Introdução aos Fundamentos e Serviços de Ethernet

HUAWEI

Foreword

- A rede de transporte pode transportar vários serviços do lado do cliente, como voz, vídeo, dados e serviços de acesso à Internet. Geralmente, os serviços de voz são transportados por E1, e outros serviços são transportados por Ethernet.
- Este curso descreve o seguinte :
  - Princípios básicos e tecnologias da Ethernet, incluindo a tecnologia de porta, comutação de camada 2 e VLAN
  - Tecnologias de concatenação e encapsulamento para serviços EoSDH em redes de transporte
  - Tipos de serviços Ethernet e cenários de aplicação suportados pela rede de transporte

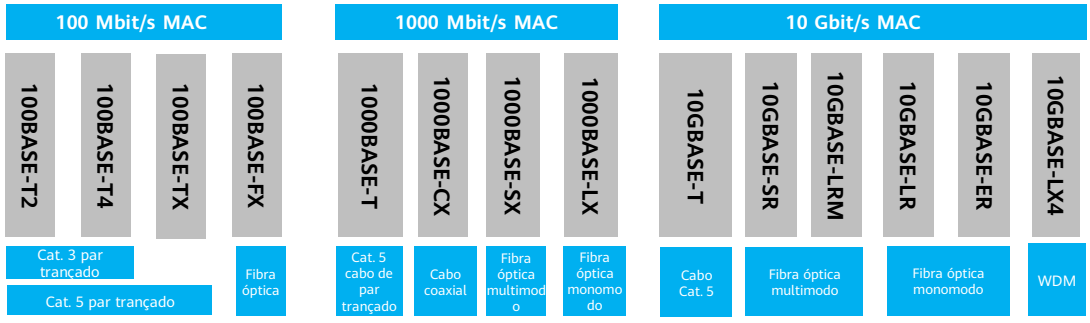
Objectives

- Ao concluir este curso, você será capaz de :
  - Descrever a classificação e os conceitos básicos da Ethernet.
  - Descrever os mecanismos de funcionamento da VLAN e dos switches de camada 2.
  - Explicar as tecnologias de concatenação e encapsulamento da Ethernet.
  - Descrever os cenários de aplicação dos serviços Ethernet.
  - Distinguir os tipos de serviços Ethernet.
  - Descrever os recursos da Ethernet.

Contents

Classificação da Ethernet

- Fast Ethernet (FE) (100 Mbit/s)
- Gigabit Ethernet (GE) (1000 Mbit/s)
- 10 Gigabit Ethernet (10000 Mbit/s)

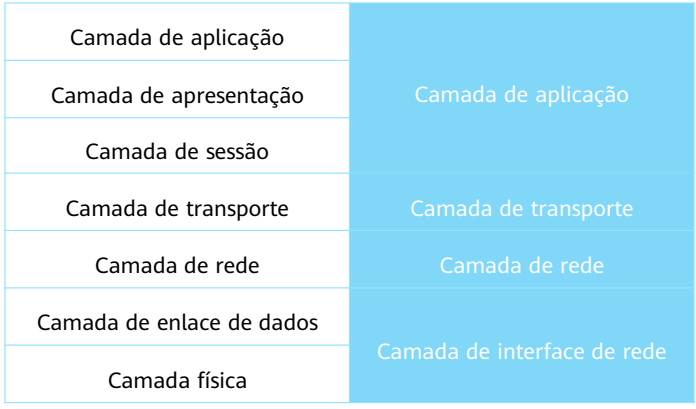


HUAWEI

- No início, a Ethernet fornecia largura de banda de 10 Mbit/s. No entanto, devido ao rápido aumento da velocidade da computação, a largura de banda de 10 Mbit/s ficou sobrecarregada no início da década de 1990. A largura de banda da rede tornou-se o gargalo da comunicação entre dispositivos. Portanto, é imperativo desenvolver uma tecnologia de comunicação com maior velocidade. O estudo da Fast Ethernet começou em 1993 e os padrões foram criados em 1995. A Fast Ethernet herda alguns padrões definidos no 10BASE-T, como o formato de quadro Ethernet, o repetidor de várias portas, a bridge e o cabeamento estruturado, mas aumenta a largura de banda em 10 vezes. Por exemplo, as linhas telefônicas que têm sido amplamente utilizadas não podem ser usadas para transportar sinais de Ethernet rápida. Isso ocorreu porque a atenuação dos sinais Fast Ethernet era muito forte nas linhas telefônicas e a radiação eletromagnética na transmissão excedia os padrões europeus e da FCC. Entre os padrões Fast Ethernet, o 100Base-TX e o 100Base-FX são usados com frequência. O 100BaseTX usa dois pares trançados de Categoria 5.
- No nome 100Base-FX, F refere-se à fibra. O 100Base-FX suporta uma distância de transmissão maior do que o 100Base-TX. Quando o 100Base-FX funciona no modo half duplex e usa uma conexão P2P, sua distância de transmissão é de 412 m devido à limitação dos domínios de colisão. No modo full duplex, a distância de transmissão é de até 2.000 m. Os outros dois padrões de Ethernet rápida são 100BASE-T4 e 100BASE-T2. O 100BASE-T4 usa quatro pares trançados de categoria 3 ou 5. O 100BASE-T2 usa dois pares trançados de Categoria 3. O 100BASE-T4 e o 100BASE-T2 não são mais usados atualmente.
- O padrão Gigabit Ethernet foi lançado oficialmente em 1998 para atender aos crescentes requisitos de largura de banda. Ele aumenta a largura de banda do sinal de fibras ou pares trançados para 1 Gbit/s. O grupo de trabalho IEEE Gigabit Ethernet foi responsável pela padronização dessa tecnologia. Seus padrões técnicos são IEEE 802.3z (fibra óptica e cabo de cobre) e IEEE802.3ab (par trançado). O padrão Gigabit Ethernet usa o protocolo de camada física modificado e a camada MAC semelhante ao padrão Standard Ethernet e Fast Ethernet. Para lidar com o problema dos domínios de colisão e garantir que a Ethernet funcione em uma taxa tão alta, o padrão Gigabit Ethernet é diferente dos padrões anteriores.

- A Gigabit Ethernet pode funcionar no modo half-duplex ou full-duplex. À medida que os preços dos dispositivos relacionados diminuem, ela é amplamente usada na interconexão da camada de backbone, da rede do campus e de dispositivos comuns. Em comparação com os padrões tradicionais de Ethernet padrão, o padrão Gigabit Ethernet mudou muito, mas ainda é considerado uma tecnologia de Ethernet padrão evoluída. Alguns dispositivos têm portas GE, FE e 10 Mbit/s ao mesmo tempo para facilitar a conexão contínua de sinais Ethernet em taxas diferentes.
- A Gigabit Ethernet define três tipos de mídia:
    - 1000Base-LX – fibra óptica de monomodo (com uma distância de transmissão de mais de 3 km)
    - 1000Base-SX – fibra óptica multimodo (com uma distância de transmissão de 300 a 550 m)
    - 1000Base-CX – cabo coaxial (com uma distância de transmissão de mais de 25 m)
    - 1000Base-T – quatro pares trançados sem blindagem (com uma distância de transmissão de 100 m)
- A camada física da LAN é frequentemente usada para a interconexão entre roteadores e switches. Embora seja chamada de LAN, se for usado o módulo óptico 10GBase-LR ou 10GBase-ER, a distância de transmissão pode chegar a 80 km. A taxa de dados da camada física da LAN é de 10,3 Gbit/s, que usa a codificação 64B/66B.
    - 10GBASE-SR (Short Range) usa fibras ópticas multimodo e suporta uma distância de transmissão de 26 a 82 m.
    - 10GBASE-LRM é derivado do IEEE 802.3aq e usa fibras ópticas multimodo de 62,5 µm de grau FDDI. A distância de transmissão pode chegar a 220 m.
    - 10GBASE-LR (Long Range) utiliza fibras ópticas monomodo de 1300 nm e suporta uma distância de transmissão de 10 a 25 km.
    - 10GBASE-ER (Extended Range) usa fibras ópticas monomodo de 1550 nm e suporta uma distância de transmissão de 40 km.
    - 10GBASE-LX4 suporta uma distância de transmissão de 240 a 300 m usando a tecnologia de multiplexação por divisão de comprimento de onda grosso e fibras ópticas multimodo. Ele usa quatro fontes de laser independentes. Os comprimentos de onda operacionais são de aproximadamente 1300 nm, mas são diferentes. A taxa dos quatro sinais de laser é de 3,125 Gbit/s. O 10GBASE-LX4 também é compatível com fibras ópticas de modo único com uma distância de transmissão de 10 km.
    - 10GBASE-T, baseado no IEEE 802.3an, fornece largura de banda de 10 Gbit/s em pares trançados tradicionais não blindados ou blindados. O 10GBASE-T suporta uma distância de transmissão de 56 a 100 m usando pares trançados de categoria 6.
- 10GBASE-SW, 10GBASE-LW e 10GBASE-EW são usados na camada física da WAN e são aplicáveis à interconexão com o equipamento SDH/SONET que usa o OC-192/STM-64 (com a taxa de sinal de 9,953 Gbit/s). Essa interface é usada quando os usuários corporativos desejam usar o sistema SDH/SONET ou WDM para transportar sinais Ethernet 10G.

Modelos TCP/IP e OSI

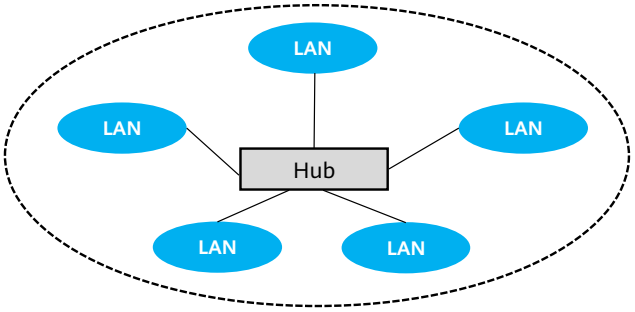


HUAWEI

- A camada física define os padrões relevantes para a mídia física que transporta as comunicações TCP/IP:
  - Os protocolos elétricos/ópticos descrevem as características do sinal, como nível de sinal, potência óptica, tempo de bit, modo de codificação e forma de onda do sinal.
  - As especificações mecânicas são especificações como dimensões do conector e tipos de mídia de transmissão.
- A camada de enlace de dados define os protocolos para controlar a camada física: como o meio é acessado e compartilhado, como os dispositivos no meio são identificados e como os dados são enquadrados antes de serem transmitidos no meio. Os protocolos comuns da camada de enlace de dados incluem IEEE 802.3/Ethernet, IEEE 802.5/Token Ring e FDDI/Fiber Distributed Data Interface.
- A camada de rede define o formato do pacote e o modo de endereçamento e é responsável pelo roteamento dos pacotes de dados na rede.
- A camada de transporte define protocolos para controlar a camada de rede. Tanto a camada de transporte quanto a camada de enlace de dados são capazes de realizar o controle de tráfego e o controle de erros. O protocolo de enlace de dados controla o tráfego no enlace de dados, que é o meio físico que conecta dois dispositivos. Já o protocolo da camada de transporte controla o tráfego no link lógico, que é a conexão E2E entre dois dispositivos cujo link lógico pode atravessar uma série de links de dados.
- A camada de aplicação no modelo TCP/IP corresponde à camada de sessão, à camada de apresentação e à camada de aplicação no modelo OSI. A camada de aplicativos fornece interfaces que os aplicativos usam para acessar a rede.

Domínio de Colisão

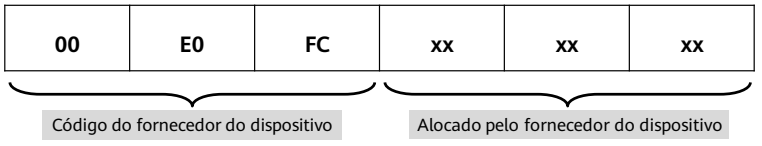
- Todos os dispositivos competem pelo mesmo meio de transmissão. Apenas um dispositivo pode enviar dados por vez.



