



Fundamentos da Tecnologia VLAN



Foreword

- A VLAN (rede local virtual) é uma tecnologia que agrupa logicamente dispositivos na mesma LAN em sub-redes diferentes para formar um grupo de trabalho virtual. Como tecnologia básica, a VLAN tem sido amplamente aplicada a vários modos e serviços de acesso, como multicast, triple play e serviços de linha privada.
- O surgimento da VLAN introduz nova vitalidade na LAN tradicional e traz uma revolução para a aplicação da LAN. Este curso descreve como implementar VLANs em switches, alterações de quadros de dados de VLAN transmitidos entre switches e configuração dinâmica de VLAN.



Objectives

- Após a conclusão deste curso, você será capaz de:
 - Entender o histórico e os recursos da tecnologia VLAN.
 - Dominar os métodos de geração de tags VLAN e as regras de aplicação de tags VLAN em diferentes cenários de interface.
 - Dominar os métodos básicos de roteamento de VLAN.



Contents

1. Visão Geral da VLAN

- O Motivo da VLAN

- O Método de Divisão da VLAN

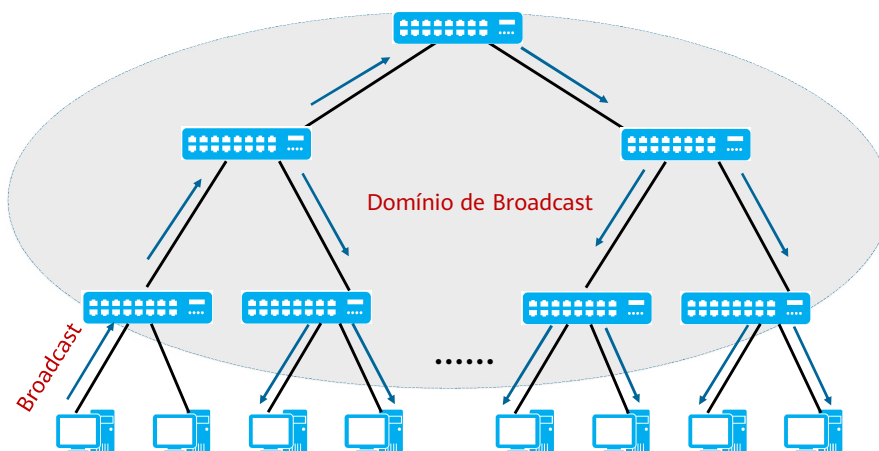
2. Configuração e Implementação de VLAN

3. Roteamento de VLAN

4. Recursos de VLANs na Rede de Acesso



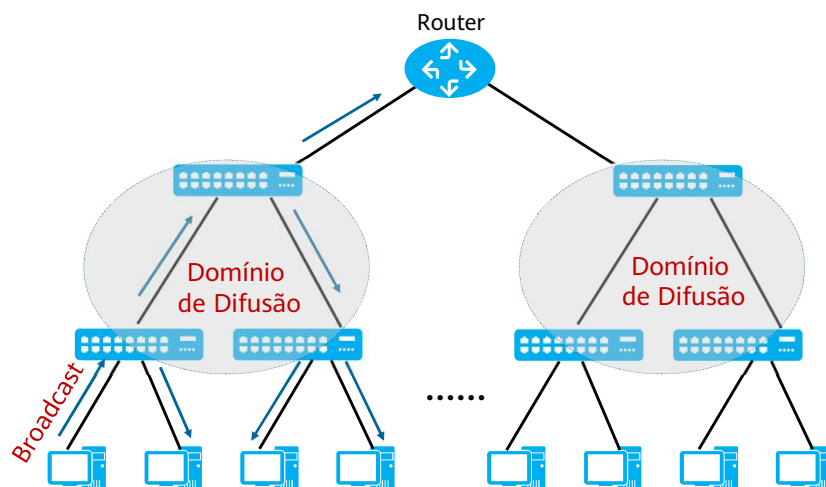
O Motivo da VLAN – Tempestade de Broadcast



- Uma LAN tradicional usa um hub. O hub tem apenas um barramento, que é um domínio de colisão. Portanto, uma LAN tradicional é uma rede plana e uma LAN pertence ao mesmo domínio de colisão. Os pacotes enviados por qualquer host são recebidos por todos os outros hosts no mesmo domínio de colisão. Mais tarde, a bridge (switch de Camada 2) é usada para substituir o hub. Cada porta pode ser considerada como um barramento independente. O domínio de colisão é reduzido a cada porta. Dessa forma, a eficiência do envio de pacotes unicast e o desempenho da rede de Camada 2 são melhorados. Se um host enviar um pacote de broadcast, o dispositivo ainda poderá receber o pacote de broadcast. Geralmente, a área onde o pacote de broadcast pode ser transmitido é chamada de domínio de broadcast. Ao transmitir o pacote de broadcast, a bridge precisa copiar o pacote de broadcast e enviá-lo para cada canto da rede. Com a expansão da escala da rede, mais e mais pacotes de broadcast são transmitidos na rede, e mais e mais recursos de rede são ocupados pelos pacotes de broadcast. Isso afeta seriamente o desempenho da rede. Isso é chamado de tempestade de broadcast.
- Devido à limitação do princípio de funcionamento da rede de camada 2, a bridge não pode resolver o problema da tempestade de broadcast. Para melhorar a eficiência da rede, uma rede é geralmente dividida em segmentos: um grande domínio de broadcast é dividido em vários domínios de broadcast menores.



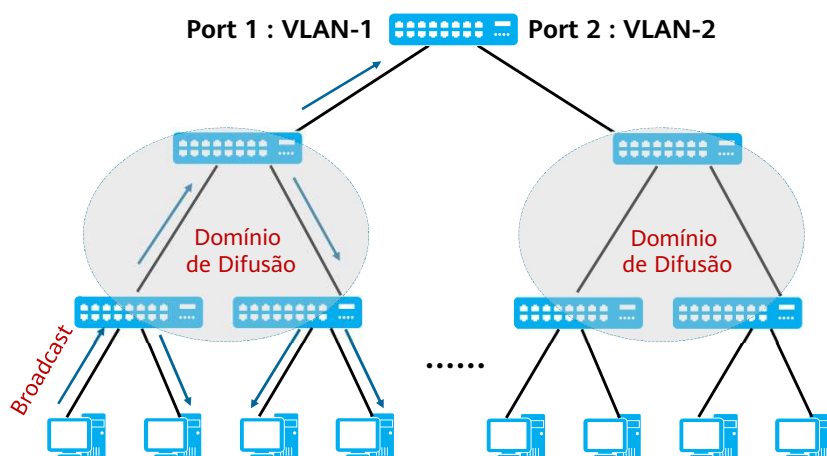
Segmentação de Redes Através de Roteadores



- No passado, os roteadores eram usados para segmentar LANs. Na figura anterior, o comutador do nó central é substituído por um roteador, de modo que o intervalo de envio de pacotes de broadcast seja bastante reduzido. Esta solução resolve o problema da tempestade de broadcast. No entanto, os roteadores são usados para isolar segmento por segmento de rede na camada de rede. O planejamento da rede é complexo, o modo de rede não é flexível e a dificuldade de gerenciamento e manutenção é aumentada. Como alternativa à segmentação de LAN, a VLAN é introduzida em soluções de rede para resolver os problemas enfrentados por grandes redes de Camada 2.



Dividindo um Domínio de Broadcast por VLAN



- A VLAN (Virtual Local Area Network) divide logicamente os recursos da rede e os usuários da rede em várias redes lógicas menores. Essas redes lógicas menores formam seus próprios domínios de broadcast, ou VLANs. Como mostrado na figura anterior, um comutador central é usado, mas os lados esquerdo e direito pertencem a VLANs diferentes e formam seus próprios domínios de broadcast. Os pacotes de broadcast não podem ser transmitidos através destes domínios de broadcast.
- Uma VLAN divide logicamente um grupo de usuários em diferentes segmentos de rede física em uma LAN. As funções e operações de uma VLAN são semelhantes às de uma LAN tradicional. Uma VLAN pode fornecer interconexão entre sistemas de terminais dentro de um determinado intervalo.



Vantagens da VLAN

- Em comparação com a tecnologia LAN tradicional, a tecnologia VLAN tem as seguintes vantagens:
 - Isola domínios de difusão e suprime pacotes de difusão;
 - Reduz os custos de movimentação e mudança;
 - Os grupos de trabalho virtuais são criados para funcionar de uma forma diferente das redes tradicionais. Os usuários não são restritos por dispositivos físicos.
 - Melhora a segurança da comunicação.
 - Melhora a robustez da rede.

