**Camada de Rede**

* **Características da camada de rede**

A camada de rede (camada 3 do modelo OSI) **fornece serviços para permitir que dispositivos finais troquem dados entre redes.** O IP versão 4 (IPv4) e o IP versão 6 (IPv6) são os protocolos de roteáveis da camada de rede. Outros protocolos da camada de rede incluem protocolos de roteamento, como o Open Shortest Path First (OSPF) e protocolos de mensagens de controle, como o Internet Control Message Protocol (ICMP). Para realizar a comunicação ponta a ponta através da rede, os protocolos da camada de rede realizam quatro operações básicas:

* Endereçamento dos dispositivos finais
* Encapsulamento
* Roteamento
* Desencapsulamento
* Switching

Ao contrário da camada de transporte (camada 4 do modelo OSI), que gerencia o transporte de dados entre os processos em execução em cada host, os protocolos de comunicação da camada de rede (ou seja, IPv4 e IPv6) especificam a estrutura do pacote e o processamento usado para levar os dados de um host para outro. Por operar sem levar em conta os dados carregados em cada pacote permite que a camada de rede transmita pacotes para vários tipos de comunicação entre vários hosts.

IP PDU: O IP encapsula o segmento (TCP) ou datagrama (UDP) da camada de transporte. O cabeçalho IP é usado para entregar o pacote ao host de destino. O cabeçalho IP é examinado por dispositivos da camada 3 à medida que trafega por uma rede até seu destino. As informações de endereçamento IP permanecem as mesmas desde o momento em que o pacote sai do host de origem até chegar ao host de destino, exceto quando traduzido por NAT (Network Address Translation) para IPv4. O roteamento executado por dispositivos intermediários examina o endereçamento da camada de rede no cabeçalho do pacote. A PDU da camada de transporte encapsulada, ou outros dados, permanece inalterada durante os processos da camada de rede.

* **Características IP**

*Connectionless*

Não há conexão com o destino estabelecido antes do envio dos pacotes de dados. O IP não tem conexão, o que significa que nenhuma conexão ponta a ponta dedicada é criada pelo IP antes do envio dos dados. Portanto, na comunicação sem conexão não há um caminho pré-estabelecido para os pacotes trafegarem. A cada nó é decidido o próximo passo com base no endereço de destino. Os pacotes podem seguir caminhos diferentes até o destino e chegarem fora de ordem (datagrama). O IP não requer troca inicial de informações de controle para estabelecer uma conexão ponta a ponta antes que os pacotes sejam encaminhados.

*Best Effort*

O IP é inerentemente não confiável porque a entrega do pacote não é garantida. O IP também não requer campos adicionais no cabeçalho para manter uma conexão estabelecida. Esse processo reduz muito a sobrecarga (overhead) do IP. No entanto, sem uma conexão ponta a ponta pré-estabelecida, os remetentes não sabem se os dispositivos de destino estão presentes e funcionais ao enviar pacotes, nem se o destino recebe o pacote ou se o dispositivo de destino é capaz de acessar e ler o pacote. O protocolo IP não garante que todos os pacotes entregues sejam, de fato, recebidos.

*Media Independent*(Independente do meio)

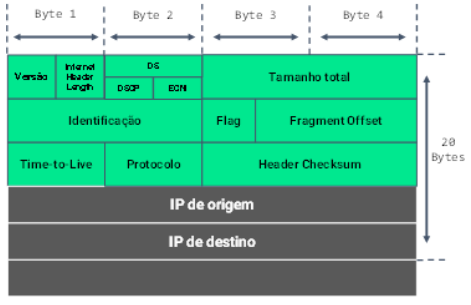
A operação é independente do meio (ou seja, cobre, fibra óptica ou sem fio) que transporta os dados. Não confiável significa que o IP não tem a capacidade de gerenciar e recuperar pacotes não entregues ou corrompidos. Se pacotes fora de ordem forem entregues, ou pacotes estiverem faltando, os aplicativos que usam os dados, ou serviços da camada superior, devem resolver esses problemas.  O IP opera independentemente da mídia que transporta os dados nas camadas inferiores da pilha de protocolo.

A camada de enlace do modelo OSI é responsável por receber um pacote IP e prepará-lo para transmissão pelo meio físico de comunicação. Isso significa que a entrega de pacotes IP não está limitada a nenhum meio específico. Uma característica que a camada de rede considera é o tamanho máximo da PDU (Maximum Transmission Unit - MTU). Em alguns casos, um dispositivo intermediário, geralmente um roteador, deve dividir um pacote IPv4 ao encaminhá-lo de um ponto para outro com um MTU menor. Esse processo é chamado de fragmentação do pacote ou fragmentação.

* **Pacotes IPv4 e IPv6**

*Estrutura do pacote IPv4*

IPv4 é um dos principais protocolos de comunicação da camada de rede. O cabeçalho (header) do pacote IPv4 é usado para garantir que esse pacote seja entregue em seu próximo ponto de processamento (nó) no caminho para seu dispositivo final de destino. Um cabeçalho de pacote IPv4 consiste em campos contendo informações importantes sobre o pacote. Esses campos contêm números binários que são examinados pelo processo da Camada 3.



