CENTRO PAULA SOUZA
ETEC PROF. HORÁCIO AUGUSTO DA SILVEIRA

ANDRÉ NOGUEIRA PISSUTO
ARTHUR BERGAMASCHI SOUZA SARRIA
JOÃO PEDRO CORREIA
MARINA SANTOS PAIXÃO RIBEIRO
MATHEUS BERNARDINO GOMES
ROGÉRIO ZANZARINI FAGÁ

CONCEITO OSI E A CAMADA DE REDES

São Paulo, 2025

O QUE SÃO REDES DE COMPUTADORES?

Redes de computadores referem-se a dispositivos de computação interconectados que podem trocar dados e compartilhar recursos entre si. Esses dispositivos em rede usam um sistema de regras, chamados de protocolos de comunicação, para transmitir informações por meio de tecnologias.

Nós e links são os blocos de construção básicos em redes de computadores. Um nó de rede pode ser um equipamento de comunicação de dados (DCE), como um modem, hub ou switch, ou um equipamento terminal de dados (DTE), como dois ou mais computadores e impressoras. A ligação entre eles(link) refere-se ao meio de transmissão que conecta dois nós. Esses links podem ser físicos como cabos ou fios, ou , via redes sem fio.

TIPOS DE REDES

Rede de área local (LAN): Uma LAN é um sistema interconectado limitado em tamanho e geografia. Normalmente conecta computadores e dispositivos em um único escritório ou edifício.

Redes de longa distância (WAN): Uma rede empresarial que abrange edifícios, cidades e até países é chamada de rede de longa distância (WAN). Enquanto as redes de área locais são usadas para transmitir dados em velocidades mais altas em estreita proximidade, as WANs são configuradas para comunicação de longa distância que é segura e confiável.Redes de provedores de serviços: As redes de provedores de serviços permitem que os clientes aluguem capacidade e funcionalidade de rede do provedor. Os provedores de serviços de rede podem consistir em empresas de telecomunicações, operadoras de dados, provedores de comunicações sem fio, provedores de serviços de Internet e operadoras de televisão a cabo que oferecem acesso à Internet de alta velocidade.

Redes em nuvem: Conceitualmente, uma rede em nuvem pode ser vista como uma WAN com sua infraestrutura fornecida por um serviço baseado na nuvem. Alguns ou todos os recursos e capacidades de rede de uma organização são hospedados em uma plataforma de nuvem pública ou privada e disponibilizados sob demanda. Esses recursos de rede podem incluir roteadores virtuais, firewalls, largura de banda e software de gerenciamento de rede, com outras ferramentas e funções disponíveis, conforme necessário.

O QUE É O MODELO OSI

O processo de enviar uma requisição para um servidor é parecido com o de enviar um pacote pelos correios, isto é, passa por algumas etapas até chegar ao destino final, esse processo pode ser chamado de Modelo OSI(Open Systems Interconnection). Outra definição que podemos dar ao modelo OSI é que ele serve como uma estrutura conceitual que divide as funções de comunicação de rede em sete camadas. Para entrarmos em contato com a internet é necessário uma grande parte de etapas e processos.

”O envio de dados por uma rede é complexo porque várias tecnologias de hardware e software devem funcionar de forma coesa além das fronteiras geográficas e políticas.”

O modelo OSI serve também como um padrão de regras e etapas para que máquinas de todo mundo consigam se comunicar seguindo o mesmo padrão de etapas, cada camada específica deve fornecer informações específicas e devem exigir dados específicos para possuir utilidade na rede, as tecnologias nas camadas superiores se beneficiam da abstração, pois podem usar tecnologias de nível inferior sem precisar se preocupar com os detalhes subjacentes da implementação.

SURGIMENTO E DESENVOLVIMENTO DO MODELO OSI

O Modelo OSI (*Open Systems Interconnection*) foi desenvolvido pela *International Organization for Standardization* (ISO) no final da década de 1970, com intenção de

ser uma resposta à crescente complexidade das redes de computadores e à necessidade de criar um conjunto de padrões que permitisse a comunicação eficaz em redes de computadores dessa forma, foi dividido o processo em sete camadas distintas.

Facilitando a visualização do processo,por ser um modelo que divide cada parte em camadas distintas a visualização é mais fácil, deixando a complexidade das redes mais fáceis pela sua forma de organização por etapas e hierarquia; As sete camadas do Modelo OSI são independentes e podem ser modificadas ou atualizadas individualmente; Diferente da arquitetura monolítica, se ocorrer uma mudança em uma camada, não prejudicará as demais camadas;O Modelo OSI estabelece um conjunto de padrões e diretrizes para a comunicação em redes, isso faz que qualquer pessoa ou empresa que deseja usar o modelo OSI pode utilizar de forma igual sem necessitar de adaptações para outras normas e regras; Ao dividir o processo de comunicação em camadas, é mais fácil isolar e diagnosticar problemas específicos em uma determinada camada; Pelo fato do modelo OSI utilizar uma estrutura padronizada e modular é mais fácil e mais eficiente de empresas e indústrias terem a comunicação em redes, mesmo sendo de fabricantes diferentes.

