



Noções básicas de comunicação de rede

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.



Foreword

- A comunicação de dados é uma rede construída por vários dispositivos, como roteadores, switches, firewalls, balanceadores de carga, IDS/IPS e servidores VPN. A função básica de uma rede de dados é implementar a comunicação de dados entre diferentes nós.
- Em 1984, a Organização Internacional de Normalização (ISO) apresentou o Open System Interconnection Reference Model (OSI RM) para resolver o problema de compatibilidade entre redes e ajudar os fornecedores a produzir dispositivos de rede compatíveis. Ele simplifica as operações de rede relacionadas, fornece compatibilidade e interfaces padrão entre dispositivos, promove padronização e é estruturalmente separável e fácil de implementar e manter.
- O modelo e protocolo OSI não são amplamente utilizados devido à sua complexidade. No entanto, o modelo TCP/IP (Transfer Control Protocol/Internet Protocol) é amplamente aplicado na prática devido à sua abertura e usabilidade, e tornou-se uma base da atual rede IP.



Objectives

- Ao concluir este curso, você estará apto a:
 - Compreender os conceitos e recursos básicos da comunicação de dados.
 - Compreender a estrutura da camada TCP/IP, as funções de cada camada e o processo de encapsulamento de dados.
 - Dominar os conceitos de endereços IP e divisão de sub-rede IP e compreenda os recursos e as funções de rotas IP e roteadores.
 - Entender o princípio operacional da Ethernet.



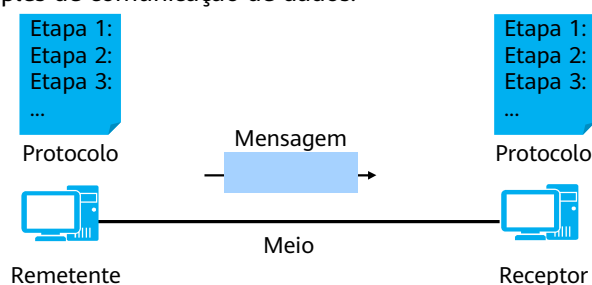
Contents

- 1. Visão geral da comunicação de dados**
2. Pilha de protocolo TCP/IP
3. Visão geral da Ethernet



O que é Comunicação de Dados?

- De acordo com o protocolo de comunicação, os dados são transferidos entre unidades funcionais utilizando a tecnologia de transmissão, de modo a realizar o intercâmbio de informações entre computadores, entre computadores e terminais e entre outros dispositivos terminais de dados.
- Uma rede de comunicação de dados é uma rede que fornece serviços de comunicação de dados.
- Entenda o processo simples de comunicação de dados:

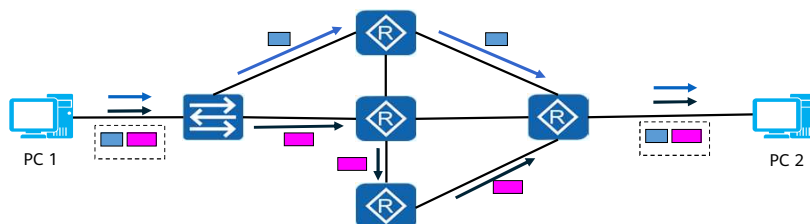


- Um sistema completo de comunicação de dados deve ser composto por cinco partes: mensagem, remetente, destinatário, meio e protocolo.
- Mensagem:
 - Um pacote é um bloco de dados em comunicação. Informações como textos, números, imagens, áudio e vídeos são codificadas e depois transmitidas em pacotes.
- Remetente:
 - O remetente refere-se ao dispositivo que envia pacotes de dados. Pode ser um computador, estação de trabalho, servidor, telefone celular, etc.
- Destinatário:
 - O receptor se refere ao dispositivo que recebe os pacotes. Pode ser um computador, estação de trabalho, servidor, telefone celular, TV, etc.
- Meio:
 - Meios de transmissão: Refere-se à portadora para a transmissão do sinal. Mídias de transmissão comuns em LANs incluem fibras ópticas, cabos coaxiais e pares trançados.
- Protocolo:
 - Um protocolo é um conjunto de regras que regem a comunicação de dados. Representa um conjunto de convenções entre dispositivos de comunicação. Sem um protocolo, mesmo se os dois dispositivos estiverem fisicamente conectados, eles não poderão se comunicar. Por exemplo, uma pessoa que só sabe falar chinês não pode ser entendida por uma pessoa que só sabe falar inglês.



Características da comunicação de dados

- Sem conexão:
 - Não existe uma ligação única entre as duas extremidades.
- Comutação de pacotes:
 - Cada pacote tem o endereço de destino, o endereço de origem e as informações de controle de erros, além de poder localizar o destino sozinho.



- A comutação de pacotes sem conexão usa a adição de informações de controle e gerenciamento para encapsular os dados do usuário para o transporte. Estas informações são adicionadas através de cabeçalho de pacote, que é usado para roteamento, controle de erros e controle de fluxo. O comprimento e o intervalo de cada pacote podem ser alterados. Assim, a comutação de pacotes suporta várias taxas.
- Na comutação de pacote sem conexão, as informações de roteamento são transportadas em cada cabeçalho de pacote. Um dispositivo de comutação verifica as informações de endereço em cada cabeçalho de pacote, seleciona uma rota com base no status da rede e envia pacotes para o dispositivo de rede do próximo nível. Portanto, pacotes diferentes do mesmo serviço podem passar por caminhos diferentes na rede.
- Na comutação de pacotes sem conexão, os pacotes ocupam os recursos da rede somente quando são transmitidos. Os recursos de rede podem ser compartilhados por vários serviços.
- Modo de transmissão:
 - Simplex:
 - No modo simplex, a comunicação é unidirecional. Apenas um dos dois dispositivos pode enviar pacotes e o outro só pode receber pacotes.
 - Teclados e monitores são dispositivos de comunicação simplex. O teclado só pode ser usado para entrada, e o monitor só pode receber saída.

- Half-duplex:
 - No modo half-duplex, cada dispositivo pode enviar e receber pacotes, mas não pode enviar e receber pacotes ao mesmo tempo. Quando um dispositivo envia pacotes, o outro dispositivo só pode receber pacotes e vice-versa.
 - O walkie-talkie é um exemplo típico de um sistema half-duplex.
- Full duplex:
 - No modo full-duplex, ambas as partes de comunicação podem receber e transmitir dados simultaneamente.
 - A rede telefônica é um exemplo típico de full duplex.



Organizações de padronização

- ISO International Organization for Standardization
- IEEE Institute of Electrical and Electronics Engineers
- ANSI American National Standards Institute
- EIA Electronic Industries Alliance
- TIA Telecommunications Industry Association
- ITU International Telecommunications Union
- IAB Internet Architecture Board



Organização Internacional de Normalização



American National Standards Institute



União Internacional das Telecomunicações



Instituto de Engenheiros Eletricistas e Eletrônicos

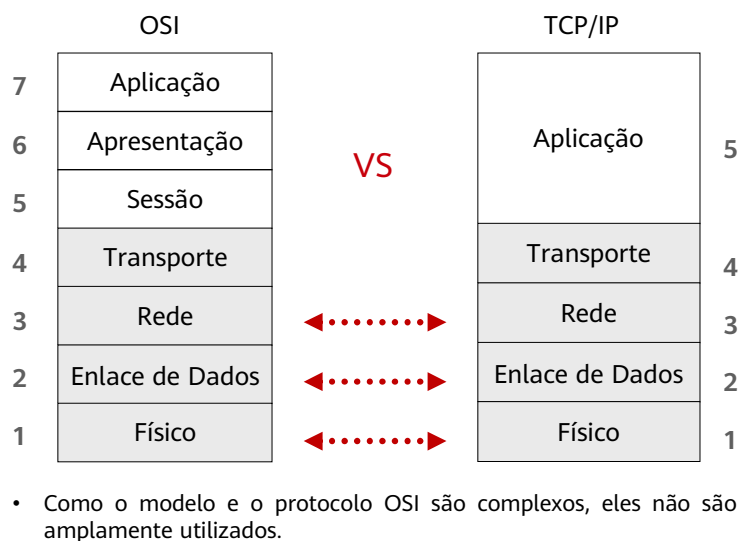


Contents

1. Visão geral da comunicação de dados
- 2. Pilha de protocolo TCP/IP**
 - **Estrutura do Modelo TCP/IP**
 - Encapsulamento de Pacote da Pilha de Protocolo TCP/IP
 - Endereçamento IP e Roteamento
3. Visão geral da Ethernet



Modelo TCP/IP



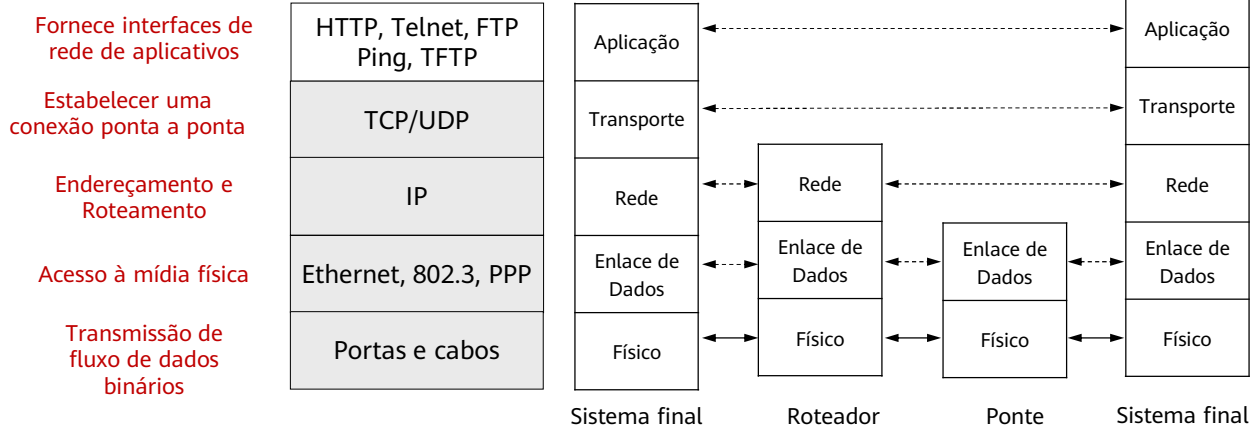
TCP/IP

- O modelo TCP/IP tem sido amplamente utilizado na prática devido à sua abertura e facilidade de uso. A pilha de protocolos TCP/IP tornou-se o protocolo principal da Internet.
- O modelo TCP/IP também usa uma estrutura hierárquica. As camadas são independentes umas das outras, mas têm estreitas relações de cooperação entre si.
- A diferença entre o modelo TCP/IP e o modelo de referência OSI é que tanto a camada de apresentação quanto a camada de sessão pertencem à camada de aplicação no modelo TCP/IP. O modelo TCP/IP é dividido em cinco camadas de baixo para cima: camada física, camada de enlace de dados, camada de rede, camada de transporte e camada de aplicação.

- Desde a década de 1960, as redes de computadores têm crescido a passos largos. Para dominar o campo da rede de comunicação de dados, os principais fornecedores lançaram seus próprios sistemas e padrões de arquitetura de rede, como SNA da IBM, Novell IPX/SPX, AppleTalk, DECnet da DEC e protocolos TCP/IP populares. Ao mesmo tempo, os principais fabricantes de seus próprios protocolos produziram um hardware e software diferente. Os esforços conjuntos de todos os fornecedores promovem o rápido desenvolvimento de tecnologias de rede e o rápido crescimento dos tipos de dispositivos de rede. No entanto, devido à coexistência de vários protocolos, a rede torna-se cada vez mais complexa. Além disso, a maioria dos dispositivos de rede de diferentes fornecedores é incompatível, o que dificulta a comunicação.
- Em 1984, a Organização Internacional de Normalização (ISO) apresentou o Open System Interconnection Reference Model (OSI RM) para resolver o problema de compatibilidade entre redes e ajudar os fornecedores a produzir dispositivos de rede compatíveis. O modelo de referência OSI está rapidamente se tornando o modelo básico de comunicação em rede de computadores. Na concepção do modelo de referência das OSI, são seguidos os seguintes princípios: cada camada tem uma fronteira clara para implementar funções específicas; A divisão de camadas é benéfica para o estabelecimento de protocolos padrão internacionais. O número de camadas deve ser suficientemente grande para evitar a duplicação de funções entre camadas.
- O modelo de referência OSI tem as seguintes vantagens: Ele simplifica as operações de rede relacionadas; Fornece compatibilidade plug-and-play e interfaces padrão entre diferentes fornecedores. Permite que os fornecedores projetem dispositivos de rede interoperáveis para promover a padronização. Impede que a alteração de rede em uma área afete a rede em outra área. As redes em diferentes áreas estão separadas. Portanto, a rede em cada área pode ser atualizada rapidamente. Decompõe problemas complexos de rede em pequenos problemas simples, que são fáceis de aprender e operar.



