1.Introdução

Todos os métodos de comunicação têm os seguintes três elementos em comum.

- **Fonte da mensagem/remetente:** As fontes da mensagem são pessoas ou dispositivos eletrônicos
- **Destino da mensagem/destinatário:** O destinatário recebe a mensagem e a interpreta
- **Canal:** Consiste na mídia que fornece o caminho pelo qual a mensagem viaja da origem ao destino

O envio de uma mensagem, seja por comunicação presencial ou por rede, é regido por regras chamadas de protocolos. Estes protocolos são específicos ao tipo de método de comunicação que está sendo usado. Os protocolos além de identificar a origem e o destino, eles definem os detalhes sobre como uma mensagem é transmitida por uma rede. Geralmente, protocolos de computador incluem a codificação da mensagem, a formatação e o encapsulamento, o tamanho e o tempo da mensagem e as suas opções de envio.

2.Codificação

A codificação é o processo de conversão de informações em outra forma aceitável para a transmissão. **A decodificação** seria reverter esse processo para interpretar as informações. Codificação entre hosts deve estar em um formato adequado para o meio físico. As mensagens enviadas pela rede são convertidas primeiramente em bits pelo host emissor, onde cada bit é codificado em um padrão de tensões em fios de cobre, luz, infravermelho em fibras ópticas ou microondas para sistemas sem fio. O host decodifica os sinais para interpretar a mensagem.

Uma mensagem enviada deve passar pelo processo de encapsulamento, um formato/estrutura específica adequada para o canal pelo qual será entregue.

Quando uma mensagem longa é enviada a outro host, ela deve ser dividida em partes menores. As regras que regem o tamanho dos quadros transmitidos são rígidas e podem diferir dependendo do canal usado. **Quadros muito longos ou muito curtos não são entregues**. Cada quadro também terá suas próprias informações de endereço. No host de destino, as partes individuais da mensagem são reconstruídas na mensagem original. Os pacotes podem tomar diferentes caminhos de rede para o mesmo destino, desde que todos cheguem ao destino. Devido à comutação de pacotes, vários computadores podem viajar sobre os mesmos fios basicamente em qualquer ordem.

Um pacote é basicamente composto pelas seguintes partes:

- **Header:** Um cabeçalho de pacote é um rótulo de tipos, que fornece informações sobre o conteúdo, a origem e o destino do pacote. Os pacotes consistem em duas partes: o cabeçalho e a carga útil (***payload***). O cabeçalho contém

informações sobre o pacote, como sua origem e endereços IP de destino. A carga útil são os dados reais.

- **Payload:** A carga útil é muitas vezes referida como dados. Isso se refere aos dados reais sendo transportados pelo pacote. Dependendo da rede, o tamanho pode variar. A carga útil é o único dado recebido pela origem e pelo destino, pois as informações do cabeçalho são retiradas do pacote quando ele chega ao destino.
- **Trailer:** O conteúdo de um trailer de pacote diferencia cada tipo de rede. Geralmente, um trailer contém alguns bits que informam ao dispositivo destinatário que ele chegou ao final do pacote, bem como uma verificação de redundância cíclica, que permite ao computador determinar se todos os pacotes foram recebidos completamente.

Teoricamente, seria possível enviar arquivos e dados pela Internet sem dividi-los em pequenos pacotes de informações. Um computador poderia enviar dados para outro computador na forma de uma longa linha ininterrupta de bits. Entretanto, essa abordagem rapidamente se torna impraticável quando mais de dois computadores estão envolvidos. Enquanto a longa linha de bits passa pelos fios entre os dois computadores, nenhum terceiro computador poderia usar esses mesmos fios para enviar informações.

A perda de pacotes de rede ocorre quando um pacote não consegue chegar ao seu destino, seja porque foi descartado ou porque o pacote se perdeu em trânsito, resultando em baixa qualidade de experiência. A temporização da mensagem inclui os seguintes processos descritos abaixo.

2.1 Controle de fluxo

Processo de gerenciamento da taxa de transmissão de dados, onde o controle de fluxo define o quanto de informação pode ser enviada e a velocidade com que pode ser entregue. Existem protocolos de rede usados pelos dispositivos de origem e destino para negociar e gerenciar o fluxo de informações.

2.2 Tempo limite da resposta

Os hosts da rede usam protocolos de rede que especificam quanto tempo esperar pelas respostas e que ação executar se ocorrer um tempo limite de resposta.