A CAMADA DE REDE

As conexões entre redes são essenciais para o funcionamento da internet. A camada de rede é responsável pelo envio de pacotes de dados entre diferentes redes, permitindo a comunicação entre dispositivos. No modelo OSI de sete camadas, a camada de rede corresponde à camada 3, sendo o Protocolo de Internet (IP) um dos principais utilizados, juntamente com protocolos de roteamento, teste e criptografia.

Uma rede consiste em um grupo de dois ou mais dispositivos de computação conectados, geralmente por meio de um roteador ou outro hub central. Além disso, as redes podem conter sub-redes, subdivisões menores capazes de gerenciar um grande número de endereços IP e dispositivos conectados. A internet pode ser entendida como uma rede de redes, onde computadores estão interligados dentro de redes menores que, por sua vez, se conectam a outras redes. Na camada de

rede, ocorrem processos como a dkefinição de rotas para os pacotes de dados, a verificação do funcionamento de servidores remotos e o endereçamento e recebimento de pacotes IP. Este último processo é fundamental, pois a maior parte do tráfego da internet utiliza o protocolo IP.

No modelo TCP/IP, a camada de rede do modelo OSI é equivalente à camada de internet. Ou seja, apesar das diferenças entre os modelos, ambas desempenham funções semelhantes na estrutura da comunicação digital. Os principais protocolos utilizados na camada de rede incluem:

IP *(Internet Protocol)*: responsável pelo endereçamento e roteamento dos pacotes de dados;

IPsec *(Internet Protocol Security)*: conjunto de protocolos que protege conexões entre dispositivos, criptografando e autenticando pacotes de IP. É frequentemente usado para configurar redes privadas virtuais (VPNs);

ICMP *(Internet Control Message Protocol)*: utilizado para envio de mensagens de erro e diagnóstico;

IGMP *(Internet Group Management Protocol)*: gerencia grupos de multicast;

GRE *(Generic Routing Encapsulation)*: encapsula diversos tipos de tráfego de rede.

O PROTOCOLO TCP/IP

A internet demonstra a viabilidade da tecnologia TCP/IP e mostra como ela pode acomodar uma variedade de tecnologias básicas de hardware. Os protocolos como o TCP e o IP fornecem regras sintáticas e semânticas para a comunicação, eles fornecem detalhes dos formatos de mensagem, descrevem a resposta do computador ao receber essa mensagem e descrevem como um computador responde ao receber a mensagem e especificam como um computador trata erros ou outras condições. Os protocolos são para a comunicação o que os algoritmos representam na computação.

Na década de 70, fora criada uma tecnologia que tornou possível conectar várias redes individuais e operá-las como uma unidade coordenada, chamada de *interligação de redes,* essa tecnologia estabeleceu as bases para a internet, acomodando várias tecnologias de hardware básicas, interconectando redes e

definindo conjuntos de convenções de comunicação que as redes usam para interoperar.

Um exemplo de interconexão de sistema aberto é a tecnologia da internet, que é chamada assim porque diferente dos sistemas disponíveis de um fornecedor, as especificações estão disponíveis publicamente.

FORMATOS DE ENDEREÇO DE IP

Os endereços IP têm diferentes maneiras de serem representados, dependendo do tipo de endereço.

O tipo IPv4 é o mais comum, possui 4 blocos de números decimais. Os blocos são separados por ponto. Cada bloco tem valor máximo de 255 e mínimo 0. Exemplo: 192.168.0.1.

O tipo IPv6 foi criado para substituir o IPv4 pela limitação de endereços possíveis. Utiliza 8 blocos de 4 caracteres, hexadecimais separados por dois pontos. Exemplo: 2001:0db8:85a3:0000:0000:8a2e:0370:7334

CLASSES DE ENDEREÇO IP

As classes são responsáveis por estabelecer um padrão para organizar melhor o espaço entre endereços IP, além de facilitar o roteamento. A principal função da divisão das classes é diferenciar redes privadas e públicas de endereços especiais, por isso o espaço dos endereçamentos é otimizado. Há cinco principais classes a seguir:

Classe A: O intervalo de Endereços é de 0.0.0.0 a 127.255.255.255 e sua máscara é /8 (ou 255.0.0.0). É útil em locais onde é necessária uma rede apenas, mas várias máquinas conectadas nela, como redes corporativas ou provedores de internet.

