Curso de Tecnologia em Sistemas de Computação
Disciplina: Redes de Computadores II
AP2 – 2º semestre de 2014 – GABARITO

Questão 1 ..... 20 pontos

Na tabela abaixo, são apresentados, nas colunas, diversos protocolos de acesso a um meio de transmissão compartilhado, e nas linhas, diversas características destes protocolos. Preencha cada célula da tabela indicando se o protocolo possui ou não a característica apresentada. Considere que, exceto em afirmação contrária, a quantidade de estações que possuem acesso ao meio em questão é constante (isto é, estações não entram e saem da rede), mas que nem todas as estações desejam transmitir a todo instante.

	S-ALOHA	CSMA/CD	ALOHA	TDMA
requer sincronização dos relógios das estações	✓	×	×	✓
não permite que uma estação detecte uma colisão e interrompa sua transmissão	✓	×	✓	✓
protocolo de acesso aleatório	✓	✓	✓	×
se o meio estiver livre, toda estação que quiser iniciar uma nova transmissão pode acessá-lo	×	✓	✓	×
permite acesso simultâneo ao meio (com ou sem colisão)	✓	✓	✓	×

Questão 2 ..... 20 pontos

Responda às seguintes perguntas sobre redes sem fio:

(a) Qual é a diferença fundamental entre o modo estruturado e o modo *ad hoc* de operação?

Resposta:

No modo estruturado, a rede possui uma infraestrutura central (tipicamente uma ou mais estações base ou pontos de acesso), que estrutura a comunicação e provê acesso a outras redes. Já em uma rede em modo *ad hoc*, esta infraestrutura não existe, de modo que a rede está sistematicamente desconectada de outras redes e as estações devem se organizar de forma independente.

(b) De que maneira o uso de mensagens de controle RTS/CTS (*request to send*/*clear to send*) resolve o problema do terminal escondido em uma transmissão?

Resposta:

A troca de mensagens RTS/CTS antes de uma transmissão serve para a parte receptora informar a todas as estações que estão ao seu alcance o emissor de quem ela aceita receber quadros naquele momento. Se uma terceira estação neste raio de alcance também quiser transmitir para o receptor, isto geraria uma colisão, que não seria detectada se ambos os transmissores estiver ocultos um para o outro. No entanto, como somente uma delas pode estar habilitada para transmitir para o receptor (pois somente uma receberá esta permissão na troca de mensagens RTS/CTS), esta transmissão simultânea não irá ocorrer.

(c) O que é o mecanismo de handoff? Quando este mecanismo ocorre?

Resposta:

O mecanismo de handoff é o processo de transição de uma estação entre pontos de acesso vizinhos, sem perda de conectividade. Este mecanismo ocorre sempre que a estação, em uma região com vários pontos de acesso disponíveis, detectar uma baixa qualidade na comunicação com o seu ponto de acesso atual e perceber que pode melhorar esta qualidade mudando de ponto de acesso.

(d) Os mecanismos de handoff e RTS/CTS podem ser aplicados tanto no modo estruturado quanto no modo ad hoc? Justifique sua resposta.

Resposta:

O mecanismo de handoff só faz sentido se existirem estações base ou pontos de acesso para que a estação faça a transição, logo ele só pode ser aplicado em redes em modo estruturado. Já o mecanismo RTS/CTS, embora mais utilizado em redes estruturadas, pode ser utilizado em redes de ambos os modos, pois qualquer estação é capaz de enviar as mensagens de controle RTS e CTS.