2.3 Método de acesso

Determina quando alguém pode enviar uma mensagem. Existem dois modos de comunicação, ***half duplex*** e ***full duplex***.

2.4 Comunicação half-duplex

Ambos os dispositivos podem transmitir e receber no meio físico, mas não podem fazer isso simultaneamente. WLANs e topologias de barramento com hubs Ethernet usam o modo half-duplex.

2.5 Comunicação full-duplex

Ambos os dispositivos podem transmitir e receber simultaneamente na mídia compartilhada. A camada de enlace de dados supõe que o meio físico está disponível para transmissão para ambos os nós a qualquer momento. Os computadores Ethernet operam em full-duplex por padrão.

3.Rede multi-acesso

Uma rede multi-acesso é uma rede que pode ter dois ou mais dispositivos finais tentando acessar a rede simultaneamente. Algumas dessas redes requerem regras para controlar como os dispositivos compartilham a mídia física. Existem dois métodos básicos de controle de acesso para meio físico compartilhado, descritos abaixo

3.1 Acesso baseado em contenção

Em redes multi-acesso baseadas em contenção, todos os nós estão operando em half-duplex, competindo pelo uso do meio. Apenas um dispositivo pode enviar por vez. Exemplos de métodos de acesso baseado em contenção incluem CSMA/CD (LANs Ethernet) e CSMA/CA (WLANs).

3.2 Acesso controlado

Em uma rede multi-acesso controlada, cada nó tem seu próprio tempo para usar o meio. Esses tipos determinísticos de redes herdadas são ineficientes porque um dispositivo deve aguardar sua vez para acessar o meio.

3.3 CSMA/CD

Acesso baseado em contenção (CSMA) são redes que operam em half-duplex, apenas um dispositivo pode enviar ou receber por vez. Isso requer um processo que determina quando um dispositivo pode enviar e o que acontece quando vários dispositivos enviam ao mesmo tempo. Se dois dispositivos transmitirem ao mesmo tempo, ocorrerá uma colisão (CD). A NIC compara os dados transmitidos com os dados recebidos ou reconhecendo que a amplitude do sinal é maior que o normal na mídia. Os dados enviados por ambos os dispositivos serão corrompidos e precisarão ser reenviados.

3.4 CSMA/CA

Outra forma de acesso baseado em contenção é o acesso múltiplo por detecção de portadora/prevenção de colisão (CA). É um método semelhante ao CSMA/CD para detectar colisões se a mídia está livre. O CSMA/CA usa técnicas adicionais. Em ambientes sem fio pode não ser possível para um dispositivo detectar colisão O

CSMA/CA tenta evitar estas colisões esperando antes de transmitir. Cada dispositivo que transmite inclui o tempo necessário para a transmissão. Todos os outros dispositivos sem fio recebem essas informações e sabem quanto tempo a mídia ficará disponível.

O método de determinação de pacote para host local ou host remoto é feito pelo dispositivo final de origem. Este dispositivo final de origem determina se o endereço IP de destino está na mesma rede em que o próprio dispositivo de origem está ou não. Isto varia de acordo com a versão do protocolo.

- **IPv4:** O dispositivo de origem usa sua própria máscara de sub-rede, juntamente com seu próprio endereço IPv4 de origem e destino para fazer a determinação.
- **IPv6:** O roteador local anuncia o endereço de rede local (prefixo) para todos os dispositivos na rede.

Dois endereços principais são atribuídos a um dispositivo em uma LAN Ethernet

- **Endereço físico (MAC):** Usado para comunicações de NIC para NIC na mesma rede Ethernet
- **Endereço lógico (IP):** Usado para enviar o pacote do dispositivo de origem para o dispositivo de destino. O endereço IP de destino pode estar na mesma rede IP da fonte ou em uma rede remota.

Uma Ethernet herdada usando uma topologia de barramento ou hubs, é um meio compartilhado e half-duplex. Ethernet sobre um meio half-duplex usa um método de acesso baseado em contenção, CSMA/CD e permite que vários dispositivos compartilhem o mesmo meio half-duplex, detectando uma colisão quando mais de um dispositivo tenta transmitir simultaneamente. Também fornece um algoritmo de recuo para retransmissão. As LANs Ethernet de hoje usam switches que operam em full-duplex. As comunicações em full-duplex com switches Ethernet não exigem controle de acesso através do CSMA/CD.

