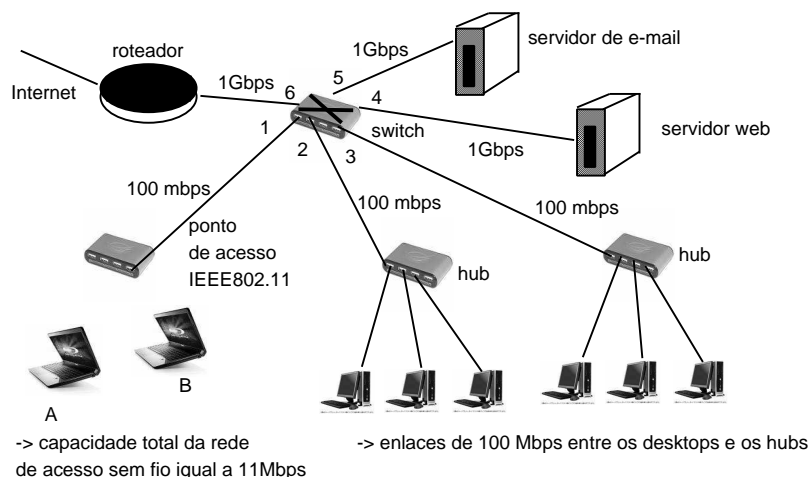


Fundação CECIERJ - Vice Presidência de Educação Superior a Distância
Curso de Tecnologia em Sistemas de Computação
Disciplina: Redes de Computadores II
Gabarito da AP2 - 2º semestre de 2009

1ª questão (4.0 pontos)

Considere a figura abaixo como sendo a rede de uma instituição. Suponha que exista um ponto de acesso sem fio IEEE802.11 para conexão de laptops. A rede sem fio possui capacidade máxima de 11Mbps (a ser compartilhada entre os terminais sem fio) conforme mostrado na figura.



1. (0.5) Qual a vazão (bits por segundo) máxima agregada que pode ser alcançada entre o conjunto composto por todos os computadores/laptops que estão conectados aos hubs/ponto de acesso sem fio e a internet ?

Resposta:

A vazão máxima agregada é de 211 Mbps.

2. (0.5) Qual a vazão (bits por segundo) que um terminal sem fio pode alcançar caso somente ele esteja conectado a rede sem fio ?

Resposta:

A vazão máxima que ele pode alcançar é de 11 Mbps.

3. (0.5) O que você faria para aumentar a vazão da rede da instituição ?

Resposta:

Substituiria os dois hubs que ligam os computadores por switches com portas de 100 Mbps.

4. (0.5) Explique o que é o problema do terminal escondido em uma rede sem fio.

Resposta:

Este problema é quando um terminal não recebe o sinal do outro pois existe algum objeto (montanha, parede, etc) entre eles que não permite que o sinal enviado por um seja recebido pelo outro.

5. O padrão IEEE802.11 tem dois modos de operação: com e sem reserva. Suponha que os quadros de reserva sejam iguais a 100Kbytes e que a sua aplicação gere pacotes com tamanho igual a 500Kbytes. Suponha os dois cenários abaixo.

- (a) (0.8) Transmissão do quadro com sucesso. Qual o overhead do protocolo nos dois casos: operação com reserva e sem reserva ? Considere a seguinte definição de overhead: *quantidade de dados transmitidos que não serão úteis para o usuário (ex: mensagens de controle) dividido pelo total dos dados transmitidos.*

Resposta:

Caso de operação com reserva: O protocolo envia duas mensagens de reserva (RTS e CTS), cada uma de 100Kbytes. Logo o overhead é igual $200/700 = 0.28$

Caso de operação sem reserva: Não existem mensagens de controle, portanto o overhead é zero.

- (b) (0.5) Transmissão do quadro sem sucesso (colisão). Neste cenário, qual o modo de operação seria mais eficiente: com ou sem reserva ? Explique porquê.

Resposta:

No caso de colisão, dado que o quadro de reserva é bem menor que o quadro de dados, a operação com reserva é mais eficiente pois o meio de transmissão ficará ocupado transmitindo informação inútil durante um tempo menor (tempo de transmissão do quadro de reserva de 100 Kbytes). Na operação sem reserva o meio ficará ocupado durante um tempo maior (tempo de transmissão de um quadro de 500 Kbytes).

6. (0.7) Suponha que o computador A queira enviar uma mensagem ao computador B mas não possua o endereço MAC de B. Que protocolo deve ser usado para que A obtenha o endereço MAC de B e que mensagens devem ser trocadas entre A e B até que A obtenha o MAC de B ?