*Versão*

Contém um valor binário de 4 bits. Com 0100 identifica um pacote IPv4.

*DS*

Differentiated Services ou DiffServ.  Chamado anteriormente de campo de tipo de serviço (Type of Service - ToS). É um campo de 8 bits usado para determinar a prioridade de cada pacote. Os 6 bits mais significativos desse campo representam o DSCP (Differentiated Services Code Point) e os outros dois o ECN (Explicit Congestion Notification).

*Header Checksum*

Usado para detectar se há algo corrompido no header IPv4.

*TTL (Time To Live)*

Contém um valor binário de 8 bits que é usado para limitar o tempo de vida do pacote. O dispositivo de origem define o TTL inicial, que é decrescido cada vez que o pacote é processado por um roteador. Se o TTL chega a zero, o roteador descarta o pacote e envia uma mensagem ICMP Time Exceeded para o IP de origem.

*Protocolo*

Esse campo de 8 bits é usado para identificar o protocolo e indica o payload que o pacote está carregando. Isso habilita a camada de rede a passar os dados para o protocolo superior de forma apropriada. Exemplos: ICMP (1), TCP (6), UDP (17).

*IP de Origem*

Valor binário de 32 bits do endereço IP de origem. É sempre um endereço unicast.

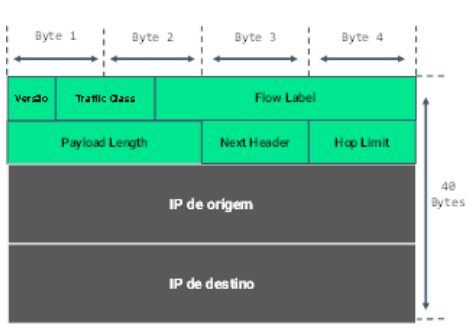
*IP de Destino*

Valor binário de 32 bits do endereço IP de destino. Pode ser um endereço unicast, multicast ou broadcast.

Os campos IHL, Tamanho Total e Header Checksum são usados para identificar e validar o pacote. Outros campos são usados para reordenar um pacote fragmentado. Especificamente, o pacote IPv4 usa os campos Identificação, Flags e Fragment Offset para rastrear os fragmentos. Um roteador pode ter que fragmentar um pacote IPv4 ao encaminhá-lo de um meio para outro com um MTU menor.

* **Estrutura do pacote IPv6**

A Figura a seguir mostra o cabeçalho do IPv6.



*Versão*

Valor binário de 4 bits. Com 0110 identifica como um pacote IPv6.

*Traffic Class*

Campo de 8 bits equivalente ao DS do IPv4.

*Payload Length*

Campo de 16 bits que indica o tamanho da porção de dados ou do payload do pacote. Não inclui o tamanho do header IPv6 (40 bytes).

*Next Header*

Campo de 8 bits equivalente ao Protocolo no IPv4. Indica o tipo do payload para habilitar a camada de rede a repassar os dados de acordo com o protocolo superior.

*Hop Limit*

Similar ao TTL do IPv4. O IPv6 não inclui o Header Checksum, pois a verificação deve acontecer nas camadas superiores e inferiores. Significa que não precisa ser recalculado em cada roteador que decrementa o campo, fornecendo melhor desempenho.

* **Roteamento**

*Encaminhamento*

No IPv4 e IPv6 os pacotes são sempre gerados no host de origem. O host de origem deve ser capaz de direcionar o pacote ao host de destino. Para fazer isso, os dispositivos hosts finais montam sua própria tabela de roteamento. Outra função da camada de rede é direcionar pacotes entre hosts. Um host pode enviar um pacote para o seguinte:

* Próprio: um host pode executar**ping** em si mesmo enviando um pacote para um endereço IPv4 especial de 127.0.0.1 ou um endereço IPv6 ::1, que é conhecido como interface de loopback.
* Host local: é um host de destino que está na mesma rede local que o host de envio. Os hosts de origem e destino compartilham o mesmo endereço de rede.
* Host remoto: é um host de destino em uma rede remota. Os hosts de origem e destino não compartilham o mesmo endereço de rede.
* Se um pacote é destinado a um host local ou remoto é determinado pelo dispositivo final de origem. Em IPv4 o dispositivo de origem usa sua própria máscara de sub-rede junto com seu próprio endereço e o de destino para fazer essa determinação. Em IPv6 o roteador local anuncia o endereço da rede local (prefixo) para todos os dispositivos da rede. Dispositivos que estão além do segmento de rede local são conhecidos como hosts remotos. Quando um dispositivo de origem envia um pacote a um dispositivo de destino remoto, é necessária a ajuda de roteadores e roteamento. O roteamento é o processo de identificação do melhor caminho para um destino. O roteador conectado ao segmento de rede local é conhecido como gateway padrão.
* ***Gateway* padrão**

O gateway padrão é o dispositivo de rede (ou seja, roteador ou switch de camada 3) que pode rotear o tráfego para outras redes. Em uma rede, um gateway padrão geralmente é um roteador com estes recursos:

* Tem um endereço IP local no mesmo intervalo de endereços de outros hosts
* Pode aceitar dados na rede local e encaminhar dados para fora da rede
* Direciona o tráfego para outras redes.

