



una

**O MELHOR**  
CENTRO UNIVERSITÁRIO  
PRIVADO DE BH

Fonte: MEC



# Datagrama IP





# Datagrama IP

O pacote apresentado abaixo é repassado à camada de enlace para que seja enviado ao equipamento destino.

0	4	8	16	19	24	31
<b>VERS</b>	<b>HLEN</b>	<b>SERVICE TYPE</b>	<b>TOTAL LENGTH</b>			
<b>IDENTIFICATION</b>			<b>FLAGS</b>	<b>FRAGMENT OFFSET</b>		
<b>TIME TO LIVE</b>		<b>PROTOCOL</b>	<b>HEADER CHECKSUM</b>			
<b>SOURCE IP ADDRESS</b>						
<b>DESTINATION IP ADDRESS</b>						
<b>IP OPTIONS (IF ANY)</b>					<b>PADDING</b>	
<b>DATA</b>						



# Datagrama IP

- **VERS:** Identifica a versão do protocolo IP que montou o pacote.
- **HLEN:** Os quatro bits desse campo determinam o comprimento do cabeçalho do pacote em múltiplos de palavras de 32 bits. O comprimento do cabeçalho é variável, pois os campos opções IP e preenchimento não possuem tamanhos fixos. O tamanho usual do cabeçalho é de 20 bytes, quando os campos opções IP e preenchimento são nulos. Nesse caso, o campo HLEN apresenta comprimento igual a 5 ( $5 * 32 \text{ bits (4 bytes)} = 20 \text{ bytes}$ )



## Datagrama IP

- **Tipo de serviço:** Contém informações que descrevem a importância do pacote (por meio de oito níveis de prioridade) e a qualidade esperada para o serviço de entrega. A qualidade do serviço é descrita por três bits: D, T e R. O bit D igual a 1 solicita um baixo atraso; o bit T igual a 1 solicita uma alta taxa de transmissão; e o bit R igual a 1 solicita uma transmissão altamente confiável. As informações desse campo são geralmente ignoradas pelos roteadores que transportam o pacote.



## Datagrama IP

- **Comprimento total:** Informa em bytes o comprimento total do pacote, incluindo o cabeçalho e o campo de dados. Como esse campo possui 16 bits, o tamanho máximo de um pacote é 2 elevado a 16 ou 64 kbytes



## Datagrama IP

- **Identificação:** Contém um número inteiro que identifica o pacote. Esse campo é utilizado no processo de fragmentação e remontagem dos pacotes. Todos os fragmentos de um pacote contêm o mesmo número de identificação. Dessa forma, o receptor consegue identificar facilmente os fragmentos que precisam ser reagrupados para remontar o pacote original.



# Datagrama IP

- **Flags:** Campo composto pelos bits DF (Don't Fragment) e MF (More Fragments). A estação transmissora assinala DF igual a 1 para indicar que o pacote não deve ser fragmentado. Nesse caso, se um roteador precisar fragmentar o pacote para adequá-lo à rede de destino, o pacote será descartado. O bit MF igual a 1 indica que o fragmento é o último pedaço do pacote original. Quando uma estação recebe um fragmento com MF igual a 0, ela sabe que deve esperar a chegada de mais fragmentos para completar a montagem do pacote.





## Datagrama IP

- **Deslocamento do fragmento:** Esse campo contém a posição relativa do fragmento em relação ao pacote original, medida em bytes. Os fragmentos de um pacote não chegam ao receptor necessariamente na mesma ordem em que foram transmitidos. Utilizando a informação do campo de deslocamento, a estação receptora consegue reordenar os fragmentos recebidos e remontar o pacote original.



## Datagrama IP

- **Tempo de vida (TTL – Time To Live):** Indica o tempo em segundos que o pacote pode permanecer na rede. Quando uma estação transmite um pacote, ela assinala o valor do TTL. Toda vez que o pacote é processado por um roteador, o TTL é decrescido em uma unidade. Quando ele expira (chega a 0), o pacote é descartado, ainda que o destino final não tenha sido atingido.



