

LISTA DE EXERCÍCIOS DE REDES DE COMPUTADORES N(2012/2) - PROFESSOR CARISSIMI
PARTE 2 DA MATÉRIA

IMPORTANTE - REGRAS DO JOGO

(regras copiadas da lista colaborativa de exercícios de SISOP do semestre anterior, criada por João Gross)

- Não exclua o que outros já escreveram, se for o caso bote um comentário no trecho que deseja discutir.
- Caso tenha uma outra resposta às perguntas da lista de exercícios, mantenha a resposta antiga e insira a sua, como resposta 2, 3, etc... não esqueça de colocar uma resposta nova com uma cor de letra diferente para separar as respostas.
- Uma dica é usar o recurso de comentários, onde devemos selecionar o texto que queremos comentar e acionar o menu “Inserir | Comentário”, que vai aparecer um balão ao lado do texto selecionado.
- A lista apresenta alguns erros de grafia, devido a falhas durante a conversão do PDF do professor para o formato do GOOGLE DOCS. A idéia é de corrigi-los à medida em que respondidas as questões.
- Manter o enunciado das questões em negrito e deixar as respostas com letra normal.
- Se alguém possuir notas e fotos das aulas, ou algum outro material, compartilhe com o pessoal colocando os links na seção AULAS.
- Sempre que possível cite a bibliografia utilizada para responder a questão, como “Aula 1, Slide 10”, para LIVROS coloque a referência completa com um identificador na seção BIBLIOGRAFIA e faça a ligação usando o identificador e a página, por exemplo [TANENBAUM5PT, página 10] para referenciar a página 10 do livro “Redes de Computadores”, 5a. Edição do autor Andrew Tanenbaum em português, conforme a bibliografia.

GLOSSÁRIO

(lista com os termos e abreviaturas usados na disciplina)

LISTA 1 DESSE SEMESTRE: [LISTA 1](#)
LISTAS DE SEMESTRES ANTERIORES: [LISTA 1](#) e [LISTA 2](#)

BIBLIOGRAFIA

- [TANENBAUM4PT] TANENBAUM, Andrew S.; WETHEREALL, David. “Redes de Computadores”. 4a Edição. Editora Campus, 2003.
- [TANENBAUM5] TANENBAUM, Andrew S.; WETHEREALL, David. “Computer Networks”. 5a Edição. Editora Prentice Hall, 2011.
- [TANENBAUM5PT] TANENBAUM, Andrew S.; WETHEREALL, David. “Redes de Computadores”. 5a Edição. Editora Pearson Education, 2011.
- [CARISSIMI] CARISSIMI, A.; ROCHOL, J.; GRANVILLE, L.Z. “Redes de Computadores”. Série de Livros Didáticos - Instituto de Informática UFRGS. Editora Bookman, 2009.
- [KUROSE] KUROSE, J.F.; ROSS, K.W. “Redes de Computadores e a Internet: uma abordagem top-down”. 5a Edição. São Paulo: Addison Wesley, 2010.
- [FOROUZAN3PT] FOROUZAN, Behrouz A. “Comunicação de Dados e Redes de Computadores”. 3a Edição. Porto Alegre: Bookman, 2006.
- [FOROUZAN] FOROUZAN, Behrouz A. “TCP/IP Protocol Suite”. 4a Edição. Boston: Mc-Graw-Hill Higher Education, 2007.
- [FOROUZAN4PT] FOROUZAN, Behrouz A. “Comunicação de Dados e Redes de Computadores”. 4a Edição. São Paulo: Mc-Graw-Hill, 2008.
- [STALLINGS] STALLINGS, William W. “Data & Computer Communications”. 6a Edição, Reimpressão.

