

# UFPE – Centro de Informática

## Infraestrutura de Comunicação

### Prova Teórica 5

2020-3

Nome do(a) aluno(a): Gabriel Nogueira Leite

Número de Matrícula/CPF: 398.068.608-61

#### 1ª Questão (3,5 Pontos)

Considere a rede institucional da Figura abaixo. Cada hub possui 30 PCs conectados. Um hacker instalou o Wireshark em um dos PCs e vem descobrindo, através da captura de pacotes DNS, quais sites são acessados pelos usuários da rede.

- a) (1,5) Explique tecnicamente porque o hacker consegue capturar pacotes de **requisições e respostas DNS** com base no funcionamento dos equipamentos de rede utilizados.

**Resposta:** O hacker consegue capturar os dados pois o hub transmite os dados para todos os PCs conectados de forma igual, com isso o hacker tendo instalado o Wireshark em qualquer uma dessas máquinas, poderá ter acesso aos pacotes, incluindo requisições e resposta DNS.

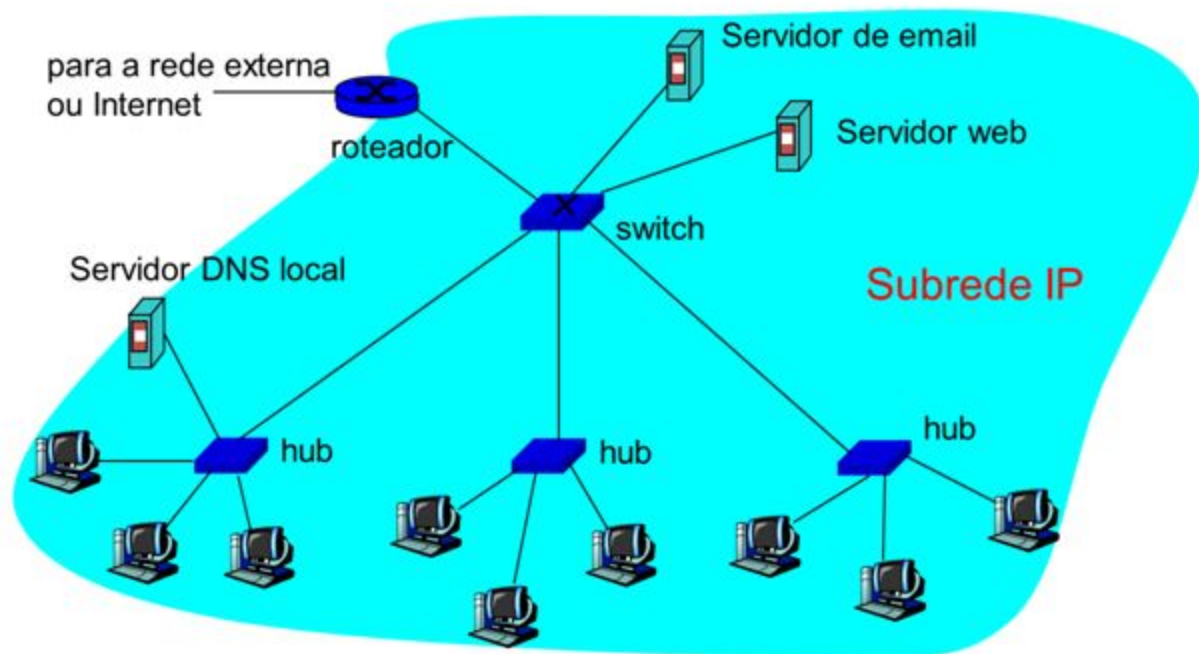
- b) (0,5) Reprojete a rede de tal forma a evitar que os PCs possam ser usados para isso. Considere que sua solução deverá ser a mais barata para a instituição em termos de equipamentos e mão de obra. Considere o seguinte em relação a equipamentos e mão de obra: hub (custo baixo), switch (custo médio), roteador (custo alto). Para mostrar como reprojeteu, explicitamente as mudanças ou faça um novo desenho da rede.

**Resposta:** Para reprojeter a rede de forma que tenha baixo custo, poderíamos trocar de lugar um dos hubs pelo switch presente na rede e substituir os outros dois hubs por novos switches, dessa forma teríamos dois equipamentos novos de custo médio.

- c) (1,0) Explique com base na teoria de funcionamento dos equipamentos usados porque sua solução resolve o problema.

**Resposta:** Dessa nova forma com switches nos locais onde antes haviam hubs o hacker não irá conseguir capturar todos os pacotes enviados na rede, pois o switch não realiza broadcast como o hub, direcionando os pacotes diretamente para o host certo. Assim utilizando o wireshark o hacker não terá acesso aos pacotes.

- d) (0,5) Explique porque sua solução é a mais em conta para a instituição. Considere o seguinte em relação a equipamentos e mão de obra: hub (custo baixo), switch (custo médio), roteador (custo alto).