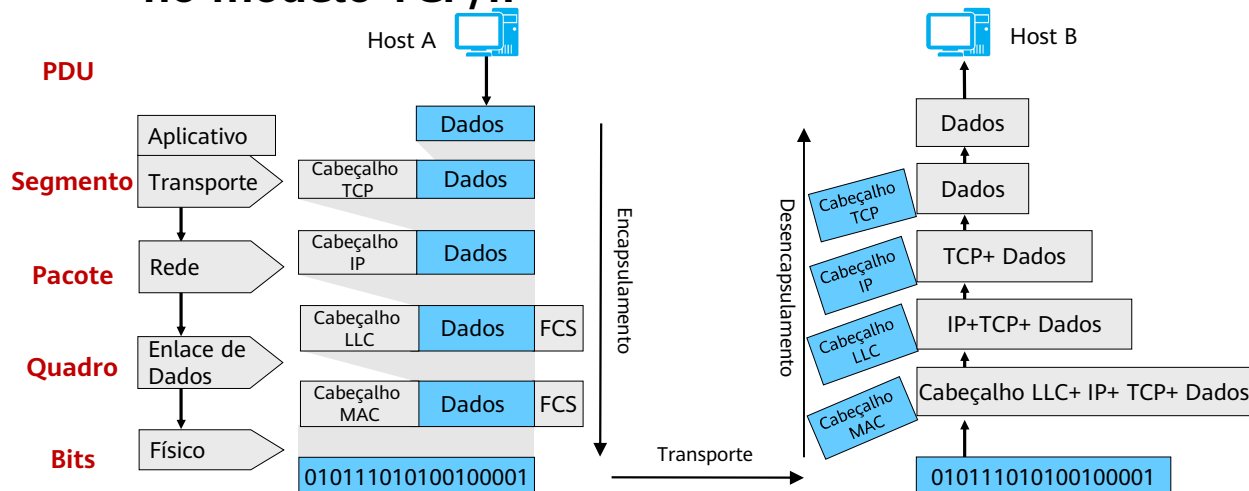
Pilha de protocolo TCP/IP



- Diferentes camadas do modelo TCP/IP correspondem a diferentes protocolos. A pilha de protocolos TCP/IP é uma coleção de protocolos de comunicação de dados, incluindo muitos protocolos. Seu nome de pilha de protocolo deriva dos dois protocolos principais, TCP (Transmission Control Protocol) e IP (Internet Protocol). A pilha de protocolos TCP/IP garante que os dispositivos de rede possam se comunicar entre si. É um conjunto de regras que governam como as informações são transmitidas pela rede.



Encapsulamento e desencapsulamento de dados no modelo TCP/IP



- Cada camada do TCP/IP permite que os dados sejam transmitidos pela rede. Essas camadas usam unidades de dados de protocolo (PDUs) para trocar informações entre si a fim de garantir que os dispositivos de rede possam se comunicar uns com os outros. As PDUs em camadas diferentes contêm informações diferentes. Portanto, PDUs em camadas diferentes têm nomes diferentes. Por exemplo, a PDU obtida depois que a camada de transporte adiciona o cabeçalho TCP aos dados da camada superior é chamada de segmento. O segmento de dados é transmitido para a camada de rede, e a PDU obtida depois que a camada de rede adiciona o cabeçalho IP é chamada de pacote. O pacote de dados é transmitido para a camada de enlace de dados, e a PDU obtida após a camada de enlace de dados encapsular o cabeçalho de dados é chamada de quadro, os quadros são convertidos em bits e transmitidos pelo meio de rede. Esse processo de passar dados pela pilha e adicionar cabeçalhos e trailers é chamado encapsulamento.
- Depois que os dados são encapsulados e transmitidos pela rede, o dispositivo receptor exclui as informações adicionadas e determina como fazer upload dos dados para o aplicativo apropriado ao longo da pilha de protocolos com base nas informações no cabeçalho. Esse processo é chamado de desencapsulamento. As camadas de peer de diferentes dispositivos se comunicam entre si através do encapsulamento e desencapsulamento.

- Conforme mostrado na figura, o host A se comunica com o host B. O host A converte os dados da camada superior de um aplicativo por meio do protocolo da camada superior e envia os dados convertidos para a camada de transporte. A camada de transporte usa os dados da camada superior como sua própria parte de dados, encapsula o cabeçalho da camada de transporte e, em seguida, envia os dados para a camada de rede. A camada de rede usa os dados recebidos da camada de transporte como seus próprios dados, adiciona um cabeçalho de camada de rede aos dados e envia os dados para a camada de link de dados. A camada de link de dados encapsula o cabeçalho da camada de link de dados e, em seguida, envia o cabeçalho encapsulado para a camada física. A camada física converte os dados em um fluxo de bits e envia o fluxo de bits para o host B em um link físico.
- Depois de receber o fluxo de bits na camada física, o host B envia o fluxo de bits para a camada de link de dados para processamento. Depois de receber o pacote, a camada de enlace de dados remove o cabeçalho do pacote da camada de enlace de dados e transmite o pacote para a camada de rede. Depois de receber o pacote, a camada de rede remove o cabeçalho do pacote IP e envia o pacote para a camada de transporte para processamento. A camada de transporte remove o cabeçalho do pacote IP do pacote e envia o pacote para a camada de aplicativo.
- O encapsulamento e o desencapsulamento de dados são realizados camada por camada. Cada camada processa os dados da camada superior ou inferior e adiciona ou remove o cabeçalho do pacote encapsulado.



A Função da Camada Física

- A camada física define os processos e funções elétricos e mecânicos para ativar, manter e remover linhas quando dois sistemas estão conectados.

- A camada física define os seguintes recursos:

- Nível de voltagem

- Taxa de transmissão de dados

| | LAN | | | | WAN | |
|--|------------------|------------------|------------------|------------------|---------------|-------------|
| Físico (Bits, sinais, temporização) | 8 0 2 3 | 8 0 2 4 | 8 0 2 5 | F D D I | V.24 G.703 | TIA/EIA-232 |

- Modo de conexão física
 - Distância máxima de transmissão

- Especifica o tipo de mídia, tipo de interface e tipo de sinalização.

- O padrão de camada física especifica o meio físico e o conector usados para conectar o dispositivo ao meio físico.
 - Padrões comuns de camada física para LANs incluem o padrão Ethernet 802.3 definido pelo IEEE, o padrão de barramento de token 802.4, o padrão de rede token ring 802.5 e o FDDI (fibre distribution data interface) definido pelo comitê X3T9.5 do ANSI (American National Standards Institute).
 - Padrões comuns de camada física para WANs incluem EIA/TIA-232 (RS-232), V.24 e V.35, e especificações físicas e elétricas de várias interfaces digitais. G.703, etc.



A Função da Camada de Link de Dados

Físico

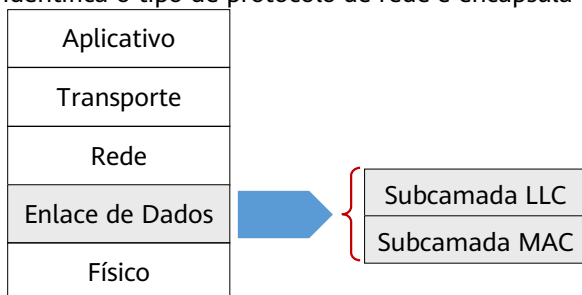
Enlace

Rede

Transporte

Aplicativo

- Subcamada MAC: Subcamada de Controle de Acesso ao Meio
 - Especifica como os dados são transmitidos em linhas físicas e se comunicam com a camada física.
- Subcamada LLC: Subcamada de Controle de Link Lógico
 - Identifica o tipo de protocolo de rede e encapsula os dados para transmissão pelo meio.



Função Principal da Camada de Enlace de Dados

- A principal função da camada de enlace de dados é transmitir dados entre a extremidade de transmissão e a extremidade de recepção por meio do meio físico.

- A camada do enlace de dados é a primeira camada lógica na camada física. A camada de enlace de dados executa o endereçamento físico no terminal para ajudar o dispositivo de rede a determinar se a mensagem deve ser transferida para cima ao longo da pilha de protocolos. Além disso, alguns campos são usados para informar ao dispositivo para qual pilha de protocolos (como IP e IPX) os dados devem ser transmitidos, e as funções de classificação e controle de tráfego são fornecidas.
- A camada de link de dados é dividida em duas subcamadas.:LLC,subcamada Controle de Link Lógico,MACs,LLC.
- A subcamada LLCestá localizada entre a camada de rede e a subcamada MAC. Ele identifica o tipo de protocolo e encapsula os dados para transmissão pela rede. A subcamada LLCexecuta a maioria das funções da camada de enlace de dados e algumas funções da camada de rede. Por exemplo, um quadro consiste nos dados a serem transmitidos, endereço e verificação CRC. Quando o quadro é recebido, ele é dividido e a identificação de endereço e a verificação de CRC são executadas. Além disso, as funções de controle de sequência de quadros, controle de erros e controle de fluxo são fornecidas. Além disso, ele executa algumas funções de camada de rede, como datagrama, circuito virtual e multiplexação.
- A subcamada MAC especifica como os dados são transmitidos em linhas físicas e se comunica com a camada física. Ele define o endereçamento físico, a topologia de rede, as especificações de linha, a notificação de erros, a entrega em ordem e o controle de tráfego.

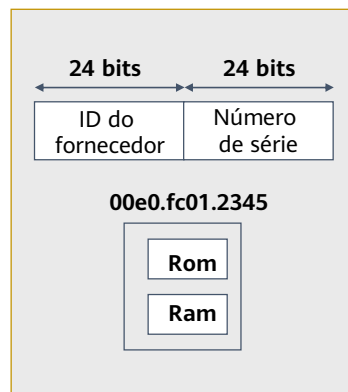


Endereço e Protocolos da Camada de Enlace

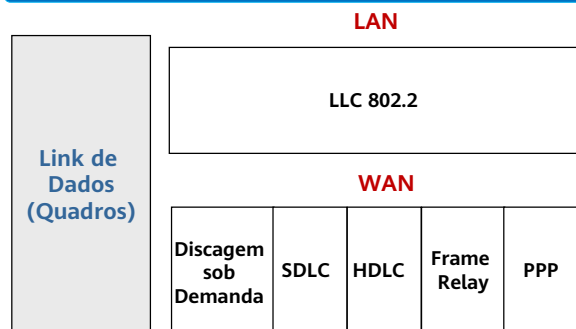
- O endereço MAC tem 48 bits, e os primeiros três bytes de produtos Huawei são 0x00E0FC.
- Protocolos LAN e WAN na camada do link de dados.



00e0.fc01.2345



Protocolos Comuns na Camada de Link de Dados



- Como se todos tivessem um nome, cada dispositivo de rede é identificado por um endereço físico, que é um endereço MAC. O endereço MAC de um dispositivo de rede é globalmente exclusivo. Um endereço MAC consiste em 48 bits binários, que geralmente são representados por dígitos hexadecimais. Os primeiros seis dígitos hexadecimais são alocados pelo IEEE aos fabricantes de dispositivos, e os últimos seis dígitos hexadecimais são alocados por cada fabricante. Por exemplo, os primeiros seis dígitos hexadecimais do endereço MAC dos produtos de rede da Huawei são 0x00e0fc.
- NIC, placa de interface de rede, também chamada de adaptador de rede, que tem um endereço MAC fixo. A maioria dos fornecedores de NIC gravam endereços MAC na ROM. Quando o adaptador de rede é inicializado, o endereço físico MAC na ROM é lido na RAM. Se uma nova placa de rede for inserida no computador, o endereço físico do computador se tornará o endereço físico da nova placa de rede.
- É importante observar que, se o seu computador tiver dois adaptadores de rede, ele terá dois endereços MAC. Portanto, alguns dispositivos de rede podem ter vários endereços MAC.
- IEEE 802.2 LLC é um protocolo de camada de link de dados comum para LANs. Protocolos comuns da camada de enlace de dados usados em WANs incluem: HDLC (Controle de enlace de dados de alto nível), PPP (Protocolo de ponto a ponto),
 - HDLC é um protocolo de camada de enlace de dados orientado a bit-synchronous desenvolvido pela ISO. Especifica o método de encapsulamento de dados de links seriais síncronos usando caracteres de quadro e soma de verificação.
 - O PPP é definido no RFC 1661. Ele consiste no Protocolo de Controle de Link (LCP), Protocolo de Controle de Rede (NCP) e conjunto de protocolos estendidos PPP. O PPP suporta links seriais síncronos e assíncronos e vários protocolos de camada de rede. PPP é o protocolo de encapsulamento padrão da camada de

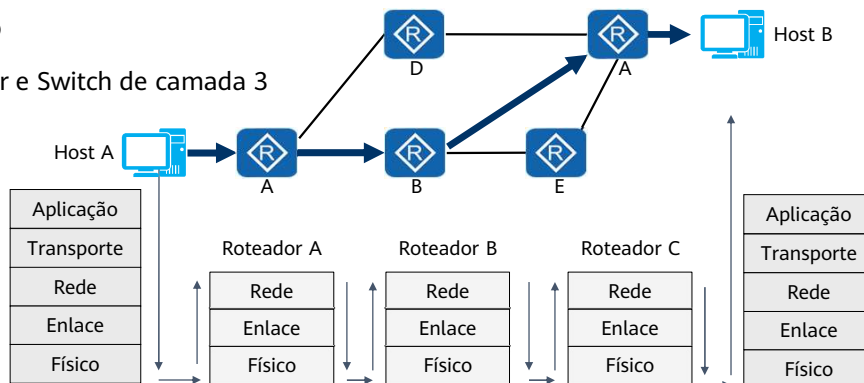
enlace de dados da interface serial em um roteador VRP.