ATENÇÃO - FOTOS e NOTAS DAS AULAS/SLIDES

AULAS TEÓRICAS (Material do Prof. Carissimi, disponível [aqui](#)):

- [Aula 1 - 27/08/2012 - Nota da Aula \(Luiz Souza\)](#)
- [Aula 2 - 29/08/2012 - Nota da Aula \(Luiz Souza\)](#)
- [Aula 3 - 03/09/2012 - Nota da Aula \(Luiz Souza\)](#)
- [Aula 4 - 12/09/2012 - Nota da Aula \(Luiz Souza\)](#)
- [Aula 5 - 17/09/2012 - Nota da Aula \(Luiz Souza\)](#)
- [Aula 6 - 19/09/2012 - Nota da Aula \(Luiz Souza\)](#)
- [Aula 7 - 24/09/2012 - Nota da Aula \(Luiz Souza\)](#)
- [Aula 8 - 26/09/2012 - Nota da Aula \(Mario Gasparoni\)](#)
- [Aula 9 - 01/10/2012 - Nota da Aula \(Luiz Souza\)](#)
- [Aula 10 - 03/10/2012 - Nota da Aula \(Mario Gasparoni, Luiz Souza\)](#)
- [Aula 11 - 08/10/2012 - Nota da Aula \(Luiz Souza\)](#)
- [Aula 12 - 10/10/2012 - Nota da Aula \(Luiz Souza\)](#)
- [Aula 13 - 15/10/2012 - Nota da Aula \(Luiz Souza\)](#)
- [Aula 14 - 17/10/2012 - Nota da Aula \(Luiz Souza\)](#)
- [Aula 15 - 22/10/2012 - Prova 1](#)
- [Aula 16 - 24/10/2012 - Nota da Aula \(Luiz Souza\)](#)
- [Aula 17 - 29/10/2012 - Nota da Aula \(Luiz Souza\)](#)
- [Aula 18 - 31/10/2012 - Nota da Aula \(Luiz Souza\)](#)
- [Aula 19 - 05/11/2012 - Nota da Aula \(Luiz Souza\)](#)
- [Aula 20 - 07/11/2012 - Nota da Aula \(Luiz Souza\)](#)
- [Aula 21 - 12/11/2012 - Nota da Aula \(Luiz Souza\)](#)
- [Aula 22 - 14/11/2012 - Nota da Aula \(Luiz Souza\)](#)
- [Aula 23 - 19/11/2012 - Nota da Aula \(Luiz Souza\)](#)
- [Aula 24 - 21/11/2012 - Nota da Aula \(Luiz Souza\)](#)
- [Aula 25 - 26/11/2012 - Nota da Aula \(Luiz Souza\)](#)
- [Aula 26 - 28/11/2012 - Nota da Aula \(Luiz Souza\)](#)
- [Aula 27 - 03/12/2012 - Nota da Aula \(Luiz Souza\)](#)
- [Aula 28 - 05/12/2012 - Nota da Aula \(Luiz Souza\)](#)
- [Aula 29 - 10/12/2012 - Nota da Aula \(Luiz Souza\)](#)
- [Aula 30 - 12/12/2012 - Prova 2](#)

AULAS PRÁTICAS (Material do Prof. Valter Roesler, disponível [aqui](#)):

- [Aula 1 - 14/09/2012 - Nota da Aula](#)
- [Aula 2 - 21/09/2012 - Nota da Aula - Exercícios Resolvidos](#)
- [Aula 3 - 28/09/2012 - Nota da Aula - Exercícios Resolvidos](#)
- [Aula 4 - 05/10/2012 - Nota da Aula](#)
- [Aula 5 - 19/10/2012 - Nota da Aula](#)
- [Aula 6 - 26/10/2012 - Nota da Aula](#)
- [Aula 7 - 09/11/2012 - Nota da Aula](#)
- [Aula 8 - 16/11/2012 - Nota da Aula](#)
- [Aula 9 - 23/11/2012 - Prova 1](#)
- [Aula 10 - 30/11/2012 - Nota da Aula](#)
- [Aula 11 - 07/12/2012 - Nota da Aula](#)
- [Aula 12 - 14/12/2012 - Nota da Aula](#)
- [Aula 13 - 21/12/2012 - Nota da Aula](#)

- [Aula 14 - 04/01/2013 - Nota da Aula](#)
- [Aula 15 - 11/01/2013 - Prova 2](#)

RESUMOS E OUTROS MATERIAIS

AULAS TEÓRICAS (Material do Prof. Carissimi, disponível [aqui](#)):