- Os pacotes de broadcast são restringidos para melhorar a utilização da largura de banda:
 - A degradação do desempenho causada por tempestades de broadcast é efetivamente resolvida. Uma VLAN forma um pequeno domínio de broadcast. Os membros de uma VLAN estão no domínio de broadcast determinado pela VLAN. Quando um pacote de dados não é roteado, o switch envia o pacote de dados para todas as outras portas da VLAN em vez de todas as portas do switch. Dessa forma, o pacote de dados é restrito a uma VLAN. A largura de banda pode ser salva até certo ponto.
- Reduz o custo do movimento e da mudança:
 - Ou seja, quando um usuário se move de um local para outro, os atributos de rede do usuário podem ser reconfigurados dinamicamente. Essa rede de gerenciamento dinâmico traz grandes benefícios para administradores e usuários de rede. Um usuário pode acessar a rede sem qualquer modificação onde quer que vá, as perspectivas são muito boas. É claro que nem todos os métodos de definição de VLAN podem fazer isso.
- Cria um grupo de trabalho virtual:
 - O objetivo final do uso de VLANs é estabelecer um modelo de grupo de trabalho virtual. Os usuários não ficam restritos por dispositivos físicos. Os usuários de VLAN podem estar localizados em qualquer lugar da rede, e as VLANs não afetam os aplicativos do usuário.

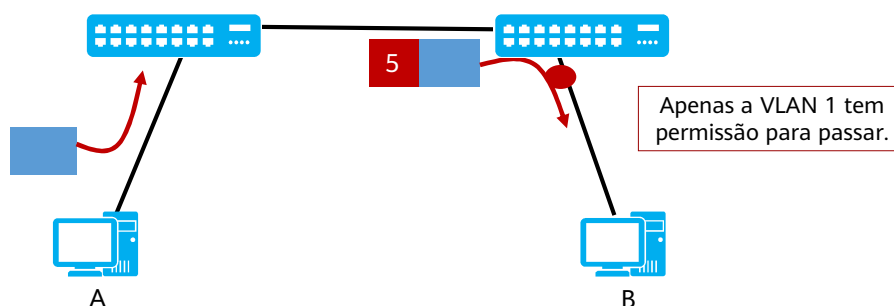
- Melhora a segurança da comunicação:
 - Os pacotes de dados de uma VLAN não são enviados para a outra VLAN. Dessa forma, os usuários de outras VLANs não podem receber os pacotes de dados dessa VLAN. Dessa forma, as informações dessa VLAN não são interceptadas pelos usuários de outras VLANs. Desta forma, a informação é mantida em segredo.
- Melhora a robustez (estabilidade) da rede:
 - Quando a escala da rede aumenta, algumas falhas de rede podem afetar toda a rede. Depois que as VLANs são introduzidas, algumas falhas de rede podem ficar restritas a uma VLAN. As VLANs são usadas para dividir logicamente uma rede. O esquema de rede é flexível e o gerenciamento de configuração é simples, reduzindo os custos de gerenciamento e manutenção.

- Enhances communication security:
 - The data packets of one VLAN are not sent to the other VLAN. In this way, the users of other VLANs cannot receive the data packets of this VLAN. In this way, the information of this VLAN is not intercepted by the users of other VLANs. In this way, the information is kept secret.
- Enhances network robustness:
 - When the network scale increases, some network faults may affect the entire network. After VLANs are introduced, some network faults can be restricted within a VLAN. VLANs are used to logically divide a network. The networking scheme is flexible and the configuration management is simple, reducing the management and maintenance costs.



Gerenciamento de Tags VLAN

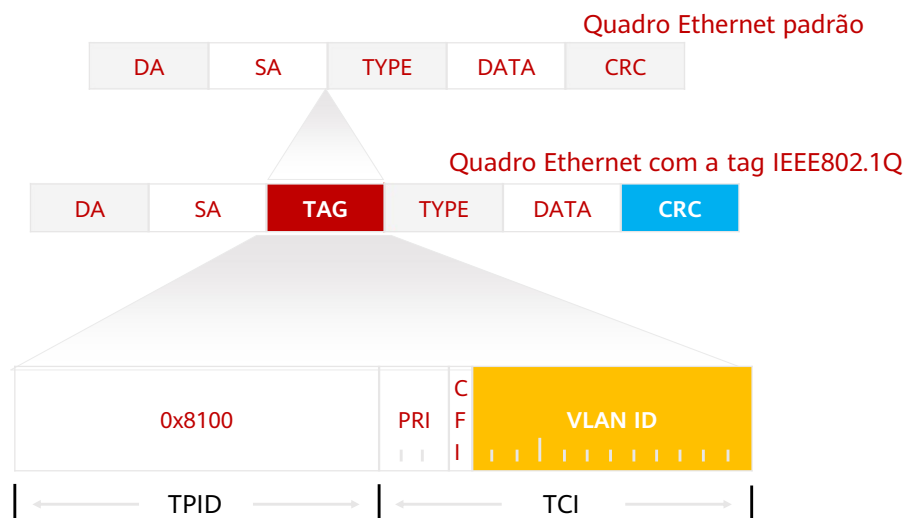
- Antes de encaminhar um quadro, o switch verifica a tag VLAN do pacote de dados.



- Para controlar o encaminhamento, o switch adiciona tags VLAN aos quadros Ethernet antes de encaminhá-los e, em seguida, determina como processar os quadros, incluindo o descarte de quadros, o encaminhamento de quadros, a adição de tags e a exclusão de tags.
- Antes de encaminhar um quadro, o switch verifica a tag VLAN do pacote de dados e determina se deve permitir que a tag passe pela porta. Conforme mostrado na figura, se o switch adicionar a tag 5 a todos os quadros enviados de A, ele pesquisará a tabela de encaminhamento da Camada 2 e encaminhará os quadros para a porta conectada a B com base no endereço MAC de destino. No entanto, essa porta está configurada para permitir que apenas a VLAN 1 passe. Portanto, os quadros enviados por A são descartados. Portanto, o switch que suporta a VLAN precisa encaminhar quadros Ethernet não apenas de acordo com o endereço MAC de destino, mas também de acordo com a configuração da VLAN da porta. Dessa maneira, o switch implementa o controle de encaminhamento de Camada 2.



Formato do Quadro VLAN



- O cabeçalho da tag 802.1Q de 4 bytes contém TPID (Tag Protocol Identifier) de 2 bytes e TCI (Tag Control Information) de 2 bytes.
- TPID é um novo tipo definido pelo IEEE. Ele indica que um quadro é adicionado com uma tag 802.1Q. O TPID tem um valor fixo de 0x8100.
- O TCI contém as informações de controle sobre quadros. Ele contém os seguintes elementos:
 - Prioridade: O padrão IEEE 802.1Q usa três bits que indicam a prioridade do quadro. São oito prioridades, que variam de 0 a 7.
 - Indicador de formato canônico (CFI): Se o valor CFI for 0, o formato será padrão. Se o valor CFI for 1, o formato não será padrão. Ele é usado no método de acesso médio FDDI de anel de token ou roteamento de origem para indicar as informações da sequência de bits do endereço transportado no quadro de encapsulamento.
 - VLAN Identifier (VLAN ID): Este é um campo de 12 bits, que indica o ID da VLAN. O valor varia de 0 a 4095. Existem 4096 IDs de VLAN no total. O intervalo real é de 1 a 4094. O pacote de dados enviado por cada switch que suporta o protocolo 802.1Q contém esse campo, indicando a VLAN à qual o pacote de dados pertence.
 - VLAN 0: indica que o quadro não carrega um ID de VLAN; neste caso, a tag 802.1Q especifica apenas uma prioridade.
 - VLAN 4095: é reservada para uso de implementação; não deve ser

configurado ou transmitido.

- Em uma rede de comutação, os quadros Ethernet têm dois formatos: quadro sem tags e quadro com tag. Um quadro sem tag é um quadro que não está marcado com o sinalizador de quatro bytes, e um quadro com tag é um quadro marcado com o sinalizador de quatro bytes.



