada VLAN é criada uma nova interface lógica cujo nome é o da interface "mãe" seguido de um ponto e do número da VLAN, e.g., `eth0.5`

   ```
   # vconfig add eth0 5
   ```

   ou

   ```
   # ip link add link eth0 eth0.5 type vlan id 5
   ```

2. Configurar as diferentes interfaces lógicas

   ```
   # ifconfig eth0.5 192.168.1.2 netmask 255.255.255.0 up
   ```

3. O endereço IP da VLAN nativa configura-se na própria interface "mãe"

   ```
   # ifconfig eth0 192.168.2.2 up
   ```

   Se não quiser usar a VLAN nativa pode remover o endereço IP que eventualmente lhe esteja atribuído

   ```
   # ifconfig eth0 0.0.0.0 up
   ```

Pode verificar a configuração de VLAN no ficheiro `/proc/net/vlan/config`. Pode também criar ficheiros para configuração permanente em `/etc/sysconfig/network-scripts/`, devendo acrescentar às interfaces VLAN a linha "`VLAN=yes`".