- FR é um protocolo de link de dados comutado padrão do setor que usa verificação sem erros para acelerar o encaminhamento de dados.



Funções e Dispositivos da Camada De Rede

- Função
 - Encaminhando pacotes de dados entre redes diferentes
- Dispositivo
 - Roteador e Switch de camada 3

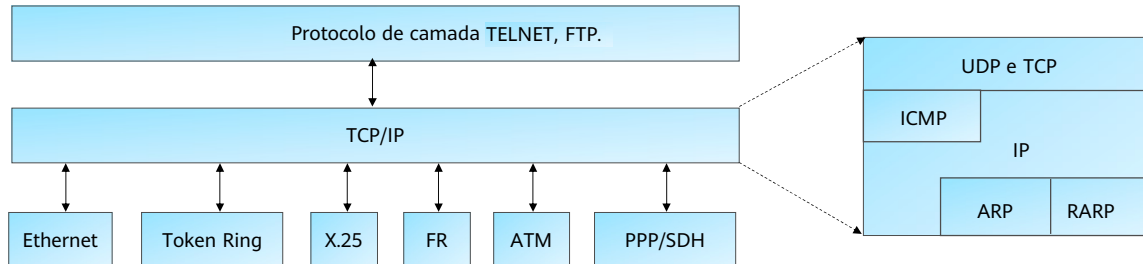


- A camada de rede é responsável pelo encaminhamento de pacotes de dados entre redes diferentes da origem para o destino. A camada de enlace de dados garante que os pacotes possam ser encaminhados entre dispositivos na mesma rede (o mesmo enlace) e a camada de rede garante que os pacotes possam ser encaminhados da origem para o destino através da rede (enlace cruzado). Há duas funções de camada de rede:
 - Fornecer endereços lógicos: Se os dados forem transmitidos pelas redes (vínculo cruzado), os endereços lógicos serão usados para endereçamento.
 - Roteamento: encaminha pacotes de dados de uma rede para outra.
- Roteadores são comumente usados na camada de rede para encaminhar pacotes entre redes diferentes. Conforme mostrado na figura, o Host A e o Host B em redes diferentes (links diferentes) se comunicam entre si. A interface do roteador na mesma rede (o mesmo link) que o Host A recebe o quadro de dados enviado pelo Host A. A camada de link do roteador analisa o cabeçalho do quadro e determina o quadro a ser enviado para si mesmo. Em seguida, o roteador envia o quadro para a camada de rede. A camada de rede determina o segmento de rede em que o endereço de destino reside, de acordo com o cabeçalho do pacote da camada de rede. Em seguida, a camada de rede encaminha o quadro para o próximo salto através da interface correspondente de acordo com a tabela até que o pacote atinja o Host B de destino.



Protocolo de Camada de Rede

- O protocolo IP fornece um modo de endereçamento unificado globalmente, que protege as diferenças de endereços de rede física e possibilita a pesquisa de rotas. Ele também fornece um formato de pacote unificado globalmente para proteger as diferenças na camada de link de rede e possibilitar a interconexão de rede.



- O IP é um dos protocolos mais importantes na arquitetura TCP/IP.
 - Os três protocolos que correspondem ao protocolo IP são o ARP (Address Translation Protocol), o RARP (Reverse Address Translation Protocol) e o ICMP (Internet Control Message Protocol).

- Protocolos comuns de camada de rede: Internet Protocol (IP), ICMP (Internet Control Message Protocol), ARP (Address Resolution Protocol), RARP (Reverse Address Resolution Protocol).
- O IP é o protocolo mais importante na camada de rede. Ele fornece endereçamento lógico, roteamento e encapsulamento de pacotes e funções de desencapsulamento. ICMP, ARP e RARP ajudam o IP.
- O ICMP é um protocolo de gerenciamento e fornece serviços de informações para IP. As mensagens ICMP são transportadas em pacotes IP.
- O ARP implementa o mapeamento dinâmico entre endereços IP e endereços de hardware, ou seja, os endereços de hardware são obtidos com base em endereços IP conhecidos.
- O RARP implementa o mapeamento dinâmico entre endereços de hardware e endereços IP. Ou seja, o RARP obtém endereços IP com base em endereços de hardware conhecidos.



Endereço da Camada de Rede

- Um endereço de rede identifica exclusivamente um dispositivo de rede na camada de rede.
- Um endereço de rede consiste em duas partes:
 - ID de rede
 - ID do host

Endereço IP

| ID de rede | ID do host |
|------------|------------|
| 10. | 8.2.48 |

- O endereço da camada de rede mencionado neste documento é o endereço IP. O endereço IP é um endereço lógico em vez de um endereço de hardware. O endereço de hardware é fixo na placa de interface de rede (NIC), como o endereço MAC mencionado acima, e é usado para comunicação entre dispositivos no mesmo link. Os endereços IP são usados para comunicação entre dispositivos em redes diferentes (links diferentes).
- Um endereço IP consiste em um endereço de rede e um endereço de host. O endereço IP consiste em 4 bytes e geralmente é representado em notação decimal pontilhada, por exemplo, 10.8.2.48. As seções a seguir descreverão os endereços IP em detalhes.



Principais Protocolos da Camada de Transporte

- Os protocolos da camada de transporte incluem TCP (Transfer Control Protocol) e UDP (User Datagram Protocol).

TCP

- Orientado a conexão
- Confiável
- Aplica-se a aplicativos com alta confiabilidade
- Alto custo

UDP

- Sem conexão
- Não confiável
- Aplica-se a aplicativos com alta eficiência
- A camada de aplicativo é responsável pela confiabilidade

Principais funções da camada de transporte

- Segmentar dados e combinar segmentos de dados
- Estabelecer conexões ponto a ponto
- Enviar segmentos de dados de um host para outro
- Garantir a exatidão da transmissão de dados (opcional).

- Embora o TCP e o UDP usem o IP como seu protocolo de camada de rede, eles fornecem serviços distintos para a camada de aplicativo.
- O TCP fornece serviços de fluxo de bytes confiáveis e orientados a conexão. Orientado a conexão significa que uma conexão TCP deve ser estabelecida entre dois aplicativos que usam TCP como o protocolo da camada de transporte antes que eles troquem dados. O TCP fornece serviços de transmissão confiáveis para aplicativos de camada superior por meio de mecanismos como confirmação, verificação e remontagem. No entanto, o estabelecimento, a validação e a verificação de conexões TCP consomem uma grande quantidade de trabalho e geram uma grande sobrecarga.
- O UDP fornece serviços simples e orientados a datagramas. O UDP não garante a confiabilidade, ou seja, os pacotes não podem alcançar o destino. O UDP é aplicável a aplicativos que se concentram mais na eficiência de transmissão, como SNMP e RADIUS. O SNMP monitora redes e envia alarmes intermitentemente. Se uma conexão TCP precisar ser configurada toda vez que uma pequena quantidade de informação for enviada, a eficiência de transmissão será reduzida. Portanto, os aplicativos que se concentram mais na eficiência de transmissão, como SNMP e RADIUS, selecionam UDP como o protocolo da camada de transporte. Além disso, o UDP também é aplicável aos protocolos da camada de aplicativos que têm mecanismos de confiabilidade.



Número da Porta da Camada de Transporte

- Formato de Segmento de Dados da Camada de Transporte

- Intervalo de números de porta: 0—65535

- 0 - 254 Público
 - 255 - 1023 Alocado para empresas
 - 1024 - acima Número de porta aleatório
 - O número de porta é usado para identificar o programa de aplicação ao qual a parte de carga útil pertence.

Números de porta comuns

| | |
|-----|-----------------------------------|
| 20 | File Transfer Protocol [Dados] |
| 21 | File Transfer Protocol [Controle] |
| 23 | Telnet |
| 25 | Simple Mail Transfer Protocol |
| 53 | Domain Name Server |
| 80 | World Wide Web HTTP |
| 119 | Network News Transfer Protocol |
| 161 | SNMP |
| 162 | SNMP TRAP |

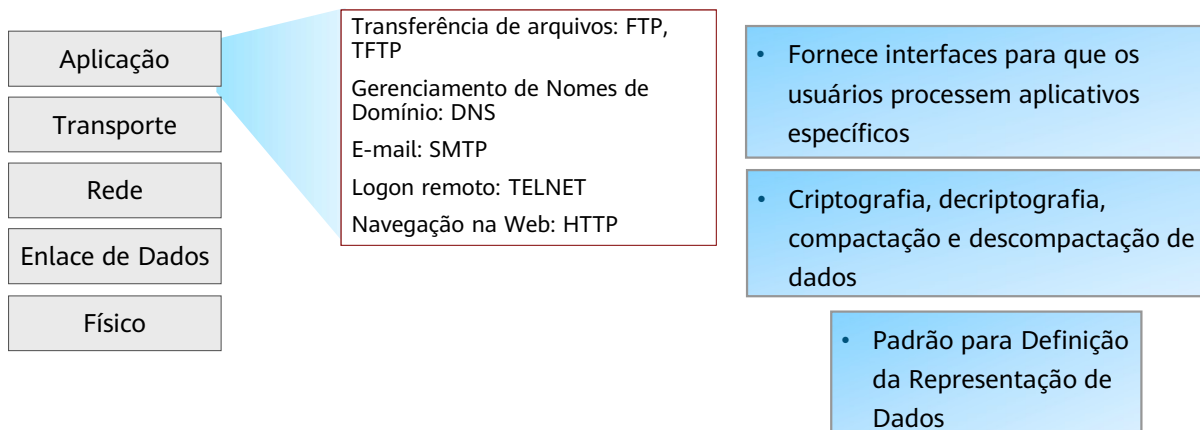
| | | | |
|------------------------------|-------------------------------|-----|---------------------------------|
| Porta de Origem (2 bytes) | Porta de Destino (2 bytes) | ... | Dados da camada de aplicação |
|------------------------------|-------------------------------|-----|---------------------------------|

- A camada de transporte protege a complexidade da rede para aplicativos de camada superior e define a conectividade completa entre aplicativos de host para implementar as seguintes funções básicas:
 - Encapsula e desapsula segmentos de dados enviados da camada de aplicativos para a camada de rede ou combina segmentos de dados enviados da camada de rede para a camada de aplicativos.
 - Estabelecimento de conexões ponta a ponta, principalmente conexões lógicas para transmissão de fluxos de dados.
 - Envia segmentos de dados de um host para outro. Envia segmentos de dados de um host para outro. Durante a transmissão, a exatidão dos dados é assegurada através do cálculo da soma de verificação e da realização de um controle de fluxo para evitar a sobrecarga do tampão.
- Alguns protocolos de camada de transporte garantem a correção da transmissão de dados. Esse mecanismo garante que os mesmos dados não sejam transmitidos várias vezes ou perdidos e que a sequência dos pacotes de dados recebidos seja a mesma que a sequência dos pacotes de dados enviados.



Funções da Camada de Aplicação

Físico Enlace Rede Transporte **Aplicativo**



- Há muitos protocolos na camada de aplicativo. Os seguintes protocolos ajudam você a usar e gerenciar a rede TCP/IP:
 - FTP (File Transfer Protocol, Protocolo de transferência de arquivos): usado para transferir arquivos independentes, geralmente para sessões interativas de usuários.
 - HTTP (Hypertext Transfer Protocol): Usado para transferir os arquivos que formam as páginas na World Wide Web.
 - TELNET : Transfere dados com informações de controle Telnet. Ele fornece um método padrão para interagir com dispositivos de terminal ou processos de terminal, e suporta conexões de terminal a terminal e computação distribuída processo a processo.
 - SMTP (Simple Message Transfer Protocol) & POP3 (Post Office Protocol).
 - DNS (Domain Name Server): os nomes de domínio podem ser convertidos em endereços IP e os recursos de nome de domínio podem ser gerenciados de maneira distribuída.
 - TFTP (Trivial File Transfer Protocol): Projeto de transferência de arquivos para fins gerais, alta taxa de transferência.
 - RIP (Routing Information Protocol): um protocolo usado por um roteador para trocar informações de roteamento em uma rede IP.
 - SNMP (Simple Network Management Protocol): coleta informações de gerenciamento de rede e troca informações de gerenciamento de rede entre o console de gerenciamento de rede e os dispositivos de rede (como roteadores, pontes e servidores).
 - Radius (Remote Authentication Dial In User Service): Protocolo de autenticação remota para acesso dial-up, que implementa autenticação, autorização e

contabilização para usuários de acesso.