Resposta:

Passo 1: A envia pacote ARP query em broadcast contendo endereço IP de B pois descobre através da sua tabela de roteamento IP que B está na mesma rede local que ele.

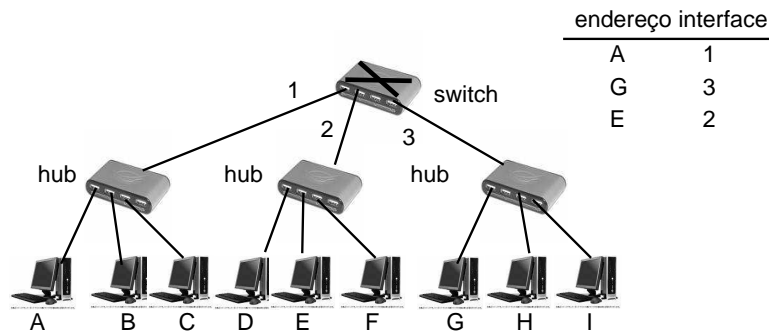
Passo 2: B recebe o pacote ARP query e envia o seu endereço MAC em um pacote unicast, cujo endereço destino é o MAC de A.

Passo 3: A recebe o pacote de B e atualiza a sua tabela ARP criando uma entrada com o endereço IP de B e o respectivo MAC. A envia quadro cujo endereço MAC de destino é o MAC de B.

2ª questão (2.0 pontos)

Interconexão de redes

Considere na rede abaixo que o *host B* envia uma mensagem para o *host F* e, em seguida, *F* responde à mensagem de *B*. Os *hosts B* e *F* estão interconectados através de um switch que possui a tabela de encaminhamento mostrada na figura abaixo.



1. (0.5) Por qual(is) interface(s) de saída do switch a mensagem do *host F* destinada ao *host B* será encaminhada ? (Explique porquê.)

Resposta: Será encaminhada pela interface 1, pois o switch, após o envio da mensagem de B para F, criará uma entrada na tabela para o host B. Esta entrada foi inserida na tabela quando o host B enviou uma mensagem para F.

2. (0.5) Construa a tabela de roteamento do switch após a troca de mensagens entre *B* e *F*.

Resposta:

endereço	interface
A	1
G	3
E	2
B	1
F	2

3. (0.5) Se ao invés de um switch, o equipamento usado para interconexão fosse um hub, por qual(is) interface(s) a mensagem de *B* para *F* seria encaminhada ? (Explique porquê.)

Resposta:

Seria encaminhada pelas interfaces 2 e 3 pois o hub é um simples repetidor: encaminha a mensagem por todas as interfaces de saída, exceto aquela pela qual recebeu a mensagem.

4. (0.5) Cite duas características que diferenciam os switches de roteadores.

Resposta:

1 - Switches não implementam algoritmo para cálculo do melhor caminho de uma origem até um certo destino na rede. As tabelas de encaminhamento são geradas através de um algoritmo de aprendizado.

2 - Switches não necessitam de intervenção de um administrador para entrarem em operação, são *plug and play*, diferentemente dos roteadores que necessitam ser configurados por um administrador.

3ª questão (2.0 pontos)

Aplicações multimídia. Responda às perguntas abaixo.

1. (0.5 ponto) Quais são as características do tipo de serviço de transporte oferecido pela Internet de hoje aos aplicativos? Cite uma garantia oferecida por este serviço.

Resposta:

O serviço de transporte oferecido pela Internet de hoje é caracterizado pelo *best-effort*. Este serviço não oferece garantias temporais, como atraso máximo ou mínimo, vazão mínima ou máxima em uma conexão, ou garantias com relação a variação de retardos. Entretanto, o serviço de transporte TCP oferece garantia de entrega dos dados, ou seja, confiabilidade (todos os pacotes enviados pelo transmissor serão entregues ao receptor).

2. (0.5 ponto) Sabemos que *jitter* é a variação do retardo fim-a-fim entre os diferentes pacotes de um mesmo fluxo. Explique porque o retardo na Internet é variável.

Resposta:

Uma parcela do retardo que os pacotes sofrem ao atravessarem uma rede está nas filas encontradas nos roteadores. Ao chegar em um roteador um pacote deve aguardar na fila até que seja transmitido. Como o tamanho das filas nos roteadores varia com o tempo, o tempo que um pacote espera na fila também varia com o tempo. Desta forma, o retardo fim-a-fim entre pacotes de um mesmo fluxo pode variar (e em geral varia) no tempo.