**Resposta:** A solução adotada seria adquirir mais dois switches novos (custo médio) e trocar o switch antigo por um dos hubs. Dessa forma seriam adquiridos dois equipamentos de custo médio e a configuração não seria complexa, visto que configurar um switch não é tarefa complexa como configurar um roteador.

## 2ª Questão (1,5 Pontos)

Analise as seguintes afirmativas:

- I) Um *switch* Ethernet constrói sua tabela de encaminhamento com base no endereço MAC de destino dos quadros recebidos.
- II) O CSMA/CD é um protocolo que pode ser utilizado eficientemente em redes sem fio.
- III) Para um grande número de nós transmitindo, a eficiência máxima do Aloha Puro é duas vezes menor do que aquela obtida pelo Slotted Aloha.

Explique se elas são verdadeiras ou falsas, justificando sua resposta.

I) **Falso.** O switch Ethernet constrói sua tabela de encaminhamento com base no endereço MAC de origem.

II) **Falso.** Em redes sem fio podem haver situações onde a detecção de erros do CSMA/CD não funcionará.

III) **Verdadeiro.** No Slotted Aloha temos que,  $N$  como sendo número de nós, uma probabilidade  $p$  e  $p^*$  que maximiza a probabilidade de que qualquer nó tenha sucesso  $Np(1-p)^{N-1}$ , quando há muitos nós, o limite de  $Np^*(1-p^*)^{N-1}$  quando  $N$  vai a infinito, indica a eficiência máxima de  $1/e = .37$ . Já o Aloha Puro é mais simples e sem sincronização, temos que sua eficiência é dada por:  $P(\text{sucesso de um dado nó}) = p * (1-p)^{2(N-1)}$ . Escolhendo  $p$  ótimo e fazendo  $N \rightarrow \text{infinito}$ , temos que  $P(\text{sucesso de um dado nó}) = 1/(2e) = .18$ . Ou seja, duas vezes menor do que aquela obtida pelo Slotted Aloha.

### 3ª Questão (1,5 Pontos)

Analise a afirmativa abaixo:

Em uma rede Ethernet nem sempre há a necessidade de se utilizar qualquer tipo de endereçamento MAC para a comunicação entre dois *hosts* adjacentes em uma mesma sub rede e com endereços IP.

A afirmativa é **verdadeira** ou **falsa**? Explique o porquê.

**Resposta: Falso.** Sabemos que uma rede Ethernet é uma rede de multi acesso, numa rede de multi acesso cada nó da rede pode acessar quaisquer outros nós da rede. A estrutura de um quadro Ethernet deve possuir o endereço MAC do nó de destino, do contrário não será entregue ao destinatário. Com isso mostramos a necessidade de se utilizar o endereçamento MAC.

#### 4ª Questão (3,5 pontos)

Suponha uma rede do tipo Ethernet em que um computador A queira se comunicar com um computador B que está na mesma subrede. Suponha que A saiba o endereço MAC de B, mas não o IP dele. Tendo como inspiração o funcionamento do protocolo ARP, elabore um protocolo da camada enlace capaz de descobrir o endereço IP de B. Explique o passo-a-passo de como o IP é descoberto, mostrando os endereços MAC utilizados nas mensagens do protocolo proposto. Assuma que todo computador conheça o seu próprio IP, estando esta informação disponível também para a camada enlace.

**Resposta:** Em nosso novo protocolo teremos em cada nó da sub rede uma tabela que irá relacionar os endereços MAC e IP, essa tabela terá um tempo máximo onde cada registro poderá ficar armazenada, chamaremos esse tempo de PMA (Período Máximo de Armazenamento), o tempo será de 2 minutos.

Para que um hospedeiro A se comunique com um hospedeiro B, primeiramente ele irá olhar na tabela no nosso protocolo presente em sua memória, em caso de não encontrar ele irá seguir o comportamento do protocolo ARP e criar um pacote que será encaminhado como broadcast para a sub rede. Esse pacote irá conter os endereços MAC e IP de origem e MAC de destino, representado na tabela abaixo.

MAC Origem	IP Origem	MAC Destino
5c:c9:d3:1e:f9:f4	138.285.451.39	6c:d9:f3:1e:b9:d2

No momento em que os pacotes chegarem aos computadores será feita a verificação dos campos para identificar se o pacote é destinado aquele host ou não, pois caso não seja o pacote será descartado. Sendo esse pacote identificado para o host, ele irá enviar uma resposta diretamente, contendo seu endereço de IP e atualizando a tabela do nosso protocolo, com os valores do remetente A, no caso de possíveis futuras comunicações.

O último passo é a chegada da resposta ao host A (origem), nessa etapa será realizada a atualização da tabela de nosso protocolo e o envio do IP destinatário e MAC destinatário.

Abaixo temos a representação da tabela do nosso protocolo:

PMA	Endereço IP	Endereço MAC
01:25	148.285.451.38	6c:d5:f3:1e:b9:d3
00:30	148.285.451.39	1c:d9:f3:1e:b9:d1

**Boa Sorte!**