- Em um domínio de colisão, uma colisão ocorre quando pacotes de dados de diferentes dispositivos são enviados ao meio compartilhado ao mesmo tempo.
- Cada dispositivo na rede pode enviar dados somente quando a rede está ociosa. Portanto, a possibilidade de colisões é maior e a eficiência da rede é menor quando há mais dispositivos na rede.
- Os pontos que compartilham o mesmo canal de informações formam um domínio de colisão. Por exemplo, se todas as portas de um hub pertencerem ao mesmo domínio de colisão, nenhuma porta poderá receber e enviar dados ao mesmo tempo.

Endereço MAC Ethernet

- Um endereço MAC é um endereço globalmente exclusivo de 48 bits.
- Um endereço MAC também pode ser um número hexadecimal de 12 dígitos.

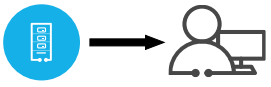


- Endereço MAC de transmissão: FF-FF-FF-FF-FF-FF
- Se o oitavo bit for 1, o endereço é um endereço multicast.

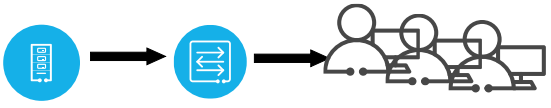
- MAC: Media Access Control
  - Um endereço MAC é o endereço físico de um dispositivo de rede. Os endereços MAC são gerenciados e alocados pelo IEEE e são globalmente exclusivos.
  - Um endereço MAC consiste em duas partes: o código do fabricante do dispositivo é usado para identificar exclusivamente o fabricante do dispositivo; os outros bytes são alocados pelos fabricantes do dispositivo.
  - Um endereço MAC tem 48 bits e geralmente é representado como uma cadeia de 12 dígitos em notação hexadecimal pontilhada.
  - Os primeiros 24 bits indicam o identificador do fabricante do dispositivo, e os últimos 24 bits são alocados pelo fabricante do dispositivo.

Endereçamento Ethernet

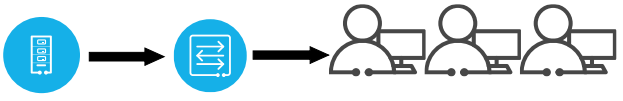
- Unicast: O endereço de destino aponta para um único host.



- Broadcast: O endereço de destino aponta para todos os hosts.



- Multicast: O endereço de destino aponta para um grupo de hosts.

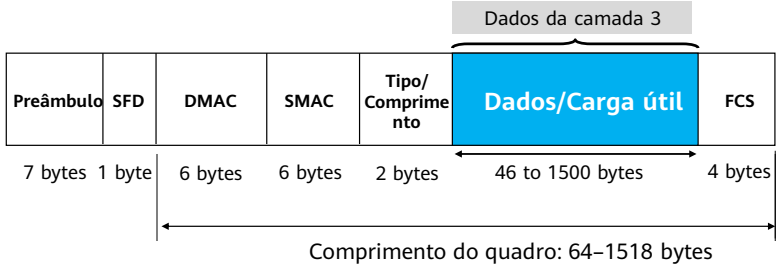


HUAWEI

- Os endereços MAC de destino nos quadros Ethernet são classificados em três tipos :
  - Endereço Unicast: somente o host especificado pode receber e processar o quadro.
  - Endereço de Broadcast: todos os hosts podem receber e processar o quadro.
  - Endereço Multicast: todos os hosts em um grupo multicast especificado podem receber e processar o quadro.

Estrutura do Quadro Ethernet e Distância de Transmissão

- Tipos comuns de quadros Ethernet:
  - Quadro Ethernet II – campo Tipo > 1500
  - Quadro IEEE 802.3 – campo Comprimento <= 1500



- A distância máxima de transmissão depende de fatores como a qualidade da linha e a atenuação do sinal.

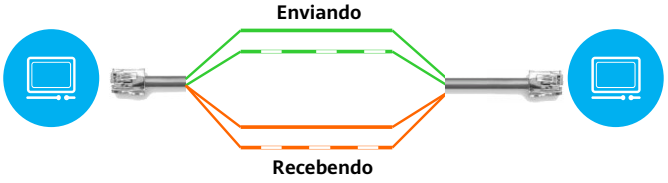
HUAWEI

- Campos de um quadro Ethernet :
  - Preâmbulo, que tem 7 bytes de comprimento. O padrão de bits de cada byte é 10101010, que é usado para sincronização de tempo entre a extremidade de transmissão e a extremidade de recepção.
  - SFD: delimitador de início de quadro (Start-of-Frame Delimiter). O padrão de bits é 10101011, usado para informar ao terminal de recepção que o próximo byte é o início do quadro.
  - DMAC: endereço MAC de destino. O comprimento é de 6 bytes.
  - SMAC: endereço MAC de origem. O comprimento é de 6 bytes.
  - Comprimento/tipo. O comprimento é de 2 bytes. Se Comprimento/Tipo > 1500, indica o tipo do quadro de dados (o tipo de protocolo da camada superior, por exemplo, 0x0800 indica que os dados da Camada 3 são um pacote IP). Se Comprimento/Tipo <= 1500, indica o comprimento dos dados e o campo de preenchimento no quadro de dados.
  - Dados: o comprimento é de 46 a 1500 bytes. Se o comprimento do campo Dados for menor que 46 bytes, o campo deverá ser preenchido para garantir que o comprimento do quadro inteiro seja de pelo menos 64 bytes.
  - FCS: sequência de verificação de quadro (Frame Check Sequence). O comprimento é de 4 bytes.

- Devido à limitação do algoritmo CSMA/CD, o comprimento do quadro da Ethernet padrão não deve ser inferior a 64 bytes, o que é determinado pela distância máxima de transmissão e pelo mecanismo de funcionamento da detecção de colisão. O uso de um comprimento mínimo de quadro evita situações em que uma estação termina de enviar o último bit de um pacote, mas o primeiro bit do pacote ainda não chegou à estação remota. Nesse momento, a estação remota percebe que a linha está ociosa e começa a enviar dados, o que leva a uma colisão. O protocolo da camada superior deve garantir que o comprimento mínimo do campo de dados em um quadro Ethernet seja de 46 bytes. Se o comprimento for menor que 46 bytes, o protocolo da camada superior deverá preencher os bits redundantes para que o comprimento do campo de dados atinja 46 bytes. Um campo de dados de 46 bytes, um cabeçalho de quadro Ethernet de 14 bytes e um código de verificação de 4 bytes formam um quadro Ethernet mínimo de 64 bytes. Em um quadro Ethernet, o comprimento máximo do campo de dados é de 1.500 bytes.

Modo Duplex

- Os modos duplex da Ethernet incluem o modo half-duplex e o modo full-duplex.
- No modo full-duplex, os dados podem ser transmitidos em velocidade máxima em ambas as direções ao mesmo tempo. Portanto, a taxa de transferência é dobrada.

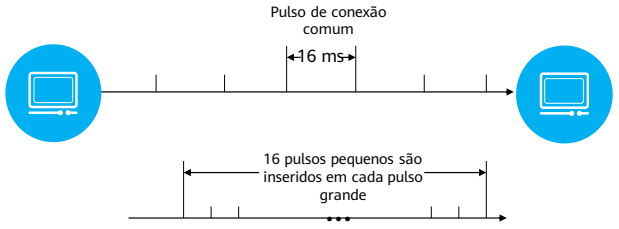


HUAWEI

- Modo half-duplex
  - Um dispositivo pode receber ou enviar dados em uma direção de cada vez.
  - CSMA/CD é necessário.
  - Esse modo se aplica à transmissão de curta distância.
- Modo full-duplex
  - Um dispositivo pode receber e enviar dados simultaneamente.
  - A taxa de transferência é dobrada em comparação com o modo half-duplex.
  - Esse modo não limita a distância de transmissão.

Auto-negociação

- O mecanismo básico da função de negociação automática é encapsular as informações de negociação em uma série de pulsos de teste de integridade de conexão modificados, que são chamados de pulsos de conexão rápida.



Um pulso grande é um pulso de conexão comum, e um pulso pequeno é um pulso de conexão rápida.

HUAWEI

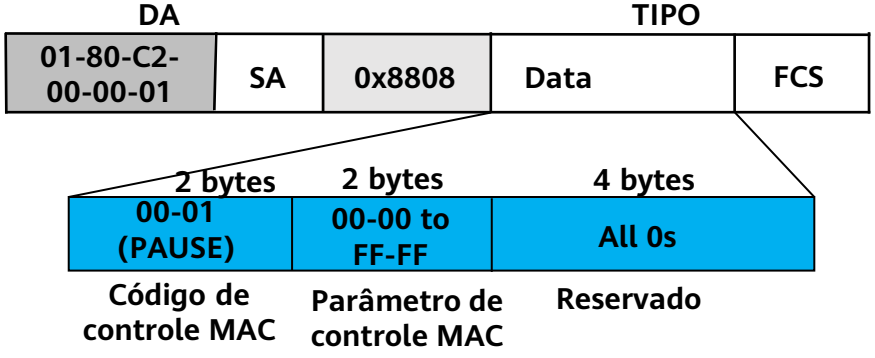
- O IEEE 802.3u definiu pela primeira vez a negociação automática, o que significa que a negociação automática foi introduzida na Ethernet 100M, mas a negociação automática poderia ser compatível com 10BASE-T. Em 1999, a negociação automática foi estendida ao IEEE 802.3ab (o protocolo Gigabit Ethernet). Para dispositivos que suportam várias taxas de transmissão (como 10 Mbit/s e 100 Mbit/s) e vários modos de trabalho (half-duplex e full-duplex), os dois dispositivos conectados podem usar o mecanismo de negociação automática para determinar o melhor modo de comunicação, sendo que "o melhor" significa que uma taxa de transmissão alta é melhor do que uma taxa de transmissão baixa. Para a mesma taxa, o modo full-duplex é melhor do que o modo half-duplex.
- Um dispositivo sem suporte à negociação automática pode não conseguir negociar com um dispositivo com suporte à negociação automática. Um dispositivo compatível com a negociação automática pode detectar a taxa do dispositivo conectado com base no sinal recebido, mas não pode detectar o modo full ou half duplex dele. Nesse momento, um dispositivo pode funcionar no modo full-duplex e outro dispositivo pode funcionar no modo half-duplex. Essa situação é chamada de incompatibilidade de modo duplex. Embora eles possam se comunicar, a eficiência da comunicação é baixa.

Controle de Tráfego

- Objetivo: o controle de tráfego evita a perda de quadros de dados em caso de congestionamento.
- Implementação :
  - Modo half-duplex: A tecnologia de back pressure é usada para controle de tráfego.
  - Modo full-duplex: Os quadros PAUSE são usados para controle de tráfego, em conformidade com o protocolo padrão IEEE 802.3x.

HUAWEI

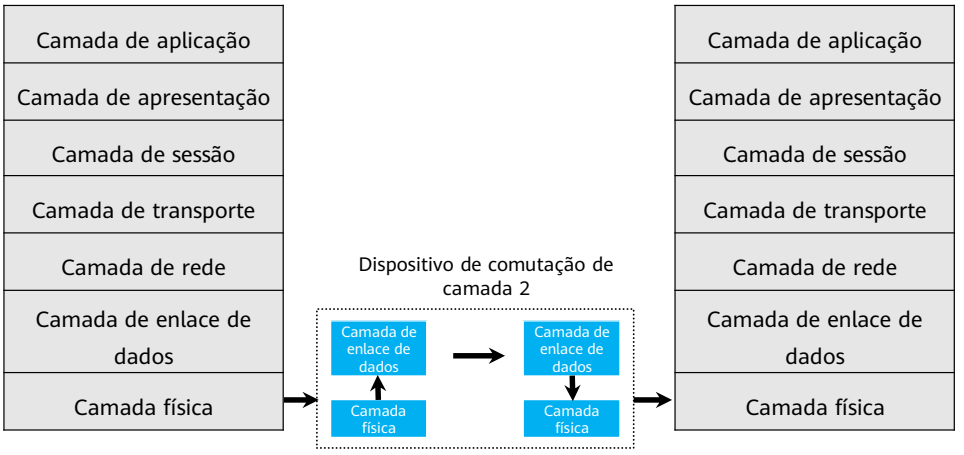
- Se ocorrer um congestionamento na fila de recebimento de uma porta Ethernet (os dados no buffer da porta de entrada excedem um determinado limite), a porta Ethernet pode enviar um sinal de jamming para simular o congestionamento da linha. Isso faz com que o dispositivo conectado reduza sua taxa de transmissão e evita a perda de pacotes.
- Uma porta Ethernet no modo half-duplex usa a tecnologia de back pressure para controlar o tráfego. Atualmente, a Ethernet half-duplex é raramente usada.
- O padrão IEEE802.3x define a tecnologia de quadro PAUSE para implementar o controle de tráfego no modo full-duplex. Um quadro PAUSE usa um endereço multicast reservado e não é encaminhado por uma bridge ou switch. Dessa forma, o quadro PAUSE não gera nenhuma informação adicional.