- Prova 1 - [Prova](#) - [Gabarito Oficial](#)
 - Luiz Souza - [Resumo](#) - [Respostas](#)
- Prova 2 - [Prova](#) - [Gabarito Oficial](#)
 - Luiz Souza - [Resumo](#) - [Respostas](#)

AULAS PRÁTICAS (Material do Prof. Valter Roesler, disponível [aqui](#)):

- Laboratório 1 - Aulas 1 e 2 - [Descrição](#): Uso de ferramentas analíticas e gráficas na representação e avaliação de um canal. Capacidade Máxima de um canal segundo Nyquist e Shannon.
 - Mário Gasparoni e Luiz Souza - [Relatório](#)
- Laboratório 2 - Aulas 3 e 4 - [Descrição](#): O Modelo de Referência OSI e a interface digital V.24/V.28 do ITU-T (ou RS232 da EIA).
 - Mário Gasparoni e Luiz Souza - [Relatório](#)
- Laboratório 3 - Aulas 5 e 7 - [Descrição](#): Sockets.
 - Mário Gasparoni e Luiz Souza - [Relatório](#)
- Laboratório 4 - Aulas 6 e 8 - [Descrição](#): Controle de Fluxo e Erros.
 - Mário Gasparoni e Luiz Souza - [Relatório](#)
- Laboratório 5 - Aulas 10, 11 e 12 - [Descrição](#): Medidas de Desempenho em Redes.
 - Mário Gasparoni e Luiz Souza - [Relatório](#)
- Laboratório 6 - Aulas 13 e 14 - [Descrição](#): Simulação de Redes.
 - Mário Gasparoni e Luiz Souza - [Relatório](#)
- Prova 1
 - Luiz Souza - [Resumo](#)
- Prova 2
 - Luiz Souza - [Resumo](#)

OUTROS MATERIAIS:

- [Proxy ARP \[FOROUZAN4PT, p.617\]](#)
- [Explicação do Prof. Carissimi sobre números de sequência](#)
- [Explicação do Prof. Carissimi sobre o uso da mesma porta para TCP e UDP](#)
- [Explicação do Prof. Carissimi sobre Proxy ARP](#)
- [Material da CISCO sobre Proxy ARP](#)
- [Dicas sobre IPs \(máscaras e subredes\)](#)
- [Estrutura de dados internas do linux para guardar a tabela ARP](#)
- [Modelos de Camadas de Redes por Grandes Pesquisadores da Área](#)
- [Curso de “Fundamentos de Redes” da Fundação Bradesco](#)
- [Curso de “Redes de Computadores” do Portal GSTI](#)
- [Artigos sobre Redes de Computadores](#)
- [eBook Free: Beej's Guide to Network Programming Using Internet Sockets](#)
- [Pilha de Protocolos de WebServices](#)
- [Aplicações Peer-To-Peer \(P2P\)](#)
- [SAM: um sistema adaptativo para transmissão e recepção de sinais multimídia em redes de computadores](#)

EXERCÍCIOS NÃO RESOLVIDOS OU PENDENTES DE REVISÃO ATÉ O MOMENTO

6, 38B, 45, 51B, 52, 54, 59, 61, 63, 68, 75,

DÚVIDAS

1. Qual a diferença entre comunicação fim-a-fim e hospedeiro-a-hospedeiro?

Resposta 1:

De acordo com o modelo de referência OSI, o nível de transporte é responsável pelo envio e pela recepção de informações entre suas entidades pares, independentemente da topologia e da quantidade de redes físicas envolvidas. Por isso o nível de transporte e seus protocolos são denominados de *fim-a-fim* (*end-to-end* ou *peer-to-peer*). Para oferecer essa funcionalidade, o nível de transporte conta com serviços providos pelo nível inferior, o nível de rede, que permite a transferência das informações entre uma origem e um destino localizados em redes diferentes. Dada essa característica, diz-se que o nível de rede garante um serviço de entrega de *hospedeiro-a-hospedeiro* (*host-to-host delivery*); ou seja, na prática, sua função é entregar dados de um equipamento para outro. Para realizar essa função, o nível de rede realiza três tarefas importantes: *endereçamento lógico*, *determinação de trajeto* e *encaminhamento de informações*.