3. (0.5 ponto) Qual problema mecanismos de redundância, como o FEC, utilizado por aplicativos multimídia na Internet se propõe a resolver?

Resposta:

O problema de perda de pacotes. Como a rede pode descartar pacotes (por falta de espaço nas filas dos roteadores), pacotes transmitidos não necessariamente chegam ao seu destino. Mecanismos de redundância ajudam a resolver este problema, enviado mais dados do que o necessário para permitir a recuperação de pacotes perdidos no destino.

4. (0.5 pontos) Explique as desvantagens do mecanismo de redundância, como o FEC, utilizado por aplicativos multimídia na Internet.

Resposta:

A desvantagem é transmitir dados que não serão utilizados. Ou seja, quando não há perda de pacotes, a redundância não é utilizada, entretanto, a informação redundante que foi transmitida consumiu desnecessariamente recursos da rede (banda, espaço em fila, por exemplo).

4ª questão (2.0 pontos)

Segurança em redes. Responda às perguntas abaixo.

1. (0.5 pontos) Considere um *firewall* que permite que os computadores que estejam dentro da rede protegida enviem email. Ou seja, o firewall possui uma regra que encaminha corretamente pacotes do protocolo TCP com porta 25 provenientes de computadores da rede protegida. Considere agora um outro aplicativo qualquer (ex. Kazaa) que utiliza o mesmo protocolo e porta se comunicar. Os pacotes gerados por tal aplicativo serão descartados pelo firewall? Explique sua resposta.

Resposta:

Não, o firewall não irá descartar tais pacotes do outro aplicativo baseando-se apenas nesta regra. O firewall é um filtro de pacotes baseado em regras, que são geralmente definidas sobre os cabeçalhos dos pacotes. Se uma regra estabelece que pacotes TCP da porta 25 são permitidos, então qualquer pacote que satisfaça a esta condição será permitido, independente do aplicativo que gerou o pacote.

2. (0.5 pontos) Explique o que é *IP Spoofing*. Explique por que *IP Spoofing* pode levar a um problema de segurança.

Resposta:

A técnica de *IP Spoofing* consiste em falsificar o endereço IP de origem de um pacote. Ou seja, construir e transmitir um pacote com endereço IP de origem diferente do endereço IP da máquina que irá transmitir o pacote. Este ataque leva a problemas de segurança pois o receptor do pacote não sabe qual IP realmente transmitiu o pacote. Desta forma, o receptor pode erroneamente responder para algum endereço IP que nem sequer sabe do pacote anterior.

3. (1.0 ponto) Suponha que Ana quer enviar uma mensagem M à Bruno. Ela deseja que somente Bruno tenha acesso ao conteúdo da mensagem e que ele também tenha certeza de que foi ela quem redigiu a mensagem. Utilizando criptografia com chaves públicas/privadas e assumindo que ambos possuem a chave pública do outro, (i) descreva os passos que Ana deve realizar para enviar tal mensagem; (ii) descreva o que Bruno precisa realizar para ler a mensagem recebida.

Resposta:

Passos que Ana precisa realizar:

- Ana deve utilizar a chave pública de Bruno para cifrar a mensagem M , gerando $K_B^+(M)$. Isto garante que apenas Bruno, através de sua chave privada, poderá ler a mensagem.
- Ana deve utilizar sua chave privada para cifrar a mensagem M , gerando $K_A^-(M)$. O resultado é a assinatura de Ana, o que irá permitir a Bruno verificar que Ana redigiu a mensagem.
- Ana deve utilizar a chave pública de Bruno para cifrar sua assinatura, gerando $K_B^+(K_A^-(M))$. Isto é necessário, pois caso contrário um intruso poderia utilizar a chave pública de Ana para ler a assinatura!
- Ana deve enviar a Bruno a mensagem e a assinatura cifrada.

Passos que Bruno precisa realizar:

- Bruno decifra $K_B^+(M)$ utilizando sua chave privada e recupera a mensagem M .
- Bruno decifra $K_B^+(K_A^-(M))$ utilizando sua chave privada e recupera a assinatura de Ana, ou seja, $K_A^-(M)$.
- Utilizando a chave pública de Ana, Bruno decifra a assinatura $K_A^-(M)$ e compara o resultado com a mensagem M , decifrada no primeiro passo. Se as duas mensagens são iguais, então Ana redigiu M .