Os endereços físicos de camada 2 são usados para entregar o quadro de enlace de dados com o pacote IP encapsulado de uma NIC para outra NIC na mesma rede. Se o endereço IP de destino estiver na mesma rede, o endereço MAC de destino será o dispositivo de destino.

O quadro Ethernet da camada 2 OSI contém o endereço MAC de destino e origem, e o pacote IP da camada 3 OSI contém o endereço IPv4 de origem e o endereço IPv4 de destino.

Quando o endereço IP de destino, IPv4 ou IPv6 estiver em uma rede remota, o endereço MAC de destino será o endereço do gateway padrão do host, ou seja, a interface do roteador. Os roteadores examinam o endereço IPv4 destino para determinar o melhor caminho para o pacote IPv4. Quando o roteador recebe o quadro

Ethernet, ele desencapsula as informações da camada 2 OSI e usa o endereço IPv4 de destino, determinando o dispositivo do próximo salto, e em seguida, encapsula o pacote IPv4 em um novo quadro de enlace de dados para a interface de saída. Se o dispositivo de salto em seguida for o destino final, o endereço MAC de destino será o NIC Ethernet do dispositivo.

Os pacotes IPv4 são associados aos endereços MAC em cada link ao longo do caminho através de um processo denominado Address Resolution Protocol (ARP), fornecendo duas funções básicas, a resolução de endereços IPv4 em endereços MAC e uma tabela de mapeamento de endereços IPv4 para endereços MAC. Para IPv6, é utilizado um processo denominado Descoberta de Vizinhos (ND).

4.Portas

Portas de rede, também conhecidas como portas de comunicação ou simplesmente portas, são mecanismos virtuais ou pontos de extremidade em um dispositivo de rede que permite a comunicação entre diferentes aplicativos, serviços ou dispositivos. Cada porta é associada a um número específico, chamado de número da porta, que é utilizado para direcionar o tráfego de dados para um serviço específico.

4.1 Portas de conexões

As portas de rede são uma parte fundamental do modelo de comunicação em rede TCP/IP (Transmission Control Protocol/Internet Protocol), que é a base da comunicação na internet. O TCP/IP utiliza o conceito de sockets para estabelecer a comunicação entre dois dispositivos. Um socket é composto pelo endereço IP do dispositivo e o número da porta associado.

As portas são categorizadas em três tipos principais:

- **Portas bem conhecidas** (0 a 1023)
- **Portas registradas** (1024 a 49151)
- **Portas dinâmicas ou privadas** (49152 a 65535)

As portas bem conhecidas são atribuídas a serviços específicos e têm um significado padrão. A função principal das portas de rede é facilitar a comunicação entre diferentes aplicativos e serviços em uma rede. Cada serviço em execução em um dispositivo é identificado por uma porta específica, permitindo que os dados sejam roteados para o serviço correto. Isso é crucial para a transmissão eficiente de dados em uma rede, garantindo que a informação alcance o destino apropriado.

Esta é uma lista de números de porta TCP e UDP usados por protocolos para operação de aplicativos de rede. O TCP e UDP apenas precisam de uma porta para tráfego bidirecional. Eles geralmente usam números de porta que correspondem aos serviços da implementação correspondente. Abaixo na tabela, estão sendo mostradas algumas das principais portas de conexão de rede.

Porta	TCP/UDP	Descrição
20	Sim/Designado	File Transfer Protocol (FTP)
21	Sim/Designado	File Transfer Protocol control
22	Sim/Designado	Secure Shell, SCP, port forwarding
23	Sim/Designado	Protocolo Telnet
25	Sim/Designado	Simple Mail Transfer Protocol (SMTP
43	Sim/Designado	WHOIS Protocol
52	Designado/Designado	Xerox Network Systems (XNS)
53	Sim/Sim	Domain Name System (DNS)
67	Designado/Sim	Bootstrap Protocol (BOOTP); Dynamic Host Configuration Protocol (DHCP)
80	Sim/Sim	Hypertext Transfer Protocol (HTTP)
115	Sim/Designado	Simple File Transfer Protocol (SFTP)
118	Sim/Sim	Structured Query Language (SQL) services
153	Sim/Sim	Simple Gateway Monitoring Protocol
401	Sim/Sim	Uninterruptible Power Supply
443	Sim/Sim	Hypertext Transfer Protocol Secure (HTTPS)
587	Sim/Designado	SMTP