Um gateway padrão é necessário para enviar tráfego para fora da rede local. O tráfego não pode ser encaminhado para fora da rede local se não houver um gateway padrão.

Uma tabela de roteamento de host geralmente inclui um gateway padrão. No IPv4 o host recebe o endereço IPv4 do gateway padrão dinamicamente do protocolo de configuração dinâmica de hosts (DHCP - Dynamic Host Configuration Protocol).

Decidindo o roteamento:

*O que acontece quando um pacote chega a uma interface do roteador?*

 O roteador examina o endereço IP de destino do pacote e pesquisa em sua tabela de roteamento para determinar para onde encaminhar o pacote. A tabela de roteamento contém uma lista de todos os endereços de rede conhecidos (prefixos) e para onde encaminhar o pacote. Essas entradas são conhecidas como entradas de rota ou rotas. O roteador encaminhará o pacote usando a melhor entrada (mais longa) de rota correspondente.

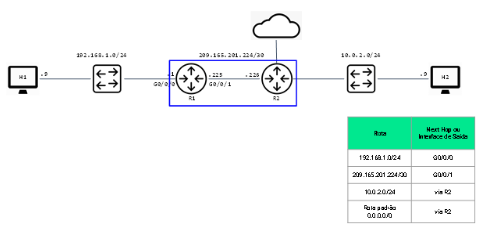
Pacote saindo de 192.68.1.9 e indo para 10.0.2.9

1) Pacote chega na interface Gigabit Ethernet 0/0/0 de R1, que por sua vez desencapsula o header Camada 2 Ethernet e o trailer.

2) R1 analisa o IP destino do pacote e procura na sua tabela de roteamento, que indica que o pacote vai ser encaminhado para R2.

3) R1 encapsula o pacote em um novo header Ethernet e encaminha para R2.

A Figura a seguir ilustra a decisão de encaminhamento de pacote do roteador R1.

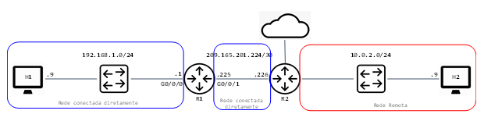


* **Tabela de Roteamento - Roteador IP**

A tabela de roteamento armazena três tipos de entradas de rota:

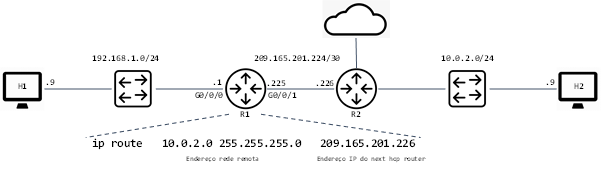
* Redes conectadas diretamente: são interfaces de roteador ativas.
* Redes remotas: são conectadas a outros roteadores.
* Rota padrão: como um host, a maioria dos roteadores também inclui uma entrada de rota padrão, um gateway de último recurso.

A Figura a seguir mostra um exemplo de redes conectadas diretamente e remota.



Roteamento Estático

As rotas estáticas são entradas de rota configuradas manualmente. A rota estática inclui o endereço de rede remota e o endereço IP do roteador do próximo salto. Se houver uma alteração na topologia da rede a tabela de roteamento deve ser atualizada manualmente. A Figura a seguir ilustra um exemplo de rota estática para a rede 10.0.2.0 da tabela de roteamento do roteador R1.



Roteamento Dinâmico

Um protocolo de roteamento dinâmico permite que os roteadores aprendam automaticamente sobre redes remotas, incluindo uma rota padrão, de outros roteadores. Os roteadores que usam protocolos de roteamento dinâmico compartilham automaticamente as informações de roteamento com outros roteadores e atualizam quaisquer alterações de topologia sem envolver o administrador da rede.

Exemplos de protocolos de roteamento dinâmico: OSPF (Open Shortest Path First), IS-IS (Intermediate System to Intermediate System), Enhanced Interior Gateway Routing Protocol (EIGRP) e BGP (Border Gateway Protocol).

A configuração básica requer apenas que o administrador da rede habilite as redes diretamente conectadas dentro do protocolo de roteamento dinâmico. O protocolo de roteamento dinâmico descobre redes remotas, mantém informações de roteamento atualizadas, escolhe o melhor caminho para as redes de destino e tenta encontrar um novo melhor caminho se o caminho atual não estiver mais disponível.

Quando um roteador é configurado manualmente com uma rota estática ou aprende sobre uma rede remota dinamicamente usando um protocolo de roteamento, o endereço de rede remota e o endereço do próximo salto são inseridos na tabela de roteamento IP. A Figura a seguir mostra um exemplo de roteamento dinâmico.