Contents

1. Visão Geral da VLAN

- O Motivo da VLAN

- **O Método de Divisão da VLAN**

2. Configuração e implementação de VLAN

3. Roteamento de VLAN

4. Recursos de VLANs na Rede de Acesso



Classificação de VLANs - Baseado na Porta

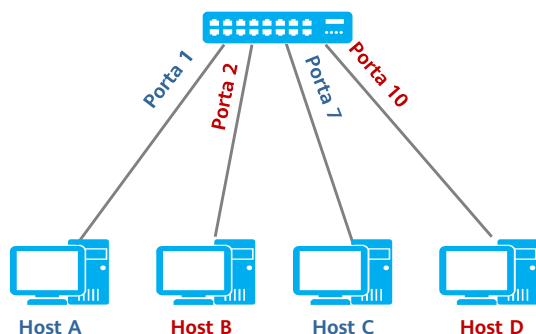


Tabela VLAN

Interface	VLAN
Porta1	VLAN5
Porta2	VLAN10
.....
Porta7	VLAN5
.....
Porta10	VLAN10

- As VLANs são divididas com base nas portas do switch Ethernet. Por exemplo, as portas 1 a 4 do switch estão na VLAN A, as portas 5 a 17 estão na VLAN B e as portas 18 a 24 estão na VLAN C. As portas na mesma VLAN podem ser descontínuas. O administrador determina como configurar as portas.
- Conforme mostrado na figura, as portas 1 e 7 pertencem à VLAN 5, e as portas 2 e 10 pertencem à VLAN 10. O host A e o host C estão conectados às portas 1 e 7, portanto, pertencem à VLAN 5. Da mesma forma, o host B e o host D pertencem à VLAN 10.
- Se houver vários switches, por exemplo, as portas 1 a 6 do switch 1 e as portas 1 a 4 do switch 2 podem ser especificadas para a mesma VLAN. Ou seja, uma VLAN pode abranger vários switches Ethernet. O método mais comum para definir VLANs é dividir VLANs com base em portas. A vantagem desse método de divisão é que é muito simples definir membros da VLAN. Você só precisa especificar todas as portas. No entanto, se o usuário da VLAN A deixar a porta original e alternar para uma nova porta de um novo switch, a VLAN A deverá ser redefinida.



Classificação de VLANs - Com base no Endereço MAC

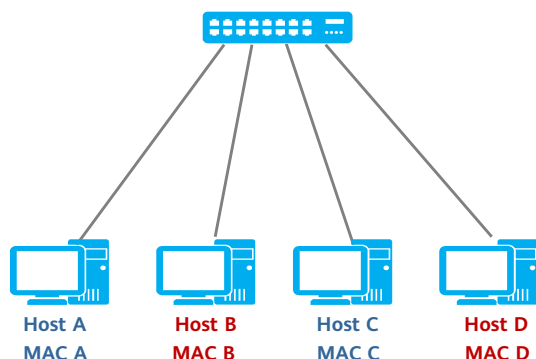


Tabela VLAN

Endereço MAC	VLAN
MAC A	VLAN5
MAC B	VLAN10
MAC C	VLAN5
MAC D	VLAN10

- Esse método é baseado no endereço MAC de cada host. Ou seja, todos os hosts são atribuídos à VLAN à qual pertencem com base em seus endereços MAC. O switch mantém uma tabela de mapeamento de VLAN, que registra o mapeamento entre endereços MAC e VLANs. A maior vantagem desse método é que, quando um usuário se move de um switch para outro, a VLAN não precisa ser reconfigurada. Portanto, esse método é baseado na VLAN do usuário.
- A desvantagem desse método é que todos os usuários devem ser configurados durante a inicialização. Se houver um grande número de usuários, a carga de trabalho de configuração será pesada. Além disso, esse método de divisão também reduz a eficiência de execução do switch, porque uma porta de cada switch pode ter muitos membros de um grupo de VLAN, de modo que os pacotes de broadcast não podem ser restritos. Além disso, para usuários de laptops, suas placas de rede podem mudar com frequência, portanto, a VLAN deve ser configurada continuamente.



Classificação de VLANs - Baseada em Protocolo

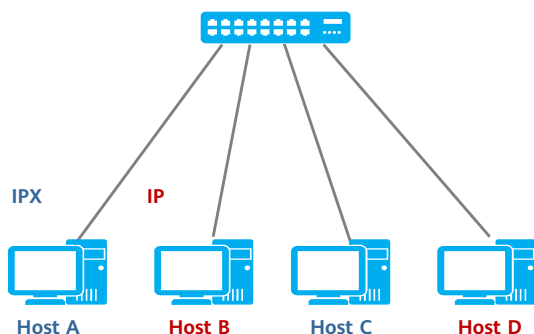


Tabela VLAN

Protocolo	VLAN
IPX	VLAN5
IP	VLAN10
.....

- Nesse caso, as VLANs são divididas com base no campo de protocolo no quadro de dados da Camada 2. O campo de protocolo nos dados da Camada 2 pode ser usado para determinar o protocolo de rede da camada superior, como IP ou IPX. Se uma rede física tiver uma rede IP e vários protocolos, como IPX em execução, você poderá usar esse método para dividir VLANs.
- Esse tipo de VLAN raramente é usado em aplicativos reais.



Classificação de VLANs - Baseado em sub-redes IP

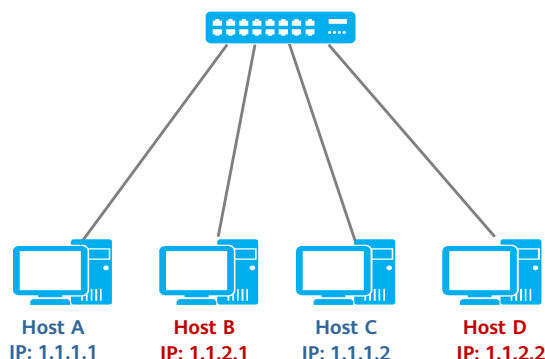


Tabela VLAN

Rede IP	VLAN
IP 1.1.1.0/24	VLAN5
IP 1.1.2.0/24	VLAN10
.....

- A VLAN baseada em sub-rede IP determina a VLAN à qual um pacote pertence com base no endereço IP no pacote. Todos os pacotes na mesma sub-rede IP pertencem à mesma VLAN. Dessa forma, os usuários na mesma sub-rede IP podem ser atribuídos à mesma VLAN.
- A figura mostra como o switch divide VLANs com base em endereços IP. O host A e o host C pertencem à sub-rede IP 1.1.1.x. De acordo com a tabela VLAN, eles pertencem à VLAN 5. Da mesma forma, o host B e o host D pertencem à VLAN 10. Se o host C alterar seu endereço IP para 1.1.2.9, o host C não pertencerá mais à VLAN 5, mas à VLAN 10.
- A definição de VLANs com base em sub-redes IP tem as seguintes vantagens:
 - Neste modo, os segmentos de rede podem ser divididos com base em protocolos de transmissão. Isso é muito tentador para os gerentes de rede que desejam organizar os usuários com serviços específicos do aplicativo.
 - Os usuários, especialmente os usuários TCP/IP, podem se mover livremente dentro da rede sem reconfigurar suas estações de trabalho.
 - A desvantagem desse método é a eficiência, porque a verificação do endereço da camada de rede de cada pacote é demorada. Além disso, os pacotes de broadcast não podem ser suprimidos porque uma porta pode ter vários membros da VLAN.

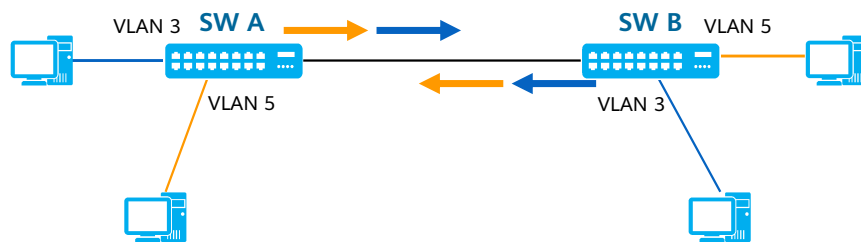


Contents

1. Visão Geral da VLAN
- 2. Configuração e Implementação de VLAN**
 - **Tipo de Link VLAN**
 - Encaminhamento de Dados de VLAN
3. Roteamento de VLAN
4. Recursos de VLANs na Rede de Acesso



A Escalabilidade da VLAN

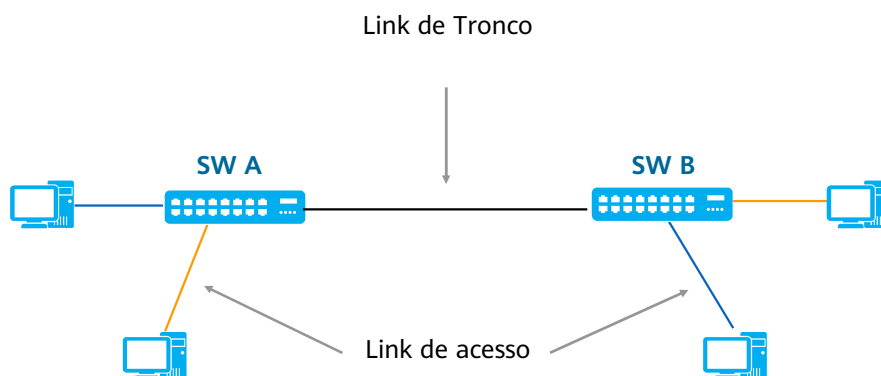


- Os dados da VLAN podem ser transferidos através de vários switches.

