INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

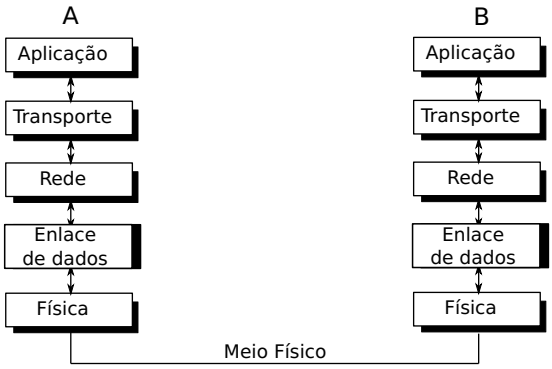
Professor: Macêdo Firmino
Disciplina: Arquitetura de Rede
Aula 14: Análise da Camada de Transporte e Protocolo UDP com Wireshark

---

Na aula de hoje iremos compreender as funções e responsabilidades da camada de transporte no modelo TCP/IP, conhecer os protocolos TCP e UDP, analisar o funcionamento e os campos do cabeçalho UDP e realizar testes práticos de comunicação via UDP. Vamos lá?? Preparados??

Camada de Transporte

A camada de transporte é responsável pela comunicação entre processos finais (programas) entre diferentes equipamentos. Embora a camada de rede gerencie a entrega de pacotes individuais da origem até seu destino, ela trata cada pacote de forma independente, como se cada um deles pertencessem a uma mensagem distinta. Desta forma, a camada de transporte poderá garantir a integridade e a ordem de entrega dos pacotes, controlar erros na transmissão, bem como o fluxo de dados.



A principal função desta camada é a entrega de uma mensagem entre processos (programas) finais. Os computadores normalmente executam vários programas ao mesmo tempo. Por essa razão, entrega origem-destino significa a entrega de uma mensagem não apenas de um computador para outro, mas também de um programa específico em um computador para um programa específico em outro. Outras funções são:

- Endereçamento por Portas: permite que várias aplicações utilizem a rede simultaneamente, associando programas a diferentes portas de origem e destino
- Controle do Enlace (opcional): permite estabelecer uma conectividade (conversa) fim-a-fim entre aplicações.
- Segmentação e Reagrupamento (opcional): permite dividir uma mensagem em vários segmentos de tamanhos variáveis, onde cada segmento contém um número deidentificação. Com este número é possivel o receptor remontar, identificar e/ou substituir pacotes extraviados;
- Controle de Fluxo (opcional): realiza um controle de fluxo fim a fim (entre programas). Ela garante que o remetente não envie dados mais rápido do que o receptor pode processar, evitando sobrecarga e perda de pacotes.;
- Controle de Erros (opcional): realiza um controle de erro fim a fim. Assegura que toda a mensagem chegue ao destino final livre de erros. A correção de erros normalmente se faz através de um pedido de retransmissão.

Os dois principais protocolos da camada de transporte são:

- UDP (*User Datagram Protocol*) é um protocolo de transporte não confiável e sem conexão. Ele implementa apenas o endereçamento por portas e um controle de erro (opcional);
- TCP *(Transmission Control Protocol)* é orientado a conexão e confiável. Ele implementa o endereçamento por portas, controle de enlace, controle de erro, segmentação e controle de fluxo.

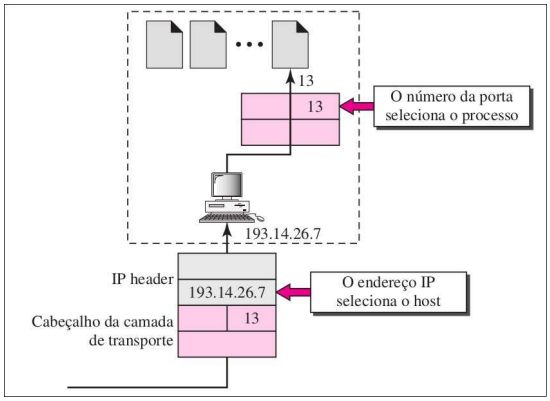
Se o programa na camada de aplicação requerer confiabilidade, necessitamos utilizar um protocolo de camada de transporte confiável (TCP) que Isso implica em um serviço mais lento e mais complexo.

Por outro lado, o programa na camada de aplicação pode não requerer confiabilidade no transporte de dados, ou por implementar mecanismos próprios de controle de fluxo, controle de erros e ordenação de pacotes, ou por requerer serviços mais rápidos, ou pela natureza do serviço não exigir controle de fluxo e de erros (aplicações em tempo real). Para esses casos, podemos usar um protocolo não confiável (UDP).

Endereçamento por Portas

Na camada de transporte, utilizamos um endereço denominado de número de porta, para escolher um entre os vários processos (programas) que estão em execução no equipamento de destino. O número da porta de destino é necessário para entrega; o número da porta de origem é necessário para resposta.

Quando uma aplicação deseja enviar dados ou receber dados, a Camada de Transporte atribui uma porta de origem ou destino ao processo (programa). Por exemplo: um navegador da web pode usar uma porta 50234 para enviar uma solicitação para um servidor na porta 80. No dispositivo de destino, o protocolo verifica a porta de destino para entregar os dados ao processo correto.



