Instruções:

A prova é, claro, com **consulta aberta** a qualquer material que vocês encontrarem (exceto a outras pessoas - dessa vez nem eu irei responder dúvidas durante a prova, **ficarei offline**). Mas percebam que em diversas questões eu destaquei o "**com suas palavras**". Isso significa que seu eu encontrar uma resposta que, mesmo correta, seja um copiar-colar de texto dos slides, do livro ou de algum site fácil de achar no Google, não considerarei a questão.

Apesar de ser à distância, a prova deve ser **individual**. Se, ao corrigir, eu encontrar semelhanças inexplicáveis entre duas ou mais provas, atribuirei zero a todas as provas envolvidas, então **por favor** tomem cuidado com isso.

Prestem atenção para fazer a versão correta (dependendo do seu NUSP e nome) das questões 3 e 4. Não aceitarei respostas que não sejam da versão correta.

Vocês deverão me entregar as respostas **digitadas** (eventuais desenhos ou diagramas que queiram fazer podem ser digitalizados e colados no documento, mas não deve ser necessário e o texto dissertativo deve ser digitado), em formato **PDF**, **no máximo até as 22h30** de hoje. A entrega deve ser feita pelo **escaninho do TIDIA**. **Se** o acesso ao TIDIA não estiver funcionando, podem enviar para jlbernardes@usp.br. Coloquem **Nome** e **NUSP** no documento com as respostas.

Não receberei entregas com atraso maior que, no máximo, 5 minutos! Sim, isso significa que se alguém me enviar uma prova linda às 22h36, ficará com zero. Por isso, para evitar frustração pra vocês e pra mim, recomendo que me entreguem antes (dá tempo, e lembrem que a nota da rec substitui a média do semestre).

Boa sorte! (E desculpem pelo tom autoritário do texto acima, mas regras são regras, ainda mais assim, à distância.)

Questões [e valor em colchetes]:

1. Com as suas palavras, liste e explique o que são todos os **tipos de atraso** que podem acontecer numa comunicação em rede, vistos durante o curso (dica: são mais de 4). Explique também se ele ocorre só no primeiro nó da rede, em todos os nós do caminho (host que envia, roteadores), ou em nenhum nó, tanto na **comutação por pacotes** como na **comutação por circuitos**. **[1.5]**

2. Imagine que um computador está se conectando pela primeira vez a uma rede através de uma interface Ethernet. Sem que o usuário saiba, entre ele e seu roteador gateway há um comutador que ainda não conhece o MAC nem do gateway nem do novo computador. Um servidor DHCP está em execução no gateway (o novo computador não tem dados sobre esse servidor, mas o servidor está configurado para responder a mensagens DHCP Discover), de forma que o usuário não precisa configurar sua conexão manualmente. Após conectar-se à rede, o usuário abre a página www.usp.br (que na verdade está no servidor web www5.usp.br e tem o IP 200.144.183.244).

a) Descreva, com suas palavras, passo a passo o que ocorre para que o computador se conecte à rede até poder enviar primeira pergunta para um servidor de nomes. Cite cada passo dos protocolos DHCP e ARP, o auto-aprendizado do comutador, diferencie endereços IP e MAC e de diga que mensagens são broadcast, quais são unicast (e para onde) e quais protocolos da camada de transporte (se forem usados), de rede e de enlace são usados pelas mensagens DHCP e ARP. **[1.0]**