Classe B: O intervalo de Endereços é de 128.0.0.0 a 191.255.255.255 e sua máscara é /16 (ou 255.255.0.0). É usada em redes médias até redes grandes, como empresas grandes ou universidades.

Classe C: O intervalo de Endereços é de 192.0.0.0 a 223.255.255.255 e sua máscara é /24 (ou 255.255.255.0). A classe C é encontrada em redes pequenas, como redes de casa, pequenas empresas, pequenos escritórios ou endereços em LANs.

Classe D: O intervalo de Endereços é de 224.0.0.0 a 239.255.255.255 e não tem máscara. O principal uso dela é em Comunicação multicast. Não é utilizada para endereços a hosts individuais.

Classe E: O intervalo de Endereços é de 240.0.0.0 a 255.255.255.255 e também não tem máscara. Essa classe não é pública e é reservada para pesquisas e experimentos futuros.

A INTERNET TCP/IP

Entre 1970 e 80, foram observadas pelas agências dos Estados Unidos a importância e o potencial da tecnologia da Internet e também financiaram pesquisas que posteriormente trouxeram a possibilidade de uma Internet global.

O protocolo IP (*Internet Protocol*) é um dos principais protocolos da camada de rede no modelo TCP/IP. Ele é responsável pelo endereçamento e roteamento dos pacotes de dados em uma rede, permitindo que as informações sejam transmitidas de um dispositivo para outro, independentemente da localização física. O IP é um protocolo não orientado à conexão e não confiável, o que significa que ele não estabelece uma conexão antes de enviar os dados e não garante a entrega correta ou a ordem dos pacotes. Caso haja perdas ou erros na transmissão, protocolos de camadas superiores, como o TCP (*Transmission Control Protocol*), assumem a responsabilidade de garantir a integridade e a ordem dos dados.

O IP trabalha com endereços lógicos, que são representados numericamente e permitem a identificação única de dispositivos dentro de uma rede. Esses endereços são organizados em duas versões principais: IPv4 e IPv6. O IPv4, a versão mais antiga e ainda amplamente utilizada, utiliza endereços de 32 bits, representados no formato decimal, como "192.168.0.1". Ele possui um espaço de endereçamento limitado a cerca de 4,3 bilhões de endereços únicos, o que levou ao desenvolvimento do IPv6, uma versão mais moderna e expansiva, que utiliza

endereços de 128 bits, escritos em hexadecimal, como "2001:0db8:85a3:0000:0000:8a2e:0370:7334". O IPv6 foi criado para solucionar o problema de esgotamento de endereços do IPv4 e traz melhorias como um cabeçalho mais simplificado e suporte nativo a segurança via IPsec.

O funcionamento do protocolo IP é baseado na divisão dos dados em pacotes individuais, que são chamados de datagramas IP. Cada datagrama IP contém um cabeçalho e uma carga útil. O cabeçalho IP contém informações essenciais para o roteamento e a entrega do pacote, incluindo o endereço IP de origem (dispositivo que enviou o pacote) e o endereço IP de destino (dispositivo que deve recebê-lo). Outros campos importantes do cabeçalho incluem a versão do protocolo IP, o tamanho do cabeçalho, o tipo de serviço (que define a prioridade do pacote), o tamanho total do pacote, um identificador único para fragmentação, flags de controle de fragmentação, um deslocamento de fragmento para reagrupamento de pacotes fragmentados, o tempo de vida (TTL) que limita o número de saltos que o pacote pode fazer antes de ser descartado, um campo de protocolo para indicar o protocolo de camada superior (como TCP ou UDP) e um checksum para verificar a integridade do cabeçalho.

Quando um pacote IP precisa ser transmitido por uma rede, ele pode passar por vários roteadores ao longo do caminho. Cada roteador examina o endereço de destino do pacote e toma decisões de encaminhamento com base em tabelas de roteamento. Essas tabelas contêm informações sobre quais caminhos são os mais adequados para encaminhar os pacotes até seu destino final. O processo de roteamento pode envolver múltiplos saltos entre roteadores diferentes, até que o pacote alcance o dispositivo de destino.

Um dos desafios do protocolo IP é a fragmentação. Como diferentes redes podem ter tamanhos máximos de unidade de transmissão (MTU) distintos, um pacote grande pode precisar ser dividido em fragmentos menores para ser transmitido com sucesso. Cada fragmento recebe seu próprio cabeçalho IP e é enviado separadamente pela rede. No destino, os fragmentos são agrupados para reconstruir o pacote original. Se algum fragmento se perder no caminho, o pacote inteiro pode se tornar inutilizável.