- Um quadro PAUSE pode solicitar que a estação remota pare de enviar dados para a extremidade local. Por exemplo, existe uma conexão full-duplex entre o dispositivo A e o dispositivo B. Se a taxa de envio de quadros de dados pelo dispositivo A for maior do que a capacidade de processamento do dispositivo B, ocorrerá um congestionamento na fila de recebimento do dispositivo B após um período de tempo. Então, o dispositivo B envia um quadro PAUSE ao dispositivo A, solicitando que o dispositivo A pare de enviar dados em um determinado período de tempo. Um quadro PAUSE usa o formato de quadro Ethernet padrão e é identificado pelo valor do campo Type (Tipo). O campo de parâmetro de controle MAC contém 16 bits, indicando a duração pela qual os quadros de dados não são enviados (unidade: 512 bits). O valor varia de 00-00 a FF-FF (notação hexadecimal). É necessário um campo reservado de 42 bytes para preencher o quadro PAUSE e atender ao requisito de comprimento mínimo do quadro Ethernet.

Contents

Estrutura de um Dispositivo de Comutação de Camada 2

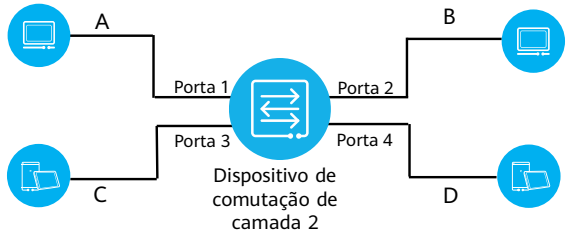


HUAWEI

- Um switch ou bridge Ethernet tem as seguintes funções:
  - Aprende os endereços MAC de origem dos quadros
  - Encaminha quadros com base nos endereços MAC de destino
  - Filtra quadros com base nos endereços MAC de destino
  - Inunda um quadro com base no endereço MAC de destino
- Um hub funciona na camada física e um switch funciona na camada de enlace de dados. Hub: um hub funciona no modo half-duplex, inunda pacotes e é ineficiente. Switch: um switch funciona no modo full-duplex, gera uma tabela CAM (Content Addressable Memory – Memória Endereçável de Conteúdo) ao aprender endereços MAC, evita colisões e cria um domínio de broadcast. Para oferecer maior largura de banda, os hubs foram amplamente substituídos por switches.

Funcionamento dos Dispositivos da Camada 2 (1)

- Autoaprendizagem com base no endereço MAC de origem



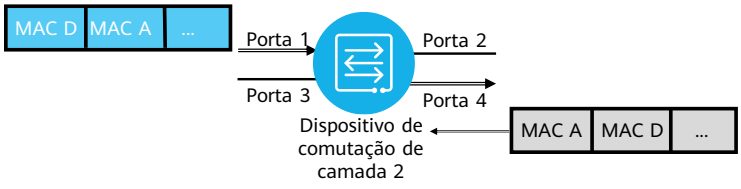
Endereço MAC	Porta
MAC A	1
MAC B	2
MAC C	3
MAC D	4

HUAWEI

- Cada dispositivo de comutação da camada 2 tem uma tabela CAM que define o mapeamento entre endereços MAC e portas e encaminha quadros com base na tabela CAM.
- Ao examinar o endereço MAC de origem de cada quadro recebido, um dispositivo de comutação da camada 2 aprende os endereços MAC dos dispositivos conectados. Quando um novo dispositivo de comutação da camada 2 é ligado, sua tabela CAM está vazia. Ao receber um quadro de dados de um dispositivo conectado, o dispositivo de comutação da camada 2 examina o endereço MAC de origem do quadro recebido e descobre o endereço MAC do dispositivo conectado. Em seguida, o dispositivo de comutação da camada 2 cria uma entrada na tabela CAM para registrar o mapeamento entre a porta e o endereço MAC do dispositivo conectado à porta. Com o tempo, o dispositivo de comutação da Camada 2 aprende os endereços MAC de todos os dispositivos conectados.
- Na figura, se o PC A enviar um quadro para o PC D, o dispositivo receberá o quadro da porta 1. Primeiro, o dispositivo verifica o endereço MAC de destino do quadro e, em seguida, consulta a tabela CAM. Se nenhuma entrada na tabela CAM corresponder ao endereço MAC de destino, o dispositivo encaminha o quadro para fora de todas as portas, exceto a porta 1, e adiciona o endereço MAC de origem do quadro à tabela CAM. O mapeamento entre a porta 1 e o endereço MAC do PC A é criado. O dispositivo estabelece a tabela CAM usando o método anterior.
- Se nenhuma entrada na tabela CAM corresponder ao endereço MAC de destino do quadro de dados recebido, o dispositivo inundará o quadro em todas as outras portas, exceto na porta em que o quadro foi recebido. O dispositivo aprende os endereços MAC por meio de flooding. O flooding não causa a perda de quadros de dados porque o dispositivo é transparente em toda a rede quando faz o flooding.
- Depois de aprender os endereços MAC por algum tempo, o dispositivo estabelece uma tabela CAM e encaminha os quadros de forma estável, consultando a tabela CAM da porta mapeada para o endereço MAC de destino, melhorando a eficiência do encaminhamento.

Funcionamento dos Dispositivos da Camada 2 (2)

- Encaminhamento com base no endereço MAC de destino



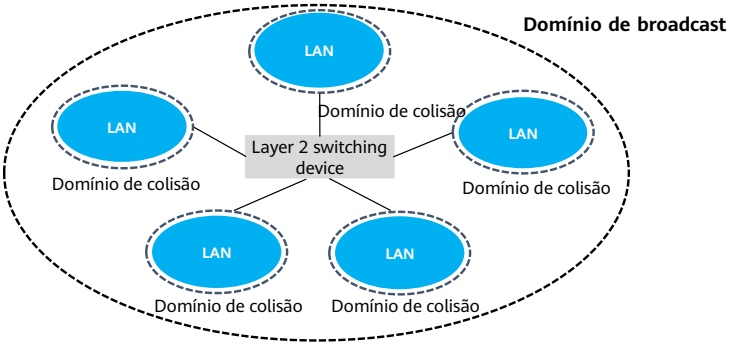
- Quando um dispositivo de comutação de camada 2 recebe um quadro de dados, ele lê o endereço MAC de destino do quadro de dados e compara o endereço MAC na tabela CAM.
  - Se o endereço MAC de destino for encontrado na tabela CAM, o quadro será encaminhado diretamente para fora da porta correspondente.
  - Se o endereço MAC de destino não existir na tabela CAM, o quadro será inundado em todas as portas, exceto na porta que o recebe.
- Mecanismo de Aging
  - A capacidade da tabela CAM é limitada. Ela contém apenas um determinado número de entradas. Os dispositivos de comutação da camada 2 fornecem um cronômetro para cada entrada de encaminhamento de MAC. O cronômetro diminui a partir de um valor inicial. Cada vez que a entrada é usada (a entrada corresponde a um quadro de dados recebido), o cronômetro é reiniciado. Se a entrada não for correspondida por um longo período e o cronômetro chegar a zero, a entrada será excluída.
  - O valor padrão do cronômetro é de 5 minutos, ou seja, o tempo de aging é de 5 minutos.

Modo de Comutação

- Cut-Through
  - O dispositivo de comutação da Camada 2 começa a encaminhar os pacotes imediatamente após receber um endereço de destino. O atraso é curto.
  - O dispositivo de comutação da camada 2 não detecta erros.
- Store-and-Forward
  - Depois de receber um quadro de dados completo, o dispositivo de comutação da Camada 2 começa a encaminhar o quadro de dados. O atraso é longo e depende do comprimento do quadro de dados.
  - O dispositivo de comutação da camada 2 detecta erros e descarta os quadros com erros.
- Fragment-free
  - Depois de receber os primeiros 64 bytes (o comprimento mínimo do quadro) de um quadro de dados, o dispositivo de comutação da camada 2 começa a encaminhar o quadro de dados.
  - Esse modo tem as vantagens dos modos cut-through e store-and-forward.

- Modo Cut-through: Os dispositivos de comutação da camada 2 que operam no modo cut-through verificam apenas os primeiros 6 bytes de um quadro. Os primeiros 6 bytes representam o endereço MAC de destino, o que é suficiente para encaminhar os quadros de dados. O modo cut-through tem um atraso curto, mas os dispositivos podem encaminhar quadros com erros porque encaminham quadros de dados sem verificar se há erros.
- Modo Store-and-forward: Antes de encaminhar os quadros de dados, os dispositivos no modo store-and-forward verificam se há erros para que apenas os quadros de dados corretos sejam encaminhados. No entanto, a eficiência do encaminhamento é baixa.
- Modo Fragment-free: Esse modo tem as vantagens do modo cut-through e do modo store-and-forward. Assim como no modo cut-through, os dispositivos no modo fragment-free podem encaminhar um quadro de dados depois de receber os primeiros 64 bytes, em vez de esperar pelo recebimento do quadro de dados completo. Assim como no modo store-and-forward, os dispositivos no modo fragment-free verificam se há erros nos primeiros 64 bytes e descartam os quadros com erros.

Domínio de Broadcast



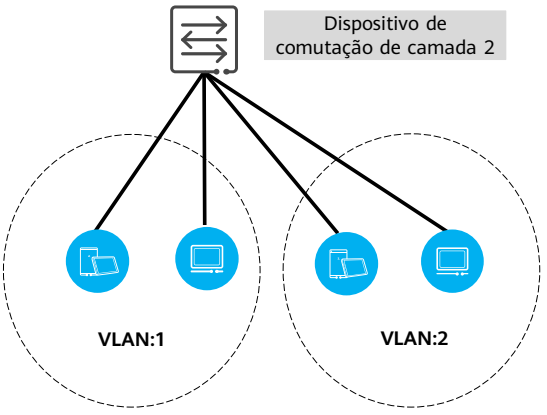
- Um dispositivo de camada 2 encaminha os quadros de dados recebidos com base nos endereços MAC. Portanto, um domínio de colisão é limitado a uma única porta, mas um domínio de broadcast não é limitado.

HUAWEI

- Conforme mostrado na figura, um dispositivo de comutação de camada 2 divide uma rede em vários domínios de colisão. Se cada porta do dispositivo se conectar a um hub, cada porta será um domínio de colisão. O dispositivo e as LANs conectadas formam um domínio de broadcast. Qualquer pacote de broadcast é inundado em todo o domínio de broadcast e todos os dispositivos podem receber o pacote de broadcast. O excesso de pacotes de broadcast transmitidos em um domínio de broadcast pode ocupar a largura de banda excessiva da rede e reduzir a eficiência do encaminhamento. Isso ocorre porque os pacotes de difusão também são enviados para os hosts que não desejam esses pacotes.

