

# Sistemas de Conectividade

## Aula 14 - Redes Virtuais - Vlans - Parte 2

# Apresentação

---

Olá, pessoal!

Na última aula entendemos que um switch é um equipamento de camada 2 (OSI) o qual possui uma inteligência para analisar o endereço físico de destino de um quadro e encaminhar esse quadro somente para a porta correta. Além disso, vimos uma introdução ao conceito de rede virtual, chamada de VLAN (*Virtual Local Area Network*).

Nesta aula conheceremos detalhadamente a tecnologia de VLAN. Iniciaremos falando das motivações para se dividir toda uma rede corporativa em redes virtuais menores, obedecendo aos limites administrativos da organização. Em seguida, estudaremos o protocolo IEEE 802.1q e observaremos quais são as modificações que ele realiza no cabeçalho de um quadro Ethernet. Analisaremos em detalhes o processo de rotular os quadros com um número que identifica a VLAN daquele quadro. Por fim, veremos como são feitas as configurações dos switches gerenciáveis para que eles implementem diversas VLANs na rede.

Boa aula!

## Objetivos

- Saber quais são as motivações para a criação de uma LAN virtual;
- Conhecer o protocolo IEEE 802.1q e seu esquema de rotulação dos quadros;
- Aprender a configurar VLAN por porta em um switch.

# Motivação para Criação de VLAN

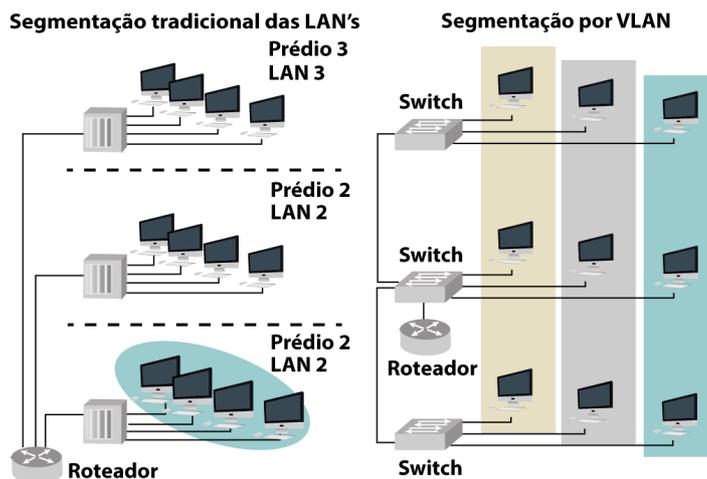
---

Antigamente, quando as primeiras redes corporativas foram criadas, o uso dos hubs era predominante, pois os switches eram muito caros. Em cada prédio da empresa, ou mesmo em cada pavimento de um prédio, colocava-se um hub (ou mesmo um switch não gerenciável) para prover conectividade e criar uma LAN com os computadores daquele prédio ou pavimento. Todas as LAN's eram interligadas através de um roteador central.

Dessa forma, existia uma LAN para cada prédio e todos os computadores daquela LAN faziam parte do mesmo domínio de broadcast e colisões (no caso de hubs). Isso começou a se tornar um problema quando as redes começaram a crescer significativamente e, principalmente, quando os computadores envolvidos em cada LAN faziam parte de diferentes departamentos ou tipos de usuários, envolvendo problemas de segurança nas comunicações.

O ideal era que a divisão da rede (segmentação das LAN's) pudesse seguir determinados critérios lógicos ou administrativos. Muitas vezes, um determinado departamento grande que possui muitos funcionários ocupa muitos prédios, e essa separação física não deveria atrapalhar a divisão lógica da rede por departamento, independentemente do prédio e/ou switch que o interliga. Pensando assim, os projetistas da IEEE elaboraram o protocolo **802.1q** que padroniza o conceito de Rede Local Virtual (VLAN - *Virtual Local Area Network*). A **Figura 1** mostra essa evolução na segmentação de toda a LAN de uma empresa com vários prédios usando VLAN.

**Figura 01** - Comparação da segmentação da LAN sem e com VLAN.



**Fonte:** Elaborada pelo Autor.

Veja na **Figura 1** que com o uso do protocolo de VLAN é possível termos uma determinada LAN departamental, por exemplo, percorrendo vários switches independentemente da sua localização física e conectividade. Isso facilita imensamente a aplicação de políticas de uso dos recursos de rede, bem como a definição de faixas de endereços IP por departamento ou tipo de usuários e a melhoria da segurança no tráfego da rede entre computadores de um mesmo grupo de usuários.

