PROVA 02 – 2012/02 (Turmas A/B) – Revisão 14.12.2012

Observação: as respostas abaixo salientam apenas os principais conceitos e não se espera que elas sejam a resposta padrão. Na resposta a prova se espera que essas ideias sejam elaboradas de acordo com o solicitado e, respostas diferentes, bem fundamentadas, são consideradas de acordo com sua correção e argumentação.

1ª Questão

(a) Tanto o IPv4 quanto o IPv6 podem ser configurados manualmente ou automaticamente via um servidor de DHCP. O IPv6 ainda possui um método automático de gerar o endereço IPv6 a partir de seu endereço MAC e, através deste, solicitar via multicast o seu endereço IPv6 global. Isso é feito através de mensagens ICMPv6. (Obs.: o DHCP é específico para cada versão de IP).

(b) IP duplicado: o protocolo diretamente afetado é o ARP. Uma máquina ao fazer ARP request do IP duplicado vai receber duas respostas, uma sobreescrendo a outra. No momento que isso ocorrer datagramas será entregues aleatoriamente para uma ou outra máquina. O TCP, devido as perdas, acabará por ter um número de retransmissões alto e um consequente aumento de seu time-out.

Máscara mais restritiva: ao aplicar uma máscara mais restritiva, máquinas que estão na rede local serão consideradas externas e com isso, ao se tentar uma comunicação, os datagramas serão enviados ao default gateway invés da máquina destino. Afeta todos os protocolos que dependem do IP (inclusive).

Máscara menos restritiva: ao aplicar uma máscara menos restritiva, máquinas externas a rede passarão a ser consideradas como pertencentes a rede local e os datagramas serão erradamente enviados para a rede local. Com isso as máquinas destinos nunca receberão os datagramas. Afeta todos os protocolos que dependem da entrega do datagrama IP.

Default gateway não configurado: não será possível entregar nenhum datagrama para máquinas em redes externas. Afeta todos os protocolos que dependem da entrega do IP (para máquinas externas).

DNS não configurado: não será possível resolver nomes simbólicos. Afetará todos os protocolos de aplicação que empregam nomes simbólicos para localizar/identificar máquinas.

2ª questão

(a) Um cliente localiza o servidor e serviço a partir do endereço IP do servidor e a porta usada pelo serviço. Esse procedimento é independente do protocolo de transporte empregado (TCP ou UDP).

(b) Em caso de haver mais de uma rota possível, a selecionada é aquela da máscara mais restritiva

IP. dst	Rota	Máscara	IP. dst AND Máscara	
195.112.92.1	1	255.255.255.255	195.112.92.1	Possível e selecionada
	2	255.255.255.240	195.112.80.0	Possível
	3	255.255.255.192	195.112.64.0	Possível
	4	0.0.0.0	0.0.0.0	Possível
195.112.94.1	1	255.255.255.255	195.112.94.1	Não tem entrada associada
	2	255.255.255.240	195.112.80.0	Possível
	3	255.255.255.192	195.112.64.0	Possível
	4	0.0.0.0	0.0.0.0	Possível
195.112.128.1	1	255.255.255.255	195.112.128.1	Não tem entrada associada
	2	255.255.255.240	195.112.128.0	Não tem entrada associada
	3	255.255.255.192	195.112.128.0	Não tem entrada associada
	4	0.0.0.0	0.0.0.0	Possível e selecionada (única)

3ª Questão

(a) As redes 200.10.0.0/26 e 200.10.0.64/64 podem ser aglutinadas formando um bloco 200.10.0.0/25. As redes 200.10.0.128/26 e 200.10.0.192/26 são agrupadas formando o bloco 200.10.0.128/25. As redes 200.10.1.0/26 e 200.10.1.64/26 também são agrupadas formando o bloco 200.10.1.0/25. Os blocos 200.10.0.0/25 e 200.10.0.128/25 formam o bloco 200.10.0.0/24. O bloco 200.10.1.0/25 é agrupado com a rede 200.10.1.128/25 gerando o bloco 200.10.1.0/24. Os blocos /24 formam o 200.10.0/23 que é o fornecido para a organização em questão.

(b) Um domínio é um nó do espaço de nomes do DNS e a sua descendência. Uma zona é caracterizada por um servidor de autoridade que mantém os RR (register records) de um domínio DNS. No exemplo, primeiro caso, se inf.ufrgs.br é apenas um subdomínio de ufrgs.br, os RRs do inf.ufrgs.br são mantidos pelo servidor de DNS ufrgs.br. Quando inf.ufrgs.br for um subdomínio de ufrgs.br e uma zona, isso significa que o domínio ufrgs.br delegou a responsabilidade (autoridade) de manter os RRs do inf.ufrgs.br para a própria inf.ufrgs.br.

4ª questão

(a) O browser é o cliente e o servidor web é o servidor. O cliente sempre abre um socket ativo e o servidor um socket passivo (associado ao estado listen). Na situação descrita existem três sockets:

socket	Endpoint local	Porta local	Endpoint remoto	Porta remota	estado
servidor	0.0.0.0	80	* (ANY)	*(ANY)	Listen
servidor	192.168.10.1	80	192.168.20.2	65432	Established
cliente	192.168.20.2	65432	192.168.10.1	80	Established

(b) O SSL emprega criptografia assimétrica na sua primeira fase onde ele negocia o estabelecimento de uma sessão segura. A criptografia assimétrica é usada porque ela permite garantir, através do emprego de certificados digitais trocados nessa fase, a autenticidade do servidor e – opcionalmente – do cliente. Os certificados digitais resolvem ainda o problema de gerenciamento e distribuição de chaves existente na criptografia simétrica. O problema da assimétrica é seu custo computacional elevado, mas como na fase de negociação o volume de dados é pequeno, o impacto desse custo é minizado.

A criptografia simétrica é usada na segunda fase do SSL: troca de dados. Ela é usada nessa etapa devido ao seu baixo custo computacional para cifragem. Como o volume de dados tende a ser importante, é importante que o método de cifragem forneça um bom desempenho. O problema da criptografia simétrica é a distribuição e gerência de chaves, mas como essas são geradas automaticamente e trocadas na primeira fase do SSL, o problema de gerir e manter é minimizado.

5ª questão

(a) A máquina cliente, o servidor de DNS e o servidor SMTP (e-mail) estão em redes diferentes. Posto isso, a ordem em que os protocolos são acionados é:

1. ARP para o default gateway, para recuperar o endereço MAC a ser usado para se comunicar com o servidor DNS (necessário para descobrir o IP do servidor de e-mail)
2. DNS para resolver o nome do servidor de e-mail
3. ARP para o default gateway para recuperar o endereço MAC a ser usado para se comunicar com o servidor de e-mail.
4. TCP para abrir uma conexão com a porta 25 com o servidor de e-mail.
5. SMTP para enviar a mensagem de correio eletrônico.

Ainda, o DNS é encapsulado no UDP que por sua vez é encapsulado no IP. O SMTP é encapsulado no TCP que por usa vez é encapsulado no IP. O ARP é encapsulado diretamente no quadro de enlace.

(b) Uma VPN serve para estabelecer uma rede (interna) virtual entre organizações ou máquina geograficamente dispersas através de uma rede pública, como a Internet. Seu princípio de funcionamento consiste em criar um túnel cifrado entre um cliente VPN e um servidor VPN. Os dados cifrados são encapsulados em um datagrama convencional que é roteado normalmente na rede pública (Internet). Tipicamente é empregado o protocolo ESP (IPsec). A propriedade mais importante a ser garantida é a confidencialidade, já que dados privativos passarão por uma infraestrutura pública.