VLAN

- Objetivos da atribuição de VLAN:
  - Aumentar a segurança
  - Melhorar a estabilidade da rede
  - Suprimir broadcast
- Modos de atribuição de VLAN:
  - Baseada em porta
  - Baseado em endereço MAC
  - Baseado em protocolo de camada 3
  - Baseado em sub-rede IP

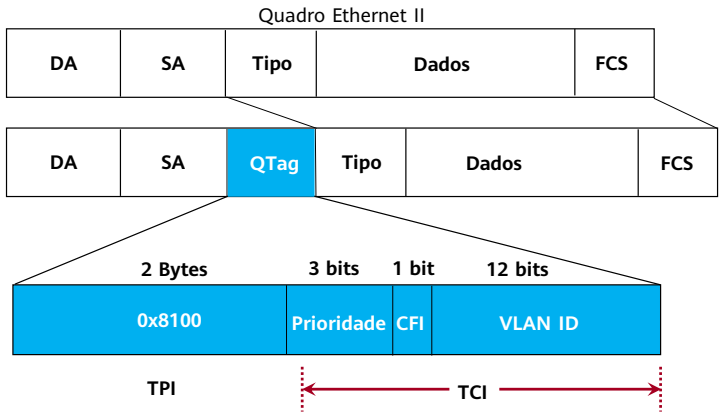


HUAWEI

- Vantagens: A tecnologia VLAN pode resolver o problema dos domínios de colisão e aumentar a segurança da comunicação.
  - Aumenta a segurança da comunicação: Os quadros de dados com uma VLAN ID não serão recebidos por hosts em outras VLANs, protegendo a segurança dos dados.
  - Aumenta a estabilidade da rede: À medida que a escala da rede se expande, algumas falhas de rede podem afetar negativamente toda a rede. Com a introdução de VLANs, as falhas de rede em uma VLAN não afetam outras VLANs.
  - Supressão de broadcast: Ao criar VLANs, o domínio de broadcast pode ser limitado às portas que pertencem à mesma VLAN.
- Desvantagens: Uma rede física é logicamente dividida em várias redes VLAN pequenas para melhorar o uso da largura de banda. No entanto, os hosts em diferentes VLANs não podem se comunicar entre si.

- Modos de atribuição de VLAN :
    - As VLANs podem ser atribuídas com base nas portas do switch Ethernet. Por exemplo, as portas 1 a 4 pertencem à VLAN A, as portas 5 a 17 pertencem à VLAN B e as portas 18 a 24 pertencem à VLAN C. Obviamente, as portas que pertencem à mesma VLAN podem ser descontínuas. O administrador determina como atribuir VLANs.
    - A atribuição de VLAN baseada em endereço MAC baseia-se no endereço da camada de rede ou no tipo de protocolo (se houver suporte para vários protocolos) de cada host. Embora essa atribuição possa se basear no endereço de rede, como o endereço IP, ela não é uma rota. Portanto, não confunda essa atribuição com a rota na camada de rede. Embora o endereço IP de cada pacote de dados seja verificado, ele não é uma rota. Portanto, nenhum protocolo de roteamento, como RIP e OSPF, é usado. Em vez disso, ele executa a comutação de ponte de acordo com o algoritmo de Spanning Tree.
    - A vantagem da atribuição de VLAN baseada em protocolo da Camada 3 é que, quando a localização física de um usuário muda, a VLAN à qual o usuário pertence não precisa ser reconfigurada. Além disso, as VLANs podem ser classificadas com base nos tipos de campos de protocolo nos quadros de dados da Camada 2. Os campos de protocolo nos dados da camada 2 podem ser usados para determinar os protocolos de rede da camada superior, como IP ou IPX. Quando vários protocolos, como rede IP e IPX, estão em execução em uma rede física, esse método de divisão de VLAN pode ser usado.
    - Com base nas sub-redes IP, as VLANs são determinadas com base nos endereços IP dos pacotes. Todos os pacotes da mesma sub-rede IP pertencem à mesma VLAN. Dessa forma, os usuários da mesma sub-rede IP podem ser alocados na mesma VLAN.

Tag VLAN 802.1Q



Quadro Ethernet com uma tag IEEE 802.IQ

HUAWEI

- O cabeçalho da tag 802.1Q contém as seguintes informações:
  - Campo Tag Protocol Identifier (TPID): 2 bytes.
  - Campo Tag Control Information (TCI): 2 bytes.
- O TPID indica a etiqueta 802. 1Q. O valor de TPID é fixado em 0x8100.
- A TCI contém as seguintes informações de controle:
  - Priority (PCP): indica a prioridade de um quadro. Há três bits, indicando as oito prioridades de 0 a 7.
  - CFI (criteria format identifier): É usado para distinguir o formato de codificação dos endereços no quadro de dados. Se o valor de CFI for 0, o quadro Ethernet é um quadro Ethernet padrão. Se o valor for 1, isso indica que o quadro é um quadro token ring ou FDDI.
  - VLAN ID: indica o valor da VLAN ID. Há 12 bits no total. Há suporte para um máximo de 4096 VLANs.
- Há dois tipos de quadros Ethernet:
  - Quadro sem tag: um quadro sem uma tag 802.1Q.
  - Quadro com tag: um quadro com uma tag 802.1Q.

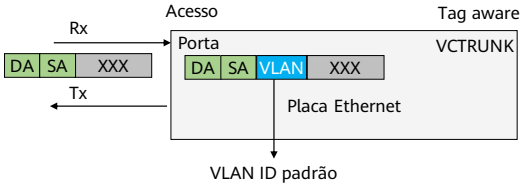
Processamento da Porta Ethernet (1)

Tipo de Porta	Tag	Untag
Tag aware (entrada)	Transmitir de forma transparente	Descarta
Tag aware (saída)	Transmitir de forma transparente	-
Acesso (entrada)	Descarta	Adiciona a VLAN ID padrão
Acesso (saída)	Retire a VLAN ID	-
Híbrida (entrada)	Transmitir de forma transparente	Adiciona a VLAN ID padrão
Híbrida (saída)	Se a VLAN ID for a mesma que a VLAN ID padrão, remova a VLAN ID; caso contrário, transmita a VLAN ID de forma transparente.	-

- Os atributos da porta UNI incluem Tag aware, Access e Hybrid.
  - Tag Aware: Recebem apenas quadros com marcação de VLAN e geralmente se conectam a um switch.
  - Access: Os quadros marcados não podem ser reconhecidos, e um PC geralmente está conectado.
  - Hybrid: Tanto os quadros marcados quanto os não marcados podem ser reconhecidos.

Processamento da Porta Ethernet(2)

- Acesso
  - Porta1 <-> VCTRUNK + VLAN padrão (VLAN = 1-4095)
  - Configuração de atributos de porta: Porta - Acesso, VCTRUNK – Tag aware

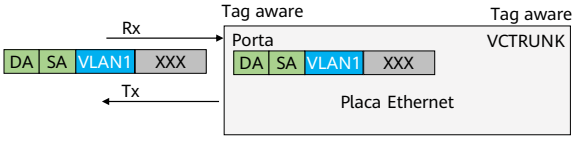


HUAWEI

- Na direção de recepção:
  - Adicionar a VLAN ID padrão aos quadros não marcados recebidos.
  - Descartar quadros marcados recebidos.
- Na direção de transmissão:
  - Retirar a VLAN ID original.

Processamento da Porta Ethernet (3)

- Tag aware
  - Porta1 + VLAN1 <-> VCTRUNK + VLAN1 (VLAN = 1-4095)
  - Configuração de atributos de porta: Porta – Tag aware, VCTRUNK – Tag aware

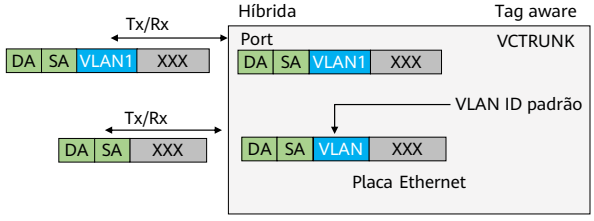


HUAWEI

- Na direção de recepção :
  - Descartar quadros sem marcação.
  - Transmitir quadros marcados de forma transparente.
- Na direção de transmissão :
  - Transmitir quadros de forma transparente.

Processamento da Porta Ethernet (4)

- Híbrida
  - Porta1 + VLAN1 <-> VCTRUNK + VLAN1
  - Porta1 <-> VCTRUNK + VLAN padrão (VLAN = 1–4095)
  - Configuração de atributos de porta: Porta – Híbrida, VCTRUNK – Tag aware



HUAWEI

- Na direção de recepção :
  - Adicionar a VLAN ID padrão aos quadros não marcados recebidos.
  - Transmitir quadros marcados de forma transparente.
- Na direção de transmissão :
  - Retirar a VLAN ID se a VLAN ID no quadro recebido for a mesma que a VLAN ID padrão.
  - Transmitir o quadro recebido de forma transparente se a VLAN ID no quadro recebido for diferente da VLAN ID padrão.

Vantagens e Desvantagens da VLAN

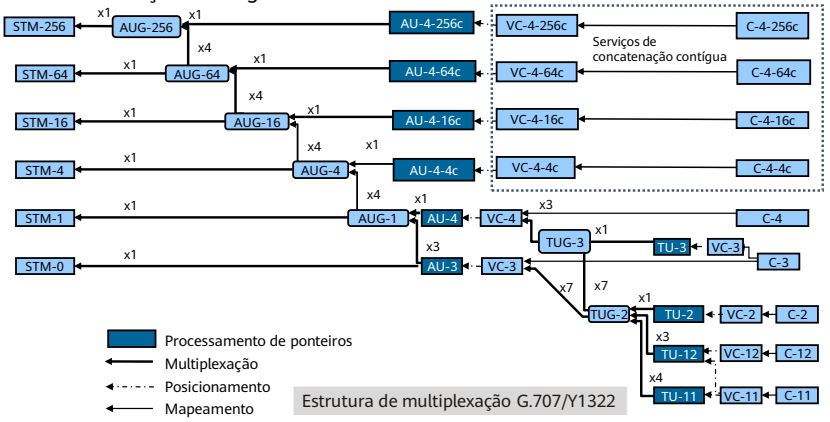
- Vantagens: A tecnologia VLAN pode resolver o problema dos domínios de colisão e aumentar a segurança da comunicação.
- Desvantagens: Uma rede física é logicamente dividida em várias redes VLAN pequenas para melhorar o uso da largura de banda. No entanto, os hosts em diferentes VLANs não podem se comunicar entre si.
- Questão: Como os hosts em diferentes VLANs podem se comunicar uns com os outros?

- Se os hosts em diferentes VLANs precisarem se comunicar entre si, deverão ser usados switches de Camada 3.

Contents

Visão Geral da Tecnologia de Concatenação

- Objetivo da concatenação: Usar a rede SDH para transmitir serviços de grande granularidade e implementar a alocação de largura de banda sob demanda.



HUAWEI

- A concatenação é um recurso importante do SDH. Ela é usada para transmitir sinais de clientes cuja capacidade é maior do que C-4 (149760 kbit/s) e não causa danos adicionais aos sinais de clientes. A concatenação é um processo de combinação que reúne vários contêineres para que sua capacidade combinada possa ser usada como um único contêiner que mantém a integridade da sequência de bits.
- A transmissão do serviço de concatenação é baseada principalmente no novo protocolo G.707 da ITU-T.

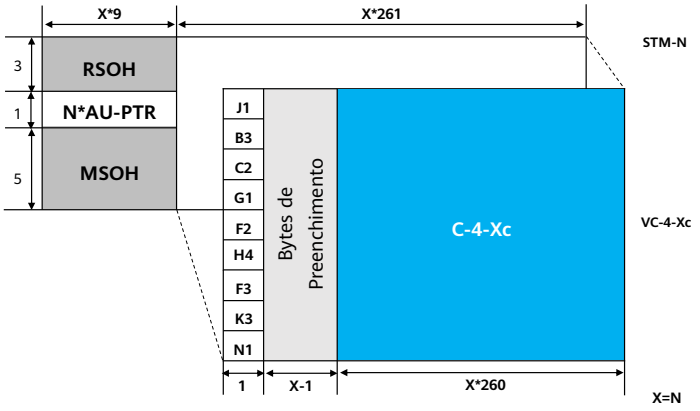
Classificação das Tecnologias de Concatenação

- Concatenação contígua
  - A implementação é simples e a eficiência da transmissão é alta.
  - Há apenas uma trilha E2E, e o serviço não tem atraso.
  - Toda a rede de transporte precisa suportar a concatenação contígua. Caso contrário, os serviços não estarão disponíveis.
- Concatenação virtual
  - Os dispositivos nas extremidades de transmissão e recepção precisam oferecer suporte à concatenação virtual.
  - Os serviços podem ser transmitidos em vários caminhos.
  - Esse modo tem alta sobrecarga, baixa eficiência de transmissão e diferença de atraso entre os serviços transmitidos em caminhos diferentes.