- As informações de VLAN podem ser transmitidas através de vários switches para switches relacionados.
- Todos os dados VLAN-3 na figura acima podem ser comunicados através de switches de transição intermediários, de modo que os dados da VLAN-5.



Tipo de Link da VLAN



- The access link refers to the link between a host and a switch. Usually, hosts do not need to know which VLAN they belong to, and the host hardware does not necessarily support frames with VLAN tags. The frames that the host requires to send and receive are frames that are not marked.
- The access link belongs to a specific port, which belongs to one VLAN. This port can not directly receive information from other VLAN, nor can it send packets to other VLAN directly. The information of different VLAN must be processed through layer 3 so that it can be forwarded to this port.
- Trunk links are links that can carry multiple VLAN data. Trunk links are usually used for interconnection between switches or for connections between switches and routers.
- When a data frame is transmitted on a trunk link, the switch must identify the VLAN of the data frame. IEEE 802.1Q defines the VLAN frame format, all the frames transmitted on the trunk link are tagged frames. Through these tags, the switch can determine which frames belong to which VLAN.
- Unlike access links, the trunk links are used to carry VLAN data between different devices (such as switches and routers, switches and switches), so the trunk links belong to no specific VLAN. By configuring, the trunk link can carry all the VLAN data, or it can be configured to transmit only the specified VLAN data.
- Although the trunk link does not belong to any specific VLAN, it can configure a PVID(port VLAN ID). When there is untagged frame transmitting on the trunk link, the switch will add PVID as VLAN tag to the frame, then handles it.



Classificação de Portas de Switches Ethernet

- Porta de acesso:
 - Conecta-se ao host do usuário e ele pertence apenas a uma VLAN.
- Porta tronco:
 - Conecta-se a outros switches, a porta de tronco pode pertencer a várias VLAN, receber e enviar vários pacotes de VLAN.
- Porta híbrida:
 - Conecta-se a hosts ou switches. A porta híbrida pode pertencer a várias VLAN, receber e enviar vários pacotes de VLAN.

- A diferença entre a porta Híbrida e a porta Tronco é que a porta híbrida permite que vários pacotes de VLAN sejam sem tag, enquanto a porta de tronco só permite que o pacote de VLAN padrão seja desmarcado. No mesmo switch, a porta híbrida e a porta de tronco não podem coexistir.



Port VLAN ID (PVID)

- A porta de acesso pertence a apenas uma VLAN, portanto, seu ID padrão é o PVID, ele não precisa ser definido.
- A porta híbrida e a porta de tronco pertencem a várias VLAN, portanto, o PVID precisa ser configurado e o padrão é 1.



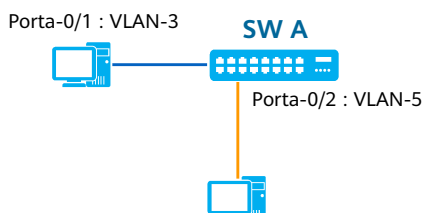
O PVID padrão é 1

- Todas as portas padrão pertencem à VLAN 1, e a VLAN 1 é a VLAN padrão, que não pode ser criada nem excluída.



Configuração do Link de Acesso

- Por padrão, todas as portas do switch pertencem à VLAN-1, ou seja, PVID (Port VLAN ID) é 1.



\\Config link-type

```
[Switch-Ethernet0/1]port link-type access  
[Switch-Ethernet0/2]port link-type access
```

\\Creat VLAN, add interfaces into VLAN

```
[Switch]vlan 3  
[Switch-vlan3]port ethernet 0/1  
[Switch]vlan 5  
[Switch-vlan5]port ethernet 0/2
```

\\Another way to add interface into VLAN

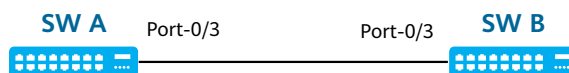
```
[Switch-Ethernet0/1]port default vlan 3  
[Switch-Ethernet0/2]port default vlan 5
```

- Todas as portas dos switches baseados em 802.1Q pertencem à VLAN-1, portanto, eles chamam a VLAN-1 de VLAN padrão.
- Aqui está um novo termo chamado PVID, o nome completo chamado Port VLAN ID, que representa a VLAN da porta. Na porta de acesso, o valor de PVID representa a VLAN à qual a porta pertence, como PVID = 100, ou seja, a porta é atribuída à VLAN100.



Configuração do Link de Tronco

- Responsável pela transmissão de dados de múltiplas VLAN
- O PVID padrão é 1



```
\\Config link-type
[Switch-Ethernet0/3]port link-type trunk

\\ Config allow-pass list
[Switch-Ethernet0/3]port trunk allow-pass vlan all

\\ Config PVID
[Switch-Ethernet0/3]port trunk pvid vlan 1
```

- A porta de tronco é responsável por encaminhar vários quadros de dados de VLAN entre switches, use o comando "port trunk allow-pass vlan [VID]" para permitir que os quadros de dados com uma VLAN específica passem.
- Aqui está um comando "port trunk PVID VLAN [VID]" para alterar o valor PVID da porta Trunk, e o significado do valor PVID da porta Trunk é diferente do PVID da porta Access. Para Porta de acesso, ela representa uma VLAN pertencente à porta, mas para a porta de tronco, representa o valor de VLAN padrão. config link-type



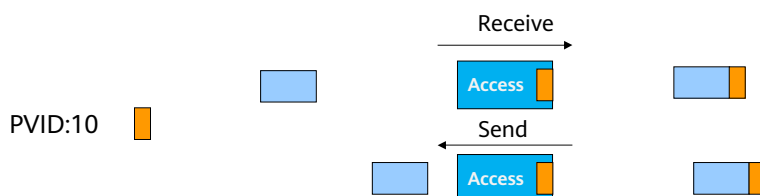
Contents

1. Visão Geral da VLAN
- 2. Configuração e Implementação de VLAN**
 - Tipo de Link VLAN
 - **Encaminhamento de Dados de VLAN**
3. Roteamento de VLAN
4. Recursos de VLANs na Rede de Acesso



Fundamentos de encaminhamento 802.1Q - Link de Acesso

- Porta de acesso recebe um quadro
 - Se o quadro não contiver o cabeçalho da tag 802.1Q, o PVID da porta será adicionado ao quadro. Se o quadro contiver o cabeçalho da tag 802.1Q e o valor do cabeçalho da tag 802.1Q for o mesmo que o PVID da porta, o switch receberá o pacote. Se forem diferentes, o comutador descarta o pacote.
- Porta de acesso envia um quadro
 - O cabeçalho da tag 802.1Q é removido.

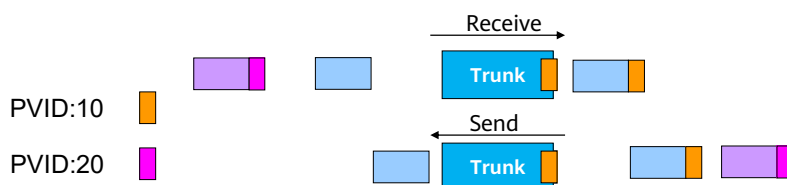


- A porta de acesso recebe o quadro
 - Se o quadro não contiver o cabeçalho da tag 802.1Q, o PVID da porta será adicionado ao quadro. Se o quadro contiver o cabeçalho da tag 802.1Q e o valor do cabeçalho da tag 802.1Q for o mesmo que o PVID da porta, o switch receberá o pacote. Se forem diferentes, o comutador descarta o pacote.
- A porta de acesso envia quadro
 - Remove o cabeçalho da tag 802.1Q e envia um quadro Ethernet comum.



Fundamentos de encaminhamento 802.1Q - Porta de Tronco

- A porta de tronco recebe quadro
 - Se o quadro não contiver o cabeçalho da tag 802.1Q, o PVID da porta será adicionado ao quadro. Se o quadro contiver o cabeçalho da tag 802.1Q, o sistema comparará o quadro com a lista de passes permitidos da porta. Se o quadro contiver o cabeçalho da tag 802.1Q, o sistema transmitirá o quadro de forma transparente. Caso contrário, o sistema descarta o quadro.
- A porta de tronco envia quadro
 - Quando o ID da VLAN do quadro é diferente do PVID da porta, ele precisa comparar a lista de passes permitidos da porta. Se a lista contiver a VLAN, o quadro será transmitido de forma transparente. Quando o ID da VLAN do quadro é o mesmo que o PVID da porta, o cabeçalho da tag 802.1Q é removido antes que o quadro seja transmitido.

