Protocolo UDP

O **User Datagram Protocol** (UDP) é um protocolo da camada de transporte, que permite que a aplicação envie um datagrama encapsulado num pacote IPv4 ou IPv6 a um destino. Dentre as principais características do protocolo a que mais se destaca é que não existe qualquer tipo de garantia que o pacote chegue corretamente (ou de qualquer modo), ao contrário de seu "irmão" TCP. O protocolo também não remove qualquer tipo de verificação de erros, pode enviar pacotes fora de ordem e não é orientado a conexão, então não é necessário estabelecer conexão antes do envio do datagrama. O propósito dessa opção é acelerar o processo de envio de dados, visto que todas as etapas de comunicação necessárias para verificar a integridade de um pacote (e para reenviá-lo, se necessário) contribuem para deixá-lo mais lento.

Devido as suas características, só valerá a pena enviar pacotes utilizando o UDP quando este for pequeno, neste caso, menor que 512KB. Ele se baseia em portas para a troca de informações, desta forma, é atribuída uma porta ao destino e uma porta a origem, como pode ser visualizado a seguir:

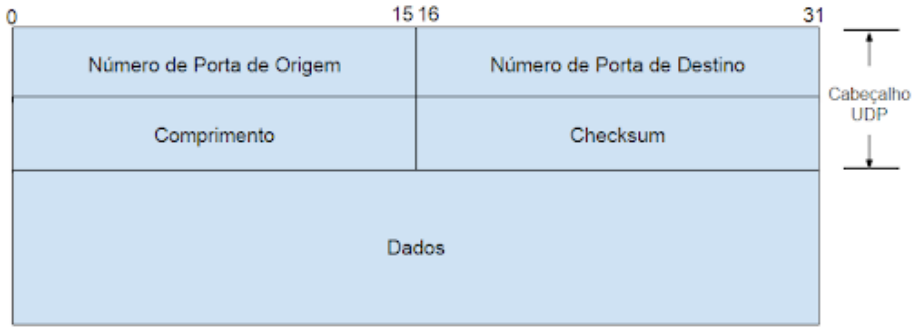

Figura01: Formato do pacote UDP

- Os campos porta de origem e porta de destino, especificam que portas que serão utilizadas na comunicação.
- O campo tamanho descreve quantos bytes terá o pacote completo.
- O campo checksum é opcional e faz uma soma verificadora para garantir que os dados estarão livres de erros

As portas que podem ser adotadas pelo UDP:

- Porta origem: Valor de 1 a 65535
- Porta de destino: Valor de 1 a 65535

Como dito previamente, o UDP é diferente do protocolo TCP, e consegue ter algumas vantagens em determinadas situações. O UDP não se importa com criar ou destruir conexões, durante uma conexão, o UDP troca apenas 2 pacotes, enquanto no TCP esse número é superior a 10, deixando-o mais rápido e mais propício à aplicações do tipo pergunta-resposta. A sua agilidez também pode ser melhor durante a transmissão de um vídeo ao vivo, por exemplo, pois é mais interessante que uma pessoa perca alguns trechos ou tenha que lidar com distorções de imagem e áudio do que esperar pelo recebimento de um pacote que se perdeu — o que pode acabar com o fator "tempo real". O UDP também é muito usado durante games online — caso você perca alguns pacotes, os personagens adversários podem se "teleportar" pela tela, no entanto não há motivos para que você receba os dados que foram perdidos, já que a partida continua mesmo sem que eles cheguem até você. Tudo o que importa é o que está acontecendo agora, não aquilo que ocorreu há alguns instantes, assim não faz sentido apostar em checagens de erro que só serviriam para aumentar a latência dos participantes. Ou seja, o protocolo UDP é admissível para fluxos de dados em tempo real, especialmente aqueles que admitem perda ou corrompimento de parte de seu conteúdo. Aplicações sensíveis a atrasos na rede, mas poucos sensíveis a perdas

de pacotes, como jogos de computadores, também beneficiam do UDP. O UDP também suporta broadcasting e multicasting, devendo, necessariamente, ser utilizado.

Em suma, o protocolo UDP é utlizado quando a comunicação requere um pacote de ida e um de volta, comunicação em tempo real e a aplicação requer controle de retransmissões.