Questão 3 ..... 25 pontos

Um dos protocolos mais utilizados na Internet para prover segurança na comunicação entre duas entidades é o *Transport Layer Security*, ou TLS. Este protocolo pode ser utilizado em conjunto com qualquer protocolo de comunicação da camada de aplicação. Uma versão simplificada do TLS é descrita no passo-a-passo a seguir, para uma comunicação entre um cliente e um servidor:

1. O cliente inicia o protocolo solicitando ao servidor o início de uma comunicação segura;
2. O servidor envia ao cliente seu certificado digital (que inclui a chave pública do servidor, que chamaremos de K_A^+) e um *nonce* n_1;
3. O cliente valida o certificado digital do servidor em uma entidade certificadora (se a validação falhar, o cliente encerra a comunicação);
4. O cliente gera um segundo *nonce* n_2, cifra-o com a chave K_A^+, e o envia de volta ao servidor;
5. Utilizando ambos os *nonce*'s (e apenas eles), o cliente e o servidor geram uma chave simétrica, que chamaremos de K_S. O mesmo algoritmo é utilizado pelo cliente e pelo servidor para gerar a chave, e é definido na especificação do protocolo TLS;

Este passo-a-passo descreve o *handshake TLS*. Após o handshake, o cliente e o servidor passam a realizar a comunicação original que desejavam, mas sempre cifrando as mensagens com a chave simétrica K_S antes de enviá-las e decifrando-as com a mesma chave ao recebê-las.

Determine se cada uma das afirmações a seguir é verdadeira ou falsa e justifique usando *apenas uma frase*. Para cada uma delas, salvo em afirmação contrária, suponha que as chaves privadas envolvidas não são conhecidas, nem o servidor nem o cliente geram *nonce*'s duplicados, e a entidade certificadora envolvida é confiável.

◯ Este protocolo garante ao servidor a autenticidade do cliente.
O cliente não envia nenhuma informação que só ele próprio poderia saber, logo é possível que um atacante finja ser o cliente e se comunique com o servidor sem ser detectado.

√ **Um atacante que tenha acesso a todas as mensagens trocadas no handshake é incapaz de obter o valor de n_2.**
Como somente $K_A^+(n_2)$ circula na rede, o atacante deveria conhecer a chave privada do servidor (K_A^-) para obter n_2.

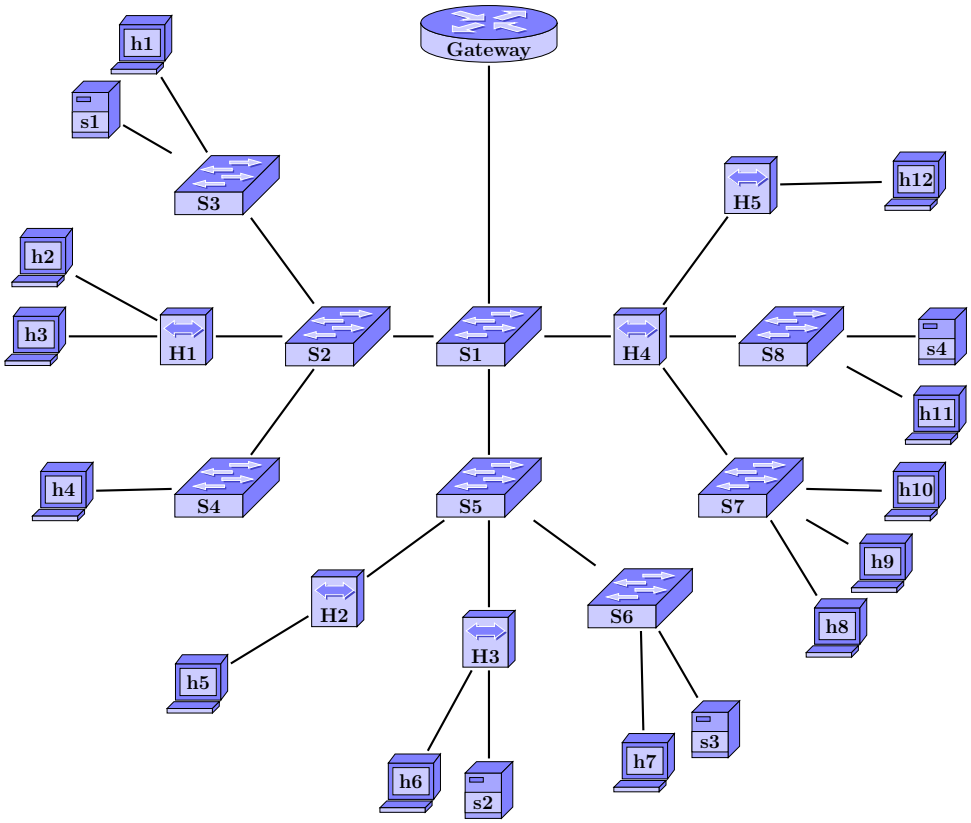
◯ Um atacante que possa modificar as mensagens é capaz de realizar um ataque do homem-no-meio sobre o handshake.
Neste ataque, o intruso deverá substituir a chave pública do servidor (K_A^+) pela sua própria chave pública, o que será detectado pelo cliente, pois a entidade certificadora irá rejeitar sua tentativa de validação do certificado.