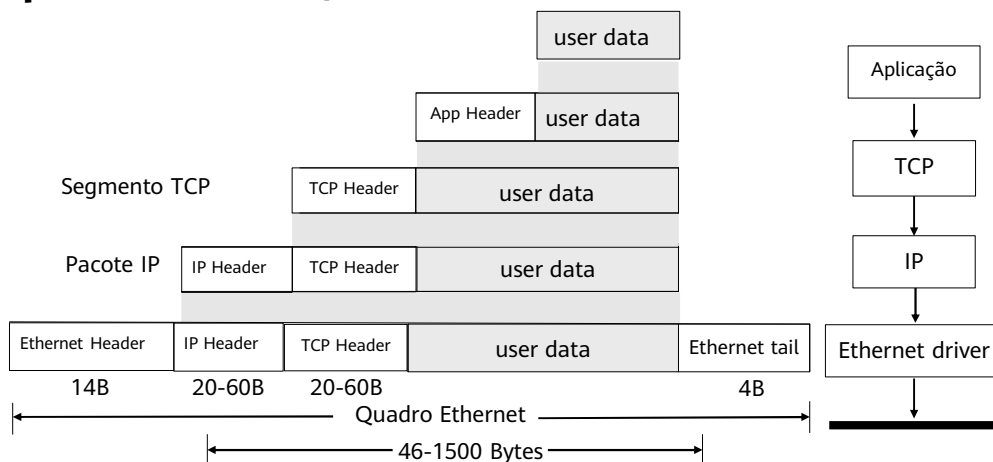


Contents

1. Visão geral da comunicação de dados
- 2. Pilha de protocolo TCP/IP**
 - Estrutura do Modelo TCP/IP
 - **Encapsulamento de Pacote da Pilha de Protocolo TCP/IP**
 - Endereçamento IP e Roteamento
3. Visão geral da Ethernet



O processo de encapsulamento da pilha de protocolo TCP/IP

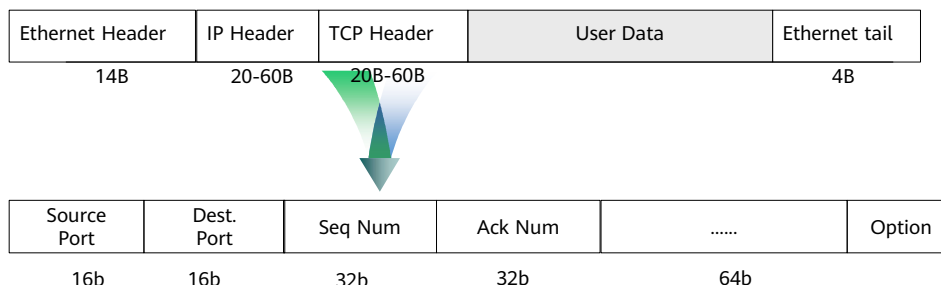


- A figura anterior mostra o processo de encapsulamento de pacotes TCP/IP quando TCP é usado na camada de transporte, IP é usado na camada de rede e Ethernet é usado na camada de link. Os dados do usuário são encapsulados pelo protocolo da camada de aplicativo e, em seguida, transmitidos para a camada de transporte. A camada de transporte encapsula o cabeçalho TCP e envia os dados para a camada de rede. A camada de rede encapsula o cabeçalho IP e, em seguida, envia os dados para a camada de link de dados. A camada de enlace de dados encapsula o cabeçalho e o trailer do quadro Ethernet e envia os dados para a camada física. A camada física envia os dados na forma de fluxos de bits para a linha física. A figura mostra o comprimento de cada campo no encapsulamento de dados Ethernet. A seguir está uma descrição do encapsulamento de cada camada de cima para baixo.



Segmento TCP

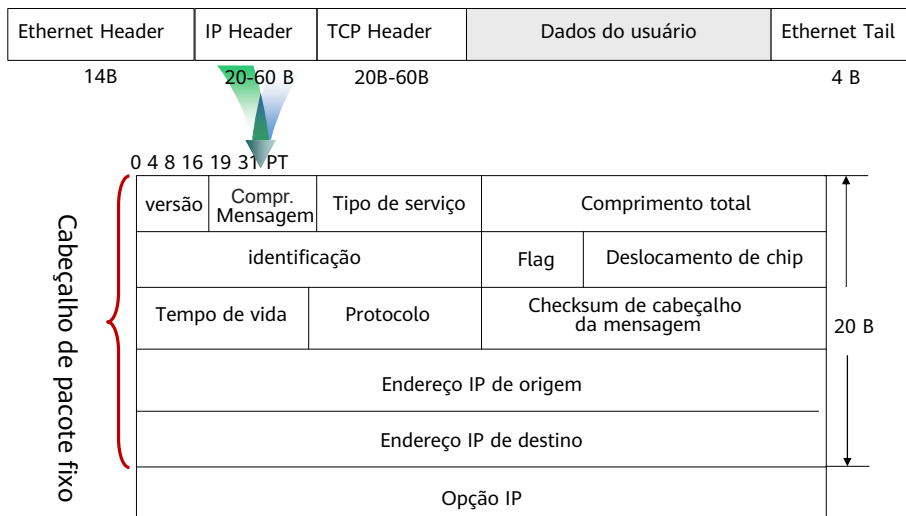
Quadro Ethernet



- O segmento de dados TCP é encapsulado no pacote de dados IP. Um pacote de dados TCP consiste em um cabeçalho TCP e um pacote de dados TCP. O cabeçalho TCP contém um máximo de 60 bytes. Se o campo Opção não estiver disponível, o comprimento normal será de 20 bytes.
- A figura a seguir mostra o cabeçalho TCP. Para obter detalhes sobre as funções do cabeçalho TCP, consulte o protocolo da camada de transporte.
 - Porta de Origem: Indica o número da porta de origem. O TCP atribui um número de porta de origem ao aplicativo.
 - Porta de Destino: número da porta de destino.
 - Número de Sequência: Identifica o fluxo de bytes de dados enviados do remetente TCP para o receptor TCP.
 - Ack Num: O número de sequência de confirmação contém o próximo número de sequência esperado pelo final do envio. Verifique se o número de sequência é o número de sequência dos dados recebidos com êxito da última vez mais 1.
 - Opção: campo Opção



Pacote IP



- Depois de receber o segmento de dados TCP da camada de transporte, a camada de rede adiciona as informações do cabeçalho IP da camada de rede ao segmento. O comprimento fixo de um cabeçalho IP comum é de 20 bytes (excluindo o campo de opção IP). Um cabeçalho de pacote IP consiste nos seguintes campos:
 - Version indica a versão do protocolo IP. Atualmente, a versão do protocolo IP é 4. O número da versão do protocolo IP de última geração é 6.
 - O comprimento do pacote refere-se ao número de palavras de 32 bits ocupadas pelo cabeçalho, incluindo quaisquer opções. É um campo de 4 bits, 24=16. Há 15 campos de valor válidos, exceto todos os itens 0. O valor máximo é 15, indicando que o cabeçalho ocupa 15 bits de 32 bits. Portanto, $32 \times 15/8 = 60$ bytes, e o comprimento máximo do cabeçalho é de 60 bytes.
 - O campo TOS (Tipo de serviço) de 8 bits inclui um campo COS (Classe de serviço) de 3 bits, um campo TOS de 4 bits e um bit não utilizado de 1 bit. O ToS de 4 bits representa o atraso mínimo, a throughput máxima, a confiabilidade máxima e o custo mínimo.
 - O comprimento total é o comprimento do datagrama IP inteiro, incluindo a parte de dados. Este campo tem 16 bits. Portanto, o comprimento máximo de um datagrama IP pode atingir 65535 bytes. Embora um datagrama IP de até 65.535 bytes possa ser transmitido, ele é fragmentado na maioria das camadas de link. Além disso, o host não pode receber pacotes de dados maiores que 576 bytes. O UDP restringe o comprimento de um pacote de dados do usuário a 512 bytes, que é menos de 576 bytes. Na verdade, a maioria das implementações atuais,

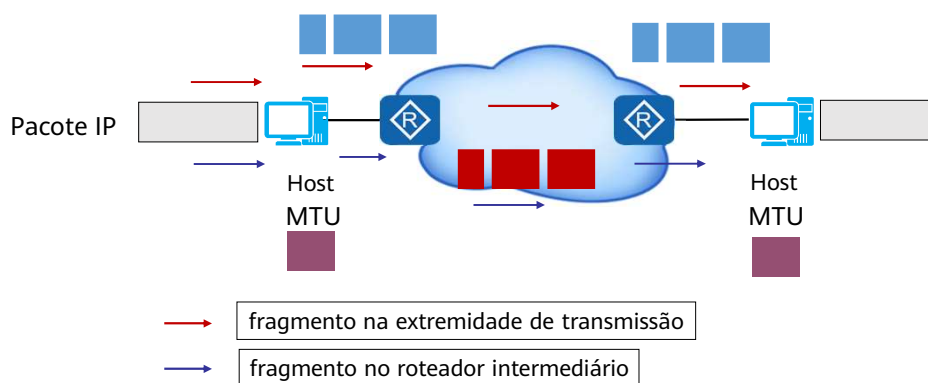
especialmente aquelas que suportam NFS, permitem datagramas IP maiores que 8192 bytes.

- O campo Identification (Identificação) identifica exclusivamente cada pacote enviado pelo host. Geralmente, o valor aumenta em uma unidade toda vez que um pacote é enviado.
- O campo Vida Útil (TTL) define o número de roteadores pelos quais um pacote pode passar. Quando um pacote passa por um roteador, o valor de TTL diminui em 1. Quando o valor de TTL é 0, o pacote é descartado.
- O campo Protocolo identifica o protocolo de camada superior carregado no pacote de dados. Semelhante ao número da porta, o protocolo IP usa o número do protocolo para identificar o protocolo da camada superior. O número de protocolo do TCP é 6 e o do UDP é 17.
- O campo checksum do cabeçalho IP é usado para calcular a soma de verificação do cabeçalho IP e verificar a integridade do cabeçalho do pacote.
- Os campos de endereço IP de origem e endereço IP de destino identificam os endereços IP dos dispositivos de origem e destino em um pacote de dados.



Problema de Fragmento IP

- Princípio do Fragmento: A camada IP compara o comprimento dos dados com a MTU. Se o comprimento dos dados for maior que a MTU, a camada IP fragmentará os dados.



- Na camada de rede física, o comprimento máximo de quadros a serem enviados cada vez é limitado. Quando a camada de IP recebe um pacote IP a ser enviado, ela precisa determinar a interface local para a qual o pacote deve ser enviado (seleção de rota) e consultar a interface para obter a MTU. O IP compara a MTU com o comprimento do pacote de dados e fragmenta o pacote de dados, se necessário.
- fragmento pode ocorrer no host do remetente original ou em um roteador intermediário.
- Depois que um datagrama IP é fragmentado, ele é remontado somente quando atinge o destino. A remontagem é executada pela camada IP da extremidade de destino. Os datagramas fragmentados podem ser refragmentados (podem ser mais de uma vez). Os dados contidos no cabeçalho IP fornecem informações suficientes para fragmentação e remontagem.
- Bit do sinalizador: 3 bits
- Vários bits de controle:
 - 0 Bit: reservado. Deve ser definido como 0.
 - 1 bit: (DF) 0 = fragmentável; 1 = não fragmentável .
 - 2 bits: (MF) 0 = último fragmento, 1 = mais fragmentos.
 - O DF e o MF não podem ser 1 ao mesmo tempo. Caso contrário, ocorrerá um conflito.
- Deslocamento do fragmento: indica onde o fragmento pertence ao fluxo de dados.
- Depois que um pacote IP é fragmentado, cada fragmento se torna um pacote de dados. Tem seu próprio cabeçalho IP e é independente de outros pacotes durante a seleção de rota.



Introdução ao Fragmento IP

- Princípio do Fragmento: A camada IP compara o comprimento dos dados com a MTU. Se o comprimento dos dados for maior que a MTU, a camada IP fragmentará os dados.
- O fragmento pode ocorrer no host do remetente ou pode ser enviado em um roteador intermediário.
- Depois que um pacote IP é fragmentado, ele só pode ser reagrupados quando chegar ao destino.
- O pacote de dados completo é retransmitido mesmo que apenas uma parte dos dados seja perdida.
- Qualquer cabeçalho de camada de transporte é exibido apenas na primeira parte dos dados.