- A concatenação contígua é realizada no mesmo STM-N, concatenando C-n contíguos em um C-n-Xc para formar uma única estrutura para transmissão. É possível saber que os VC-4-Xc concatenados de forma contígua compartilham o mesmo conjunto de POH. Portanto, a concatenação contígua deve manter a largura de banda contínua durante todo o processo de transmissão. Essa tecnologia exige o suporte de todos os dispositivos da rede, e a maioria dos dispositivos existentes não tem esse recurso.
- Na concatenação virtual, os VC-ns (que podem ser da mesma rota ou de rotas diferentes) distribuídos em diferentes STM-Ns podem ser concatenados para formar um VC-n-Xv virtual para transmissão. Cada VC-n na concatenação virtual tem uma estrutura independente e seu próprio POH, formando uma estrutura VC-n completa. A concatenação virtual de VC-n é equivalente à intercalação de VC-n. Em termos de equipamento, somente os dispositivos em ambas as extremidades precisam suportar a tecnologia de concatenação.

Mecanismo de Concatenação Contígua

- Estrutura do quadro na concatenação contígua SDH

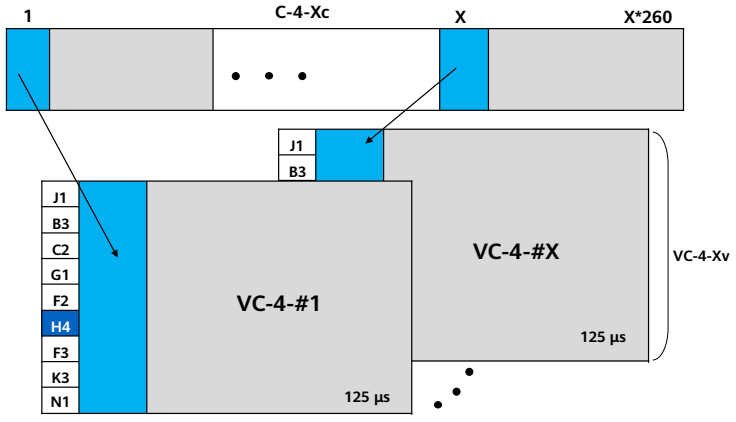


HUAWEI

- A indicação de concatenação no ponteiro AU-4 é usada para indicar que várias cargas úteis C-4 transportadas em um único VC-4-Xc devem ser mantidas juntas. A capacidade disponível do mapeamento é X vezes a capacidade do C-4 (por exemplo, quando X=4, a capacidade é de 599.040 kbit/s; quando X=16, a capacidade é de 2.396.160 kbit/s).
- As colunas 2 a X do VC-4-Xc são bits de preenchimento fixo, e a coluna 1 do VC-4-Xc é usada como POH. Esse POH é alocado para o VC-4-Xc.
- O primeiro AU-4 no AU-4-Xc deve ter um valor de ponteiro normal. Todos os AU-4s subsequentes no AU-4-Xc devem definir seus ponteiros como indicações de concatenação. Ou seja, os bits 1-4 são definidos como "1001", os bits 5-6 não são especificados e os bits 7-16 são definidos como "1111111111". A indicação de concatenação especifica que o processador de ponteiro deve executar as mesmas operações que as do primeiro AU-4 no AU-4-Xc.

Mecanismo da Concatenação Virtual

- Estrutura do quadro na concatenação virtual SDH



HUAWEI

- Um VC-4-Xv fornece uma capacidade de X vezes de 149.760 kbit/s para a área de carga útil de X contíguos C-4 (C-4-Xc), e o contêiner é mapeado para X VC-4s independentes que constituem o VC-4-Xv. Cada VC-4 tem seu próprio POH. A especificação do POH de cada VC-4 é a mesma do VC-4 comum. O byte H4 no POH é usado como o número de sequência especificado e a indicação de multiframe (MFI - multiframe indication) da concatenação virtual.
- A MFI é gerada em todos os VC-4s do VC-4-Xv. Ela é transmitida nos bits 5-8 do byte H4 em todos os VC-4s. A indicação de multiframe é numerada de 0 a 15.

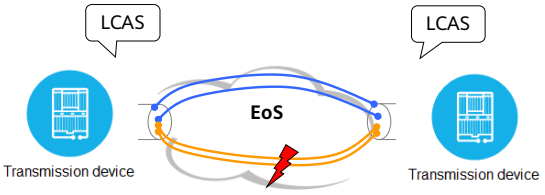
Aplicações das Tecnologias de Concatenação

- Concatenação contígua
  - Quando o OptiX OSN está interconectado a equipamentos de dados no modo de concatenação contígua, por exemplo, interconectado a um roteador com portas PoS STM-4, a placa de linha do OptiX OSN pode acessar e processar diretamente os serviços VC4-Xc sem conversão.
- Concatenação virtual
  - As placas EoS do equipamento OptiX OSN formam um VCTRUNK no modo de concatenação virtual.

- Devido aos requisitos de processamento dos serviços de concatenação contígua SDH, todos os NEs intermediários para os serviços E2E devem ser capazes de processar os serviços VC4-Xc. No entanto, é difícil para a rede atender a esse requisito. Portanto, os serviços são convertidos de VC4-Xc para VC4-Xv na borda da rede que fornece acesso aos serviços de concatenação contíguos. Nesse caso, os sites intermediários da rede não precisam processar VC4-Xcs e só precisam processar VC4s individuais. A conversão entre VC4-Xcs e VC4-Xvs é realizada na borda da rede.
- Atualmente, as placas de linha SDH do OptiX OSN suportam o acesso a serviços de concatenação contíguos.
- A maioria das placas de dados EoS dos dispositivos OptiX OSN utiliza o modo de concatenação virtual para formar VCTRUNKs. A rede é flexível e suporta transmissão por vários caminhos. Além disso, as placas de dados podem ser usadas com o LCAS para ajustar a largura de banda do link.

LCAS - Link Capacity Adjustment Scheme

- Função LCAS
  - A largura de banda pode ser ajustada sob demanda, e o aumento ou a diminuição dinâmica dos membros do VCTRUNK não afeta os serviços. Quando um membro de um grupo de concatenação virtual falha, a largura de banda pode ser ajustada rapidamente para garantir a transmissão normal dos dados. Quando o membro com falha se recupera, a largura de banda do grupo de concatenação virtual é restaurada automaticamente.



4xVC-4 em estado normal
2xVC-4 em estado de falha

- O LCAS é um esquema de ajuste de capacidade de link e uma extensão da tecnologia de concatenação virtual. O LCAS suporta as seguintes funções:
  - A largura de banda do serviço pode ser ajustada dinamicamente (adicionada ou excluída) sem afetar a disponibilidade dos serviços originais;
  - Quando alguns dos canais físicos em um grupo de concatenação virtual falham, com o LCAS, os canais com falha são suprimidos e os outros canais físicos ainda transportam os serviços normalmente. Isso evita que os serviços sejam interrompidos quando alguns dos canais físicos falham.
- O LCAS é uma das tecnologias que podem melhorar o desempenho da concatenação virtual. O princípio geral do LCAS é usar os bytes de cabeçalho reservados do SDH (o byte H4 é usado para a concatenação virtual de ordem superior e o byte K4 é usado para a concatenação de ordem inferior) para transmitir as informações de controle e ajustar dinamicamente o número de contêineres virtuais usados para mapear os serviços necessários para atender a diferentes requisitos de largura de banda de serviço e melhorar a utilização da largura de banda.
- The LCAS mechanism is as follows:
  - Aumentar e diminuir a largura de banda e suprimir e restaurar membros com falha usando o protocolo de handshake entre o NE de origem e o NE de destino.
  - Use o byte de sobrecarga SDH H4/K4 (H4 para a concatenação virtual de ordem superior e K4 para a concatenação virtual de ordem inferior) para transportar as informações de controle e realizar a operação de handshake entre o NE de origem e o NE de destino.

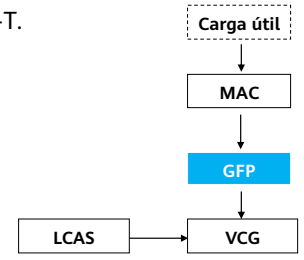
Tecnologia de Encapsulamento EoS

Descrição	HDLC	ML-PPP	LAPS	GFP
Função	Realização de comunicação na camada de enlace	Ser um protocolo de extensão PPP e vincular a função de concatenação virtual com base no protocolo PPP	Estabelecimento de links ponto a ponto orientados para a sincronização de bytes	Mapeamento de sinais de dados para sinais SDH ou OTN
Recurso	Tecnologia madura	Vinculação de vários links físicos como um link lógico para aumentar a largura de banda de transmissão Solução dos problemas de atraso de transmissão de vários caminhos e fornecimento de modos de rede mais flexíveis Baixa eficiência e implementação complexa	O PPP-HDLC é otimizado para fornecer os recursos das soluções IP Over SDH e Ethernet Over SDH, melhorando assim a eficiência do encapsulamento de pacotes de dados de grande granularidade. Não tem a capacidade de vincular vários canais. Como resultado, a concatenação virtual é necessária para controlar a largura de banda.	Adota o controle de erros para enquadramento. Oferece suporte ao mapeamento de quadros e à transmissão transparente. É um protocolo de encapsulamento padrão.
Modo de link suportado	Multiponto a ponto	Ponto a ponto	Ponto a ponto	Ponto a ponto ou anel

- O MSTP define três protocolos de encapsulamento padrão: HDLC (High-Level Data Link Control), LAPS (Link Access Protocol-SDH), GFP (Generic Framing Procedure). Os fornecedores podem usar protocolos de encapsulamento diferentes. Em sistemas reais, geralmente são selecionadas uma ou duas opções. Entretanto, algumas opções são diferentes, mesmo que o mesmo protocolo de encapsulamento seja usado.
- A compatibilidade do formato de encapsulamento é importante. Se os formatos de encapsulamento de diferentes fornecedores puderem ser compatíveis entre si, os serviços Ethernet GE ou FE poderão atravessar redes SDH de diferentes fornecedores e as duas extremidades da rede poderão usar dispositivos SDH de diferentes fornecedores. Dessa forma, a rede SDH formada por dispositivos de diferentes fornecedores se tornará um canal transparente para os serviços Ethernet, possibilitando redes de camada 2 para grandes organizações.
- O protocolo GFP é altamente padronizado. É um modo padrão no qual os serviços de dados são mapeados para SDH/OTN e está em conformidade com a norma ITU-T G.7041. Há dois modos de GFP: mapeado por quadro e transparente. O GFP coleta estatísticas sobre sinais de dados e multiplexa os sinais. A GFP evita quadros com erros causados por erros de bits e facilita o interfuncionamento entre dispositivos de diferentes fornecedores.

Protocolo de Encapsulamento GFP

- Generic Framing Protocol (GFP)
  - É uma tecnologia de mapeamento genérico, que pode mapear cargas úteis de comprimento variável em um canal de transmissão no qual os bytes são sincronizados.
  - Está em conformidade com a Recomendação G.7041 da ITU-T.
- Recursos :
  - Suporta multiplexação estatística
  - Suporta redes de anel lógico
  - Suporta OAM na banda
  - Apresenta baixa sobrecarga e alta eficiência de encapsulamento

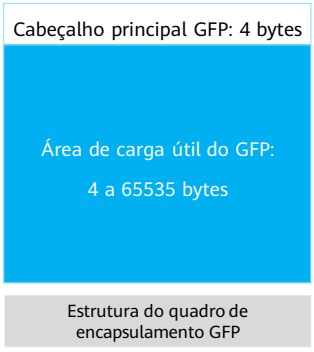


HUAWEI

- O GFP, definido como G.7041, fornece codificação de cabeçalho de dados e multiplexa várias interfaces físicas em um único canal de rede.
- O mais importante é que o GFP oferece modos transparentes e com mapeamento de quadros para dar suporte a mais aplicativos.
  - O GFP com mapeamento de quadro encapsula sinais de cliente com quadro em quadros GFP. É compatível com ajuste de taxa e multiplexação no nível de subtaxa.
  - O Transparent GFP recebe sinais digitais originais sem nenhuma alteração e é usado somente no quadro SDH com baixa sobrecarga e encapsulamento digital de baixa latência.
- O GFP pode encapsular pacotes de qualquer protocolo e garantir que os pacotes de protocolos comuns sejam transmitidos na camada óptica. Ele também garante flexibilidade e granularidades de largura de banda mais finas.