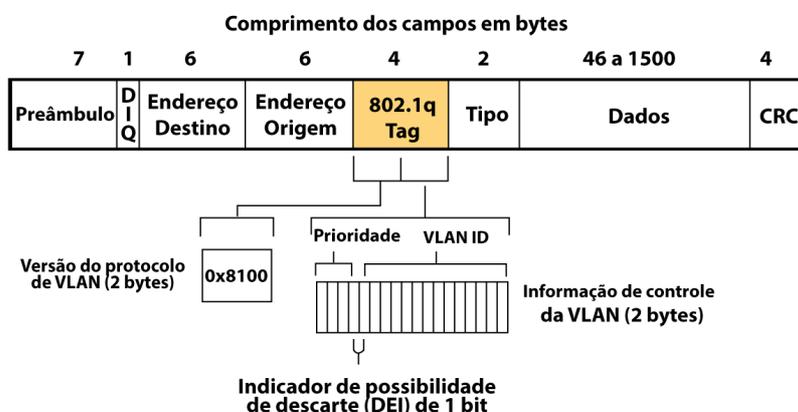
Nas seções seguintes veremos como o protocolo de VLAN funciona e como podemos configurar os switches para implementarmos esse importante recurso.

## O Protocolo 802.1q

O protocolo 802.1q que implementa o conceito de VLAN usa como princípio básico da segmentação da rede a utilização de uma espécie de rótulo, chamado de VLAN ID, em cada quadro Ethernet gerado na respectiva LAN virtual. Ou seja, se um quadro Ethernet foi gerado por um computador da VLAN 1, por exemplo, esse quadro possui um campo em seu cabeçalho com essa identificação da VLAN, permitindo que os switches repassem o quadro apenas para as portas que fazem parte da VLAN 1.

Como o quadro Ethernet original não possuía nenhum campo em seu cabeçalho que pudesse ser usado a fim de identificar a VLAN, os projetistas tiveram de alterar o cabeçalho do quadro Ethernet acrescentando um novo campo chamado de **802.1Q Tag** de 4 bytes. Em razão disso, *switches* que não entendem o protocolo 802.1q podem não reconhecer o quadro Ethernet com esse campo e simplesmente descartá-lo. Assim, sempre que você for implementar a VLAN em uma rede corporativa, é importante verificar se todos os switches suportam o protocolo 802.1q. A **Figura 2** apresenta o formato do quadro Ethernet modificado contendo o campo que identifica a VLAN à qual o quadro pertence.

**Figura 02** - Formato do quadro Ethernet com o campo 802.1q Tag.



**Fonte:** Elaborado pelo Autor.

Podemos observar na **Figura 2** que o campo de *tag* (rótulo ou etiqueta em inglês) possui 4 bytes, assim divididos: 2 bytes para indicar a versão do protocolo de VLAN, os quais atualmente tem como valor em hexadecimal 0x8100; e 2 bytes (16 bits) com a informação de controle da VLAN contendo outros 3 subcampos – Prioridade, DEI e VLAN ID, assim definidos:

- **Prioridade** (3 bits): refere-se ao protocolo 802.1p de Classe de Serviço e indica o nível de prioridade do quadro. Os 8 (23) possíveis valores para esse subcampo são usados para priorizar diferentes classes de tráfego (voz, vídeo, dados, etc.) por parte do *switch* no encaminhamento dos quadros.

- **DEI - Drop Eligible Indicator** (1 bit): esse subcampo pode ser utilizado separadamente ou em conjunto com o campo de prioridade para indicar que o quadro é elegível a ser descartado na presença de congestionamento da rede.
- **VLAN Identifier** (12 bits): um subcampo que especifica a VLAN à qual o quadro pertence. Os valores (hexadecimais) 0x000 e 0xFFF são reservados. Todos os outros valores podem ser usados como identificadores de VLAN, permitindo até 4.094 VLANs distintas. O valor 0x000 indica que o quadro não identifica um ID e, nesse caso, a etiqueta 802.1Q especifica apenas uma prioridade, sendo referida, dessa forma, como uma etiqueta de prioridade. Nos *switches*, o VLAN ID 0x001 é frequentemente reservado para a VLAN de gerenciamento dos ativos da rede e previamente configurada com todas as portas do switch sendo, por isso, chamada de VLAN padrão (Default). O valor de VLAN ID 0xFFF é reservado e não deve ser configurado.

Destes quatro campos (versão do protocolo, prioridade, DEI e VLAN ID), o mais importante na prática é o de VLAN ID que identifica a VLAN. Como veremos na seção seguinte, é o valor desse campo que o switch observará a fim de determinar para quais portas o quadro deverá ser encaminhado.