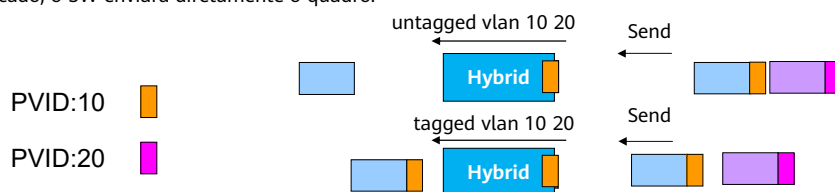


- A porta de tronco recebe quadro
 - Se o quadro não contiver o cabeçalho da tag 802.1Q, o PVID da porta será adicionado ao quadro. Se o quadro contiver o cabeçalho da tag 802.1Q e o valor da tag for o mesmo que o PVID da porta, o switch receberá o pacote. Se forem diferentes, o comutador descarta o pacote.
- A porta de tronco envia quadro
 - Quando o ID da VLAN do quadro é diferente do PVID da porta, a porta precisa comparar a lista de passes permitidos da porta. Se a lista contiver a VLAN, o quadro será transmitido de forma transparente. Quando o ID da VLAN do quadro é o mesmo que o PVID da porta, o cabeçalho da tag 802.1Q é removido antes que o quadro seja transmitido.



Fundamentos de encaminhamento 802.1Q - Porta Híbrida

- A porta híbrida recebe o quadro
 - Se o quadro não tiver uma tag VLAN, o SW adicionará PVID de interface híbrida ao quadro.
 - Se o quadro tiver uma tag VLAN, o SW verificará se a interface híbrida permite que o quadro passe. Caso contrário, o quadro será descartado.
- A porta híbrida envia o quadro
 - O switch verifica se a interface é adicionada à VLAN no modo não marcado ou marcado. Se a interface for adicionada à VLAN no modo não marcado, o switch excluirá a tag VLAN e, em seguida, enviará o quadro. Se a interface for adicionada à VLAN no modo marcado, o SW enviará diretamente o quadro.



- O SW processa os quadros recebidos na interface híbrida da seguinte forma:
 - A interface recebe o quadro.
 - O SW verifica se o quadro carrega uma tag VLAN:
 - Se o quadro não contiver a tag VLAN, o SW verificará se o PVID da VLAN híbrida está na lista de ID de VLAN permitida:
 - Se sim, o SW marca o quadro com o PVID e, em seguida, prossegue para a etapa 3.
 - Caso contrário, o SW descarta o quadro.
 - Se o quadro tiver uma tag VLAN, o SW verificará se a interface híbrida permite que o quadro passe. Se a interface híbrida permitir que o quadro passe, o SW prosseguirá para a etapa 3. Caso contrário, o quadro será descartado.
 - O switch procura a configuração de VLAN com base no endereço MAC de destino e no ID de VLAN do quadro e determina a interface de saída do quadro.
 - O switch envia quadros através da interface de saída. Se a interface de saída for uma interface híbrida, o SW verificará se a interface foi adicionada à VLAN no modo não marcado ou marcado. Se a interface for adicionada à VLAN no modo não marcado, o SW excluirá a tag VLAN e enviará o quadro. Se a interface for adicionada à VLAN no modo marcado, o SW enviará diretamente o quadro.

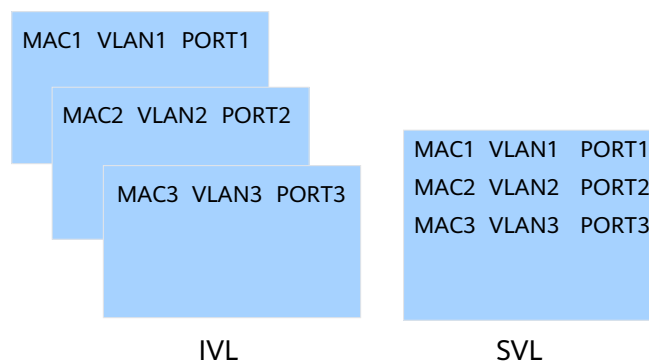
- **Como funcionam Interfaces híbridas ???**

- <https://www.youtube.com/watch?v=WvKnNRPBfJg>



Mecanismo de Encaminhamento de Pacotes de Switches

- O endereço MAC existe em diferentes tabelas de endereços, que podem ser expressas como:



- IVL : Independent VLAN Learning
 - Pesquisa a tabela L2FDB com base no ID da VLAN no cabeçalho da tag do quadro para determinar o intervalo de pesquisa.
 - Localiza a interface de saída com base no endereço MAC de destino e encaminha o pacote se a entrada correspondente for encontrada.
 - Se o endereço MAC de destino não puder ser encontrado na tabela L2FDB, o pacote será encaminhado através de todas as portas (exceto a porta de origem) na VLAN no modo broadcast.
- SVL : Shared VLAN Learning
 - O switch procura na tabela de encaminhamento MAC (ou seja, L2FDB) uma entrada correspondente com base no endereço MAC de destino.
 - Se uma entrada correspondente for encontrada, o sistema verificará se a VLAN à qual a interface pertence é a mesma que a VLAN transportada no pacote. Se sim, o sistema encaminha o pacote. Se não, o sistema descarta o pacote.
 - Se nenhuma entrada correspondente for encontrada com base no endereço MAC de destino, o pacote será transmitido na VLAN à qual o pacote pertence (excluindo a porta de origem).
- No modo IVL, cada VLAN tem uma tabela de mapeamento de porta MAC. Um

endereço MAC pode estar contido em várias tabelas (VLANs diferentes). No modo SVL, uma tabela grande é criada no switch e a relação de mapeamento é MAC-VLAN-port. Além disso, um endereço MAC aparece apenas uma vez na tabela e pertence a apenas uma VLAN. Obviamente, o SVL deve ser um pouco mais fácil de implementar. Parece ser uma implementação de patching, mas não é uma VLAN real. Muitos dos primeiros switches VLAN usam o modo SVL.

Para IVL. A maioria dos documentos na rede diz que uma tabela é criada para cada VLAN. Parece que há muitas tabelas. Na verdade, a tabela mencionada aqui se refere a uma tabela lógica. Na verdade, há apenas uma tabela no switch. Se registros com o mesmo VID forem extraídos para formar uma tabela, uma tabela física poderá ser logicamente considerada como várias tabelas.

- In IVL mode, each VLAN has a MAC-port mapping table. A MAC address can be contained in multiple tables (different VLANs). In SVL mode, a large table is created in the switch, and the mapping relationship is MAC-VLAN-port. In addition, a MAC address appears only once in the table and belongs to only one VLAN. Obviously, SVL should be a bit easier to implement. It seems to be a patching implementation, but it is not a real VLAN. Many early VLAN switches use the SVL mode.
- For IVL. Most documents on the network say that a table is created for each VLAN. It seems that there are many tables. Actually, the table mentioned here refers to a logical table. Actually, there is only one table in the switch. If records with the same VID are extracted to form a table, a physical table can be logically considered as multiple tables.



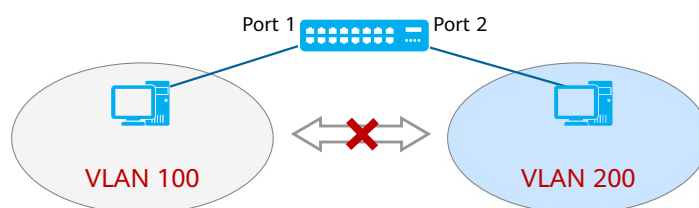
Contents

1. Visão Geral da VLAN
2. Configuração e Implementação de VLAN
- 3. Roteamento de VLAN**
 - **Fundamentos do Roteamento de VLAN**
 - Configuração e Implementação de Roteamento de VLAN
4. Recursos de VLANs na Rede de Acesso



Desvantagens da VLAN

- As VLANs isolam os domínios de difusão da Camada 2 e, portanto, o tráfego de VLANs diferentes é isolado. Usuários em VLANs diferentes não podem se comunicar uns com os outros.