Estrutura do quadro no encapsulamento GFP

- Tipo de encapsulamento GFP
  - GFP-F: Frame-Mapped GFP
  - GFP-T: Transparent GFP
- Estrutura do quadro no encapsulamento GFP
  - Cabeçalho principal
  - Área de carga útil

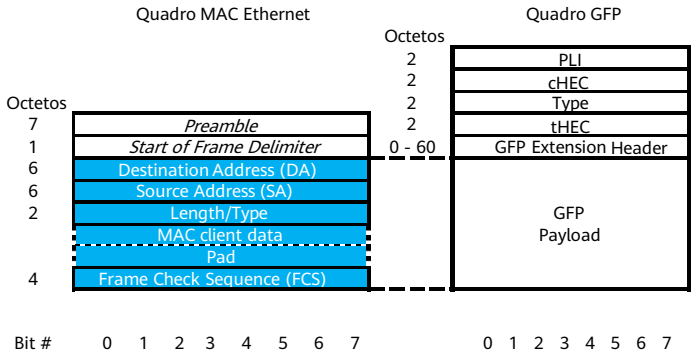


Estrutura do quadro de encapsulamento GFP

HUAWEI

- A GFP tem dois modos :
  - O GFP com mapeamento de quadro (GFP-F) é um modo de processamento orientado para PDU (como IP e Ethernet). O mapeamento entre a PDU da camada superior e a PDU GFP dos quadros MAC Ethernet é um mapeamento de um para um.
  - O GFP transparente (GFP-T) é um modo de processamento orientado para blocos de codificação de dados (como Fibre Channel e ESCON). O mapeamento transparente é usado para mapear a carga útil 8B/10B para GFP a fim de implementar uma transmissão de baixo atraso. Os sinais que podem ser mapeados de forma transparente incluem Fibre Channel, ESCON, FICON e GE. Nesse modo, não é necessário armazenar em buffer o quadro inteiro. Cada palavra do sinal do cliente é decodificada e, em seguida, mapeada para o GFP de um comprimento fixo, independentemente de a palavra do cliente ser uma palavra de dados ou uma palavra de controle. Assim, a palavra de controle 8B/10B do sinal do cliente é protegida.

Aplicações EoS do GFP-F



HUAWEI

- Encapsulamento de quadros MAC Ethernet
  - O conteúdo do quadro Ethernet MAC, desde o endereço de destino até a sequência de verificação do quadro, é colocado no campo de informações de carga útil do GFP, e a ordem dos bytes e a sequência de bits no quadro GFP não são alteradas.
- Exclusão e recuperação do IFG (Inter-Frame Gap)
  - Quando o sinal do cliente não é um cliente local que passa pelo mapeamento do quadro GFP, o IFG pode precisar ser excluído e restaurado de acordo com as seguintes regras:
    - O IFG é excluído antes da adaptação de GFP na extremidade da fonte e é inserido após a adaptação de GFP na extremidade do coletor.
    - Quando o quadro Ethernet MAC é extraído dos dados do cliente, o IFG é excluído. Em seguida, o quadro Ethernet MAC extraído é processado na extremidade de origem do GFP e encapsulado em quadros GFP.
    - Depois que o quadro Ethernet MAC é extraído do quadro GFP recebido, o IFG é restaurado. A restauração do IPG (InterPacket Gap) garante que haja bytes suficientes contendo 00 entre os quadros Ethernet MAC consecutivos recebidos para atender ao requisito do IFG

mínimo (16 bytes).

Quiz

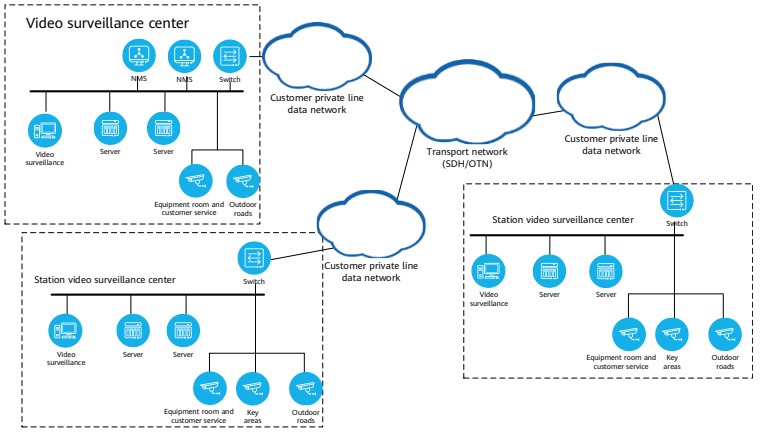
1. (Single-answer question) Which of the following statements is incorrect?
   A. A MAC address is a globally unique 48-bit address.
   B. The length of an Ethernet frame ranges from 64 bytes to 1518 bytes. The maximum payload length is 1500 bytes.
   C. When two ports that support different rates and auto-negotiation are connected, the actual transmission rate depends on the port with a higher rate.
   D. When the LCAS link is dynamically adjusted, for example, the bandwidth is increased, current services are not affected.
2. (Multiple-answer question) If client-side services carry VLAN IDs, which of the following attributes can be set for an Ethernet port?
   A. Access
   B. Tag Aware
   C. Hybrid
   D. Trunk

- Answer: 1. C 2. BC

Contents

Cenário de Ferrovias

- Vigilância por vídeo realizada na rede de transmissão

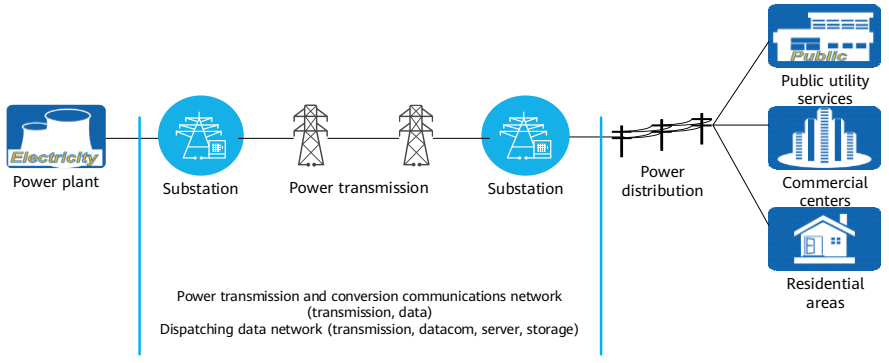


HUAWEI

- Imagens de vídeo de estações base GSM-R ao longo da ferrovia, estações de retransmissão de sinal, unidades internas e externas na sala de equipamentos de tração, unidades internas e externas de estações de energia e pontes ferroviárias

Cenário de Fornecimento de Energia Elétrica

- Sistema de distribuição de energia



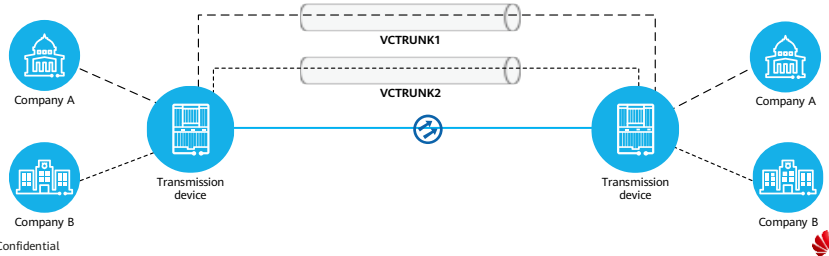
HUAWEI

- A rede de dados de despacho de energia elétrica oferece o serviço de programação de produção. É uma das principais redes de informatização de energia elétrica.
- No sistema de programação de energia, os dados de programação são transmitidos na rede de transmissão e na rede de dados na forma de serviços Ethernet.

Contents

EPL

- Ethernet private line (EPL): A Ethernet transmite serviços de forma transparente. Cada usuário ocupa exclusivamente a largura de banda de um VCTRUNK. A latência dos serviços dos usuários é baixa, e a segurança e a privacidade dos dados do usuário são bem protegidas.
- Transmissão transparente ponto a ponto: A transmissão transparente E2E é implementada em portas Ethernet sem compartilhamento.



- O serviço EPL é transparente, o que significa que os dispositivos de acesso, terminação e transporte intermediário formam uma linha privada para os dados do usuário.
- No serviço EPL, cada usuário ocupa exclusivamente um VCTRUNK e não precisa compartilhar a largura de banda com outros usuários. Portanto, o serviço EPL tem garantia estrita de largura de banda e isolamento do usuário, e não requer outros mecanismos de QoS e de segurança.
- Conforme mostrado na figura anterior, o serviço é transmitido de forma transparente de ponta a ponta, sem compartilhamento de largura de banda.
  - A Empresa A e a Empresa B transmitem serviços de dados por meio dos dispositivos de transmissão. Cada local tem uma placa de processamento de serviços Ethernet. Os serviços da Empresa A e da Empresa B são completamente isolados. A largura de banda usada pela Empresa A e pela Empresa B pode ser determinada pelo número de VC-12s, VC3s e VC-4s.
  - A transmissão transparente P2P permite que o serviço EPL ocupe exclusivamente a largura de banda da linha e seja isolado de outros serviços para garantir a segurança. Esse método se aplica a clientes VIP.

EVPL

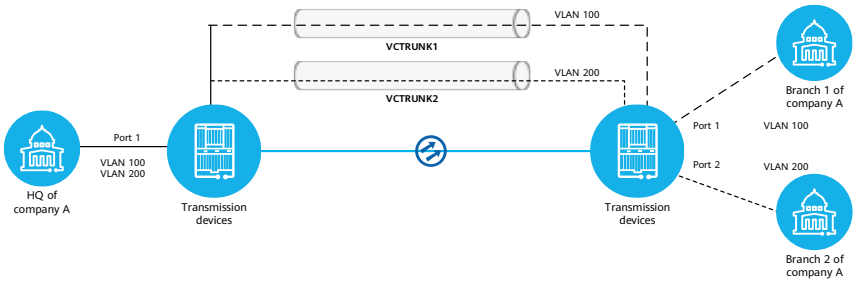
- A linha privada virtual Ethernet (EVPL - Ethernet Virtual Private Line) também é conhecida como linha privada VPN. A vantagem é que diferentes fluxos de serviço compartilham um canal VCTRUNK, de modo que uma única porta física pode fornecer várias conexões de serviço P2P com o mesmo desempenho em cada direção. A largura de banda de acesso é ajustável e gerenciável, e os serviços podem ser convergidos e agregados para economizar recursos da porta.

EVPL com VCTRUNK compartilhado	EVPL com portas compartilhadas
• Isolamento de VLAN ID • Isolamento de rótulo MPLS • Isolamento de VLAN QinQ aninhada	• Isolamento de VLAN ID

- Os serviços EVPL podem ser isolados por VLAN ID, rótulo MPLS e tecnologias QinQ, permitindo o compartilhamento de portas e de VCTRUNK.

EVPL - Compartilhamento de Portas Externas

- Os serviços são isolados em portas MAC externas com base em IDs de VLAN.