Os campos no cabeçalho IP usados na fragmentação:

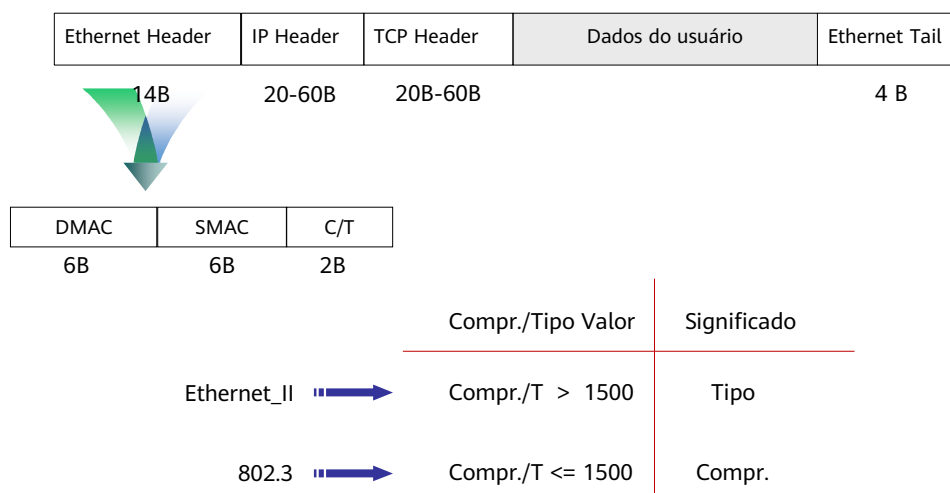
| | | | | |
|--------------------------|------------------------------|-----------------|-----------------------|------------------------------|
| versão | Compr. Cabeçalho | Tipo de serviço | Comprimento total | |
| Identificador de 16 bits | | | Flag | Deslocamento de fragmentação |
| Tempo de vida | Protocolo da camada superior | | Checksum de cabeçalho | |
| Endereço IP de origem | | | | |
| Endereço IP de destino | | | | |
| Opções IP | | | | |

- Depois que um datagrama IP é fragmentado, ele é remontado somente quando atinge o destino. (A remontagem aqui é diferente de outros protocolos de rede, que exigem a remontagem na próxima estação, não no destino final). A remontagem é feita pela camada IP de destino, que tem como objetivo tornar o processo de fragmentação e remontagem transparente para a camada de transporte (TCP e UDP), exceto por alguns possíveis saltos. Os datagramas fragmentados podem ser refragmentados (podem ser mais de uma vez). Os dados contidos no cabeçalho IP fornecem informações suficientes para fragmentação e remontagem.
- Os seguintes campos no cabeçalho IP são usados para o fragmento: Cada datagrama IP enviado pelo remetente tem um valor exclusivo no campo Identificador. Esse valor é copiado para cada fragmento quando o datagrama é fragmentado (agora vemos para que serve esse campo). O campo Sinalizadores usa um dos bits para indicar "mais fatias". Exceto para o último fragmento, esse bit é definido como 1 para cada fragmento que forma um datagrama. O campo Deslocamento do fragmento indica o deslocamento do fragmento desde o início do datagrama original. Além disso, depois que um datagrama é fragmentado, o comprimento total de cada fragmento deve ser alterado para o comprimento do fragmento. Finalmente, há um bit no campo flag chamado de bit "não-fragmento". Se esse bit for definido como 1, o IP não fragmentará o datagrama. Em vez disso, ele descarta o pacote e envia um pacote de erro ICMP para a extremidade de origem. O pacote de erro indica que o fragmento é necessário, mas o bit sem fragmento está definido.

- Depois que um datagrama IP é fragmentado, cada fragmento tem seu próprio cabeçalho IP e é independente de outros fragmentos durante a seleção de rota. Nesse caso, os fragmentos podem estar fora de ordem quando chegam ao destino, mas o cabeçalho IP contém informações suficientes para que o receptor monte corretamente os fragmentos.
- Embora o processo de fragmento de IP pareça transparente, há uma coisa que você não quer usar: ele retransmite o datagrama inteiro mesmo que apenas uma parte dos dados seja perdida. Por que isso aconteceu? A camada IP não tem um mecanismo de retransmissão de tempo limite. A camada superior é responsável pelo tempo limite e retransmissão (o TCP tem mecanismos de tempo limite e retransmissão, mas o UDP não. Alguns aplicativos UDP também executam timeouts e retransmissões). Quando um fragmento de um segmento de pacote TCP é perdido, o TCP retransmite o segmento de pacote TCP inteiro após o timeout. Este segmento de pacote corresponde a um pacote IP. Não há como retransmitir apenas um fragmento de um datagrama. Na verdade, se o pacote for fragmentado por um roteador intermediário, em vez do sistema de origem, o sistema de origem não poderá saber como o pacote é fragmentado. Por essa razão, o fragmento é frequentemente evitado.



Quadro de Ethernet



- O cabeçalho Ethernet consiste em três campos:
 - DMAC: indica o endereço MAC do terminal de destino.
 - SMAC: indica o endereço MAC de origem.
 - Campo COMPRIMENTO/TIPO: o significado varia de acordo com o valor:
 - Quando LENGTH/TYPE > 1500, o tipo de quadro de dados (como o tipo de protocolo da camada superior) é representado pelos seguintes tipos de protocolo:
 - Pacote IP 0X0800
 - 0X0806 Pacote de solicitação/resposta ARP
 - 0X8035 Pacote de solicitação/resposta RARP
 - Quando LENGTH/TYPE < 1500, indica o comprimento do quadro de dados.
 - DATA/PAD: Indica dados específicos. De acordo com a Ethernet, o comprimento mínimo da parte de dados é de 46 bytes, mas o comprimento é inferior a 46 bytes. Bytes de preenchimento precisam ser adicionados à parte de dados.
 - Campo FCS: campo de sequência de verificação de quadro, que é usado para determinar se um erro ocorre em um quadro de dados.



Contents

1. Visão geral da comunicação de dados
- 2. Pilha de protocolo TCP/IP**
 - Estrutura do Modelo TCP/IP
 - Encapsulamento de Pacote da Pilha de Protocolo TCP/IP
 - **Endereçamento IP e Roteamento**
3. Visão geral da Ethernet



Encapsulamento de Dados na Camada de Rede

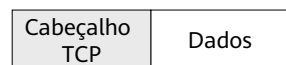
- Um endereço IP identifica exclusivamente um dispositivo de rede e consiste em 32 bits binários.

- O endereço IP é exibido em notação decimal pontuada

- O endereço IP é dividido em duas partes:

- Endereço de rede
- Endereço do host

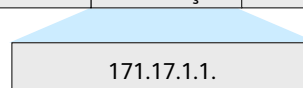
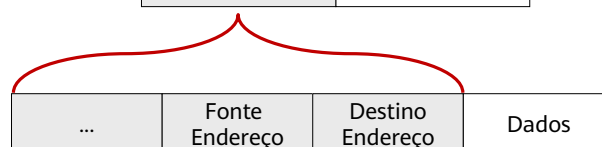
IP
Endereço



Transporte



Rede



Endereço IP

- O endereço IP é um número binário de 32 bits de 4 bytes em notação decimal pontuada.

- Exemplo :10000000.00000001.11111111.11111110 Notação decimal: :128.1.255.254

- A camada de rede recebe dados da camada de transporte e adiciona os endereços de origem e destino aos dados.
- Os endereços MAC são geralmente armazenados no espaço de endereço de um plano e não têm uma hierarquia de endereço clara. Portanto, os endereços MAC são aplicáveis somente à comunicação de hosts no segmento de rede local. Além disso, os endereços MAC são fixos no hardware e têm pouca flexibilidade. Para a comunicação entre redes diferentes, o endereço IP, que é um endereço de camada de rede, é geralmente usado para fornecer mais flexibilidade.
- Um endereço IP também é chamado de endereço lógico. Como um endereço MAC, um endereço IP é exclusivo. Cada dispositivo de rede é identificado exclusivamente por um endereço IP.
- Um endereço IP consiste em 32 bits binários. Esses bits binários são divididos em quatro octetos. A camada de rede recebe dados da camada de transporte e adiciona os endereços de origem e destino aos octetos nos dados. O endereço IP pode ser expresso da seguinte forma:
 - Em notação decimal pontilhada: 10.110.128.111
 - Binário geminado: 00001010.01101110.10000000.01101111
 - Hexadecimal: 0a.6e.80.6f
 - Geralmente, um endereço IP é expresso em notação decimal pontilhada. Ela raramente é expressa em notação hexadecimal.

- A solução de endereço IP em camadas é semelhante à solução de número de telefone comum. O número de telefone é único em todo o mundo. Por exemplo, para um número de telefone 010-82882484, o campo 010 indica o código de área de Pequim e o campo 82882484 indica um número de telefone em Pequim. O mesmo é verdadeiro para endereços IP. A primeira parte indica um segmento de rede e a segunda parte indica um dispositivo no segmento de rede.
- Os endereços IP são projetados de maneira hierárquica. Dessa forma, cada dispositivo de rede da camada 3 não precisa armazenar o endereço IP de cada host, mas armazena o endereço de rede de cada segmento de rede (o endereço de rede representa todos os hosts no segmento de rede). Isso reduz muito o número de entradas de roteamento e melhora a flexibilidade do roteamento.
- Endereço IP: identifica exclusivamente um host na rede.



Classificação do Endereço IP

| | | | | | | | | | | | |
|----------|---------------------------|--|---------------|--|----------------|----------------|----------------|---------------|--------------------|--|-----------|
| | 1.0.0.0~126.255.255.255 | | | | | | | | | | |
| Classe A | 0 | | Rede (7 bits) | | Host (24 bits) | | | | | | |
| | 128.0.0.0~191.255.255.255 | | | | | | | | | | |
| Classe B | 1 | | 0 | | Rede (14 bits) | Host (16 bits) | | | | | |
| | 192.0.0.0~223.255.255.255 | | | | | | | | | | |
| Classe C | 1 | | 1 | | 0 | | Rede (21 bits) | Host (8 bits) | | | |
| | 224.0.0.0~239.255.255.255 | | | | | | | | | | |
| Classe D | 1 | | 1 | | 1 | | 0 | | Endereço Multicast | | |
| | 240.0.0.0~255.255.255.255 | | | | | | | | | | |
| Classe E | 1 | | 1 | | 1 | | 1 | | 0 | | Reservado |

- A parte de rede de um endereço IP é chamada de endereço de rede. Um endereço de rede identifica exclusivamente um segmento de rede ou uma agregação de vários segmentos de rede. Os dispositivos de rede no mesmo segmento de rede têm o mesmo endereço de rede. A parte de host de um endereço IP é chamada de endereço de host, que identifica exclusivamente um dispositivo de rede no mesmo segmento de rede. Por exemplo, o endereço IP da classe A é 10.110.192.111, o endereço de rede é 10 e o endereço do host é 110.192.111.
- Como distinguir o endereço de rede e o endereço de host de um endereço IP? Inicialmente, os designers de redes de interconexão definem as classes de endereço com base na escala da rede. Os endereços IP são classificados em cinco classes: A, B, C, D e E.
- O endereço de rede de um endereço IP classe A é o primeiro octeto e o primeiro byte começa com 0. Portanto, o número de bits válidos de um endereço de rede da classe A é 7 (8 - 1), e o primeiro byte do endereço de rede da classe A varia de 1 a 126 (127 é reservado). Por exemplo, 10.1.1.1 e 126.2.4.78 são endereços da classe A. O comprimento do endereço do host de um endereço de classe A são os últimos três bytes (24 bits). Os endereços IP da Classe A variam de 1.0.0.0 a 126.255.255.255. Cada rede da classe A tem 224 endereços IP da classe A.
- O endereço de rede de um endereço IP de classe B é o primeiro de dois octetos e o primeiro byte começa com 10. Portanto, o número de bits válidos de um endereço de rede da classe B é 14 (16 - 2), e o primeiro byte do endereço de rede da classe B varia de 128 a 191. Por exemplo, 128.1.1.1 e 168.2.4.78 são endereços da classe B. O

comprimento do endereço do host de um endereço de classe B são os últimos dois bytes (16 bits). Os endereços IP da Classe B variam de 128.0.0.0 a 191.255.255.255. Cada rede de classe B tem 2¹⁶ endereços IP de classe B.

- O endereço de rede de um endereço IP de classe C é o primeiro de três octetos e o primeiro byte começa com 110. Portanto, o número de bits válidos de um endereço IP de classe C é 21 ($24 - 3$), e o primeiro byte do endereço IP de classe C varia de 192 a 223. Por exemplo, 192.1.1.1 e 120.2.4.78 são endereços da classe C. O endereço do host em um endereço de classe C é o último octeto (8 bits). Os endereços IP da classe C variam de 192.0.0.0 a 223.255.255.255. Cada rede da classe C tem $2^8 = 256$ endereços IP da classe C.
- O primeiro octeto de um endereço de classe D começa com 1110. Portanto, o primeiro byte de um endereço de classe D varia de 224 a 239. Os endereços da classe D são geralmente usados como endereços multicast.
- O primeiro byte de um endereço de classe E varia de 240 a 255 e é reservado para pesquisa científica.