O IP por si só não inclui mecanismos para garantir a entrega dos pacotes ou para corrigir erros durante a transmissão. Se um pacote for perdido ou corrompido, ele

simplesmente será descartado. Para lidar com esses problemas, outros protocolos complementares são usados. O ICMP *(Internet Control Message Protocol)*, por exemplo, é utilizado para enviar mensagens de erro e diagnóstico, como quando um pacote não pode ser entregue ou quando o TTL se esgota antes de alcançar o destino. O protocolo ARP (*Address Resolution Protocol*) é responsável por mapear endereços IP para endereços MAC em redes locais, permitindo que os pacotes IP sejam entregues corretamente dentro de uma rede Ethernet.

A transição do IPv4 para o IPv6 é uma questão importante no contexto atual da Internet. O esgotamento dos endereços IPv4 levou ao desenvolvimento de soluções temporárias, como o uso de NAT (*Network Address Translation*), que permite que múltiplos dispositivos compartilhem um único endereço IP público. No entanto, essas soluções não resolvem completamente o problema da escassez de endereços e podem introduzir desafios adicionais na comunicação entre dispositivos. O IPv6, por sua vez, foi projetado para fornecer um número praticamente ilimitado de endereços, eliminando a necessidade do NAT em muitas situações e simplificando o roteamento e a conectividade global.

O protocolo IP é um dos pilares fundamentais da Internet moderna, possibilitando a comunicação entre bilhões de dispositivos em todo o mundo. Seu design modular e sua capacidade de adaptação permitiram que ele permanecesse relevante por décadas, apesar das mudanças tecnológicas e do crescimento exponencial da rede. Com a adoção gradual do IPv6, espera-se que a infraestrutura da Internet continue a evoluir, suportando novas aplicações e garantindo a conectividade global para as próximas gerações.

O TCP (*Transmission Control Protocol*) é um dos principais protocolos da camada de transporte no modelo TCP/IP. Ele é um protocolo orientado à conexão, confiável e responsável por garantir que os dados sejam entregues corretamente entre dois dispositivos em uma rede. Ao contrário do IP, que apenas encaminha pacotes sem garantir a entrega, o TCP estabelece uma conexão antes da transmissão dos dados e utiliza diversos mecanismos para garantir que as informações cheguem ao destino na ordem correta e sem erros.

Quando dois dispositivos precisam se comunicar usando o TCP, eles primeiro realizam um processo chamado "*Three-Way Handshake*" (aperto de mão em três etapas), que é essencial para estabelecer uma conexão confiável. Esse processo

ocorre quando o dispositivo de origem envia um pacote com um SYN (*synchronize*) para iniciar a conexão, o dispositivo de destino responde com um SYN-ACK (*synchronize-acknowledge*) para confirmar a recepção, e finalmente o dispositivo de origem envia um ACK final, estabelecendo oficialmente a conexão. Após essa etapa, os dados podem ser transmitidos de maneira confiável. O TCP divide os dados em segmentos e os encapsula com um cabeçalho contendo informações essenciais para controle e reenvio, caso necessário. Cada segmento TCP contém campos como o número de sequência, que identifica a ordem dos bytes enviados, e o número de reconhecimento (ACK), que confirma a recepção de dados do outro lado da conexão.

Uma das características mais importantes do TCP é seu mecanismo de controle de fluxo, que evita que o remetente sobrecarregue o receptor com mais dados do que ele pode processar. Isso é feito utilizando a técnica de janela deslizante, onde o receptor informa ao remetente o tamanho da janela, ou seja, a quantidade de dados que pode receber sem problemas. Se a capacidade do receptor mudar, ele pode ajustar esse valor dinamicamente. Outro recurso essencial do TCP é o controle de congestionamento, que impede que a rede fique sobrecarregada quando há muitos pacotes sendo transmitidos simultaneamente. Ele utiliza algoritmos como o *Slow Start* (início lento), que começa enviando poucos pacotes e aumenta gradualmente a taxa de transmissão conforme percebe que a rede pode suportar mais tráfego sem perdas.

Para garantir a confiabilidade, o TCP adota um mecanismo de retransmissão baseado em temporizadores e confirmações. Se um segmento for perdido ou corrompido durante a transmissão, o receptor não enviará um ACK correspondente, e o remetente retransmite automaticamente o segmento ausente. Além disso, o TCP implementa a técnica de detecção de duplicatas, descartando pacotes duplicados caso cheguem mais de uma vez devido a problemas na rede.

