BC1513 – Redes de Computadores
Prof. João Henrique Kleinschmidt
Aula Prática 4 – Protocolos TCP – IP – ARP – DHCP

1. TCP

1.1 Execute a aplicação socket TCP cliente/servidor em Java. Envie uma mensagem de um cliente para o servidor (em outra máquina do laboratório) e capture os pacotes com o Wireshark.

Qual é o endereço IP e porta TCP usado pelo cliente? E pelo servidor?
Execute novamente o cliente. Verifique a porta e IP do cliente.
Qual o número de sequência do segmento TCP SYN usado para iniciar a conexão TCP entre cliente e servidor? Qual é o número do segmento SYNACK enviado pelo servidor em resposta ao SYN enviado pelo cliente? Qual o valor campo de reconhecimento do cabeçalho TCP para o segmento SYNACK? Como o servidor determinou este valor?
Identifique e explique os demais campos do cabeçalho TCP identificados na troca de mensagens cliente/servidor (janela de recepção, flags, etc).
É possível achar no campo de dados as mensagens enviadas pelo cliente e servidor?

1.2 Acesse uma página web.
Identifique e explique o processo de estabelecimento de conexão. É similar ao programa Java executado?
Identifique os segmentos TCP trocados entre o cliente (navegador) e o servidor (site web).
Identifique o RTT (*round trip time*) – tempo de ida e volta dos 6 primeiros segmentos. Calcule o RTT estimado para 2 segmentos através da seguinte equação:
RTT Estimado = 0,875. RTT Estimado + 0,125.RTT
(Para o primeiro segmento considere que o RTT estimado é igual ao RTT medido pelo Wireshark.)

2. IP – Internet Protocol

2.1 Comando ping

O comando ping testa a conectividade entre a máquina local e uma máquina remota. Adicionalmente, ele mostra informações de tempo de atraso e de perda de pacotes entre essas duas máquinas. É implementado através de mensagens ICMP. A máquina de origem envia uma mensagem “ICMP Echo Request” e a máquina de destino responde com “ICMP Echo Reply”.

Execute o comando “ping www.terra.com.br”. Repare nas mensagens que ele mostra na tela.
Execute o comando “ping X.X.X.X” (escolha um endereço IP). Veja que é possível executar o comando para um endereço IP diretamente.
Execute o comando “ping www.receita.fazenda.gov.br”. Houve resposta? Qual pode ser o problema?
Configure o Wireshark para fazer nova captura.

Execute o comando “ping www.terra.com.br” novamente. Pare a captura e observe os pacotes capturados. Identifique os pacotes ICMP com as mensagens “echo request” e “echo reply”. Quais informações são possíveis de verificar nos pacotes?
Execute o comando ping para vários endereços:
· Para a sua máquina
· ping 127.0.0.1
· ping www.ufabc.edu.br
· ping www.unicamp.br
· ping www.google.com
· etc.
Explique o tempo de resposta obtido para os diversos endereços.

2.2 Comando traceroute

O comando traceroute consegue traçar uma rota de origem a destino. Ele envia repetidamente mensagens com o campo TTL (do cabeçalho IP, veja no Wireshark) igual a 1, depois 2, 3, 4, ... Todo roteador decrementa o campo TTL quando encaminha um pacote. Quando o valor do TTL chega a zero, ele envia uma mensagem ICMP “TTL Expired” para a máquina de origem.

Execute o comando traceroute na linha de comando para alguns destinos escolhidos.
- traceroute www.terra.com.br
- traceroute www.ufabc.edu.br
- traceroute www.globo.com , etc.
O que é possível observar?
Agora execute o traceroute capturando os pacotes com o Wireshark. Filtre os pacotes ICMP e verifique a sequência de pacotes enviada. Como funciona o traceroute?

3. ARP

Quando uma máquina deseja saber um endereço MAC, ela envia um pacote contendo o endereço IP para um endereço MAC de difusão (broadcast = FFFFFFFF), que é recebida por todas as outras na rede local. A máquina cujo endereço IP está sendo requisitado responde com o seu endereço MAC.
Assim como o DNS, o ARP armazena temporariamente as respostas, para não ter que fazer essa tradução para todos os pacotes enviados, o que seria ineficiente. No entanto, o tempo de duração deste cache é curto, para que possíveis alterações (de placas) na rede não causem problemas.

1. Use o comando “arp -a” (na linha de comando) para trabalhar com o cache ARP. Verifique quais são os endereços que estão no cache.
2. Inicie uma captura no Wireshark e execute ping para um computador da rede local ainda não acessado e depois verifique novamente a tabela ARP (ex.: ping 192.168.253.1). Verifique os pacotes ARP capturados. Veja os campos de cabeçalho, observando a requisição e a resposta. Verifique quais são os endereços MAC.
3. Repita os mesmos procedimentos. Foram capturados pacotes agora? Por quê?
4. Remove entradas da tabela ARP com o comando “arp –d IP”. Execute esse comando. Agora os pacotes ARP foram capturados? Por quê?
5. Execute o comando “arp” sem complementos para ver quais opções ele suporta.

4. Comando route

O comando route permite visualizar e configurar a tabela de roteamento.

1. Use o comando ”route” para observar a tabela de roteamento do seu computador. Verifique que existem rotas para a rede local, além de várias outras rotas.
2. Anote o endereço do roteador padrão da sua rede (default gateway).
3. Exclua a rota padrão (default) da tabela de roteamento, com o comando “sudo route del default”. A rota padrão vem da configuração do roteador padrão (gateway default) da sua rede.
4. Tente acessar um servidor externo, como o UOL. Ocorreu algum problema? Por quê? Execute um ping para esse servidor, de preferência para o seu endereço IP. Qual foi a mensagem de erro?
5. Execute um ping para uma máquina da rede interna da UFABC (ou de outro local com NAT; ex.: ping 192.168.253.1). Esse comando foi executado. Por quê?
6. Adicione novamente a rota padrão, com o comando “sudo route add default gw X.X.X.X”. Repita o ping para o UOL.

5. DHCP

O protocolo DHCP (*Dynamic Host Configuration Protocol*), permite a configuração dinâmica de endereços IP (e outras configurações, como servidor DNS, roteador padrão, máscara de sub-rede, etc.).
1. Libere o endereço IP, executando o comando “sudo ifconfig eth0 down”. Execute “ifconfig” para verificar o seu endereço IP. O que aconteceu? O seu computador ainda tem endereço IP? Tente acessar qualquer coisa da rede (o UOL, por exemplo).
2. Obtenha novas configurações de rede (incluindo o endereço IP) executando o comando “sudo dhclient eth0”. Execute novamente o comando “ifconfig” e tente acessar a rede.

6. Comando neststat

O comando netstat mostra estatísticas de protocolos e o estado atual das conexões TCP.

1. Use o comando ”netstat” para observar as conexões TCP abertas no seu computador. O que é possível observar?

2. Outras opções:
· netstat –e: mostra estatísticas de Ethernet
· netstat –s: mostra estatística de IP, ICMP, TCP e UDP
O que é possível observar?