Endereço IP Especial

| Rede | Host | Tipo de Endereço | Função |
|-----------|-----------|-----------------------|---|
| Qualquer | Todos "0" | Endereço de rede | Indica um segmento de rede. |
| Qualquer | Todos "1" | Endereço de Broadcast | Todos os nós em um segmento de rede especificado |
| 127 | Qualquer | Endereço de Loopback | Teste de loopback |
| Todos "0" | | Todas as Redes | Roteadores VRP Huawei são usados para especificar a rota padrão |
| Todos "1" | | Endereço de Broadcast | Todos os nós no segmento de rede atual |

- Um endereço IP é usado para identificar exclusivamente um dispositivo de rede, mas nem todos os endereços IP estão disponíveis. Alguns endereços IP especiais são usados para várias finalidades e não podem ser usados para identificar dispositivos de rede.
- Um endereço IP cuja parte do host é todos 0s é chamado de endereço de rede. Um endereço de rede identifica um segmento de rede. Por exemplo, endereço classe A 1.0.0.0, endereço privado 10.0.0.0 e 192.168.1.0.
- Um endereço IP cuja parte do host é todo 1s é chamado de endereço de broadcast de segmento de rede. Um endereço de difusão identifica todos os hosts em uma rede. Por exemplo, um roteador pode encaminhar pacotes de broadcast em segmentos de rede como 10.0.0.0 ou 192.168.1.0, por exemplo, 10.255.255.255 e 192.168.1.255. Um endereço de broadcast é usado para enviar pacotes de dados para todos os nós no segmento de rede local.
- Um endereço IP cujo segmento de rede é 127, como 127.0.0.1, é normalmente usado para testes de loop.
- O endereço IP 0.0.0.0 com todos os 0s representa todos os hosts. Os roteadores da série Huawei VRP usam o endereço IP 0.0.0.0 para especificar a rota padrão.
- O endereço IP completo 255.255.255.255 também é um endereço de broadcast. 255.255.255.255 representa todos os hosts e é usado para enviar pacotes de dados para todos os nós na rede. Tais pacotes de broadcast não podem ser encaminhados por roteadores.
- Conforme mencionado acima, cada segmento de rede tem alguns endereços IP que

não podem ser usados como endereços IP de host. A seguir está uma descrição de como calcular os endereços IP disponíveis.

- Por exemplo, um segmento de rede classe B 172.16.0.0 tem 16 bits de host, portanto tem 216 endereços IP. Depois que 172.16.0.0 é removido, um endereço de broadcast 172.16.255.255 não pode ser usado para identificar um host. Portanto, há um total de $2^{16}-2$ endereços disponíveis.
- O segmento de rede de classe C 192.168.1.0 tem 8 bits de host e um total de $2^8 = 256$ endereços IP. Depois que o endereço de rede 192.168.1.0 e o endereço de broadcast 192.168.1.255 forem excluídos, haverá 254 endereços de host disponíveis.
- O número de endereços de host disponíveis em cada segmento de rede pode ser calculado usando a seguinte fórmula: Se o número de bits na parte de host do segmento de rede for n , o número de endereços de host disponíveis será 2^n-2 .
- Dispositivos de camada de rede, como roteadores, usam endereços de rede para representar hosts no segmento de rede local. Isso reduz muito o número de entradas de roteamento em roteadores.



Endereço IP Privado

- Endereços IP privados não podem ser usados na Internet.
- Endereço IP Privado
 - 10.0.0.0~10.255.255.255
 - 172.16.0.0~172.31.255.255
 - 192.168.0.0~192.168.255.255

- Durante o planejamento de endereço IP, os endereços IP privados são geralmente usados na rede interna de uma empresa.
- Os endereços IP privados são reservados pela InterNIC e alocados pelas intranets das empresas. Um usuário não pode acessar diretamente a Internet usando um endereço IP privado. A razão é simples. O endereço IP privado não pode ser usado na rede pública. Não há rota para o endereço IP privado na rede pública. Portanto, ocorre o problema de conflito de endereço. Quando os usuários acessam a Internet, a tecnologia de conversão de endereço de rede (NAT) é usada para converter endereços IP privados em endereços IP públicos que podem ser identificados pela Internet. Os seguintes segmentos de rede são reservados como endereços IP privados para a InterNIC:
 - Classe A 10.0.0.0~10.255.255.255;
 - Classe B 172.16.0.0~ 172.31.255.255;
 - Classe C 192.168.0.0~192.168.255.255
- O uso de endereços IP privados não apenas reduz o investimento na compra de endereços IP públicos, mas também economiza recursos de endereços IP.



Introdução à Máscara de Sub-rede

- Use a máscara para distinguir a parte da rede da parte do host.
- O formato da máscara é o mesmo do endereço IP.
- Na máscara, a parte da rede e a parte da sub-rede são representadas por 1, e a parte do host é representada por 0.
- A máscara e o endereço IP são expressos da mesma maneira. Na máscara, 1 indica o bit de rede e 0 indica o host. Um octeto 255 indica oito uns.
- Por padrão, a máscara de sub-rede da rede de classe A é 255.0.0.0, a da rede de classe B é 255.255.0.0 e a da rede de classe C é 255.255.255.0.

Por exemplo, a máscara de sub-rede da rede de classe B é 255.255.0.0.



Endereço de Rede e Máscara de Sub-rede

- Endereço IP Classful:
 - Há três tipos de id de rede: 8, 16 e 24
- Endereço IP Classless:
 - O id de rede pode ser definido para qualquer valor de 1 a 32.
- Vantagens dos endereços IP sem classe:
 - Funcionamento em rede flexível e gerenciamento fácil
 - Reduzindo o desperdício de endereços IP
- Conforme mostrado na figura anterior, 192.168.1.100 é um endereço Classe C padrão e a máscara de sub-rede é 255.255.255.0. O endereço de rede desse endereço é 192.168.1.0.

Endereço IP :

| | |
|-----------|-----|
| 192.168.1 | 100 |
|-----------|-----|

Máscara de sub-rede:

| | |
|-------------|---|
| 255.255.255 | 0 |
|-------------|---|

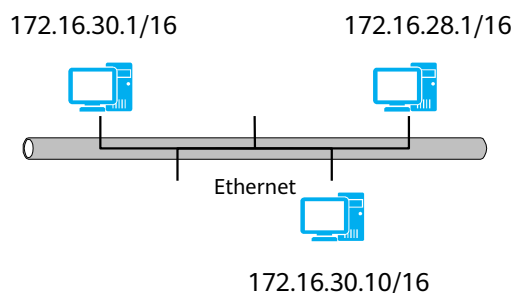
Endereço de rede:

| | |
|-----------|---|
| 192.168.1 | 0 |
|-----------|---|



Endereçamento sem Sub-rede

- O endereçamento sem sub-rede usa máscaras naturais e não divide segmentos de rede. Para endereços IP Classful, o comprimento do id de rede pode ser 8, 16 ou 24.
- Por exemplo, o segmento de rede da classe B 172.16.0.0 usa a máscara natural 255.255.0.0.

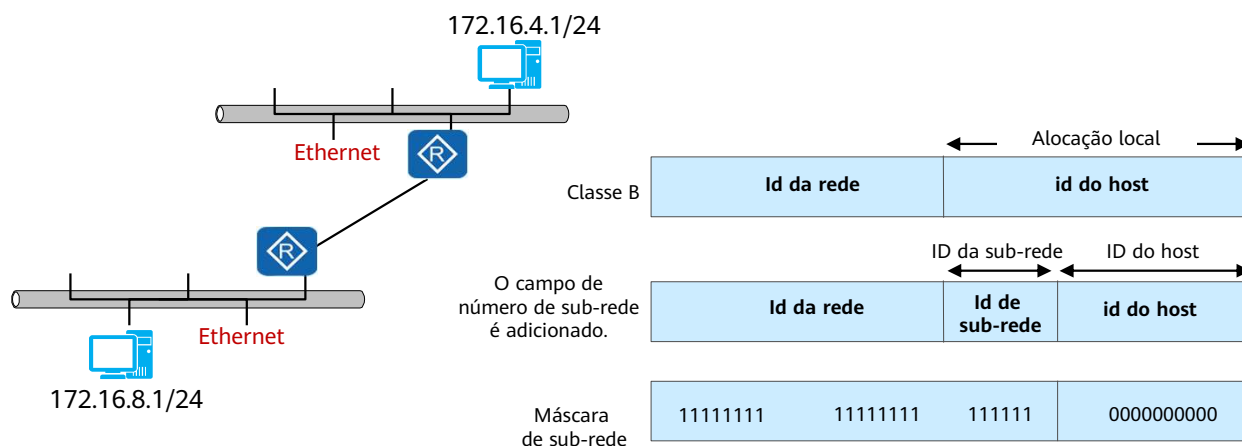


- Para uma organização de endereço IP que não tem uma sub-rede, a rede externa considera a organização como uma rede única e não precisa conhecer a estrutura interna. Por exemplo, todas as rotas para o endereço 172.16.X.X são consideradas na mesma direção, independentemente do terceiro e quarto pacotes de 8 bits do endereço. Essa solução tem a vantagem de reduzir o número de entradas na tabela de roteamento.
- No entanto, esta solução não distingue diferentes segmentos de sub-rede em uma rede grande. Como resultado, todos os hosts da rede podem receber pacotes de broadcast na rede grande, o que diminui o desempenho da rede e dificulta o gerenciamento da rede.
- Por exemplo, uma rede Classe B pode conter 65.000 hosts. Se um usuário que solicita um endereço de classe B precisa apenas de 100 endereços IP, os endereços IP restantes não podem ser usados por outros usuários, o que causa um grande desperdício. Portanto, é necessário um método para dividir a rede em diferentes segmentos de rede. Gerencia sub-redes por sub-rede.



Endereço IP Classless

- Segmento de rede de classe B 172.16.0.0



- Da perspectiva da atribuição de endereço, uma sub-rede é uma extensão de um endereço de segmento de rede. O administrador da rede determina o tamanho da sub-rede com base nas necessidades de crescimento da organização.
- Os dispositivos de rede usam máscaras de sub-rede para determinar qual parte de um endereço IP é a parte da rede e qual parte é a parte do host.
- A máscara de sub-rede está no mesmo formato que o endereço IP. A rede e as partes de sub-rede da máscara de sub-rede são todas 1 e a parte do host é toda 0. Por padrão, a máscara de sub-rede da rede de classe A é 255.0.0.0, a máscara de sub-rede da rede de classe B é 255.255.0.0 e a máscara de sub-rede da rede de classe C é 255.255.255.0. Usando sub-redes, o uso de endereços de rede é mais eficiente. Externamente, a rede ainda é uma rede. Internamente, a rede é dividida em sub-redes diferentes.
- Conforme mostrado na figura anterior, 172.16.0.0 é dividido em dois segmentos de rede: 172.16.4.0 e 172.16.8.0.
- Suponha que o departamento financeiro de uma empresa use o segmento de sub-rede 172.16.4.0. 172.16.8.0 é usado pelo Departamento de Engenharia. Dessa forma, o roteador pode executar o roteamento de acordo com o endereço da sub-rede de destino, e os pacotes de broadcast de uma sub-rede são impedidos de serem enviados para outros segmentos de rede, sem afetar a eficiência da rede.



Representação de Máscara de Sub-rede

- De acordo com a pilha do protocolo TCP/IP, uma máscara de sub-rede de 32 bits é usada para indicar o comprimento do campo de número de sub-rede.
- A máscara de sub-rede consiste em uma série de 1 e 0.

- O valor 1 corresponde à rede campos número e número de sub-rede.

| | | | | | | | |
|----------|----------|----------|----------|----------|---|---|---|
| IP | 192 | . | 168 | . | 1 | . | 7 |
| Endereço | 11000000 | 10101000 | 00000001 | 00000111 | | | |

- O valor 0 corresponde ao campo de número de host.

| | | | | | | | |
|------------------|----------|----------|----------|----------|-----|---|-----|
| Máscara Sub-rede | 255 | . | 255 | . | 255 | . | 240 |
| | 11111111 | 11111111 | 11111111 | 11110000 | | | |

- 1 e 0 não podem ser usados ao mesmo tempo.

Número de bits de máscara de sub-rede

$$8 + 8 + 8 + 4 = 28$$

Máscara de sub-rede

192. 168. 1 . 7 / 28

- Com um bom comando de conversões binário-para-decimal, a correspondência entre endereços IP e máscaras de sub-rede em sistemas binários e decimais é fácil de entender. O número de bits na máscara de sub-rede é 28 ($8 + 8 + 8 + 4 = 28$), indicando que o número de 1s consecutivos na máscara de sub-rede é 28 (1, indicando que há 28 bits de rede).
- Outra representação da máscara de sub-rede é /28=255.255.255.240, que é chamada de notação de barra invertida.
- Os endereços IP são hierárquicos;
- O endereço IP é diferente do número de telefone, que não pode refletir a localização geográfica do host;
- Um host que pertence a várias redes e tem vários endereços IP (como um roteador). As redes e sub-redes desses endereços IP são diferentes.



Conversão do Sistema de Endereço IP

- Endereço IP: 192.168.1.11 (Decimal)

| Byte (8 bits) | Byte (8 bits) | Byte (8 bits) | Byte (8 bits) |
|-----------------------------------|-----------------------------------|-----------------------------------|-----------------------------------|
| $2^7 2^6 2^5 2^4 2^3 2^2 2^1 2^0$ | $2^7 2^6 2^5 2^4 2^3 2^2 2^1 2^0$ | $2^7 2^6 2^5 2^4 2^3 2^2 2^1 2^0$ | $2^7 2^6 2^5 2^4 2^3 2^2 2^1 2^0$ |
| 1 1 0 0 0 0 0 | 1 0 1 0 1 0 0 | 0 0 0 0 0 0 1 | 0 0 0 0 1 0 1 1 |
| 192 | 168 | 1 | 11 |

- Número binário :
 - 11000000.10101000.0000001.00001011

- Cada endereço IP é um valor de 32 bits gravado em quatro bytes de 8 bits. Isso significa que há quatro grupos, cada um contendo oito bits binários, como mostrado na figura acima.