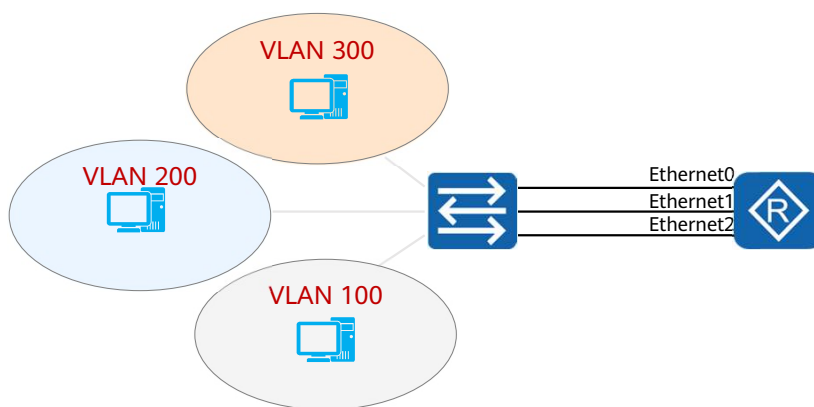


- As VLANs isolam os domínios de difusão da Camada 2 e, portanto, o tráfego de VLANs diferentes é isolado. Usuários em VLANs diferentes não podem se comunicar uns com os outros.



Implementação de VLAN Interredes - Cada VLAN Tem uma Conexão Física

- As VLANs são configuradas no comutador de Camada 2. Cada VLAN é conectada a uma interface do roteador através de uma conexão física exclusiva.

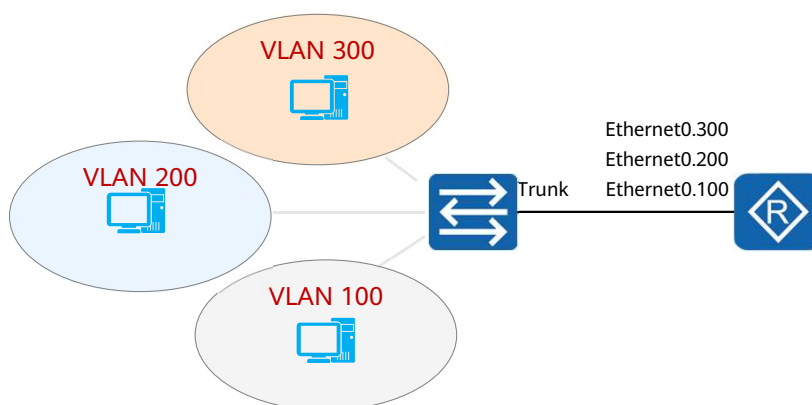


- O primeiro método para resolver o problema da comunicação entre VLAN é alocar uma interface de roteador independente para cada VLAN. A comunicação de dados entre VLANs é implementada através do roteamento de camada 3 do roteador. Dessa forma, as VLANs podem se comunicar umas com as outras. No entanto, à medida que o número de VLANs em cada switch aumenta, isso inevitavelmente exigirá um grande número de interfaces de roteador. Esta solução não é aplicável à seleção de rotas entre VLAN devido a considerações de custo. Além disso, algumas VLANs podem não se comunicar umas com as outras com frequência. Como resultado, as interfaces do roteador não são totalmente usadas.



Implementação de VLAN Interredes - Usando o Entroncamento de VLAN

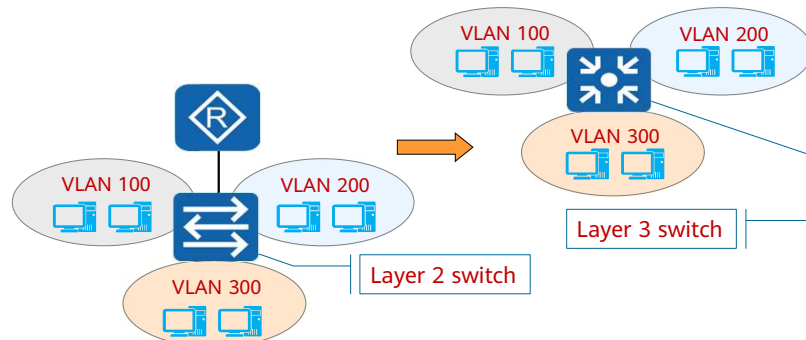
- O entroncamento de VLAN é configurado no switch e no roteador de Camada 2 para permitir que várias VLANs compartilhem a mesma rota de conexão física.



- Para resolver o problema dos requisitos excessivos de interface física, um roteador de um braço é introduzido no desenvolvimento de tecnologias de VLAN. O roteador de um braço (one arm) é um dispositivo de rede de Camada 3 que implementa a comunicação entre VLANs. O roteador de um braço requer apenas uma interface Ethernet. Ao criar subinterfaces, o roteador de um braço pode funcionar como o gateway de todas as VLANs e encaminhar dados entre VLANs.
- Como mostrado na figura anterior, o roteador fornece apenas uma interface Ethernet e três subinterfaces são configuradas na interface como os gateways padrão de três usuários de VLAN. Quando um usuário na VLAN 100 precisa se comunicar com um usuário em outra VLAN, o usuário só precisa enviar pacotes de dados para o gateway padrão. O gateway padrão modifica a tag VLAN do quadro de dados e, em seguida, envia o quadro de dados para a VLAN do host de destino, a comunicação entre as VLANs está concluída.



Implementação de VLAN Interredes - Integração de Comutação e Roteamento

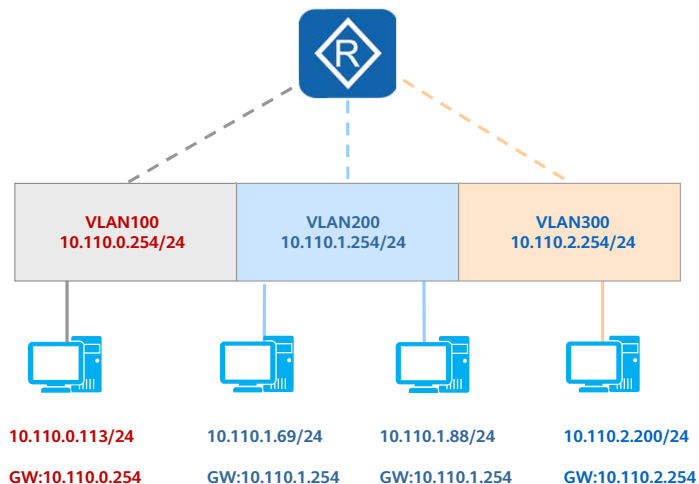


- O switch de Camada 2 e o roteador são integrados para formar um switch da Camada 3. O switch de Camada 3 implementa a divisão de VLAN, a comutação de Camada 2 dentro de uma VLAN e o roteamento entre VLAN.

- A terceira solução é um switch de Camada 3, que combina as vantagens de roteadores e switches.



Modelo de Função de switch de camada 3



- O roteador na figura é equivalente a um módulo de software de roteamento no switch, que implementa o roteamento e o encaminhamento da Camada 3. Um switch funciona como um módulo de comutação de Camada 2 e implementa o encaminhamento rápido de Camada 2 em uma VLAN. O gateway padrão definido pelo usuário é o endereço IP da interface VLAN virtual no switch de Camada 3.

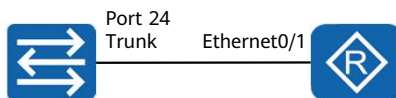


Contents

1. Visão Geral da VLAN
2. Configuração e Implementação de VLAN
- 3. Roteamento de VLAN**
 - Fundamentos do Roteamento de VLAN
 - **Configuração e Implementação de Roteamento de VLAN**
4. Recursos de VLANs na Rede de Acesso



Configuração de Rota One-Arm



Switch Configuration

//Configure the VLAN ID for Ethernet ports 0/1 and 0/2

```
[SWA]vlan 100
[SWA-vlan100]port ethernet 0/1
[SWA]vlan 200
[SWA-vlan200]port ethernet 0/2
```

// Configure ports 0/24 in trunk mode and transparently transmit packets of all VLANs

```
[SWA]interface ethernet 0/24
[SWA-Ethernet0/24]port link-type trunk
[SWA-Ethernet0/24]port trunk permit vlan all
```

Router Configuration

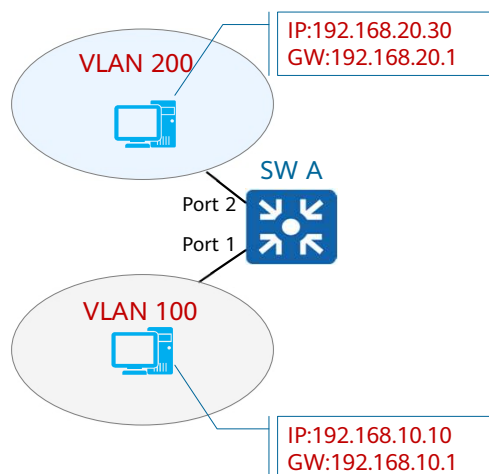
//Configure the sub-interface of Ethernet 0/1

```
[RTA]interface ethernet 0/1.1
[RTA-Ethernet0/1.1]vlan dot1q vid 100
[RTA-Ethernet0/1.1]ip address 192.168.10.1 255.255.255.0
[RTA]interface ethernet 0/1.2
[RTA-Ethernet0/1.2]vlan dot1q vid 200
[RTA-Ethernet0/1.2]ip address 192.168.20.1 255.255.255.0
```

- Usando o comando **vlan dot1q vid**, você pode configurar uma subinterface Ethernet ou uma subinterface Eth-Trunk como uma interface de membro da VLAN e especificar o modo de encapsulamento da VLAN.
- Depois de entrar na visualização da subinterface Ethernet, você deve configurar o encapsulamento de VLAN. Caso contrário, você não poderá definir parâmetros como o endereço IP e a MTU.
- Nota: Este comando pode ser configurado apenas em subinterfaces.