Quando a comunicação entre os dispositivos termina, o TCP usa um processo chamado "*Four-Way Handshake*" (aperto de mão em quatro etapas) para encerrar a conexão de maneira ordenada. O primeiro dispositivo envia um FIN (*finish*) para indicar que deseja encerrar a conexão, o segundo dispositivo responde com um ACK para confirmar a recepção, em seguida envia seu próprio FIN para indicar que também quer encerrar a conexão, e por fim o primeiro dispositivo responde com um

ACK final, finalizando a comunicação.

O cabeçalho do TCP possui campos fundamentais para garantir o controle e a confiabilidade da transmissão. Ele inclui informações como porta de origem e destino, que identificam os aplicativos que estão se comunicando, além de diversos flags que indicam o estado da conexão (como SYN, ACK, FIN, RST). O campo *checksum* permite verificar a integridade dos dados, detectando erros que possam ter ocorrido durante a transmissão. O TCP é amplamente utilizado em aplicações que exigem confiabilidade e ordem na entrega dos dados, como navegação na web (HTTP/HTTPS), envio de e-mails (SMTP, IMAP, POP3), transferência de arquivos (FTP) e muitas outras. Em contraste, alguns aplicativos preferem usar o UDP (User Datagram Protocol), que é mais rápido, porém menos confiável, como acontece com streaming de vídeos e jogos online.

Embora o TCP tenha sido projetado para ser eficiente e confiável, ele pode apresentar alguns desafios, como latência em conexões de longa distância e consumo maior de recursos devido ao controle rigoroso da transmissão. Por isso, novas versões e otimizações do protocolo vêm sendo estudadas e implementadas, como o *TCP Fast Open* (TFO), que reduz o tempo necessário para estabelecer conexões, e o QUIC, um protocolo mais recente que combina benefícios do TCP e do UDP. O TCP continua sendo um dos pilares da comunicação na Internet moderna, garantindo que bilhões de dispositivos possam trocar informações de maneira confiável, mesmo em redes complexas e de grande escala.

ENDEREÇAMENTO IPV4

IP significa *Internet Protocol version* e v4 significa Versão Quatro (IPv4),É o sistema mais amplamente usado para identificar dispositivos em uma rede. Ele usa um conjunto de quatro números, separados por pontos (como 192.168.0.1), para dar a cada dispositivo um endereço exclusivo. Esse endereço ajuda os dados a encontrarem seu caminho de um dispositivo para outro pela internet.

FORMATO DE ENDEREÇAMENTO IPV4

Um endereço IPv4 consiste em 32 bits (dígitos binários), agrupados em quatro seções conhecidas como octetos ou bytes. Como cada octeto tem 8 bits, ele pode representar 256 números variando de 0 a 255. Esses quatro octetos são representados como números decimais, separados por pontos conhecidos como notação decimal pontuada . Por exemplo, o endereço IPv4 185.107.80.231 consiste em quatro octetos.

PARTES DO IPV4

Parte de rede: Identifica a rede onde o dispositivo está conectado.

Parte de host: Identifica o dispositivo dentro daquela rede.

Número de sub-rede : Esta é a parte não obrigatória do IPv4. Redes locais que têm números massivos de hosts são divididas em sub-redes e números de sub-rede são designados para isso.

TIPOS DE ENDEREÇAMENTO IPV4

O IPv4 basicamente suporta três tipos diferentes de modos de endereçamento:

Modo de endereçamento unicast : Este modo de endereçamento é usado para especificar um único remetente e um único destinatário. Exemplo: Acessando um site.

Modo de endereçamento de transmissão: Este modo de endereçamento é usado para enviar mensagens para todos os dispositivos em uma rede. Exemplo: enviar uma mensagem na rede local para todos os dispositivos.

Modo de endereçamento multicast: Este modo de endereçamento é normalmente usado dentro de uma rede local ou entre redes e envia mensagens para um grupo de dispositivos. Exemplo: Transmitir áudio para vários dispositivos ao mesmo tempo.

VANTAGENS DO IPV4

A segurança IPv4 permite criptografia para manter a privacidade e a segurança. A alocação de rede IPV4 é significativa e atualmente conta com cerca de 85.000 roteadores funcionais. Fica fácil conectar vários dispositivos em uma rede descomunal sem NAT. Este é um modelo de comunicação que proporciona um serviço de qualidade e também uma transferência econômica de conhecimento. Os endereços IPV4 são redefinidos e permitem uma codificação perfeita. O roteamento é escalável e econômico por abordar seu coletivo de forma mais eficaz. A comunicação de dados pela rede se torna muito específica em organizações multicast.