No modelo Internet, os números de porta são inteiros de 16 bits entre 0 e 65.535. A IANA (Internet Assigned Number Authority) dividiu o número das portas em três faixas:

- Portas conhecidas. As portas na faixa de 0 a 1023 são atribuídas e controladas pela IANA e usadas para servidores. Estas são as portas conhecidas (well-known port numbers).

- Portas registradas. As portas na faixa de 1024 a 49151 não são atribuídas ou controladas pela IANA. Elas podem ser registradas na IANA para impedir duplicação.

- Portas dinâmicas. As portas na faixa de 49152 a 65535 não são controladas nem registradas. Elas podem ser usadas por qualquer processo cliente. Estas são denominadas portas efêmeras.

Exemplos de portas conhecidas:

Porta	Descrição
20 e 21	FTP (download)
22	SSH (acesso remoto)
25	SMTP (envio de e-mail)
53	DNS (resolver domínio)
80	HTTP (acesso web)
123	NTP (horário pela internet)

Exemplos de portas registradas:

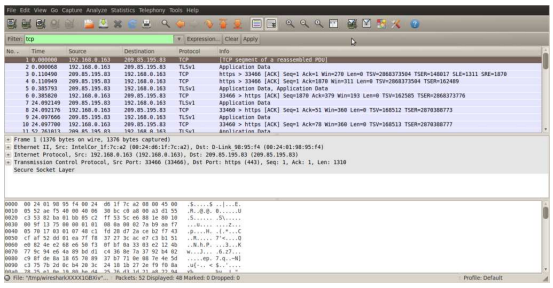
Porta	Descrição
2400	Age of Empires II
3074	*Xbox LIVE*
25565	Minecraft: Jogo Online
28960	Call of Duty 2
36963	Counter Strike

Wireshark

Para analisarmos protocolos de rede são utilizadas ferramentas chamadas de analisadores de tráfego. Na aula de hoje iremos utilizar um analisador de tráfego gratuito chamado de Wireshark. Com ele iremos visualizar o funcionamento dos protocolos TCP e UDP.

O Wireshark é um programa (conhecido como *sniffer*) que verifica os pacotes transmitidos pelo dispositivo de comunicação (placa de rede, placa de fax modem, etc.) do computador. O programa analisa o tráfego de entrada e saída e organiza-os por protocolo. Já utilizamos em outras aulas desta disciplina.

Para selecionar os pacotes baseados no protocolo, basta digitar o nome do protocolo no qual você está interessado no campo *Filter* (Filtro) e pressione o botão "Apply" (aplicar) para iniciar o filtro. A Figura abaixo mostra um exemplo de filtragem sobre o protocolo TCP.



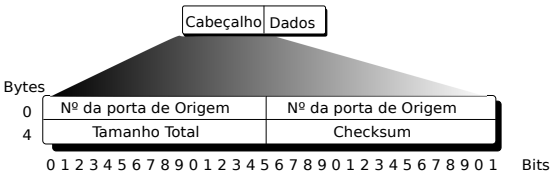
Protocolo UDP

O Protocolo UDP (*User Datagram Protocol*) é um protocolo da camada de transporte do modelo TCP/IP, utilizado para enviar dados entre computadores de forma rápida e eficiente, sem a necessidade de estabelecer uma conexão prévia. Ele é classificado como protocolo sem conexão e não confiável, ou seja, não garante que os dados enviados cheguem ao destino, nem que cheguem na ordem correta.

O UDP não realiza controle de fluxo, controle de erros ou retransmissão após a recepção de um segmento incorreto. O UDP apenas inicia a transferência de dados sem quaisquer preliminares formais. Assim o UDP não introduz qualquer atraso para estabelecer uma ligação. Desta forma, o UDP é utilizado em aplicações que podem tolerar uma pequena quantidade de perda de pacotes e são sensíveis à velocidade, entre elas:

- DNS (Domain Name System): consultas rápidas para resolver nomes de domínio.
- VoIP (Voice over IP) e videoconferência: atrasos pequenos são preferíveis a perda de pacotes.
- Jogos online: comunicação em tempo real entre jogadores.
- Streaming de vídeo e IPTV: transmissão ao vivo, onde pequenos erros são toleráveis.
- DHCP (Dynamic Host Configuration Protocol): para atribuição de endereços IP em redes.

Os datagrama UDP possuem um cabeçalho de tamanho fixo, de 8 bytes. com os seguintes campos:



- Porta de origem: especifica o número da porta usada pelo processo em execução no host de origem.
- Porta de destino: especifica o número da porta usado pelo processo em execução no host de destino.
- Comprimento: campo de 16 bits que define o comprimento total de um datagrama UDP, compreendendo cabeçalho mais dados.
- Checksum: campo de 16 bits é usado para detectar erros na transmissão de datagrama UDP (cabeçalho mais dados). O cálculo do checksum e sua inclusão em um datagrama UDP são opcionais.

Atividade

Em duplas, iremos realizar uma Análise do protocolo UDP com o Wireshark. Ao final enviei um documento as respostas dos quesitos 04 e 05 e envie no Google Sala de Aula.

01. Começe a captura de tráfego na rede com o Wireshark;

02. Utilize o navegador para acessar o site `www.ifrn.edu.br`;

03. No Wireshark, use o filtro udp para isolar apenas os pacotes UPD.

udp

04. Escreva quais são campos existentes no cabeçalho de um segmento UDP (*User Datagram Protocol*)? Quais são as funções de cada campo do cabeçalho?

05. Escreve pelo menos 5 número de portas UDP encontradas (Source Port e Destination Port).