## Atividade 01

---

1. O campo VLAN ID do campo 802.1q Tag possui 12 bits e seu valor é usado para determinar a qual VLAN o quadro pertence. Assim, qual o máximo de VLANs que podem ser criadas na rede?
2. Pesquise um modelo de *switch* do mercado e verifique qual a sua capacidade máxima de criação de VLANs. Compare com a capacidade máxima suportada pelo protocolo 802.1q.

Para ver as respostas, clique [aqui](#).

## Respostas

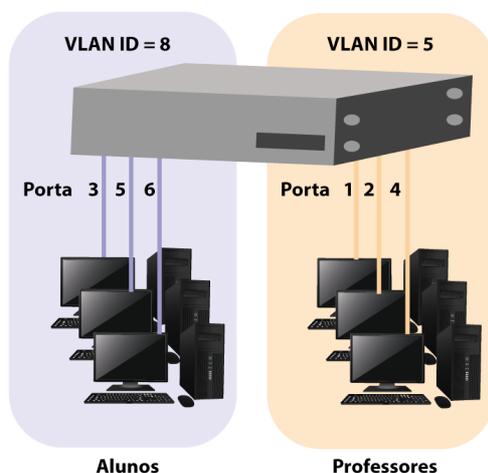
1. Com 12 bits podemos fazer  $2^{12}$  combinações de números, o que dá 4.096 números. Assim, é possível criar até 4.094 VLANs em uma rede, já que o primeiro e o último número são reservados e não podem ser utilizados para isso.

## Configuração de VLAN por Porta no Switch

Como já vimos, os *switches* gerenciáveis que suportam o protocolo 802.1q são os equipamentos da rede que criarão os quadros Ethernet com rótulos (*tag*) tencionando identificar a qual VLAN cada quadro pertence. Nesta seção veremos alguns termos e definições importantes para entendermos como configurar o switch a fim de segmentar a rede através da conectividade provida por cada porta.

A configuração mais simples de VLAN que podemos fazer em um switch seria dizer a ele a qual VLAN cada porta pertence. Para isso, bastaria criar as VLANs desejadas e depois associar cada porta a uma das VLANs criadas. Vejamos, por exemplo, o *switch* hipotético de 6 portas da **Figura 3**. Foram criadas duas VLANs, uma para os computadores dos professores (VLAN ID = 5) e uma para os computadores dos alunos (VLAN ID = 8).

**Figura 03** - Formato do quadro Ethernet com o campo 802.1q Tag.



**Fonte:** Elaborado pelo Autor.

Sabendo que os computadores dos alunos estão ligados nas portas 3, 5 e 6 do switch, estas foram associadas à VLAN 8. No caso da VLAN 5, ela agrupa as portas 1, 2 e 4, que são as portas ligadas aos computadores dos professores. Com essa configuração, os computadores dos alunos estão isolados dos professores e vice-versa.

E se o computador de um aluno precisasse se comunicar com o de um professor ou vice-versa, isso seria possível? Se o *switch* da **Figura 3** é um tradicional, dito de camada 2 apenas, não seria possível essa comunicação entre computadores de VLANs diferentes, visto que eles fazem parte de redes distintas, com endereços de rede IP diferentes para cada VLAN. Entretanto, se esse switch fosse de camada 3 (rede), ele seria capaz de entender o protocolo IP e rotear os pacotes entre essas redes, atuando também como um roteador.

Podemos citar, ainda, um problema apresentado no início desta aula, sendo a motivação para se padronizar um protocolo de VLAN: o de uma rede ser composta por mais de um switch em diferentes prédios. Trazendo para o nosso cenário de exemplo é como se tanto a rede dos alunos como a dos professores fossem grandes e compostas por diversos switches em diversas edificações. Como cada switch deverá ser configurado para que uma VLAN seja composta por diversas portas de diversos switches? A resposta a essa pergunta será apresentada na próxima seção.

## VLAN *Tagging*

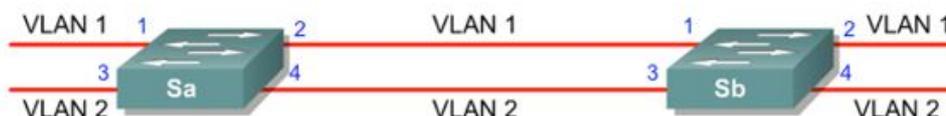
---

Você viu que o conceito de VLAN consiste na divisão da rede por portas do switch Ethernet, através de um número (VLAN ID) que identifica a qual rede a porta pertence. Assim, para que diversas VLANs percorram diversos switches, todos os switches no caminho devem conhecer todos os IDs de numeração das VLANs da rede e saber quais são as portas associadas a cada VLAN para poder encaminhar os quadros. Entretanto, somente isso não é suficiente e veremos a seguir o porquê.