A Função do Roteador

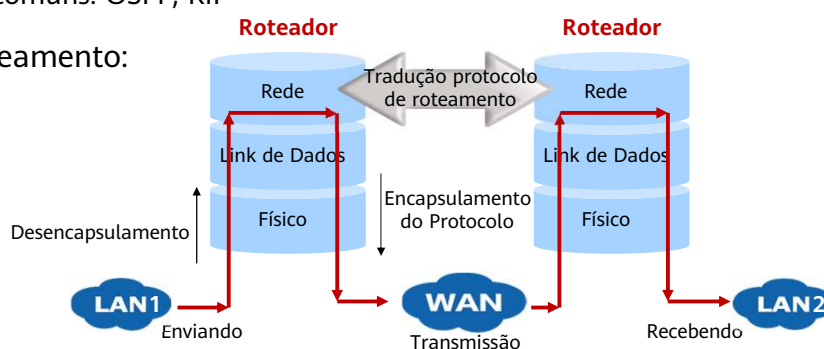
- Os roteadores operam na camada de rede e implementam a interconexão de redes.
 - Geram uma tabela de roteamento.
 - Encaminham pacotes de dados para outras redes.
- Encaminhamento de Pacotes de Dados
 - **Roteamento:** Criação, atualização e consulta da tabela de roteamento.
 - **Adaptação de Taxa:** Ajuste da taxa de transmissão entre sub-redes.
 - **Isolamento de Redes:** Previnem tempestades de rede e especificam regras de acesso (firewalls).
 - **Interconexão de Redes Heterogêneas:** Conectam diferentes tipos de redes.

- Roteadores são usados para conectar redes diferentes. Os dados podem ser encaminhados na Internet.
- Encaminhamento de dados: os roteadores devem ser capazes de encaminhar pacotes de dados com base em seus endereços de rede de destino.
- Roteamento: Para encaminhar dados, um roteador deve ser capaz de estabelecer e atualizar a tabela de roteamento e encaminhar pacotes de dados com base na tabela de roteamento.
- Backup e controle de tráfego: Para garantir a operação confiável da rede, os roteadores fornecem as funções de comutação entre links ativos e em espera e de controle de tráfego.
- Adaptação de taxa: interfaces diferentes têm taxas diferentes. Os roteadores podem usar seus próprios caches e protocolos de controle de fluxo para adaptação de taxa.
- Rede isolada: os roteadores podem isolar redes de difusão para evitar tempestades de difusão. Além disso, os roteadores podem implementar políticas flexíveis de filtragem de pacotes (firewalls) para garantir a segurança da rede.
- Interconexão das redes heterogêneas: a intenção original da Internet é implementar interconexão heterogênea de rede. Roteadores modernos geralmente implementam mais de dois protocolos de rede para implementar interconexão de rede heterogênea.



O Processo de Funcionamento do Roteador

- A tabela de roteamento pode ser configurada estaticamente ou gerada por um protocolo de roteamento dinâmico, como:
 - Entradas de roteamento geradas por protocolos de roteamento;
 - Protocolos de roteamento comuns: OSPF, RIP
- Conteúdo da Tabela de Roteamento:
 - Endereço de Destino
 - Máscara
 - Interface de saída
 - Próximo Salto



- Conforme mostrado na figura, o processo de trabalho de um roteador é o seguinte:
 - A camada física recebe um pacote de uma porta de roteador e o envia para a camada de enlace de dados.
 - A camada de enlace de dados remove o encapsulamento da camada de enlace e envia o pacote para a camada de rede com base no campo de protocolo do pacote.
 - A camada de rede verifica se o pacote é enviado para o dispositivo local. Se o pacote for enviado para o dispositivo local, a camada de rede será removida e o pacote será enviado para a camada superior. Se o endereço IP de destino do pacote não estiver na tabela de roteamento, o roteador pesquisará na tabela de roteamento uma rota com base no endereço IP de destino do pacote. Se uma rota for encontrada, o roteador enviará o pacote para a camada de enlace de dados da porta correspondente. Depois que o pacote é encapsulado na camada do enlace de dados, o roteador envia o pacote. Se nenhuma rota for encontrada, o pacote será descartado e as informações de erro serão enviadas conforme necessário.
- A tabela de roteamento é a chave para roteadores encaminharem pacotes de dados. Cada roteador armazena uma tabela de roteamento. Cada entrada de roteamento na tabela especifica a porta física do roteador através da qual o pacote de dados é enviado para uma sub-rede ou um host. Em seguida, o pacote de dados pode ser enviado ao próximo roteador ao longo do caminho ou enviado ao host de destino na rede conectada diretamente sem passar por outros roteadores.

- A tabela de roteamento contém as seguintes entradas-chave:
 - Endereço de destino: Identifica o endereço de destino ou a rede de um pacote IP.
 - Mask: Este parâmetro e o endereço de destino identificam o endereço do segmento de rede onde o host ou roteador de destino está localizado. O endereço do segmento de rede do host ou roteador de destino pode ser obtido depois que a operação lógica E é executada no endereço de destino e na máscara de rede.
 - Interface de saída: Indica a interface do roteador a partir da qual o pacote IP é encaminhado.
 - Próximo salto : indica o endereço de interface do próximo roteador pelo qual o pacote IP passa.



Contents

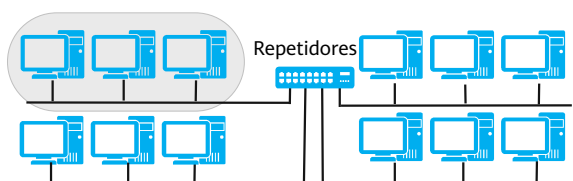
1. Visão geral da comunicação de dados
2. Pilha de protocolo TCP/IP
- 3. Visão geral da Ethernet**



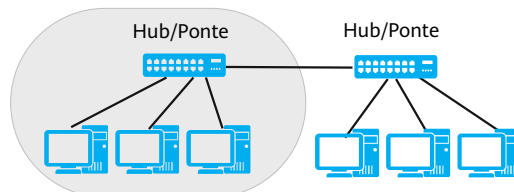
O que é Ethernet?

- Ethernet é uma tecnologia de implementação de redes locais (LAN) definida na norma IEEE 802.3 e faz parte do padrão de LAN/MAN.
- A suíte de protocolos 802.X especifica o modo de acesso à rede. As tecnologias de Ethernet comutado e Fast Ethernet são conhecidas como o protocolo 802.X.

Tipo de barramento (10BASE2 e 10BASE5 iniciais)



Estrela (outras Ethernets após 10BASE-T)



- Padrão Ethernet IEEE802.3
- Padrão Fast Ethernet IEEE802.3u 100BASE-T
- Padrão Gigabit Ethernet IEEE802.3z/ab 1000 Mbit/s
- Padrão Ethernet IEEE802.3ae 10GE



Protocolo Ethernet (1)

| Velocidade de transmissão | Padrão |
|---------------------------------|--|
| Ethernet padrão 10 Mbps | A Ethernet pode ser conectada através de vários meios de transmissão, como cabos coaxiais grossos, cabos coaxiais finos, pares trançados sem blindagem, pares trançados blindados e fibras ópticas. A norma IEEE 802.3 define diferentes padrões da camada física para diversos meios de transmissão. |
| Fast Ethernet 100 Mbps | Pode proteger efetivamente o investimento dos clientes na infraestrutura de cabeamento. Suporta a conexão de pares trançados Categoria 3, 4 e 5 e fibras ópticas, e pode efetivamente usar as instalações existentes. O padrão fast Ethernet de 100 Mbps é dividido em três subcategorias: 100BASE-TX, 100BASE-FX e 100BASE-T4. |
| Ethernet Gigabit 1000 Mbit/S | A tecnologia gigabit ainda é uma tecnologia Ethernet. Como esta tecnologia não muda a aplicação desktop nem o sistema operacional da Ethernet tradicional, ela pode funcionar bem com as velocidades de 10 Mbps ou 100 Mbps da Ethernet. A atualização para Ethernet Gigabit maximiza a proteção do investimento sem alterar as aplicações de rede, os componentes de gerenciamento de rede ou o sistema operacional de rede. A tecnologia Ethernet Gigabit possui dois padrões: IEEE 802.3z e IEEE 802.3ab. |

- A Ethernet é a tecnologia dominante nas LANs atuais. A maior parte do tráfego na Internet inicia e termina em uma conexão Ethernet. Desde a década de 1970, a Ethernet evoluiu para atender à crescente demanda por LANs de alta velocidade. Quando o novo meio, fibra óptica, é fabricado, a Ethernet é adotada, aproveitando ao máximo a enorme largura de banda e a baixa taxa de erro da fibra óptica. Usando o mesmo protocolo básico, a taxa de transmissão de dados pode chegar a 100 Gbit/s em 1973.
- O sucesso da Ethernet está em sua simplicidade e facilidade de manutenção, sua capacidade de incorporar novas tecnologias, sua confiabilidade e seus baixos custos de instalação e atualização.
- Cabos IEEE802.3: além de cabos coaxiais e pares torcidos, os cabos IEEE802.3 também incluem fibras 10BASE-F. 10BASE-F tem sido usado na fase inicial e sua distância de transmissão pode chegar a cerca de 2 km.
- Fast Ethernet (FE): a tecnologia FE é uma tecnologia de rede de área local (LAN) de alta velocidade que fornece alta largura de banda de rede para usuários de desktop e servidores ou clusters de servidores. IEEE802.3u é o padrão definido pelo IEEE para Fast Ethernet.: par trançado e fibra óptica
- Gigabit Ethernet é uma extensão do IEEE802.3 Ethernet. Com base no protocolo Ethernet, o Gigabit Ethernet aumenta a taxa de transmissão do Fast Ethernet em 10 vezes para 1 Gbit/s. Dois padrões:

- IEEE802.3z (cabo de fibra e cobre)
- IEEE802.3ab (par trançado)



Protocolo Ethernet (2)

| Velocidade de transmissão | Padrão |
|---------------------------|--|
| 10 Gbit/s Ethernet | A especificação de Ethernet 10GE (10 Gigabit Ethernet) está incluída no padrão IEEE 802.3 (IEEE 802.3ae). Ela estende o protocolo IEEE 802.3 e a especificação MAC para suportar a taxa de transmissão de 10 Gbit/s. |
| 40/100Gbit/s Ethernet | O padrão 802.3ba atende às exigências de largura de banda de um número crescente de aplicações em data centers, redes de operadoras e outros ambientes de computação de alto desempenho e tráfego intensivo. As necessidades de virtualização e o uso crescente de máquinas virtuais (VMs) nos data centers, além dos serviços de rede convergente, vídeo sob demanda (VOD) e redes sociais, também impulsionaram a formulação desse padrão. |

- O protocolo Ethernet é um conjunto de protocolos de LAN definidos pelo IEEE 802.3.



Funcionamento da Ethernet Compartilhada - CSMA/CD

- CSMA/CD: Acesso Múltiplo com Escuta de Portadora e Detecção de Colisão
- CS (Carrier Sense, Sensor da portadora):
 - Monitora os dados antes de enviá-los para garantir que a linha esteja ociosa e reduzir a possibilidade de colisão.
- MA (Acesso Múltiplo)
 - Qualquer dado enviado por um dispositivo (nó) pode ser recebido por todos os outros dispositivos conectados ao mesmo meio de transmissão ao mesmo tempo.
- CD (Detecção de colisão):
 - Detectando ao transmitir. Ao detectar um conflito, o remetente interrompe o envio de pacotes e continua a enviá-los após um atraso aleatório.

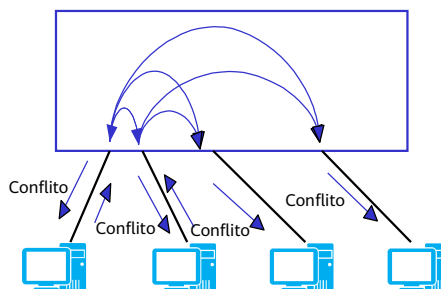
- Distância máxima de transmissão: é determinada por fatores como qualidade da linha e atenuação do sinal.
- Comprimento mínimo do frame (64 bytes): determinado pela distância máxima de transmissão e pelo mecanismo de detecção de colisão.



Ethernet compartilhada

- HUB

- Quando qualquer porta recebe um pacote, ela o encaminha diretamente para todas as portas. Logicamente, é um meio compartilhado.
- Se duas ou mais portas receberem pacotes ao mesmo tempo, ocorrerá um conflito. O DTE executa o algoritmo CSMA/CD.
- Somente um DTE pode enviar pacotes por vez.