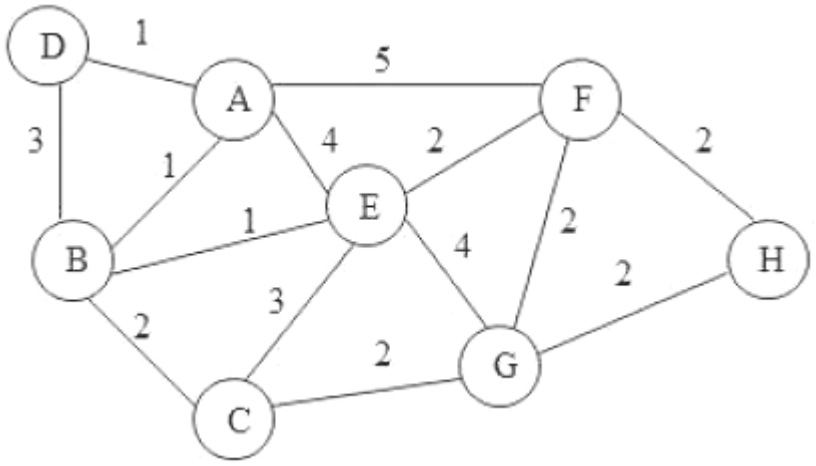
b) Imagine que seu servidor de nomes local tenha acabado de ter seu cache apagado, conhecendo somente o IP de um servidor de nomes raíz. Quais perguntas e respostas, e em que protocolo, seu computador troca com servidor de nomes local para obter o IP para poder abrir a página? Que perguntas e respostas seu servidor de nomes local troca com outros servidores de nomes? Não deixe de especificar nas respostas os tipos de Registro de Recurso (A, CNAME, NS ou MX) e os campos de resposta (Question, Answer, Authority e Additional). Se sua resposta incluir servidores cujos nomes e IP você não conhece, deixe essas informações indicadas e explicadas. **[1.0]**

c) Explique que mensagens são trocadas, e em que ordem, para abrir a conexão TCP, obter o primeiro objeto da página (seu arquivo html) e fechar essa conexão. **[0.5]**

3) Se o algarismo menos significativo do seu NUSP é par: Mostre um algoritmo (usando máquina de estados ou pseudo-código) para um remetente realizando entrega confiável sobre IP e utilizando **Go-Back-N** com uma janela de tamanho fixo de N pacotes, um único timer e **controle de fluxo**. **[2.5]**

Se o algarismo menos significativo do seu NUSP é impar: Mostre um algoritmo (usando máquina de estados ou pseudo-código) para um remetente realizando entrega confiável sobre IP e utilizando **Repetição Seletiva** com uma janela de tamanho fixo de N pacotes e **Retransmissão Rápida** (ou seja, ao receber o terceiro ACK com o mesmo número de sequência o remetente reenvia os pacotes necessários). **[2.5]**

4) Considere a rede mostrada na figura abaixo:



Se o seu primeiro nome começa com uma letra entre A e E (inclusive): Usando o algoritmo de Djikstra, mostre (usando a tabela vista em aula, em que cada linha representa uma interação do algoritmo) como encontrar a melhor rota do nó **B** para todos os outros. **[1.5]**

Se o seu primeiro nome começa com uma letra entre F e J (inclusive): Usando o algoritmo de Djikstra, mostre (usando a tabela vista em aula, em que cada linha representa uma interação do algoritmo) como encontrar a melhor rota do nó **E** para todos os outros. **[1.5]**

Se o seu primeiro nome começa com uma letra entre K e P (inclusive): Usando o algoritmo de Djikstra, mostre (usando a tabela vista em aula, em que cada linha representa uma interação do algoritmo) como encontrar a melhor rota do nó **F** para todos os outros. **[1.5]**

Se o seu primeiro nome começa com uma letra entre R e Z (inclusive): Usando o algoritmo de Djikstra, mostre (usando a tabela vista em aula, em que cada linha representa uma interação do algoritmo) como encontrar a melhor rota do nó **G** para todos os outros. **[1.5]**

5) Explique **com as suas palavras** e **em detalhe** como funciona o SSL, não esquecendo de falar de como é a negociação antes da comunicação começar, como são usados certificados, chaves simétricas e pública/privada (não esqueça do Master Secret e para que é usado) e que mecanismos usa para se defender de cada ataque (por exemplo ataques de repetição na mesma sessão ou em outra sessão, forçar a escolha de criptografia fraca etc.). **[2.0]**