Devido a sua simplicidade e praticidade, alguns protocolos utilizam UDP, como:

- TFTP (Trivial File Transfer Protocol)

Este protocolo é semelhante ao FTP (protocolo padrão/genérico independente de hardware sobre um modo de transferir arquivos/ficheiros e também é um programa de transferência)porém sem confirmação de recebimento pelo destino ou reenvio. É geralmente utilizado para transferir pequenos ficheiros entre hosts numa rede, tal como quando um terminal remoto ou um cliente inicia o seu funcionamento, a partir do servidor.

- SNMP (Simple Network Management Protocol)

O SNMP ajuda o gestor da rede a localizar eventuais problemas e falhas em sua rede. Através de um gerente SNMP (SLAview, por exemplo), pode-se visualizar gráficos referentes a estatísticas de tráfego, nível do toner em impressoras, CPU e memória de diversos dispositivos. Até mesmo a quantidade de processos que estão sendo executados em um dado dispositivo pode ser analisada.

- DHCP (Dynamic Host Control Protocol)

Trata-se de um protocolo utilizado em redes de computadores que permite a estes obterem um endereço IP automaticamente. É utilizado em redes que sofrem constantes alterações na topologia e o administrador não pode verificar o IP (Internet Protocol) de cada máquina devido a enorme quantidade, então o roteador distribui IPs automaticamente para as estações. Como esta atribuição é feita com a utilização do UDP, caso haja algum problema o usuário terá que pedir o reenvio ou reiniciar a máquina. O único problema técnico deste protocolo é que como os IPs são atribuídos aleatoriamente, fica mais difícil para o administrador ter controle sobre o que cada host está fazendo

- DNS (Domain Name Service)

É uma coleção de bancos de dados que traduz nomes de host para endereços únicos de IP. Neste caso, imaginemos que um usuário esteja acessando a internet e deseja ir para outra página. Ele digita o endereço no campo apropriado e entra. Se a página, por acaso, não abrir por não ter reconhecido o endereço, o problema poderá ter sido no envio ou resposta do servidor de nomes utilizando o UDP, e então o usuário tentará de novo acessar a página e provavelmente conseguirá. Agora, imagine que isto fosse feito com o TCP, provavelmente esta falha não ocorreria, porém o tempo gasto para o computador saber qual IP se refere àquele nome seria inimaginável para as necessidades atuais.

Devido ao uso de portas, o UDP é vulnerável a ataques. Os mais comuns incluem: IP Spoofing - trocar o IP do host de origem por um outro qualquer; UDP flood - tipo de ataque Denial of Service (DoS) no qual o atacante sobrecarrega portas aleatórias no host alvo com pacotes IP contendo datagramas UDP; Fraggle - utiliza o UDP como protocolo de transporte. Ele causa uma chuva ao enviar um pacote UDP para uma lista de endereços de broadcast; e New Teardrop - diminui a parte de dados do pacote e o tamanho total do protocolo UDP é falsificado. Este ataque provoca o travamento das máquinas invadidas.

Enquanto uma proteção a ataques não pode ser 100% garantida, existem maneiras de suavizá-los. Geralmente, um firewall pode filtrar ou bloquear pacotes UDP maliciosos. Impedir a transmissão e/ou recepção de IPs inválidos, também ajuda. Uma possível solução para ataque tipo flood é o uso de proteção DDoS usando

encaminhamento Anycast para balancear a quantidade de ataques sobre um processo de Deep Packet Inspection (DIP).

Na captura, conseguimos ver que o YouTube usa o protocolo UDP para envio de pacotes. Isso acontece pois live video streaming, como vimos antes, consegue se beneficiar da perda de alguns pacotes e não requere verificação. Caso TCP fosse usado, o buffering seria muito lento, vale mais a pena uma pequena perda de qualidade à uma grande lentidão por um vídeo de 10 minutos. Na nossa captura, conseguimos captar os pacotes de UDP do Youtube e vimos que usa a porta 443 (geralmente reservada para HTTPS) e o checksum (unverified). O UDP é colocado dentro de um IP que é envelopado ela Ethernet até a camada física mandar via Youtube.