A **Figura 4** mostra uma configuração de dois switches (Sa e Sb) de segmentação em VLANs apenas pela separação das portas do *switch* por cada VLAN. Os números em azul representam o número da porta em cada switch. Assim, a VLAN 1 no switch

Sa é composta pelas portas 1 e 2, e a VLAN 2 pelas portas 3 e 4. Por coincidência, as mesmas portas estão atribuídas às mesmas VLANs no switch Sb. Mas poderiam ser outras portas, visto que a numeração delas é irrelevante

**Figura 04** - Configuração de VLANs entre switches usando apenas a separação por porta.



**Fonte:** Elaborado pelo Autor.

O problema dessa configuração dos *switches*, vista na **Figura 4**, é que cada *switch* separa uma porta de interligação com outro switch para passar os quadros que fazem parte de cada VLAN. Além de ser um desperdício grande de portas, ainda tem outro problema: e se tivermos um número de VLANs maior que o número de portas do switch?

Para resolver esses problemas, foi criado o conceito de **VLAN tagging**, que é a essência de funcionamento do protocolo 802.1q, o qual consiste na rotulação (*tagging*) do quadro Ethernet com o valor do campo VLAN ID de seu cabeçalho identificando a VLAN, independentemente da porta por onde esse quadro chegou no *switch*. Assim, algumas portas do *switch* poderão ser capazes de pertencer a mais de uma VLAN e separar os quadros que chegam observando apenas o seu VLAN ID (rótulo). Da mesma forma, quando o switch for encaminhar um quadro por uma porta que pertence a mais de uma VLAN, ele deverá rotular esse quadro com o VLAN ID correspondente. A **Figura 5** mostra esse tipo de configuração de VLAN entre dois *switches*, a qual é a mais utilizada atualmente nas redes corporativas.

**Figura 05** - Configuração de VLANs entre switches usando portas *Trunk*.



**Fonte:** Elaborado pelo Autor.

Quando uma porta do switch pertence a mais de uma VLAN e é usada para passar o tráfego das VLANs para um outro switch, dizemos que essa porta é do tipo **Trunk** ou **Tagged**. No exemplo da **Figura 5**, as portas 12 de Sa e 24 de Sb são portas *Trunk* e por elas passarão o tráfego das VLANs 1 e 2 entre esses dois switches. Dessa

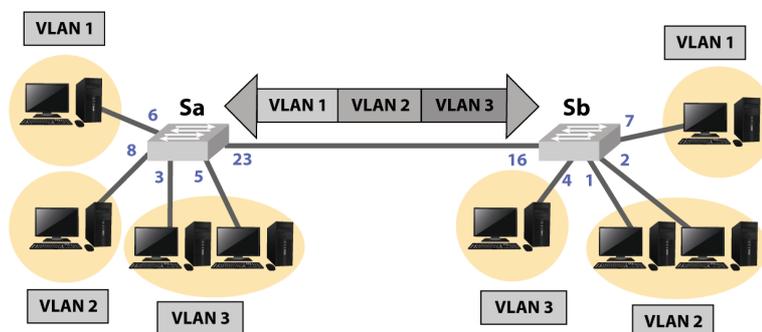
forma, todo quadro Ethernet que chega ou sai por esse tipo de porta deve possuir o campo 802.1q Tag em seu cabeçalho, permitindo identificar, pelo subcampo VLAN ID, a qual VLAN o quadro pertence.

Com esse esquema, se uma porta for configurada como *Trunk*, ela não deve ser conectada a um equipamento que não entenda o protocolo 802.1q, pois ele receberá os quadros Ethernet modificados através do campo de *Tag*. Assim, quando uma porta do switch é ligada a um equipamento de usuário final, ela é classificada como porta do tipo **Access** ou **Untagged**, e os quadros Ethernet que forem transmitidos por ela não terão em seus cabeçalhos o campo de rótulo de VLAN (802.1q Tag).

## Atividade 02

1. A **Figura 6** mostra uma topologia de rede com dois switches Sa e Sb interligando computadores que pertencem a três VLANs: 1, 2 e 3. Os números em azul representam os números das portas em cada switch.