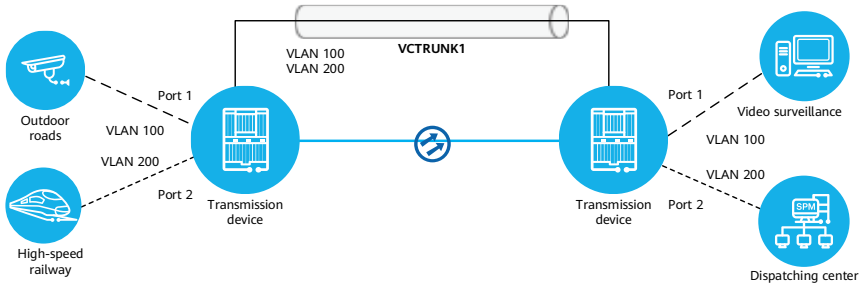


HUAWEI

- Usando VLAN IDs, as portas das placas de processo de serviço Ethernet podem ser compartilhadas, proporcionando flexibilidade na rede. A transmissão transparente P2MP pode ser fornecida aos usuários. Os quadros de dados de uma porta Ethernet podem ser enviados a diferentes destinos com base nos IDs de VLAN, e os quadros de dados de várias fontes podem ser agregados em uma porta Ethernet de destino.
- Conforme mostrado na figura anterior, os dados enviados da sede precisam ser enviados a diferentes departamentos. Os dados enviados da sede contêm diferentes VLAN IDs, que podem ser usadas para diferenciar os sinais de serviço enviados a diferentes departamentos. A largura de banda é alocada de acordo com o VCTRUNK. Nesse aplicação, os serviços de uma VLAN são alocados a um VCTRUNK independente. Ou seja, a largura de banda da VLAN pode ser garantida. Dessa forma, a aplicação de rede ponto a multiponto do serviço Ethernet é implementada. Vários serviços podem compartilhar uma porta e ser distinguidos por tags de VLAN.

EVPL - Compartilhamento de VCTRUNK (VLAN ID)

- Os serviços são isolados em VCTRUNKs por VLAN IDs.



HUAWEI

- Uma placa de processamento de serviços Ethernet pode fornecer um número limitado de VCTRUNKs. Nesse caso, o compartilhamento de VCTRUNK pode ser implementado para transmitir dados Ethernet de várias VLANs por meio do mesmo canal VCTRUNK. Nesse caso, a largura de banda de uma VLAN não pode ser garantida.
- Conforme mostrado na figura anterior, os dados de monitoramento e os dados de agendamento compartilham o mesmo VCTRUNK e são isolados pelo uso de VLAN IDs diferentes. Quando mais de dois usuários compartilham um VCTRUNK, os recursos de largura de banda de determinados usuários não podem ser garantidos. Por exemplo, dois usuários compartilham um VCTRUNK. Se um usuário ocupar 90% da largura de banda, a largura de banda disponível para o outro usuário será de apenas 10%. A função de taxa de acesso autorizada (CAR - Committed Access Rate) pode ser usada para controlar a taxa de acesso de uma porta externa, definindo o parâmetro de taxa de informação autorizada (CIR - Committed Information Rate) para diferentes usuários. Nesse modo, os serviços podem ser convergidos e a largura de banda pode ser compartilhada na linha. Vários serviços podem compartilhar um VCTRUNK e ser distinguidos por tags de VLAN. Os usuários que compartilham um VCTRUNK competem pela largura de banda. Portanto, esse método é adequado para usuários cujos picos de serviços dos usuários ocorrem em diferentes períodos de tempo.

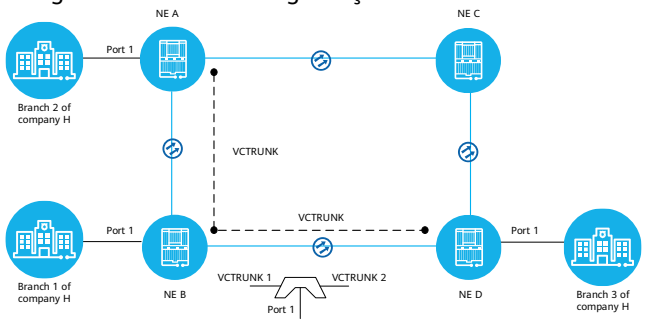
EVPL - Outros Formas

- Multiprotocol label switching (MPLS)
  - Os rótulos MPLS são usados para isolar os serviços.
- VLAN stacking technology (QinQ)
  - Os pacotes QinQ contêm dois tipos de tags: tag C-VLAN e tag S-VLAN.

- **MPLS**: Multi-Protocol Label Switching (MPLS) é uma nova tecnologia que usa rótulos para orientar a transmissão de dados eficiente e de alta velocidade em uma rede de comunicações aberta. Multiprotocolo significa que o MPLS não só oferece suporte a vários protocolos da camada de rede, mas também é compatível com várias tecnologias da camada de enlace de dados na camada 2.
- A tecnologia QinQ encapsula uma tag de VLAN privada em uma tag de VLAN pública para que os pacotes passem pelas redes de backbone das operadoras com tags de VLAN duplas. Nas redes públicas, os pacotes são transmitidos de acordo com a tag de VLAN externa, e a tag de VLAN privada é protegida. Dessa forma, os fluxos de dados são diferenciados. Além disso, o número de tags de VLAN disponíveis é expandido porque a tag de VLAN privada é transmitida de forma transparente e as tags de VLAN de diferentes usuários podem ser usadas repetidamente, desde que a tag de VLAN externa seja exclusiva em redes públicas.

EPLAN - 802.1d Bridge

- A LAN privada Ethernet (EPLAN - Ethernet Private LAN), também chamada de serviço de comutação de camada 2, implementa conexões de serviço multiponto a multiponto. A largura de banda de acesso é ajustável e gerenciável, e os serviços podem ser convergidos e agregados. As vantagens são semelhantes às do EPL, ou seja, o usuário ocupa exclusivamente a largura de banda e a segurança é boa.



- O EPLAN usa comutação de camada 2. O EPLAN é compatível com todos os tipos de rede de EPL e EVPL, exceto MPLS. O EPLAN também oferece suporte a redes multiponto.
- Conforme mostrado na figura anterior, as três filiais da empresa H estão localizadas no NE A, NE B e NE D. As filiais precisam compartilhar informações e se comunicar umas com as outras. Nesse caso, a placa Ethernet do NE B precisa implementar a função de comutação da camada 2 da Ethernet. O serviço EPLAN realiza o compartilhamento dinâmico multiponto de serviços Ethernet, que está em conformidade com os recursos dinâmicos dos serviços de dados e economiza recursos de largura de banda. Para evitar tempestades de transmissão, os serviços EPLAN Ethernet devem estar livres de loop. Portanto, se a topologia em anel for usada, o Spanning Tree Protocol (SPT) deverá ser ativado para evitar loops e as consequentes tempestades de broadcast. O EPLAN é implementado com base no IEEE802.1d. Portanto, o EPLAN também é chamado de ponte 802.1d.

EVPLAN - 802.1q Bridge

- IEEE 802.1q bridge: Os pacotes são encaminhados com base nos endereços MAC e VLAN IDs contidos nos pacotes.

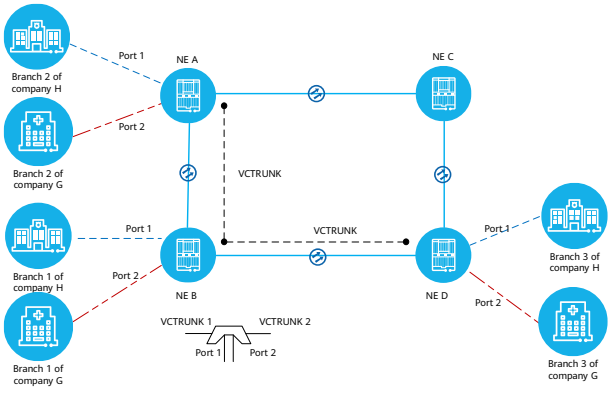


Tabela de filtragem VLAN (empresa H)	
VLAN 100	VCTRUNK 1
	VCTRUNK 2
	PORTA 1

Tabela de filtragem VLAN (empresa G)	
VLAN 200	VCTRUNK 1
	VCTRUNK 2
	PORTA 2

HUAWEI

- IEEE 802.1q bridge: Oferece suporte a uma camada de tags de VLAN para isolamento de dados. A ponte 802.1q verifica as tags de VLAN dos quadros de dados e realiza a comutação da camada 2 com base nos endereços MAC de destino e nos IDs de VLAN dos quadros de dados.
- Conforme mostrado na figura, as filiais da empresa H precisam se comunicar entre si, e as filiais da empresa G precisam se comunicar entre si, e os dados da empresa H precisam ser isolados dos dados da empresa G. Portanto, a ponte virtual (VB) configurada no NE B precisa distinguir os dados das duas empresas por VLAN IDs. As portas conectadas à VB no NE B incluem PORT 1, PORT 2, VCTRUNK 1 e VCTRUNK2, e uma tabela de encaminhamento de VLAN precisa ser configurada.

EVPLAN - 802.1ad Bridge

- IEEE 802.1ad bridge: Os pacotes são encaminhados com base no endereço MAC e nas tags S-VLAN contidas nos pacotes.

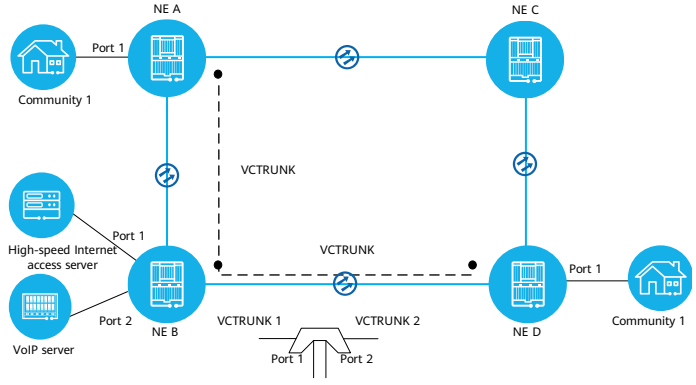


Tabela de filtragem VLAN (acesso à Internet de alta velocidade)	
S-VLAN 100	VCTRUNK 1
	VCTRUNK 2
	PORTA 1

Tabela de filtragem VLAN (VoIP)	
S-VLAN 200	VCTRUNK 1
	VCTRUNK 2
	PORTA 2

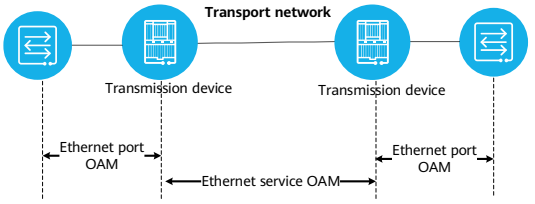
HUAWEI

- IEEE 802.1ad bridge: São suportados quadros de dados com duas camadas de tags de VLAN. A tag S-VLAN externa é usada para isolamento de VLAN. Somente as portas cujos atributos de porta são C-Aware e S-Aware podem ser usadas.
  - A ponte 802.1ad não verifica as tags de VLAN dos quadros de dados e realiza a comutação da Camada 2 com base nos endereços MAC de destino.
  - A ponte 802.1q verifica as tags de VLAN dos quadros de dados e executa a comutação da camada 2 com base nos endereços MAC de destino e nas IDs de S-VLAN dos quadros de dados.
- Conforme mostrado na figura, os serviços de VoIP e de Internet de alta velocidade das duas comunidades residenciais precisam ser conectados separadamente ao servidor de VoIP e ao servidor de acesso à Internet de alta velocidade, respectivamente. Durante a transmissão, o VoIP e os serviços de Internet de alta velocidade precisam ser programados e isolados separadamente no lado da rede de transmissão. Nesse caso, a VB configurada no NE B precisa adicionar diferentes tags S-VLAN aos quadros de dados para identificar os dois tipos de serviços. Quando os serviços chegam ao VB no NE B, as tags de S-VLAN precisam ser adicionadas. Quando os serviços chegam ao próximo salto, as tags de S-VLAN precisam ser removidas.

Contents

ETH OAM (1)

- Como um protocolo baseado na camada MAC, o ETH-OAM detecta links Ethernet transmitindo pacotes OAM. Além disso, o ETH OAM é um protocolo de baixa taxa que ocupa pouca largura de banda. Ele não afeta os serviços realizados nos links.



