**ALUNO: THIAGO SANTOS DE LIRA.**

**DHCP**

1. Abra o Wireshark e comece uma captura.
2. Abra o prompt de comandos (windows) ou shell (linux):

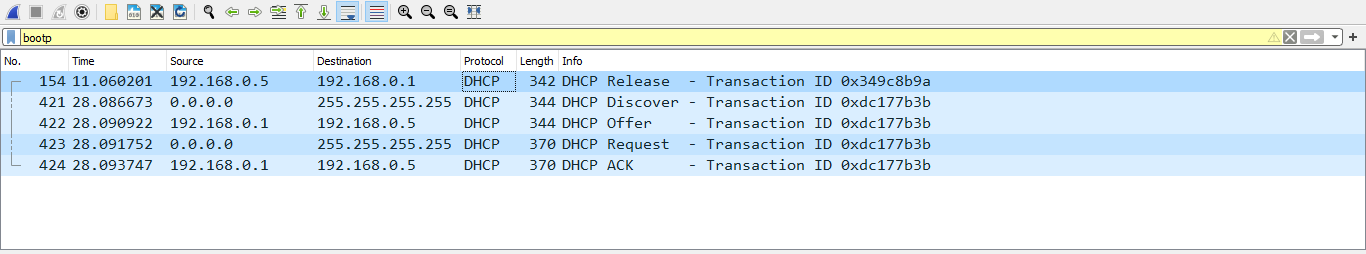
Windows:

1. Digite **ipconfig /release**. Este comando libera o endereço IP atual.
2. Digite **ipconfig /renew**. Este comando solicita informações da rede.

Linux:

1. Digite sudo dhclient *nome\_interfacerede* (ex.: **sudo dhclient wlp6s0**)
2. Pare a captura dos dados no Wireshark e utilize o filtro “bootp” (antigo nome do protocolo dhcp) ou “dhcp” para visualizar as mensagens DHCP.

Observe os pacotes capturados e responda:



1. Quais são as mensagens DHCP trocadas entre cliente e servidor (discover, ack, inform, request, etc)?

Cliente -> Cliente: DHCP Release

Cliente -> Servidor: DHCP Discover

Servidor -> Cliente: DHCP Offer

Cliente -> Servidor: DHCP Request

Servidor -> Cliente: DHCP ACK

1. As mensagens DHCP obtidas são enviadas via UDP ou TCP?

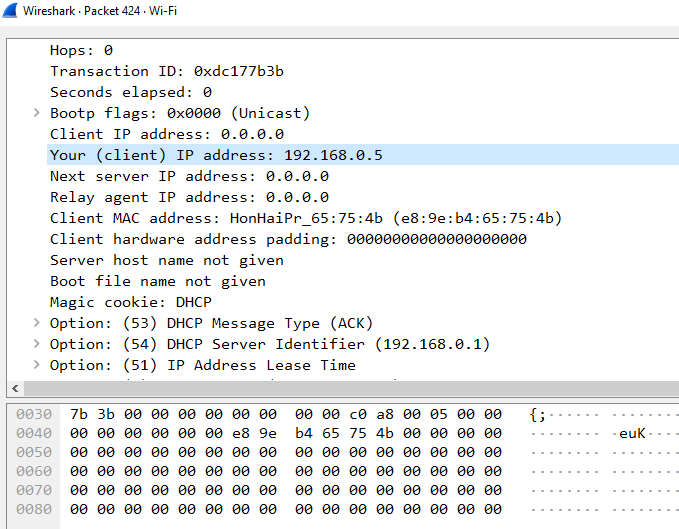
Resposta: UDP

1. Qual o endereço IP de Origem e de Destino utilizados no primeiro pacote (discover) do protocolo DHCP? Por quê são utilizados estes endereços?

Resposta: O cliente utilisa o IP 0.0.0.0 (se não me engano o padrão) e o broadcast recebe para sí com o IP 255.255.255.255 que seria meio como uma “máscara”. Onde são utilizados esses endereços por conta que foi a primeira vez da solicitação do cliente para acesso da rede, utilizando do serviço DHCP.

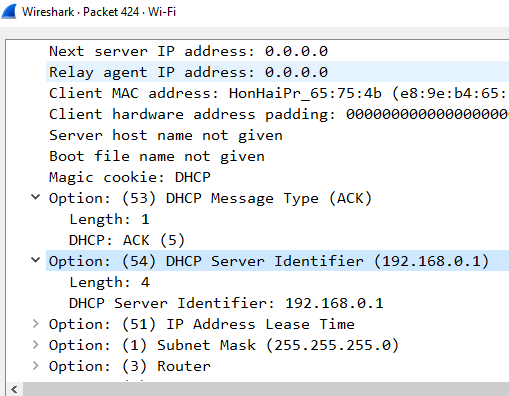
1. Qual o endereço IP que o servidor DHCP oferece? Mostre a mensagem que contém o endereço oferecido.

