

INATEL Instituto Nacional de Telecomunicações	Avaliação de TP-311 - Redes IP	
	Profº: Evandro Luís Brandão Gomes	03/07/2010

RESPOSTAS - Prova 2

Observações:

- Prova individual com duração de 90 minutos;
- Sem consulta
- Não é permitido o empréstimo de qualquer tipo de material;
- As listas de exercícios (A e B) devem ser entregues antes do início da prova.
- Valor da prova: 70 pontos. Valor das listas de exercícios: 30 pontos
- Boa prova!!

Questão 1 (15 pontos): As afirmativas descritas a seguir estão relacionadas aos protocolos do suíte TCP/IP. **Marque apenas as afirmativas corretas:**

	Para oferecer um serviço confiável de transporte de dados para as aplicações, é utilizado o protocolo TCP, que também provê um serviço não orientado a conexão. Os dados são transferidos por meio de unidades conhecidas como segmentos. O TCP espera que a recepção dos segmentos transmitidos seja confirmada pelo destino e retransmite segmentos cuja recepção não seja confirmada.
	O protocolo UDP é utilizado em aplicações cujo transporte de dados possa ocorrer sem conexão, mas de forma confiável devido a multiplexação das portas de serviço entre hosts cliente e servidor.
	O <i>Internet Protocol</i> (IP) provê serviço não-orientado a conexão, e não garante a entrega dos datagramas enviados. Outra importante responsabilidade do IP é rotear os datagramas por meio de redes interligadas. O roteamento é feito usando o endereço IP.
	Para reportar erros ou enviar mensagens de controles, alguns hosts da rede IP utilizam o protocolo ICMP para tal função. Estas mensagens ICMP são sempre encapsuladas em datagramas IP.
	A fragmentação ocorre toda vez que o datagrama IP for maior que 64Kbytes e a desfragmentação é feita somente no host de destino.
	O cabeçalho do protocolo IP v4 possui vários campos que não são utilizados em algumas situações, enquanto que no IP v6 este problema foi resolvido com um cabeçalho básico e conforme a necessidade pode-se anexar a este, vários outros cabeçalhos, tornando-se assim mais eficiente.
	Os cabeçalhos das versões 4 e 6 do protocolo IP são totalmente compatíveis, tornando fácil à migração entre eles.
	O protocolo TCP controla o fluxo da transmissão por meio de mecanismo de janela deslizante (Sliding Windows). Vários pacotes poderão ser enviados antes de a origem aguardar uma confirmação de recepção. Este mecanismo além de controlar o fluxo, otimiza o uso da largura de banda da rede.
	É função do protocolo TCP calcular dinamicamente o tempo que a origem de um pacote deve aguardar até retransmitir a informação caso a recepção não seja confirmada (<i>timeout</i>), possibilitando que atrasos variáveis sejam acomodados. Isso deverá ser feito por meio de um algoritmo de retransmissão adaptativo que periodicamente ajusta o <i>timeout</i> da rede.
	Quando um datagrama é fragmentado, todos os fragmentos são enviados pelo mesmo caminho na rede (rota).

INATEL Instituto Nacional de Telecomunicações	Avaliação de TP-311 - Redes IP	
	Profº: Evandro Luís Brandão Gomes	03/07/2010

Questão 2 (10 pontos): Considere os pares de endereços de hosts e suas respectivas máscaras listados abaixo e **marque os itens nos quais o par citado pertence a uma mesma sub-rede:**

	192.168.4.167/255.255.255.224 e 192.168.4.207/255.255.255.224
	195.100.2.115/255.255.255.128 e 195.100.2.135/255.255.255.128
	200.168.1.97/255.255.255.224 e 200.168.1.118/255.255.255.224
	201.180.0.43/255.255.255.192 e 201.180.0.66/255.255.255.192
	202.8.3.34/255.255.255.240 e 202.8.3.46/255.255.255.240

Questão 3 (10 pontos): Um roteador pode descartar pacotes recebidos em suas interfaces por diversos motivos e situações diferentes. Quais são estes motivos e situações de descarte? Descreva e explique objetivamente cada motivo/situação citada.