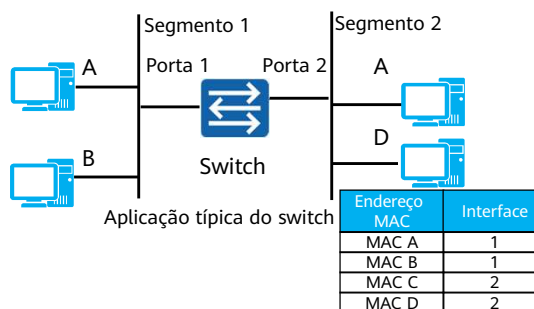
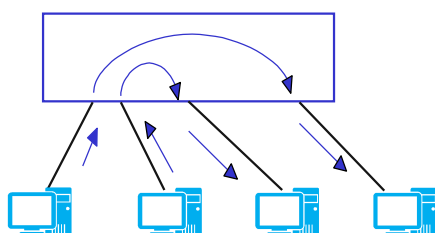


- A partir do conteúdo anterior, podemos saber que a Ethernet construída por hubs é uma Ethernet compartilhada em essência. Portanto, a Ethernet compartilhada tem as seguintes desvantagens:
 - Conflito grave
 - Inundação de transmissão
 - Sem segurança
- Um hub é um dispositivo Ethernet que funciona com base no mecanismo CSMA/CD. O princípio de funcionamento de um hub é o seguinte: Um hub encaminha os quadros de dados (unicast ou broadcast) recebidos de qualquer interface para qualquer outra interface (exceto a interface que recebe os quadros de dados) sem selecionar nenhuma interface.
- Portanto, pode-se dizer que um hub somente altera uma topologia física de uma Ethernet, e uma estrutura lógica da Ethernet ainda é uma topologia de barramento.
- O hub não usa o endereço MAC. Ele apenas duplica e encaminha dados e não filtra dados.



Ethernet comutada

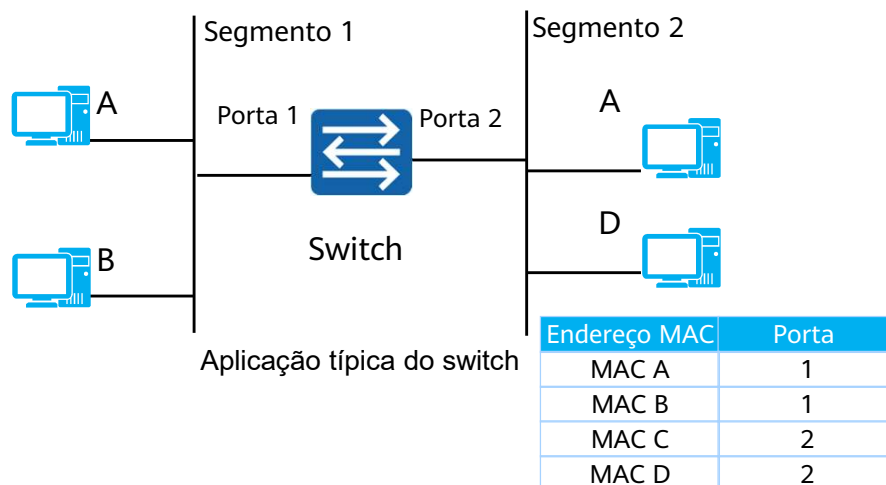
- Bridge (SWITCH LAN)
 - Aprende o endereço com base no EO do pacote recebido e realiza o mapeamento entre o endereço e a porta.
 - Após receber um pacote, pesquisa a tabela com base no ED no pacote e o encaminha para a porta especificada.
 - Vários DTEs podem transmitir dados ao mesmo tempo sem interferir uns nos outros.



- O switch funciona na camada de link de dados. Duas funções básicas de uma ponte em um switch Ethernet são as seguintes:
 - Aprendizagem de endereços MAC;
 - Encaminhamento e filtragem de decisões.



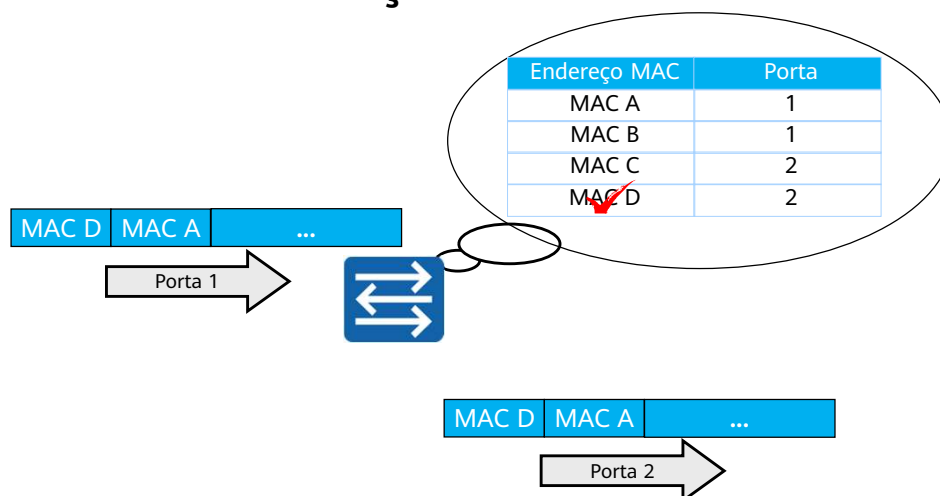
Ethernet Comutada - Aprendizado Baseado no Endereço de Origem



- Vamos analisar primeiro o aprendizado de endereço MAC.
- Uma ponte encaminha quadros de dados com base na tabela de endereços MAC. A tabela de endereços MAC é aprendida pela ponte com base no endereço MAC de origem. Geralmente, a tabela de endereços MAC de um switch de Camada 2 é criada com base no mapeamento entre endereços MAC e portas de switch.
- A ponte escuta o endereço de origem do quadro de dados e cada porta do switch escuta o endereço de origem do quadro de dados recebido.
- Durante a inicialização, a tabela de endereços MAC do switch está vazia.
- Por exemplo: Quando o switch recebe o quadro da porta 1, ele primeiro verifica o endereço MAC de destino e, em seguida, a tabela de endereços MAC no cache do switch. Entretanto, a tabela de endereços MAC está vazia. Por que o switch faz isso? Encaminhe o quadro para qualquer porta (exceto a porta 1 que recebe o quadro). Verifique o endereço MAC de origem do quadro e estabeleça um mapeamento entre a porta 1 e o endereço MAC do site A. O endereço MAC de origem do quadro é o endereço físico do site A. Por analogia, cada site estabelece uma relação de mapeamento com uma porta diretamente conectada, formando assim uma tabela de endereços MAC.
- Se uma porta estiver conectada a um hub, uma porta poderá corresponder a vários endereços MAC. Uma porta em um switch corresponde a um domínio de colisão.
- Observação: Em multicast, as entradas de endereço não são aprendidas, mas obtidas por meio de protocolos como espionagem de IGMP.



Ethernet Comutada - Encaminhamento com Base nos Endereços de Destino



- A segunda função básica dos switches: encaminhamento baseado no endereço de destino.
 - Procura na tabela de encaminhamento MAC os endereços que não estão incluídos na tabela e transmite os pacotes.
 - Os mecanismos de envelhecimento e aprendizagem automática de endereço são usados para manter a tabela de endereços.
 - Geralmente, o formato do quadro não é modificado. (O formato do quadro da VLAN precisa ser modificado e a tag precisa ser adicionada.)
- Princípios dos switches de camada 2:
 - Recebe todos os quadros de dados no segmento de rede.
 - O endereço MAC de origem no quadro de dados recebido é usado para estabelecer a tabela de endereços MAC (autoaprendizado do endereço de origem). O mecanismo de envelhecimento de endereço é usado para manter a tabela de endereços MAC.
 - O S9300 procura na tabela de endereços MAC o endereço MAC de destino do quadro de dados. Se o endereço MAC de destino for encontrado, o S9300 enviará o quadro de dados para a porta correspondente (excluindo a porta de origem). Se o endereço MAC de destino não for encontrado, o S9300 enviará o quadro de dados para todas as portas (excluindo a porta de origem).
 - Encaminha quadros de broadcast e quadros de multicast (excluindo a porta de origem) a todas as portas.



Ethernet Compartilhada vs Ethernet Comutada

| | Ethernet compartilhada | Ethernet comutada |
|-----------------------------|--|------------------------------------|
| Topologia | Topologia de barramento ou estrela | Topologia Estrela |
| Modo de Trabalho | Half-duplex | Full duplex |
| Largura de banda | Largura de banda do meio compartilhada | Largura de banda do meio exclusiva |
| Dispositivo | Hub e repetidor | Bridge |
| Camada | Física | (Sub) Camada MAC |
| Principais tecnologias | CSMA/CD | Aprendizado e o troca de encereço |
| Complexidade do dispositivo | Simple | Complexo |

- Os switches suportam três modos de switching: Cut-Through, Store-and-Forward e Fragment-Free. Os recursos de cada modo de switching são os seguintes:
 - Corte-Através
 - Após receber o endereço de destino, o switch inicia o processo de encaminhamento.
 - Atraso baixo
 - O switch não detecta erros e encaminha quadros de dados diretamente.
 - Armazenar e Encaminhar
 - O switch começa a encaminhar o quadro somente depois de receber o quadro completo.
 - O atraso é grande. O atraso depende do comprimento do quadro de dados.
 - O switch detecta erros e descarta pacotes de erro.

- Sem fragmento
 - Depois de receber os primeiros 64 bytes (um comprimento mínimo de quadro) do pacote de dados, o switch pesquisa a tabela de encaminhamento com base nas informações do cabeçalho do quadro.
 - Este modo de comutação combina as vantagens do modo Cut-Through e do modo Store-and-Forward. Semelhante ao modo Cut-Through, o quadro pode ser encaminhado depois que 64 bytes são recebidos, sem esperar que o quadro de dados completo seja recebido. Além disso. Como o modo Store-and-Forward, ele pode detectar os erros dos primeiros 64 bytes e descartar os quadros de erro.
- O L2 traz um grande salto à frente para a tecnologia Ethernet, resolve o problema de conflito da Ethernet e melhora muito o desempenho da Ethernet. A segurança da Ethernet também é aprimorada. No entanto, a inundação de broadcast existe na Ethernet e a segurança não pode ser garantida.



Quiz

1. (Single Choice) Which one of following statements about the MAC address is wrong? ()
 - A. A device on the network has a unique MAC address
 - B. A MAC address consists of 48 bits and is generally expressed in 12-bit hexadecimal format.
 - C. The MAC address is a logical address and can be configured as required.
 - D. The last six hexadecimal digits are managed by each vendor
2. What are the functions of each layer of the TCP/IP protocol stack?
3. What are the packet encapsulation and de-encapsulation processes in the TCP/IP protocol stack?
4. What is the difference between a MAC address and an IP address?

- C
- Quais são as funções de cada camada da pilha de protocolos TCP/IP?
 - A pilha de protocolos TCP/IP consiste em cinco camadas: camada física, camada de link de dados, camada de rede, camada de transporte e camada de aplicação. A camada física define as características mecânicas, elétricas e funcionais e os processos necessários para a transmissão de dados. A camada de link de dados controla a camada física, detecta e corrige possíveis erros e ajusta o tráfego (opcional). A camada de rede verifica a topologia da rede para determinar a rota ideal para a transmissão de pacotes. A função básica da camada de transporte é segmentar os dados enviados da camada de aplicativo para a camada de rede ou combinar os segmentos de dados enviados da camada de rede para a camada de aplicativo. Conexões completas são estabelecidas para enviar segmentos de dados de um host para outro, garantindo a correção da transmissão de dados. A camada de aplicativos fornece serviços de rede para aplicativos.
- Quais são os processos de encapsulamento e desencapsulamento de pacotes na pilha do protocolo TCP/IP?
 - Encapsulamento e desencapsulamento de pacotes são processos opostos. No encapsulamento, o cabeçalho de cada camada é adicionado de cima para baixo. No desencapsulamento, o cabeçalho de cada camada é removido de baixo para cima.
- Qual é a diferença entre um endereço MAC e um endereço IP?
 - O endereço MAC é um endereço físico de 48 bits fixado no hardware do dispositivo e não pode ser alterado. Um endereço IP é um endereço de 32 bits na camada de rede e pode ser modificado. Os endereços IP são classificados em endereços IP públicos e privados. Os endereços públicos são globalmente exclusivos, enquanto os endereços privados podem ser reutilizados em uma LAN.



Summary

- A pilha de protocolos TCP/IP consiste em cinco camadas: camada física, camada de link de dados, camada de rede, camada de transporte e camada de aplicação. Encapsulamento e desencapsulamento de pacotes são processos opostos. No encapsulamento, o cabeçalho de cada camada é adicionado de cima para baixo. No desencapsulamento, o cabeçalho de cada camada é removido de baixo para cima.
- A tabela de roteamento contém as seguintes entradas-chave: Destino, Máscara, Interface e Próximo Salto.
- Um switch de Camada 2 funciona na camada de enlace de dados e precisa implementar duas funções básicas: aprendizagem do endereço MAC de origem e encaminhamento baseado no endereço MAC de destino.



Thank You

www.huawei.com