Configuração do Switch de Camada 3



//Create a VLAN Layer 3 interface on the SWA

```
[SWA]interface vlan-interface 100
[SWA-Vlan-interface100]ip add 192.168.10.1 255.255.255.0
[SWA]interface vlan-interface 200
[SWA-Vlan-interface200]ip add 192.168.20.1 255.255.255.0
```

- Usando o comando **interface vlan-interface *VLAN-ID***, você pode inserir a visualização da interface VLAN depois que uma VLAN for criada.
- A ID de uma interface VLAN deve corresponder a uma VLAN existente.
- O VRP considera que a função de roteamento é habilitada depois que a interface VLAN de Camada 3 é habilitada no switch. Ou seja, uma vez que a interface VLAN de Camada 3 é configurada, as duas VLANs podem se comunicar entre si por meio de suas respectivas interfaces de VLAN.



Contents

1. Visão Geral da VLAN
2. Configuração e Implementação de VLAN
3. Rota da VLAN
4. **Recursos de VLANs na Rede de Acesso**



Tipo e Atributo de VLAN

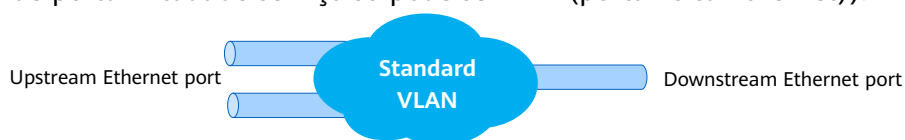
- O OLT suporta 4000 VLANs, variando de 2 a 4093.
- A tabela a seguir lista os tipos e atributos de VLAN:
 - Tipo:
 - Standard
 - Smart
 - MUX
 - Atributo:
 - Common
 - QinQ
 - Stacking

- 4000 VLANs para o OLT, variando de 2 a 4093
- A seguir estão VLANs especiais:
 - VLAN 1: VLAN padrão no sistema. É a VLAN inteligente padrão e pode ser substituída, mas não pode ser excluída.
 - VLAN 4094 e VLAN 4095 são reservadas no sistema. Eles não podem ser configurados como VLANs reservadas.
 - VLAN 4079: Por padrão, a VLAN é reservada quando o sistema é iniciado. Por padrão, **o sistema reserva 15 VLANs consecutivas** (VLANs 4079-4093 por padrão).
- Super VLAN
 - O conceito de super VLAN economiza recursos de endereço IP. **É uma VLAN de Camada 3.**
 - Uma super VLAN é formada pela agregação de várias sub-VLANs. Através da interface da Camada 3 da super VLAN, os serviços de diferentes sub-VLANs podem ser encaminhados para a Camada 3. Dessa forma, a eficiência do uso do endereço IP é melhorada. Uma sub-VLAN pode ser uma VLAN *smart* ou uma *MUX*, mas não pode ser uma VLAN *QinQ* seletiva ou uma *Stacking*. Em uma super VLAN, as sub-VLANs são isoladas na Camada 2, mas podem se comunicar umas com as outras por meio do proxy ARP (Address Resolution Protocol).



Tipo de VLAN - VLAN Standard

- VLAN *Standard* definida pelo IEEE 802.1Q, que tem os seguintes recursos:
 - As interfaces na mesma VLAN podem se comunicar umas com as outras na Camada 2.
 - Interfaces em VLANs diferentes são isoladas umas das outras na Camada 2.
 - O tipo de porta virtual de serviço só pode ser ETH (porta física Ethernet)).



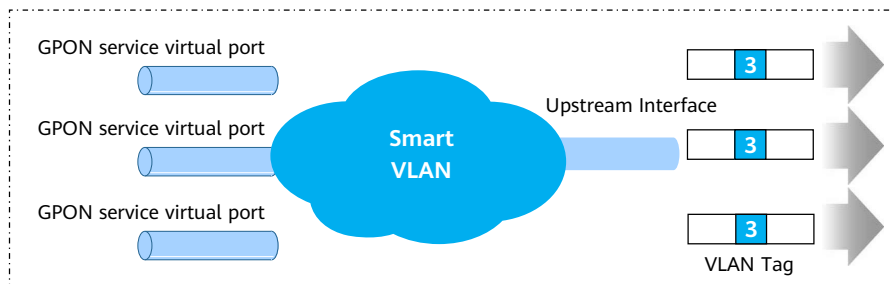
No OLT, uma VLAN *Standard* pode conter apenas portas Ethernet, mas não portas de serviço GPON. Uma VLAN *Standard* pode conter várias portas Ethernet e geralmente é usada para serviços de Ethernet subtending ou P2P.

- Standard VLAN
 - As portas em uma VLAN standard são portas Ethernet standard que são logicamente equivalentes.
 - Portas Ethernet na mesma VLAN standard podem se comunicar entre si, e portas Ethernet em diferentes VLANs standard estão isoladas uns dos outros.
- Default VLAN
 - VLAN ID: 1
 - Tipo: Smart VLAN
 - Você pode executar o comando `default vlan modify` para modificar o tipo de VLAN. A VLAN não pode ser excluída.
 - VLAN reservada padrão
 - Intervalo de VLAN: 4079-4093
 - Você pode executar o comando `vlan reserve` para modificar a VLAN reservada do sistema.



Tipo de VLAN – Smart VLAN

- Uma VLAN Smart pode conter várias portas upstream e portas de serviço.
 - Use para criar grupos de usuários. Diferentes grupos de usuários pertencem a VLANs diferentes.
 - Os usuários na mesma VLAN são isolados uns dos outros na Camada 2.
 - Quando o número de VLANs é limitado, esse tipo de VLAN pode ser usado para economizar recursos de VLAN.

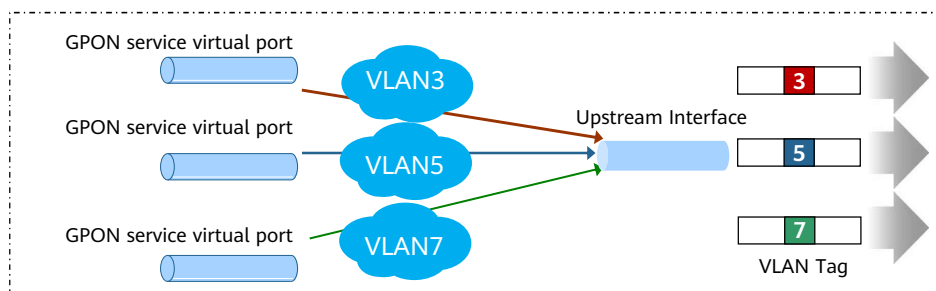


- Smart VLAN
 - A VLAN do tipo smart é uma VLAN especial. Além de todos os recursos da VLAN padrão, a VLAN *Smart* tem seus próprios recursos exclusivos:
 - Em uma VLAN *Smart*, as portas são classificadas em portas upstream e portas de serviço.
 - As portas de serviço são isoladas umas das outras e não podem se comunicar umas com as outras.
 - As portas upstream podem se comunicar diretamente umas com as outras.
 - A porta virtual de serviço e a porta upstream podem se comunicar diretamente entre si.
 - O domínio de broadcast de cada porta numa VLAN padrão contém todas as portas na VLAN. No entanto, o domínio de broadcast da porta upstream da VLAN *Smart* abrange todas as portas da VLAN, mas o domínio de broadcast da porta de serviço abrange apenas a porta upstream.