**Figura 06** - Switches interligando computadores de três VLANs.



**Fonte:** Elaborado pelo Autor.

Considerando estas configurações nos dois switches, diga, para cada switch, quais são as portas de cada VLAN e se ela é do tipo Acesso ou *Trunk*.

Para ver as respostas, clique [aqui](#).

## Respostas

1. A seguinte tabela mostra a configuração de cada porta em cada switch.

<b>VLAN</b>	<b>Switch Sa</b>		<b>Switch Sb</b>	
	<b>Porta(s)</b>	<b>Tipo</b>	<b>Porta(s)</b>	<b>Tipo</b>
1	6	Acesso	7	Acesso
2	8	Acesso	1 e 2	Acesso
3	3 e 5	Acesso	4	Acesso
1,2 e 3	23	Trunk	16	Trunk

# Leitura Complementar

---

- IEEE Std. 802.1Q-2005, Virtual Bridged Local Area Networks.  
<http://standards.ieee.org/getieee802/download/802.1Q-2005.pdf>  
Documentação da IEEE de especificação do padrão 802.1q, versão mais recente de 2005.
- O que é 802.1Q e Quando Usar.  
<https://under-linux.org/entry.php?b=1538>  
Descrição resumida do que é o 802.1q feita por um profissional da área de redes.

## Resumo

---

Nesta aula, você conheceu em detalhes a tecnologia de VLAN. Viu as motivações para dividirmos uma grande rede corporativa em redes virtuais (VLAN) menores, definidas de maneira administrativa por departamento ou tipo de usuário. Conheceu as modificações que o protocolo 802.1q provoca nos cabeçalhos dos quadros Ethernet para que todos os switches saibam como encaminhar os quadros de cada VLAN para as respectivas portas. Estudou também as configurações que são feitas nos switches e sabe agora como classificar as portas do switch que fazem parte de uma VLAN.

Esse assunto é de suma importância para todo bom profissional de redes. A tecnologia de VLAN é muito demandada em toda empresa que possui uma rede de médio a grande porte. Dominar esse assunto pode ser um diferencial significativo para você que adora a área de redes de computadores. Por isso, recomendo que leia os materiais listados na leitura complementar para se aprofundar ainda mais.

# Autoavaliação

---

1. O que significa VLAN?
2. Em poucas palavras, como funciona o protocolo 802.1q?
3. Faça uma analogia entre roteamento de VLAN (camada 2) e roteamento via IP 0 (camada 3).
4. Imagine uma grande rede de computadores de uma universidade com diversos prédios. Nessa rede, pretende-se implementar uma rede Wi-Fi única a todos os alunos para facilitar a implantação de políticas de acesso. Quais seriam as VLANs que você, como técnico de TI, criaria nessa rede?

Para ver as respostas, clique [aqui](#).

## Respostas

1. O termo VLAN, que é uma abreviação para Virtual LAN, é um mecanismo de divisão da rede a nível da camada de enlace em redes virtuais menores. É dito virtual porque essa divisão é feita de maneira lógica, via software do switch. Uma VLAN pode se estender por diversos switches espalhados dentro da grande rede corporativa, facilitando a implantação de recursos e políticas de uso por cada sub-rede.
2. O protocolo 802.1q altera o cabeçalho do quadro Ethernet acrescentando mais um campo, chamado de VLAN Tag, no qual se definem algumas informações de controle para o encaminhamento do quadro, em especial o número de identificação da VLAN (VLAN ID), a qual o quadro pertence. Observando esse número de VLAN, o switch só encaminha o quadro para as portas que fazem parte dessa VLAN.
3. Quem já estudou roteamento de pacotes pelo protocolo IP pode, realmente, perceber uma certa similaridade com o roteamento de quadros feitos pelos switches via protocolo de VLAN. As diferenças entre eles estão basicamente na informação usada para o roteamento - endereço IP de destino / VLAN ID - e para onde é encaminhada a

PDU após a decisão de roteamento – próximo roteador / porta do switch.

4. As VLANs que criaríamos seriam: uma para cada departamento da universidade, a fim de diminuir o domínio de broadcast e facilitar a implementação de políticas de uso da rede mais adequada para cada departamento; e uma VLAN para a rede Wi-Fi do campus, pelo mesmo motivo da implantação de políticas.

## Referências

---

FOROUZAN, B. **Comunicação de dados e redes de computadores**. 3. ed. Bookman, 2006.

KUROSE, J.; ROSS, K. **Redes de computadores e a internet**. 3. ed. São Paulo: Addison Wesley, 2006.

TANENBAUM, A. S. **Redes de computadores**. 4. ed. Editora Campus, 2003.