TTL = 0 → quando o roteador decrementar o campo TTL da datagrama e o mesmo for igual a 0 (zero), o mesmo será descartado e um aviso de descarte será enviado ao host de origem (via ICMP).

Time-out no Fragmento → quando o tempo máximo pela espera de algum fragmento “estourar” o “datagrama será descartado”, ou seja, todos os fragmentos deste datagrama que já foram recebidos são descartados e um aviso é enviado ao host de origem (via ICMP).

Buffer Cheio → quando o buffer de entrada do roteador está totalmente cheio, ele irá descartar o datagrama que está chegando e avisará ao host de destino o motivo do descarte (via ICMP).

Erro no Check-sum → ao desencapsular o datagrama, o roteador refaz o cálculo do check-sum para verificar a integridade do mesmo. Se existir algum erro o datagrama será descartado. O roteador avisa o host de origem (via ICMP).

Falha de Rota → quando o roteador não encontrar em sua tabela de rotas uma rota para a rede de destino e também não existe uma rota default configurada, o datagrama será descartado. O roteador avisa o host de origem (via ICMP).

Fragmentação → quando o roteador necessita fragmentar o datagrama para enviar para o “próximo-salto” e o bit DF no campo FLAGS do datagrama está “setado” (igual a 1) não permitindo que o roteador faça a fragmentação; neste caso o roteador descarta o datagrama e avisa o host de origem o motivo do descarte (via ICMP).

OBS:

Existem outras situações como QoS, ACL (Listas de Controle de acesso), etc; que não foram vistas no curso mas aceitei como resposta se algum aluno já tinha esse conhecimento.

Nesta questão, o acerto de cada item teve 2 pontos na nota, ou seja, não precisaria citar todas as condições, apenas 5 delas.

INATEL Instituto Nacional de Telecomunicações	Avaliação de TP-311 - Redes IP	
	Profº: Evandro Luís Brandão Gomes	03/07/2010

Questão 4 (10 pontos): Suponha a existência de quatro roteadores entre os hosts de origem e destino em um rede. Baseado nesta situação, responda:

a) Um datagrama IP (sem fragmentação) enviado do host de origem até o host de destino passará por quantas interfaces de rede? Justifique a resposta.

O datagrama irá passar por 10 interfaces de rede: 1 no host de origem (saída), 2 em cada roteador (entrada e saída) e 1 no host de destino (entrada), totalizando 10 interfaces.

b) E quantas tabelas de rotas serão analisadas durante todo o trajeto deste datagrama? Justifique a resposta.

O datagrama será verificado em 6 tabelas de rotas: a do host de origem, as dos 4 roteadores e a do host de destino.

c) Se for enviado um PING do host de origem ao host de destino, e supondo que esta aplicação (PING) inicializa o campo TTL com o valor 128, o host de origem irá receber a resposta deste PING com qual valor de TTL? Justifique a resposta.

O campo TTL (Time to Live) é decrementado em cada roteador na rota, portanto a resposta do ping (ICMP Echo Reply) será enviada com TTL=128 e chegará no host que gerou o ping (origem) com o valor de 124 (128-4).

Questão 5 (10 pontos): Uma aplicação gera uma mensagem de tamanho 100Kbytes. Sabendo que esta aplicação usa uma transferência confiável (TCP) com tamanho de segmento igual a 20Kbytes e tamanho da janela igual a 3 segmentos, responda:

a) Quantos datagramas serão necessários para enviar esta mensagem? Justifique sua resposta.

Cada datagrama irá transportar um segmento TCP de tamanho 20Kbytes. Portanto serão necessários 5 datagramas (100K / 20K = 5).

b) Explique como o tamanho da janela (zero, um, valor pequeno e valor grande) altera o controle de fluxo na transmissão do protocolo TCP

Quanto maior o tamanho da janela mais segmentos serão transmitidos, mas em contrapartida se a rede estiver congestionada irá ocorrer muitas retransmissões por timeout ou ACKs duplicados.

