# CAMADA DE TRANSPORTE

**Definição:** é a quarta camada do modelo OSI. A camada de transporte providência um nível satisfatório de confiabilidade que é independente da rede física utilizada.

**Diferença entre camada de rede e de transporte**

A camada de rede faz a transferência de dados entre computadores, já a de transporte faz a transferência de dados entre processos.

O objetivo principal da camada de transporte é providenciar eficiência, confiança e serviço de transmissão de dados eficaz para os usuários.

Multiplexação: por ter portas, a camada de transporte permite que as aplicações em um mesmo computador acessem a rede de forma simultânea.

O software e/ou hardware que faz o serviço da camada de transporte é a entidade de transporte, que pode estar localizado no kernel do sistema, em uma biblioteca nas conexões de rede, em um processo separado ou até mesmo no NIC.

A camada de transporte é parecida com a de rede, mas o código de transporte é utilizado na máquina do cliente, já na camada de rede, ele é utilizado majoritariamente nos roteadores, controlados pela operadora.

**Mas se é tão parecida, por qual motivo é necessário a camada de transporte?**

Se a camada de rede não funciona adequadamente, ou seja, se tem muitas perdas de pacotes, a camada de transporte entra em cena, ela visa colocar mais qualidade de serviço caso a camada de rede funcione de forma inadequada.

Quando um processo deseja estabelecer uma conexão ele deve indicar em que lugar deseja se conectar. Para isso, são definidas portas de transporte onde cada processo pode escutar por conexão, na internet esses endpoints são chamados de portas, ou em palavras mais formais TSAP (Transporte Service Access Point), eles são formados por 16 bits, ou seja, é possível ter 65.536 portas ($2^{16}$).

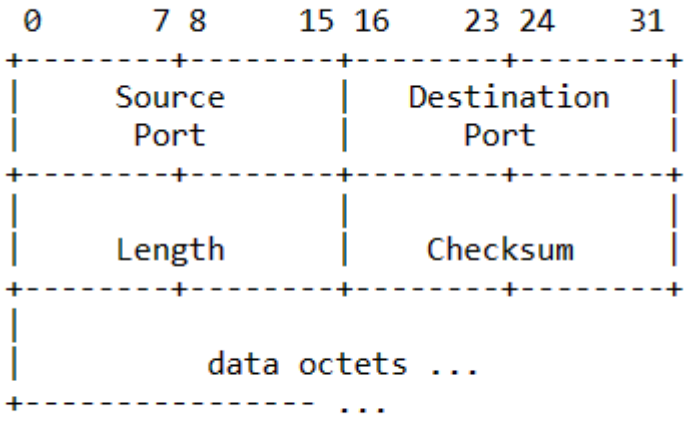
Há dois protocolos na camada de transporte: o UDP e TCP. O UDP não é orientado a conexão como o TCP.

**Protocolo UDP - User Datagram Protocol**

Ele estabelece padrões para que aplicações enviem **datagramas** IP encapsulados sem a necessidade de conexão.

- Não é confiável, pois não tem verificação de integridade de informação.
- 1 -> n - uma estação pode enviar um pacote para diversas estações, ou seja, consegue transmitir grandes quantidade de dados em um espaço pequeno de tempo.
- Não tem handshake.
- O protocolo UDP é utilizado em lugares que precisam de transmissão de dados de forma mais rápida, como streaming e jogos onlines.

Estrutura do cabeçalho UDP.




Fonte: RFC 768

**Source port** - porta de origem

**Destination port** - porta de destino

**Length** - comprimento em bytes do cabeçalho + dados carregados.

**Checksum** - código utilizado para verificar a integridade do dado

O número de porta de origem e o checksum é opcional no IPv4.

**Protocolo TCP - Transmission Control Protocol**

O protocolo TCP é um protocolo orientado a conexão, ou seja, é necessário estabelecer uma conexão entre os hosts antes que os dados sejam trafegados.

- Tem confiabilidade: o destino e a origem devem ter a mesma informação, essa confirmação é feita pelo número de verificação (checksum).
- Full Duplex - comunicação se dá dos dois lados, podem ser simultânea.
- Entrega ordenada - cada pacote TCP tem um número sequencial, (às vezes os pacotes podem seguir rotas distintas, podendo chegar em ordem diferente na origem) possibilitando a ordenação dos pacotes quando chegam no destino.
- Point to point - às conexão tem exatamente dois pontos, TCP não suporta multicast ou broadcast.
- TCP envia pacotes chamados de **segmentos.**
- Utilizado em aplicações que necessitam de muita confiabilidade, como envio de e-mail e download de arquivos.

**Como estabelecer a conexão TCP**

Por meio do **Three-way handshake**

O host que deseja iniciar a conexão envia um segmento (PDU do protocolo TCP) com a flag SYN (SYN indica o início de uma conexão) ativa, indicando qual o número de porta do servidor de destino que se deseja conectar.

O servidor responde com um segmento com a flag SYN e seu número de sequência inicial. A resposta também vem com a flag ACK confirmando o recebimento.

O host que iniciou a conexão confirma o segmento SYN enviando outro segmento com a flag ACK ativa.

Depois disso o processo de estabelecimento de conexão está pronto, esse é o Handshake de três vias.

**Por que o handshake, ou o estabelecimento de conexão é necessário**

O cliente e o servidor precisam confirmar um para o outro que podem receber pacotes, bem como, precisam saber se o outro pode receber seus pacotes.

Observação: portas abaixo de 1024 (portas baixas) são reservadas para serviços padrão como FTP, SSH, HTTP, HTTPS e SMTP.

## REFERÊNCIAS


https://docente.ifrn.edu.br/tadeuferreira/disciplinas/2016.1/arq-tcp-ip/Aula17.pdf

http://www.bosontreinamentos.com.br/redes-computadores/curso-de-redes-protocolo-tcp-handshake-de-tres-vias/

https://www.youtube.com/watch?v=O4X57EUIhuY&ab_channel=B%C3%B3sonTreinamentos

https://edisciplinas.usp.br/pluginfile.php/5353537/mod_resource/content/1/2020_Aula12_Camada_de_Transporte_parte1_2020.pdf

http://www.bosontreinamentos.com.br/redes-computadores/curso-de-redes-protocolo-udp-user-datagram-protocol/

https://networkengineering.stackexchange.com/questions/24068/why-do-we-need-a-3-way-handshake-why-not-just-2-way

https://www.rfc-editor.org/rfc/rfc768

TANENBAUM, Andrew S; WETHERALL, David J. Redes de Computadores. Quinta edição. Pearson, 2011.