◯ Um atacante que tenha acesso a todas as mensagens trocadas no handshake e obtenha o valor de n_2 é incapaz de decriptar todas as mensagens enviadas após o handshake.
De posse de n_1 (que foi enviado abertamente na rede) e n_2, o atacante é capaz de gerar K_S utilizando o mesmo algoritmo executado pelo cliente e pelo servidor (que é publicamente conhecido).

√ **Este protocolo garante a confidencialidade da comunicação após o handshake.**
Somente o cliente e o servidor conhecem a chave K_S, e é impossível ter acesso aos dados cifrados sem conhecer esta chave.

Questão 4 ..... 15 pontos

Considere a seguinte rede local, formada por estações (indicadas pela letra h), servidores (s), hubs (H) e switches (S), cuja saída para a Internet se dá através de um único gateway.



(a) Suponha que ocorre a transmissão de um fluxo de quadros de s4 para h1. Por quais equipamentos (estações, servidores, hubs e switches) esse fluxo irá transitar?

Resposta:

A transmissão será vista por h1, h12, H4, H5, s4, S1, S2, S3, S7 e S8.

(b) Considere que todos os servidores e estações possuem dados a transmitir para a Internet. Qual o número máximo destes equipamentos que podem realizar essa transmissão simultaneamente, sem que ocorram colisões? Descreva um cenário em que este máximo é atingido.

Resposta:

Pode haver no máximo 11 transmissões simultâneas para a Internet, sem que haja colisão. Este máximo é atingido, por exemplo, com transmissões de h1, h2, h4, h5, h6, h7, h8, h9, h10, s1 e s3.

Questão 5 ..... 20 pontos

Considere um servidor realizando *streaming* de um vídeo para um cliente. Essa transmissão é composta de 22 pacotes numerados, enviados em slots de tempo pré-determinados (um pacote por slot).

Suponha também que, para cada grupo de 3 pacotes consecutivos, o servidor irá criar um pacote adicional FEC, contendo o XOR destes pacotes. Este pacote será incluído na transmissão, logo após o grupo correspondente, e sua transmissão irá ocupar um slot a mais. Caso o último grupo tenha menos que 3 pacotes, o último FEC será aplicado nos pacotes restantes.

(a) Qual é o objetivo da transmissão destes pacotes FEC?

Resposta:

O objetivo é permitir que pacotes que eventualmente sejam perdidos durante a transmissão possam ser recuperados sem que o cliente precise pedir que o servidor transmita-os novamente, pois este procedimento é muito demorado para reprodução de vídeo por *streaming*.

(b) Quantos pacotes (tanto vídeo como FEC) o servidor irá enviar ao cliente nesta transmissão?

Resposta:

Serão transmitidos 30 pacotes, sendo 22 pacotes de vídeo e 8 pacotes FEC.

(c) Suponha que, nos slots 1, 3, 11, 15, 16, 24 e 30, os pacotes enviados se percam durante a transmissão (nos slots restantes, o pacote chega com sucesso). Quais pacotes de vídeo o cliente não irá receber?

Resposta:

O cliente não irá receber os pacotes de vídeo 1, 3, 9 e 12.

(d) No cenário descrito do item anterior, quais pacotes de vídeo o cliente não irá reproduzir?

Resposta:

Utilizando os pacotes FEC e os outros pacotes recebidos, o cliente somente será capaz de recuperar o pacote 9. Logo, ele não irá reproduzir os pacotes de vídeo 1, 3 e 12.