[CARISSIMI, p.208]

2. O que é um Sistema Autônomo?

Resposta 1:

Um sistema autônomo é um conjunto de redes e de sistemas intermediários, vinculados a uma mesma unidade administrativa, domínio ou empresa. Isso permite a adoção de um mesmo protocolo de roteamento nas suas diferentes redes de acordo com suas conveniências. Por exemplo, podemos pegar a rede da UFRGS, onde cada escola/faculdade/instituto possui a sua própria rede e a ligação entre as unidades é feita através de roteadores (que são os sistemas intermediários). Desse modo os administradores da rede da UFRGS podem escolher um protocolo de acordo com suas necessidades e, independentemente de outras universidades. Esse protocolo comum de roteamento é denominado de *protocolo de roteamento interior ou intradomínio* (IRP - Interior Routing Protocol).

[CARISSIMI, p.232]

3. Um Access Point (AP) define quantos domínios de colisão? E de broadcast?

Resposta 1:

O Access Point (AP) é um equipamento de Nível 2, ou seja, trabalha na camada de Enlace. Ele atua como uma bridge, definindo um domínio de colisão para o lado *wireless* e outro para o lado *wired*. Forma um único domínio de broadcast. Não é sinônimo de roteador (apesar das propagandas dos fabricantes): os fabricantes incluem facilidades de roteamento, NAT, filtragem, firewall em bases wireless (ponto de acesso) o que, neste caso, as transformam em equipamentos com funcionalidades de Nível 3 ou mesmo Nível 4.

[Aula 13, Slide 23]

LISTA

1. Sob o ponto de vista conceitual, a introdução do IPv6 implica em se redefinir o funcionamento do protocolo ARP, ou ele pode apresentar o mesmo comportamento do IPv4 ? JUSTIFIQUE sua resposta.

Resposta 1:

O funcionamento do ARP continua sendo o mesmo (solicitação(IP) em broadcast e resposta(MAC) em multicast), porém no IPV6 esse procedimento é realizado pelo ICMPv6.

Resposta 2:

O IPV6 utiliza o NDP (*Neighbor Discovery Protocol*). O NDP é muito similar ao ARP, porém, o NDP é parte do IPV6, enquanto que o ARP não roda sob o IP. O NDP também utiliza pacotes *multicast* ao invés de pacotes *broadcast* como o ARP.

NDP substitui o ARP no IPV6. Ele é equivalente ao ARP, RDISC e ICMP do IPV4.

Para requisições de endereço, utiliza ICMPv6 tipo 135 para requisição e tipo 136 para resposta.

fonte: <http://www.ucl.ac.uk/computing/courses/earlier/ipv6-basics/x84>

Resposta 3:

O NDP - como outros (ICMPv6) - é a forma de uma máquina IPV6 gerar seu endereço IPV6 com base no endereço físico (MAC). São formas de autoconfiguração. Como o MAC e o IPV6 são relacionados, em certos casos, se pode de um deduzir o outro. Com o ARP isso não é possível. (Resposta do professor)

2. Considerando os protocolos IP, ICMP e ARP, responda :

a. Como você faria um software para, no momento da inicialização de uma máquina, determinar se o endereço IP a ser atribuído a esta máquina já não está sendo utilizado por uma outra máquina nessa mesma sub-rede ?

Faria uma requisição de echo ICMP (*ICMP echo request*) para o IP, caso retornasse um *echo reply*, a máquina está ligada. Este método não é muito confiável, pois uma máquina com um IP na rede pode ter um firewall bloqueando as requisições de echo ICMP. Ou enviaria um ARP

b. Como você faria um software para determinar a MTU de uma rede entre um ponto A e um ponto B da rede. A solução proposta funcionaria sempre ? Caso negativo, qual é o problema dessa sua solução ?

Resposta do Professor:

Se eles simplesmente descartassem, não haveria como saber qual fez isso. Eles descartam E enviam um ICMP com a mensagem de erro. Sempre, qualquer coisa baseada em ICMP, pode ser filtrada e não funcionar.

Resposta 1:

Técnica "Path MTU discovery".