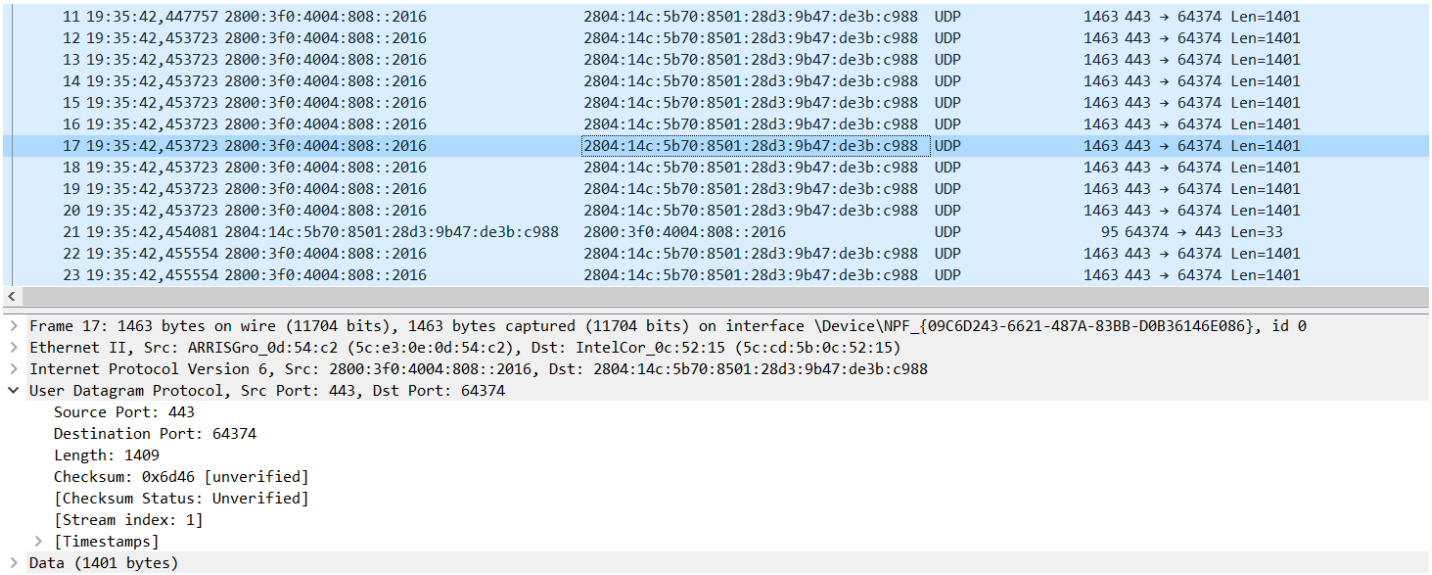

Figura 2: Captura feita pelo Wireshark

Referências

https://pt.wikipedia.org/wiki/User_Datagram_Protocol

https://www.tecmundo.com.br/internet/57947-internet-diferenca-entre-protocolos-udp-tcp.htm

https://edisciplinas.usp.br/pluginfile.php/3257113/mod_resource/content/1/61-Revisao-udp-v5.pdf

https://pt.wikipedia.org/wiki/Trivial_File_Transfer_Protocol

https://pt.wikipedia.org/wiki/File_Transfer_Protocol

https://www.telcomanager.com/blog/o-que-e-snmp/

https://www.tecmundo.com.br/internet/2079-o-que-e-dhcp-.htm

https://tecnoblog.net/283932/o-que-e-dns/

https://canaltech.com.br/internet/o-que-e-dns/

http://www.cbpf.br/~sun/pdf/udp.pdf

https://pt.wikipedia.org/wiki/Ataque_UDP_flood#:~:text=UDP%20flood%20%C3%A9%20um%20tipo,retorna%20um%20pacote%20Destination%20Unreachable.

https://www.cisco.com/c/pt_br/support/docs/security/ios-firewall/13367-3.html

https://www.quora.com/What-is-the-reason-behind-Youtube-using-TCP-and-not-UDP

https://pt.wikipedia.org/wiki/Lista_de_portas_dos_protocolos_TCP_e_UDP

Figura1:

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

Figura2: provida pelos alunos