- O OAM do serviço Ethernet concentra-se na manutenção dos links Ethernet de ponta a ponta. Com base nos serviços, o OAM do serviço Ethernet realiza a verificação de ponta a ponta de acordo com cada domínio de manutenção. Ou seja, ele realiza a manutenção segmentar nos segmentos de rede pelos quais um serviço passa na rede.
- O OAM de porta Ethernet concentra-se na manutenção do link Ethernet ponto a ponto entre dois dispositivos diretamente conectados na Ethernet na primeira milha (EFM). O OAM da porta Ethernet não se concentra em um serviço específico. Ele mantém o link Ethernet ponto a ponto executando a descoberta automática de OAM, o monitoramento do desempenho do link, a verificação de falhas, o loopback remoto e a verificação de selfloop.

ETH OAM (2)

- Gerenciamento de OAM de Serviços Ethernet
  - Ponto de manutenção (MP): cada MP tem uma ID exclusiva em uma associação de manutenção (MA). As informações de cada MP são registradas na tabela de endereços MAC, na tabela MP e na tabela de rotas. O tipo de serviço, a ID de serviço e a tag de VLAN são os principais conteúdos das informações de configuração do MP. Um MP transmite periodicamente pacotes de protocolo que carregam suas informações para outros MPs relacionados ao mesmo serviço. Depois de receber os pacotes de protocolo, outros MPs registram as informações para uso futuro.
  - Domínio de manutenção (MD): um MD é uma unidade de gerenciamento baseada em segmento de rede que gerencia os segmentos de rede pelos quais um fluxo de serviço passa. Além disso, diferentes fluxos de serviço precisam ser gerenciados separadamente.
  - Associação de manutenção (MA): uma VLAN corresponde a uma instância de serviço. Ao dividir as MAs, você pode detectar as falhas de conectividade da rede que transmite uma determinada instância de serviço.

- Os parlamentares são classificados em MEPs e MIPs.
  - Maintenance association end point (MEP): Um MEP define os pontos inicial e final de um MA e está associado a serviços.
  - Maintenance association intermediate point (MIP): não pode iniciar pacotes OAM. Ele pode responder e encaminhar um pacote LB (loopback) ou LT (link trace) e só pode encaminhar um pacote CC (continuity check).
- MD:
  - O OAM do serviço Ethernet mantém a Ethernet realizando verificações de ponta a ponta com base em MDs. Com relação ao OAM, um MD é uma coleção de todos os MPs em uma aplicação de serviço. Esses MPs consistem em MEPs e MIPs.
  - Para que um segmento de gerenciamento seja mantido, os MEPs podem ser estabelecidos em ambas as extremidades, de modo que o intervalo do MD seja especificado. Além disso, os MIPs em outras posições nesse segmento de gerenciamento podem ser estabelecidos conforme necessário. Ao executar operações nesses MPs, você pode monitorar o estado do segmento sob gerenciamento, detectar falhas e localizar as falhas, se houver.
- MA:
  - Uma AM é uma parte de um MD. Um domínio de manutenção (MD) pode ser dividido em uma ou mais MAs.
  - O nível de uma MA é igual ao nível do MD ao qual ela pertence.

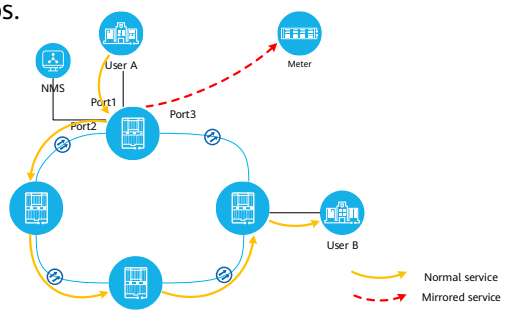
ETH OAM (3)

- Operações de OAM de Serviço Ethernet
  - Verificação de continuidade (CC): Os MEPs enviam periodicamente mensagens de verificação de continuidade (CCMs) uns aos outros para verificar a conectividade entre eles.
  - Loopback (LB): Verifica o status do link do MEP de origem para qualquer MP no mesmo MD.
  - Rastreamento de link (LT): O método LT pode localizar um link defeituoso específico em uma única tentativa, fornecendo um recurso aprimorado de localização de falhas com base no método LB.
  - OAM ping: É um método de teste on-line que pode simular a taxa de perda de pacotes e a latência causada por erros de bits. Com base na verificação de conectividade, o ping fornece um gerenciamento refinado do desempenho dos links Ethernet na camada de enlace MAC.

- CCM: continuity check message
- LB: loopback
- LT: link trace

Espelhamento de Porta

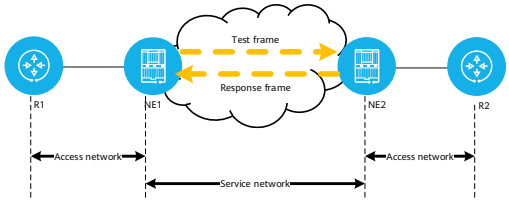
- A tecnologia de espelhamento de porta permite que você copie o tráfego de uma porta ou de alguns serviços de uma porta para outra porta. Com o medidor, você pode localizar rapidamente a falha e monitorar o tráfego do serviço em tempo real sem afetar os serviços.



- O espelhamento de portas tem os seguintes recursos:
  - Toda a porta física pode ser espelhada.
  - O espelhamento de portas aplica-se ao diagnóstico de falhas on-line. Ele espelha o tráfego ou alguns serviços de uma porta para outra porta e, em seguida, um analisador é usado para o diagnóstico de falhas.
  - Depois que o espelhamento de porta é usado, o tráfego pode ser monitorado com um analisador.
  - Direction of Mirror Source Function Point (Direção da Fonte de Espelho Ponto de Função).
    - Entrada: O tráfego recebido pela porta de origem do espelho é replicado para a porta de destino do espelho.
    - Egresso: O tráfego transmitido pela porta de origem do espelho é replicado para a porta de destino do espelho.
    - Bidirecional: O tráfego recebido e transmitido pela porta de origem do espelho é replicado para a porta de destino do espelho.
- Diferentemente do espelhamento de porta, que apenas copia e monitora os serviços em toda a porta, o espelhamento de tráfego de porta combina espelhamento de porta e espelhamento de fluxo. Ele copia e monitora os serviços em uma porta com base em informações como tag de VLAN, prioridade de VLAN, prioridade de IP, MAC de destino, tornando a localização de falhas mais precisa.

Quadro de Teste

- Os quadros de teste são usados principalmente para o comissionamento de serviços Ethernet ou para a localização de falhas no serviço Ethernet.
- A função de quadro de teste significa que os quadros de teste são enviados entre as portas para detectar o status de funcionamento da rede.



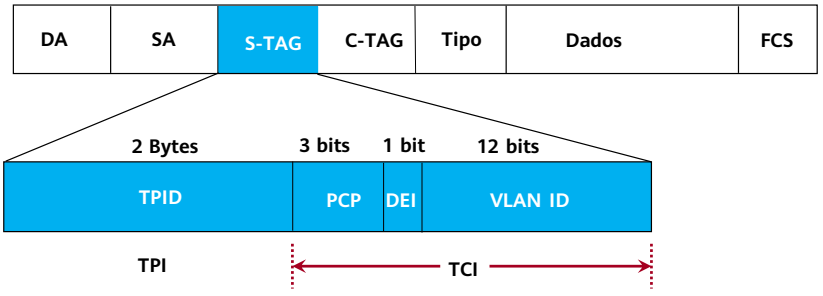
- Em casos normais, R1 e R2 trocam dados por meio da rede de serviços. Se um usuário detectar que a rede está anormal, os engenheiros poderão transmitir quadros de teste e quadros de resposta entre NE1 e NE2 para localizar a falha ou descartar a possibilidade de falha entre NE1 ou NE2 e restringir o ponto de falha à rede de acesso.

HUAWEI

- Ao enviar quadros de teste durante um teste, não é recomendável realizar nenhuma outra operação. O envio de quadros de teste afetará os serviços dos usuários. Portanto, tenha cuidado ao executar essa operação.

QinQ

- O QinQ é um protocolo de túnel de camada 2 baseado no encapsulamento IEEE 802.1q. A tecnologia QinQ encapsula uma tag de rede local virtual (VLAN) privada em uma tag de VLAN de operadora. Portanto, os pacotes com duas camadas de tags de VLAN podem ser transmitidos na rede de backbone de uma operadora. Dessa forma, o QinQ fornece túneis de rede privada virtual (VPN) de camada 2.



Quadro Ethernet com uma C-TAG e uma S-TAG

HUAWEI

- As principais funções da tecnologia QinQ são as seguintes :
  - Com a aplicação da tecnologia QinQ, o número de VLAN IDs pode chegar a 4094 x 4094. Isso atende aos crescentes requisitos de VLAN IDs.
  - Os clientes e operadores podem planejar os recursos de VLAN de forma independente e flexível. Portanto, a configuração e a manutenção da rede são simplificadas.
  - A tecnologia QinQ substitui a tecnologia MPLS para oferecer uma solução de VPN de camada 2 mais barata e mais simples.
  - A tecnologia QinQ permite a expansão dos serviços Ethernet das redes locais (LANs) para as redes de área ampla (WANs).
- Em um quadro Ethernet com um C-TAG e um S-TAG, o S-TAG é adicionado antes do C-TAG. As diferenças entre o S-TAG e o C-TAG são as seguintes :
  - O TPID é diferente. Conforme definido no IEEE 802.1ad, o valor do TPID no S-TAG é 0x88a8, enquanto o valor do TPID no C-TAG é 0x8100.
  - O indicador de elegibilidade de queda (DEI) substitui o CFI. O DEI trabalha com o PCP para indicar a prioridade do S-TAG.
- O QinQ oferece uma solução de VPN de camada 2 muito mais barata e fácil do que o MPLS (multi-protocol label switch). Ao usar a tecnologia VLAN QinQ, os pacotes de dados carregam duas camadas de tags de VLAN para distinguir diferentes serviços. Isso altera a limitação de que apenas uma tag de VLAN é usada para marcar os pacotes de dados e aumenta o número de VLAN IDs. A tag de VLAN interna é uma tag de VLAN de cliente (C-VLAN) e a VLAN externa é uma tag de VLAN de provedor de serviços (S-VLAN).

RMON

- O monitoramento remoto de rede (RMON) é usado para monitorar o tráfego de dados em um segmento de rede ou em toda a rede. Atualmente, o RMON é um dos padrões de gerenciamento de rede mais usados.

Grupo de Gerenciamento de Monitoramento Remoto	**Função**
Statistics Group	O grupo de estatísticas permite que os usuários consultem o desempenho da porta em tempo real, como o número de pacotes recebidos e enviados com o comprimento especificado e o número de eventos de perda de pacotes em um determinado período.
Alarm Group	O grupo de alarmes permite que os usuários monitorem o desempenho de portas importantes. Quando o desempenho monitorado ultrapassa um limite, um alarme é relatado. Os limites incluem o de bytes em pacotes ruins recebidos e o de perdas de pacotes.
History Control Group	O grupo de controle de histórico permite que os usuários coletem e armazenem periodicamente os dados de desempenho de porta necessários.
History Group	O grupo de histórico permite que os usuários consultem e filtrem os dados históricos de desempenho necessários para análise e diagnóstico de falhas.

- RMON: Remote Network Monitoring
- As estatísticas RMON do equipamento são armazenadas no agente RMON de uma unidade Ethernet. O NMS usa comandos básicos do SNMP (Simple Network Management Protocol) para trocar estatísticas e coletar estatísticas do agente RMON. Com essas estatísticas, a equipe de operação e manutenção pode realizar monitoramento em tempo real, detecção de erros e análise e tratamento de falhas nos serviços de Ethernet.

Quiz

1. (Multiple-answer question) Which of the following service types support point-to-multipoint transmission?
   A. EPL
   B. EVPL
   C. EPLAN
   D. EVPLAN

HUAWEI

- Answer: CD

Quiz

2. (Multiple-answer question) Which of the following operations do not affect normal services?
   A. ETH OAM
   B. Test frame
   C. Port mirroring
   D. RMON

HUAWEI

- Answer: ACD

Summary

- Princípios básicos e tecnologias de Ethernet
- Tecnologias de concatenação e encapsulamento de EoS
- Cenários e tipos comuns de serviços Ethernet
- Recursos de Ethernet

Thank you.

把数字世界带入每个人、每个家庭、
每个组织，构建万物互联的智能世界。

Bring digital to every person, home, and organization for a fully connected, intelligent world.