## Datagrama IP

- **Protocolo:** Indica o tipo de protocolo de transporte encapsulado no campo de dados do pacote que poder TCP ou UDP.
- **Checksum do cabeçalho:** Contém o checksum de todos os bytes que compõem o cabeçalho de controle, excluindo apenas o próprio campo de checksum.



# Datagrama IP

- **Endereço IP de origem:** Contém o endereço IP que identifica a estação transmissora.
- **Endereço IP de destino:** Contém o endereço IP que identifica a estação de destino.
- **Opções IP:** Esse campo possui tamanho variável e pode conter uma série de códigos em sequência, cada um deles definindo uma opção relativa ao processamento dos pacotes. As opções são geralmente relacionadas a aspectos como segurança, roteamento, relatórios de erro, depuração etc.



## Datagrama IP

- **Preenchimento:** Esse campo completa a sequência do campo opções com bits de preenchimento de valor 0, garantindo que o tamanho total dos campos opções somados ao preenchimento seja múltiplo de 32 bits.
- **Dados:** Contém os dados transportados pelo pacote, os quais correspondem geralmente à unidade de dados do protocolo de transporte TCP ou UDP.



## Fragmentação e remontagem

Um pacote IP pode ter até 64 kbytes. Entretanto, alguns protocolos de camadas inferiores podem não suportar pacotes desse tamanho. Um exemplo muito conhecido é o caso do IP sobre Ethernet, cujo quadro tem um tamanho máximo de 1500 bytes. Nesses casos, o IP (e vários outros protocolos) usam os recursos de fragmentação e remontagem.



## **Fragmentação e remontagem**

O roteador negocia com os periféricos de rede e com o próximo roteador o tamanho máximo que pode ser usado naquela sub-rede e pacotes com tamanhos maiores são fragmentados. A operação de fragmentação consiste em quebrar os dados do pacote em unidades transportáveis, copiar o cabeçalho para cada uma delas e, por fim, enviar.



# Protocolo ARP

O protocolo ARP (Address Resolution Protocol) é responsável por realizar o mapeamento de endereços lógicos (endereços IP) em endereços físicos (endereços MAC) e foi proposto e aceito pela RFC 826.

Para poder transmitir um pacote, a estação transmissora precisa conhecer todas as informações de endereçamento relacionadas ao destinatário. No modelo de referência TCP/IP todas as referências aos endereços das estações são feitas via endereços IP. O endereço físico é descoberto dinamicamente pelo transmissor antes de efetuar a comunicação utilizando o protocolo ARP.





## Protocolo ICMP

O protocolo ICMP está presente em redes que utilizam os protocolos o modelo de referência TCP/IP. Qualquer equipamento que utilizar endereço IP, quando não conseguir comunicar-se com outro, reportará seu insucesso emitindo uma mensagem de erro seguindo o padrão do protocolo ICMP. Existem 12 tipos de mensagens ICMP, sendo as mais importantes listadas a seguir.



# Protocolo ICMP

Tipo de mensagem	Descrição
Destination unreachable	Pacote não pode ser entregue.
Time exceeded	Campo tempo de vida chegou a 0.
Parameter problem	Campo de cabeçalho inválido.
Source quench	Pacote regulador. Essa mensagem era utilizada para ajustar hosts que estivessem enviando pacotes demais. Essa mensagem é raramente utilizada já que o controle de congestionamento é feito na camada de transporte.
Echo request	Perguntar a uma máquina se ela está viva.
Echo replay	Resposta da mensagem de Echo request



## Protocolo NAT

O NAT (Network Address Translation – Tradução de Endereço de Rede) não é um protocolo e também não se refere a um padrão especificado por entidades internacionais. O NAT é apenas uma série de tarefas que um roteador (ou equipamento equivalente) deve realizar para converter endereços IPs entre redes distintas.



# Protocolo NAT

O equipamento com recurso de NAT deve ser capaz de analisar todos os pacotes de dados que passem por ele e trocar os endereços desses pacotes de maneira adequada, substituindo o endereço IP origem do pacote (endereço não roteável) pelo endereço IP do roteador (endereço roteável). Além dessa substituição, o NAT armazena em sua tabela a relação porta origem versus IP origem a fim de devolver ao emissor o pedido feito.