LIMITAÇÕES DO IPV4

O IP depende de endereços da camada de rede para identificar pontos finais na rede, e cada rede tem um endereço IP exclusivo. O suprimento mundial de endereços IP exclusivos está diminuindo e, teoricamente, eles podem acabar. Se houver vários hosts, precisamos dos endereços IP da próxima classe.

Configuração complexa de host e roteamento, endereçamento não hierárquico, endereços difíceis de renumerar, grandes tabelas de roteamento, QoS (Qualidade de Serviço), mobilidade e multi-homing, multicasting, etc. são as grandes limitações do IPv4, e é por isso que o IPv6 entrou em cena.

FRAGMENTAÇÃO DE PACOTES

A fragmentação é o processo de divisão de pacotes de dados em partes menores para possibilitar uma transmissão mais eficiente em redes de comunicação. Essa divisão é necessária devido às variações nos limites de tamanho máximo de pacote, conhecidos como MTU *(Maximum Transmission Unit)*, que podem diferir entre redes e protocolos.

IMPORTÂNCIA DA FRAGMENTAÇÃO

A fragmentação é essencial por diversas razões, tais como: Limitações do MTU:

Redes distintas possuem diferentes tamanhos de MTU. Por exemplo, a Ethernet tradicional suporta um MTU de 1500 bytes, enquanto outras redes podem ter valores menores ou maiores. Quando um pacote excede esse limite, ele precisa ser fragmentado para ser transmitido.

Eficiência na transmissão: A divisão de pacotes grandes pode otimizar o desempenho da rede, reduzindo a probabilidade de congestionamento e minimizando a necessidade de retransmissão em caso de erros.

Compatibilidade entre redes: Em redes heterogêneas, a fragmentação permite que os pacotes trafeguem por diferentes segmentos de rede, independentemente das restrições de MTU.

PROCESSO DA FRAGMENTAÇÃO

Quando um pacote ultrapassa o MTU da rede, ele é dividido em fragmentos menores. Cada fragmento é transmitido separadamente e contém informações necessárias para sua remontagem no destino final.

Os principais campos do cabeçalho IP relacionados à fragmentação são:

Identification: número único atribuído a cada pacote para auxiliar na remontagem dos fragmentos.

Fragment Offset: posição do fragmento dentro do pacote original.

More Fragments (MF): bit que indica se há fragmentos adicionais.

Após a recepção de todos os fragmentos, o pacote é reconstituído no destino. Caso algum fragmento se perca, o pacote completo não poderá ser remontado corretamente, exigindo retransmissão.

DESAFIOS DA FRAGMENTAÇÃO

Apesar da importância da fragmentação para a comunicação em redes, esse processo apresenta desafios, como:

Aumento da sobrecarga: Cada fragmento carrega um cabeçalho adicional, reduzindo a eficiência na transmissão de dados.

Perda de fragmentos: A perda de um único fragmento compromete a remontagem do pacote original, exigindo retransmissão completa e aumentando a latência.

Riscos de segurança: Atacantes podem explorar a fragmentação para contornar sistemas de firewall e detecção de intrusão, dividindo pacotes maliciosos de forma a evitar sua identificação.

MÁSCARAS DE SUB-REDE

As máscaras de sub-rede são fundamentais para o endereçamento IP. Elas definem quais bits do endereço IP identificam a rede e quais identificam o host. Esse mecanismo permite subdividir uma rede grande em redes menores (sub-redes), contribuindo para: Otimização do tráfego**:** Reduzindo o domínio de broadcast e, consequentemente, evitando congestionamentos; Administração simplificada: Facilita a gestão e a organização dos endereços IP dentro de uma organização; Uso eficiente do espaço de endereços: Permite a alocação adequada de endereços de acordo com as necessidades reais de cada segmento.

FUNCIONAMENTOS E EXEMPLOS

Em IPv4, um endereço é composto por 32 bits, geralmente representados em notação decimal pontilhada (por exemplo, 192.168.1.10). A máscara de sub-rede, também representada dessa forma (por exemplo, 255.255.255.0), indica quais bits do endereço pertencem à parte da rede (os bits “1”) e quais pertencem aos hosts (os bits “0”).

EXEMPLO PRÁTICO:

Endereço IP: 192.168.1.10

Máscara de Sub-rede: 255.255.255.0

Representação Binária:

IP: 11000000.10101000.00000001.00001010

Máscara: 11111111.11111111.11111111.00000000

Resultado da operação AND:

Endereço de Rede: 192.168.1.0

Essa divisão possibilita que dispositivos que compartilhem o mesmo “prefixo” se comuniquem diretamente sem a necessidade de roteamento externo.