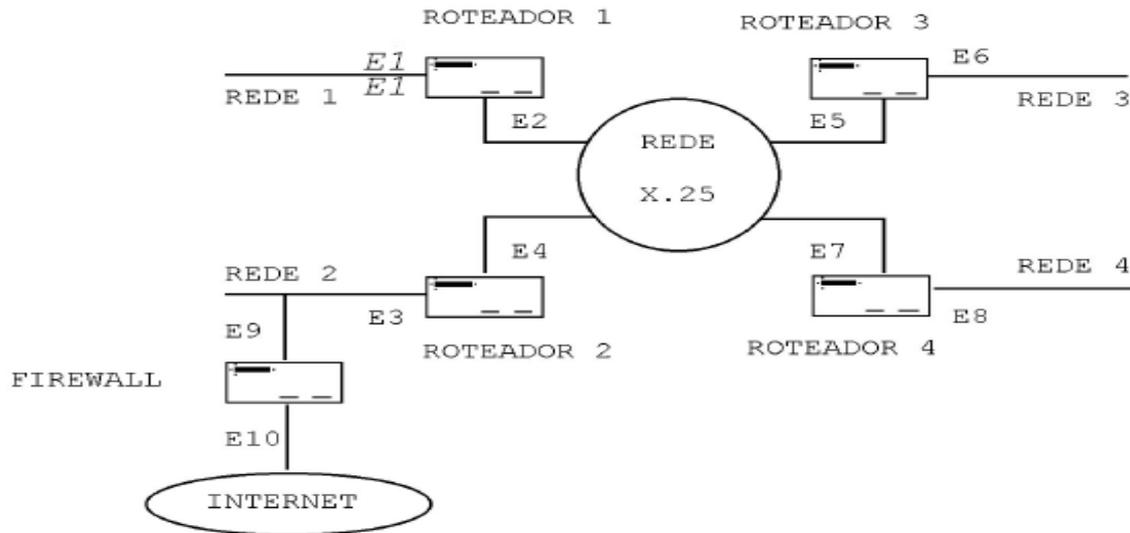
Se o tamanho da janela for pequeno serão transmitidos poucos segmentos e se a rede estiver com um bom throughput isto pode representar um desperdício de canal de transmissão.

O tamanho da janela pode ser 1 fazendo com que a transmissão funcione como STOP-AND-WAIT (desperdiçando canal de transmissão)

E se o tamanho da janela for 0 causa uma parada na transmissão de segmentos.

O fluxo de transmissão ideal deverá ser medido instantaneamente a cada inicio de transmissão pelo tempo inicial gasto com um segmento transmitido e uma confirmação recebida (RTT – Round Trip Time).

Questão 6 (15 pontos): A rede de uma empresa cujo esquema está ilustrado a seguir é composta por 4 redes TCP/IP locais. Essas redes TCP/IP são interligadas por uma rede X.25 (X.25 é um protocolo de camada 3), que opera como túnel para as 4 redes. As interfaces dos computadores pertencentes a essas redes são numeradas com endereços IP das redes 10.0.0.0 ou 164.41.0.0. Um *firewall* protege a rede no acesso à Internet, sendo que, a partir de qualquer máquina na rede, pode-se acessar a Internet. A partir dessas informações, julgue os itens a seguir, relativos à rede da referida empresa, considerando o seu correto funcionamento e **marque a(s) resposta(s) correta(s)**:



	Os endereços E2, E4, E5 e E7 devem estar em uma mesma sub-rede.
	Os pacotes X.25 são transferidos dentro de datagramas IP.
	A rota <i>default</i> na tabela de roteamento do roteador 2 é o endereço E10.
	Não devem ter sido atribuídos endereços X.25 aos roteadores 1, 2, 3 e 4.
	A rota <i>default</i> nas tabelas de roteamento dos roteadores 1, 3 e 4 é o endereço E4.
	É correto utilizar a máscara 255.255.0.0 para segmentar a rede.
	Os endereços de E1 a E9 podem ser endereços na rede 10.0.0.0.
	O endereço E10 deve ser um endereço na rede 164.41.0.0.
	Os endereços na rede 10.0.0.0 são visíveis pelas máquinas que estiverem na Internet.
	O <i>firewall</i> deve traduzir entre os endereços na rede 10.0.0.0 e os endereços na rede 164.41.0.0.