Resposta : IP 192.168.0.5



1. Qual o endereço do servidor DHCP?

Resposta: IP 192.168.0.1



1. Para cada mensagem DHCP trocada, informe o tipo de endereçamento (unicast ou broadcast) utilizado nos campos IP destino e de origem do protocolo de rede.

Resposta:

DHCP Discover:

Source → Unicast

Destination → Broadcast

DHCP Offer:

Source →Unicast

Destination →Unicast

DHCP Request:

Source →Unicast

Destination → Broadcast

DHCP ACK:

Source →Unicast

Destination →Unicast

**DNS**

1. Abra algum browser.
2. Abra o Wireshark e comece uma captura.
3. No wireshark, utilize o filtro “ip.addr == seu.num.ip.ip and dns” para remover todos pacotes que não são DNS.
4. Inicie a navegação para a página [www.ifsc.edu.br](http://www.ifsc.edu.br/)
5. Pare a captura dos dados.

Observe os pacotes capturados e responda:

1. As mensagens DNS obtidas são enviadas via qual protocolo de transporte?

Resposta: Através do protocolo UDP

1. Qual a porta de origem e destino de uma pergunta DNS? Qual a de origem e destino de uma resposta DNS?

Envio:

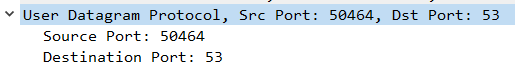
Porta Origem: 50464

Porta Destino: 53

Resposta:

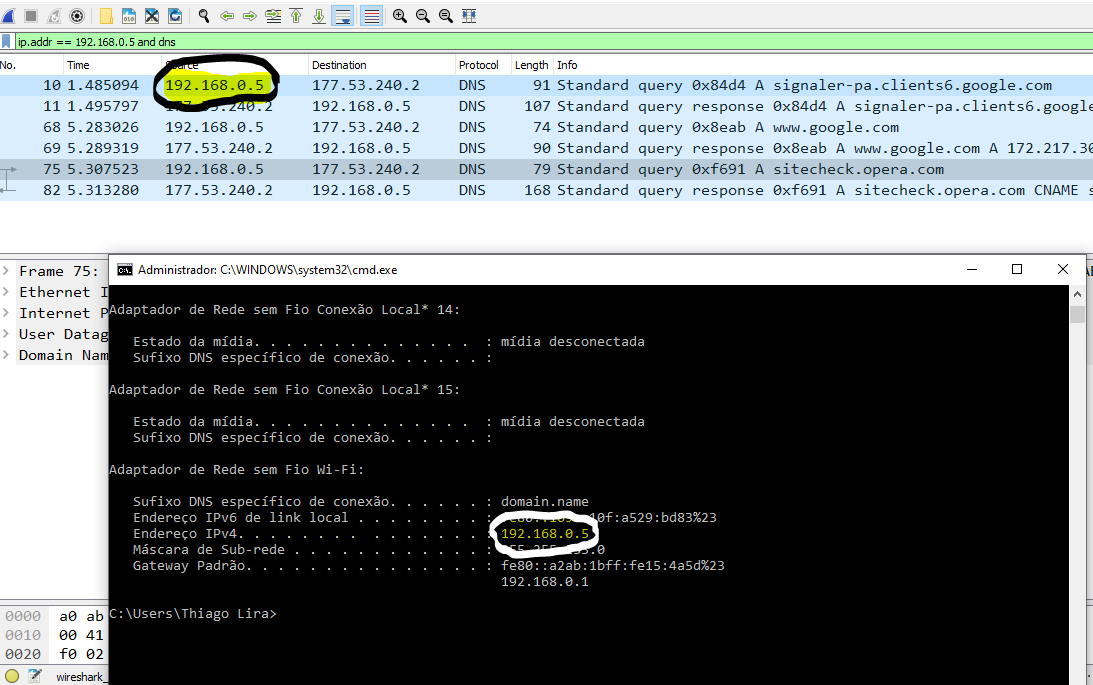
Porta Origem: 53

Porta Destino: 50464



1. Para qual endereço IP as perguntas DNS são enviadas? No Windows, use o comando ipconfig para ver o endereço IP do servidor DNS local. No Linux, utilize **grep "nameserver" /etc/resolv.conf**

Os endereços são os mesmos?



Resposta: Sim, são os mesmos.