ROTEAMENTO

O roteamento é o processo pelo qual os pacotes de dados são encaminhados de uma rede para outra, permitindo que a comunicação aconteça entre dispositivos localizados em segmentos diferentes da rede. Ele opera na camada de rede do modelo OSI e envolve diversas técnicas e protocolos para determinar a melhor rota a seguir.

CONCEITOS BÁSICOS

Roteadores: São dispositivos que, utilizando tabelas de roteamento, decidem qual o próximo salto (next hop) para um pacote chegar ao seu destino.

Tabelas de Roteamento: Armazenam informações sobre as rotas disponíveis e os custos associados a cada caminho.

Algoritmos de Roteamento: Podem ser baseados em distância (distance vector) ou estado de enlace (link state). Estes algoritmos ajudam a escolher a rota mais eficiente com base em critérios como número de saltos, largura de banda, atraso e confiabilidade.

TIPOS DE ROTEAMENTO

ROTEAMENTO ESTÁTICO:

a. Configurado manualmente pelo administrador.
b. É adequado para redes pequenas ou para caminhos que raramente mudam.

ROTEAMENTO DINÂMICO:

a. Utiliza protocolos (como RIP, OSPF e BGP) que permitem aos roteadores trocarem informações e se adaptarem a alterações na topologia da rede.
c. Garante que, caso um caminho fique indisponível, outra rota seja automaticamente selecionada.

PROTOCOLOS DE ROTEAMENTO

RIP *(Routing Information Protocol)*: Um protocolo de vetor de distância que utiliza o número de saltos como métrica.

OSPF *(Open Shortest Path First)*: Um protocolo de estado de enlace que calcula o caminho mais curto com base em custos atribuídos às conexões.

BGP *(Border Gateway Protocol)*: Utilizado para troca de informações de roteamento entre Sistemas Autônomos na Internet, sendo essencial para a escalabilidade global.

Esses protocolos permitem que os roteadores mantenham tabelas de roteamento atualizadas e distribuam informações sobre a topologia da rede, possibilitando a escolha de rotas que maximizem a eficiência e minimizem atrasos.

NAT - NETWORK ADDRESS TRANSLATION

O NAT (*Network Address Translation*) é uma técnica utilizada em redes de computadores para converter endereços IP privados (usados internamente) em

endereços IP públicos (usados na Internet) e vice-versa. Essa tradução é feita por um dispositivo, geralmente um roteador, que atua como “ponte” entre a rede interna e a externa.

PRINCIPAIS FUNÇÕES

Conservação de Endereços IPv4: Devido à escassez de endereços IPv4, o NAT permite que múltiplos dispositivos compartilhem um único endereço IP público.

Segurança: Ao ocultar os endereços internos, o NAT dificulta ataques diretos à rede privada, funcionando como uma barreira adicional.

Flexibilidade e Gerenciamento: Facilita a reorganização e segmentação da rede sem a necessidade de alterar os endereços públicos.

TIPOS DE NAT

Static NAT: Mapeamento um-para-um, onde um endereço IP interno é fixamente associado a um endereço IP público.

Dynamic NAT: Um conjunto de endereços IP públicos é atribuído dinamicamente aos dispositivos internos conforme necessário.

PAT *(Port Address Translation)*, também conhecido como *NAT Overload:* Permite que vários dispositivos usem o mesmo endereço IP público, diferenciando as conexões por meio dos números de porta.

Exemplo Prático:

Em uma rede doméstica, os computadores e smartphones possuem endereços IP privados (por exemplo, 192.168.1.x). Ao acessar a Internet, o roteador utiliza NAT (geralmente PAT) para traduzir esses endereços para o endereço público atribuído pelo provedor.

DHCP - DYNAMIC HOST CONFIGURATION PROTOCOL

O DHCP *(Dynamic Host Configuration Protocol)* é um protocolo que automatiza a atribuição de endereços IP e outros parâmetros de configuração (como máscara de sub-rede, *gateway* padrão e servidores DNS) a dispositivos em uma rede. Isso elimina a necessidade de configurar manualmente cada dispositivo.

FUNCIONAMENTO

Modelo Cliente-Servidor:

a. DHCPDISCOVER: O cliente inicia a comunicação enviando uma mensagem de descoberta na rede, buscando um servidor DHCP.
b. DHCPOFFER: Um ou mais servidores DHCP respondem oferecendo um conjunto de configurações.
c. DHCPREQUEST: O cliente escolhe uma das ofertas e solicita oficialmente os parâmetros.
d. DHCPACK: O servidor confirma a atribuição, enviando um reconhecimento com os dados finais.

Renovação: Os dispositivos renovam periodicamente seu lease (tempo de uso do endereço) para manter a configuração.

