Laboratório 04 – Protocolos da Camada de Rede
17/Outubro/2011

Objetivo:

Este laboratório tem o objetivo de explorar as informações contidas no cabeçalho do protocolo IP, o protocolo ICMP e o protocolo ARP.

1. O Protocolo ICMP e os comandos traceroute e ping

Os comandos **traceroute** e **ping** são comandos muito utilizados por administradores de redes para verificar a conectividade da rede. Ambos confiam em respostas ICMP emitidas por hosts e roteadores conectados na internet, embora nem todos equipamentos estejam habilitados a responder tais pacotes.

A – Captura de Pacotes.

- Inicie a captura de pacotes no Wireshark
- Execute o comando traceroute: **traceroute www.uol.com.br**
- Execute o comando ping: **ping www.google.com -c 3**
- Lembre de utilizar servidores de destinos diferentes para separar facilmente os pacotes resultantes no Wireshark
- Pare a captura de pacotes no Wireshark

B – Análise de Pacotes

a) Interprete a saída exibida no terminal para cada um dos comandos.

b) Identifique os pacotes resultantes do comando traceroute e ping.

c) Para esses pacotes, descreva o padrão observado nos valores do campo *Identification* do cabeçalho dos datagramas IP.

d) Para os pacotes ICMP, identifique os números correspondentes a tipo e código ICMP?

e) No cabeçalho IP, verifique quais os protocolos utilizados nas camadas superiores para cada comando.

f) Descreva como cada um dos comandos funcionam em termos dos pacotes enviados e recebidos. Lembre-se que o comando traceroute faz uso do campo TTL.

g) É possível implementar esses comandos utilizando as APIs vistas no curso? Se não, o que uma API deve prover para que tal implementação seja possível?

2. Fragmentação de Pacotes IPs

O valor do MTU designa a quantidade máxima de bytes que podem ser transportados por um dagrama IP e normalmente é determinado pela tecnologia na camada de enlace. O MTU engloba tanto a carga útil de um datagrama IP, quanto seu cabeçalho. O valor do MTU pode ser verificado utilizando o comando: **ifconfig**. Nesta parte será utilizado o comando ping novamente para forçar a fragmentação de pacotes.

A – Captura de Pacotes.

- Inicie a captura de pacotes no Wireshark
- Execute o comando ping: **ping www.google.com -c 3 -s 5000**
- Pare a captura de pacotes no Wireshark

B – Análise de Pacotes

a) Você compreende os parâmetros utilizados no comando ping acima?

b) Quais campos podem ser verificados no cabeçalho IP para identificar datagramas que são fragmentos de pacotes maiores? Quais valores nesses campos indicam fragmentação?

c) Como obter o Payload (carga útil) em cada datagrama?

d) Qual a carga útil de cada fragmento? Verifique fragmentos pertencentes a um mesmo pacote, a carga útil total resulta em 5000 bytes? Explique.

3. Juntando os protocolos DNS, ARP e Http

Em sala de aula foi visto um exercício (Exercício 2 postado no COL no módulo da Camada de Redes) que aborda mensagens trocadas entre hosts utilizando os protocolos DNS, ARP e Http. Neste momento do curso é possível compreender a interação existente entre os equipamentos existente em uma rede de computadores.

A – Captura de Pacotes.

- Para evitar a captura de pacotes indesejáveis, feche todas janelas de browsers em sua máquina
- Inicie a captura de pacotes no Wireshark
- Verifique a tabela ARP de seu computador executando o comando: **arp**
- Apague cada entrada nesta tabela utilizando o comando: **sudo arp -d** *hostname*
- Requisite um arquivo utilizando http com o comando: **wget www.uol.com.br**
- Pare a captura de pacotes no Wireshark

B – Análise de Pacotes

a) A configuração existente no laboratório é parecida com a existente no Exercício 2. Identifique os IPs utilizados no laboratório.

b) Ordene os pacotes por endereço de origem e identifique os pacotes enviados por sua máquina. Quais são os endereços MAC de destinos para esses pacotes?

c) Identifique os pacotes ARPs gerados. Caso nenhum tenha sido gerado, é possível gerá-los enviando um ping ao hospedeiro do seu vizinho.

d) Quais são os endereços MAC e IP de origem e destino de tais pacotes?

e) Em qual camada os pacotes ARP são gerados? Como pacotes gerados nesta camada são diferenciados pela camada abaixo?

f) Quais são os tipos de mensagens ARP utilizados?