Tipo de VLAN – VLAN MUX

- Uma VLAN MUX pode conter várias portas upstream, mas apenas uma porta de serviço.
 - O mapeamento um-para-um é estabelecido entre usuários e IDs de VLAN.
 - Isola os usuários da Camada 2 e diferencia os usuários.
 - Uma VLAN corresponde a uma conexão virtual de Camada 2.



- MUX VLAN
 - A VLAN MUX é uma VLAN que contém a porta upstream e a porta virtual de serviço.
 - Uma vlan MUX pode conter várias portas upstream, mas apenas uma porta de serviço.
 - Os fluxos de serviço de diferentes VLANs MUX são isolados uns dos outros.
 - A MUX VLAN possui mapeamento um-para-um com usuários de acesso. Portanto, os usuários de acesso podem ser diferenciados por VLAN.



Introdução aos Atributos de VLAN

Attribute	Description
Common	Um quadro Ethernet contém apenas uma marca VLAN. Ele pode ser usado como uma VLAN de Camada 2 comum ou uma interface virtual de Camada 3 de VLAN. Geralmente é usado quando o OLT tem apenas uma VLAN para transmissão upstream.
QinQ	O pacote contém a tag VLAN interna da rede privada do usuário e a tag VLAN externa alocada pelo OLT. Por meio da tag VLAN externa, um túnel VPN de Camada 2 é configurado entre as redes privadas do usuário para transmitir serviços de forma transparente. Você também pode vincular usuários ou diferenciar tipos de serviço por tags de VLAN duplas.
Stacking	O pacote contém as marcas de VLAN internas e externas alocadas pelo OLT. O dispositivo de camada superior pode realizar a autenticação VLAN dupla de acordo com as tags duplas, o que aumenta o número de usuários de acesso. Na rede de camada superior no modo de trabalho L2, os pacotes podem ser encaminhados através da tag VLAN externa para fornecer o serviço de atacado para o ISP.



Quadros Ethernet com uma única tag VLAN

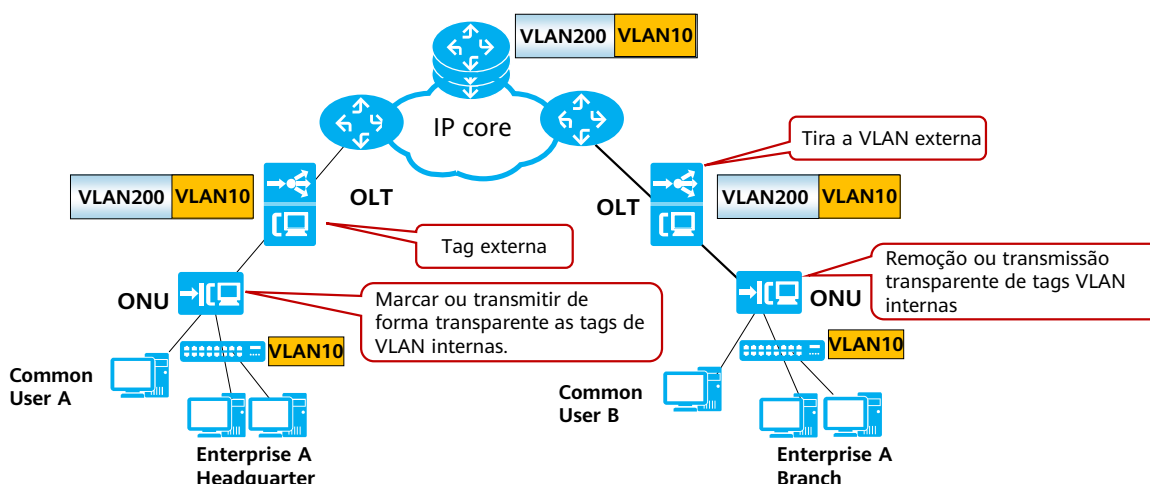


Quadros Ethernet com tags VLAN duplas

- Common VLAN
 - Comum é o atributo padrão de uma VLAN. Ou seja, a VLAN não possui o atributo QinQ ou stacking. Uma VLAN com o atributo comum pode ser usada como uma VLAN de Camada 2 comum. Quando o encaminhamento da Camada 3 é executado, uma interface virtual da Camada 3 pode ser criada com base na VLAN com o atributo comum.
- Stacking VLAN
 - Se o empilhamento de VLAN for usado para estender o número de VLANs ou identificar usuários, o BRAS precisará implementar a autenticação de usuário com marcação dupla.
 - Se o empilhamento de VLAN for usado para fornecer o serviço de atacado de linha alugada, a rede de camada superior deverá funcionar no modo de Camada 2 e encaminhar pacotes com base na VLAN e no endereço MAC.
- QinQ VLAN
 - A VLAN QinQ é geralmente usada para fornecer o serviço de linha privada ou para vincular usuários com precisão.



Exemplo de Aplicação de VLAN QinQ



- Processo do serviço de VLAN QinQ
 - Os usuários podem se comunicar uns com os outros na mesma rede privada (VLAN 10) em diferentes áreas por meio de VLANs QinQ. Os pacotes de serviço são processados da seguinte forma:
 - A empresa A envia pacotes não marcados para a sede.
 - A ONU adiciona (ou transmite de forma transparente) a tag VLAN de rede privada (VLAN 10) ao pacote e envia o pacote upstream para o OLT.
 - O OLT adiciona uma tag de VLAN pública (VLAN 200) ao pacote e transmite o pacote para a rede de camada superior.
 - O dispositivo de rede de camada superior transmite o pacote de forma transparente de acordo com a tag VLAN de rede pública (VLAN 200).
 - Depois de receber os pacotes, o OLT de mesmo nível remove a tag VLAN pública (VLAN 200) dos pacotes e transmite de forma transparente os pacotes para a ONU.
 - A ONU identifica e remove (ou transmite de forma transparente) a tag VLAN de rede privada (VLAN 10) e encaminha o pacote não marcado para o switch na rede privada. Em seguida, o switch encaminha o pacote para o usuário da ramificação da empresa A.
 - Conforme descrito acima, a sede e a filial da empresa A podem se comunicar entre si na VLAN 10 por meio da VLAN QinQ.



Quiz

1. Quais são os métodos de divisão da VLAN?
2. Qual é a diferença entre a porta de tronco e a porta de acesso ao enviar pacotes?
3. Quais são as diferenças entre os quadros de dados VLAN e os quadros de dados Ethernet padrão?
4. O que aconteceu quando a interface do tronco recebeu um quadro não marcado?

- Baseado em porta, MAC, baseado em protocolo e baseado em sub-rede.
- Quando uma porta de tronco envia um pacote, se a tag VLAN do pacote for a mesma que o PVID da porta de envio, a tag VLAN será removida antes que o pacote seja enviado. Se as tags de VLAN forem diferentes, compare a lista de passes permitidos. Se a lista contiver as tags VLAN dos pacotes a serem enviados, os pacotes serão transmitidos de forma transparente. Antes de enviar pacotes, a porta de acesso compara os PVIDs. Se os PVIDs forem os mesmos, a porta de acesso removerá a tag VLAN.
- Os quadros de dados da VLAN são marcados entre o endereço MAC original e o tipo. Em uma rede de comutação, os quadros Ethernet estão em dois formatos: quadros não marcados e quadros não marcados, quadros marcados.
- Adicione o PVID ao quadro de dados e verifique se o allow-pass contém o PVID. Se sim, aceite o quadro. Caso contrário, o pacote será descartado.



Summary

- Em comparação com as LANs tradicionais, as VLANs são usadas para isolar domínios de broadcast e suprimir pacotes de broadcast, reduzindo os custos de mobilidade e alterações. Grupos de trabalho virtuais são criados, que estão além do modo de trabalho das redes tradicionais. Melhora a segurança da comunicação. Melhora a robustez da rede.
- Em um quadro Ethernet padrão, a tag é adicionada entre os campos de endereço MAC de origem e o Tipo. Um quadro Ethernet tem dois formatos: quadro sem tags e quadro com tag. Um quadro sem tag é um quadro que não está marcado com o sinalizador de quatro bytes. Um quadro com tag é um quadro marcado com o sinalizador de quatro bytes.
- As VLANs são divididas com base em portas, endereços MAC, protocolos e sub-redes. Geralmente, as VLANs são divididas com base em portas.
- As regras para receber e encaminhar quadros de dados com tag e sem tag em uma interface de acesso, tronco ou híbrida são diferentes.
- Configuração de diferentes VLANs no switch de camada 3 criando vlan vlan-interface para comunicação.