BENEFÍCIOS

Automatização: Reduz erros de configuração e facilita a administração, especialmente em redes com muitos dispositivos.

Escalabilidade: Permite a fácil adição de novos dispositivos à rede sem intervenção manual.

Flexibilidade: Possibilita a mudança rápida de configurações em toda a rede (por exemplo, alteração do gateway ou servidores DNS).

Exemplo Prático:

Ao conectar um laptop a uma rede Wi-Fi, o dispositivo envia uma solicitação DHCP e recebe automaticamente seu endereço IP, a máscara de sub-rede, o gateway e os servidores DNS, permitindo que o usuário acesse a Internet sem configurações manuais.

CONCLUSÃO

A camada de redes é um componente fundamental na arquitetura de redes de computadores, sendo responsável por assegurar a comunicação eficiente e confiável entre dispositivos localizados em diferentes redes. Situada entre a camada de enlace de dados e a camada de transporte no modelo OSI e no modelo TCP/IP, a camada de redes tem como função primária o roteamento, endereçamento e controle do tráfego de pacotes entre dispositivos, permitindo que informações sejam transmitidas de forma segura e eficaz através de diversas redes.

A camada de redes utiliza o protocolo IP (Internet Protocol), que permite a identificação única de dispositivos por meio de endereços IP, possibilitando o direcionamento correto dos pacotes de dados para o destino final. Através da definição de máscaras de sub-rede, a camada de redes pode dividir grandes redes em sub-redes menores, o que melhora o gerenciamento do tráfego e aumenta a segurança da rede. Além disso, a camada de redes lida com o roteamento, que é o processo de determinar o melhor caminho para os pacotes entre redes distintas. Esse processo é realizado por dispositivos chamados roteadores, que analisam o endereço de destino dos pacotes e escolhem o melhor trajeto para sua entrega.

Outro aspecto importante dessa camada é a utilização de protocolos de controle, como o ICMP (Internet Control Message Protocol), que auxilia na detecção e notificação de erros, como a falha na entrega de pacotes ou problemas de comunicação entre dispositivos. A camada de redes também é responsável por dividir dados em pacotes e gerenciar o fluxo de informações, além de lidar com problemas relacionados à fragmentação e reassembly de pacotes, assegurando que os dados sejam corretamente transmitidos, independentemente do tamanho ou da rede pela qual passam.

Através desses processos e protocolos, a camada de redes não só facilita a comunicação entre dispositivos em uma rede local, mas também permite a interconexão de redes globais, como a Internet, que envolve a comunicação entre milhões de dispositivos ao redor do mundo. Além disso, a camada de redes tem um papel vital na escalabilidade das redes, permitindo a adição de novos dispositivos e a expansão de redes sem comprometer a eficiência ou a segurança da comunicação.

Portanto, a camada de redes é essencial para o funcionamento de qualquer infraestrutura de rede, pois garante a entrega de dados de maneira precisa, eficiente e segura. Sua importância vai além da simples comunicação entre dispositivos, uma vez que, por meio de tecnologias como o roteamento, endereçamento e controle de tráfego, ela viabiliza a criação de redes complexas, escaláveis e interconectadas, como a Internet. Sem a camada de redes, a comunicação entre dispositivos e a conexão global que conhecemos atualmente seriam impossíveis de serem realizadas de maneira estruturada e confiável.

REFERÊNCIAS BIBLIOGRÁFICAS:

Disponível em:
<https://www.cisco.com/c/pt_br/support/docs/ip/routing-information-protocol-rip/13769-5.epub >. Acesso em: 04 mar. 2025.

Interligação de Redes com TCP/IP. Disponível em:
<https://books.google.com.br/books?hl=pt-BR&lr=&id=F1_jBwAAQBAJ&oi=fnd&pg=PT5&dq=protocolo+ip&ots=k1r6loo8Bu&sig=qhy-SqcenerUSZ1RMJA2Tobe0SE#v=onepage&q&f=true> . Acesso em: 04 mar. 2025.

O que é camada de rede? Camada de rede x camada de internet. Disponível em: <https://www.cloudflare.com/pt-br/learning/network-layer/what-is-the-network-layer/>. Acesso em: 07 mar. 2025

RFC 791 - Internet Protocol. *Specification of Internet Protocol*, 1981. Disponível em: < https://tools.ietf.org/html/rfc791 >. Acesso em: 11 mar. 2025.

RFC 1122 - Requirements for Internet Hosts - Communication Layers. *Internet Engineering Task Force (IETF)*, 1989. Disponível em: < https://tools.ietf.org/html/rfc1122 >. Acesso em: 04 mar. 2025.