Cada pacote IP é enviado com seus bits de cabeçalho definidos para indicar que nenhuma fragmentação poderá ser realizada. Se um roteador receber um pacote muito grande, ele gera um pacote de erro que retorna a origem. O roteador pode também trucar o pacote que excedem sua MTU. Baseado na quantidade de dados descartados, o origem saberia que os pacotes foram descartados pelo tamanho da MTU. [TANENBAUM5] pg273

Resposta 2:

Problema: o ICMP pode estar sendo bloqueado por firewall. O MTU também pode modificar dinamicamente, pois o caminho pode se alterar.

3. O que é proxy ARP ? Como funciona ?

Resposta 1:

Um host 1 quer se comunicar com o host 2 em outra rede. Como o host 1 e 2 estão em redes

separadas, o pacote deve ser enviado para um gateway. Uma das maneiras no host 1 conhecer o gateway é através do proxy ARP. O host 1, após não encontrar o mapeamento do IP em um MAC na sua cache, envia uma mensagem de broadcast. Todos os dispositivos, inclusive o proxy arp recebe a requisição. O proxy ARP responde a requisição com o seu MAC.

Resposta 2: (Ver questão 25)

O *proxy ARP* é um método do protocolo ARP (pertencente à *Camada de Rede*) que faz resolução de endereços MAC (descobre o endereço MAC a partir de um endereço IP). Este método é usado principalmente na *entrega indireta*, ou seja, ele é usado para descobrir um endereço MAC efetuar a entrega para um endereço MAC de um IP de destino que não está na mesma rede do endereço de origem usando um gateway.

No método proxy ARP, o sistema de origem, após não encontrar uma correspondência de mapeamento entre o *Endereço IP-Endereço MAC* em sua cache ARP, envia em broadcast um *ARP Request*. Todos os dispositivos da rede, incluindo o gateway da rede, recebem essa requisição e analisam o endereço IP de destino. Aquele cujo endereço IP for igual ao endereço IP destino da requisição responde com seu endereço MAC com um *ARP Reply*. Porém, se o endereço IP de destino não pertencer à mesma rede que da origem, quem responde com seu endereço MAC é o gateway. Portanto, qualquer requisição ARP com endereço IP de destino diferente da rede de origem será resolvida para o endereço MAC do gateway da rede. É importante ressaltar que esse método não realiza o procedimento do “E” lógico para determinar se origem e destino estão na mesma rede (como no caso de uma *entrega direta*).

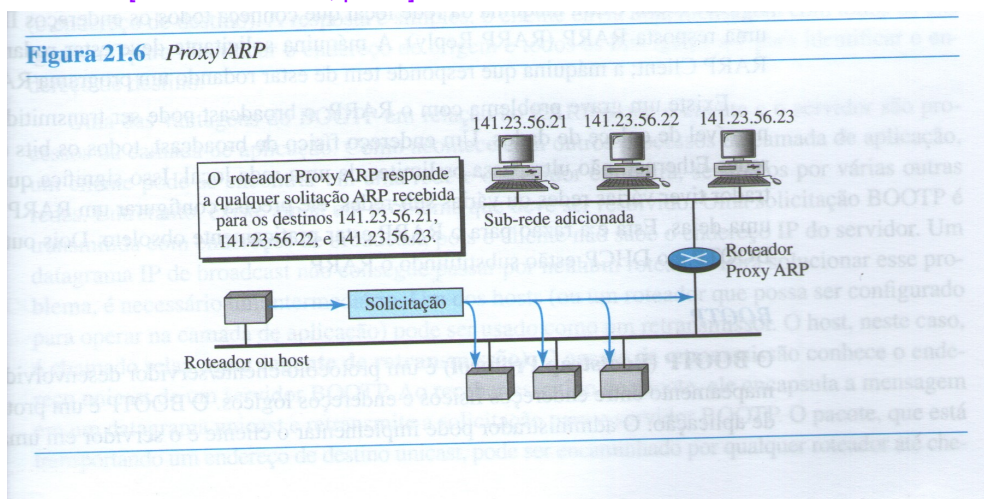
[CARISSIMI, Páginas 243 e 244]

Resposta 3:

O *proxy ARP* é um método do protocolo ARP (pertencente à *Camada de Rede*) que faz resolução de endereços MAC (descobre o endereço MAC a partir de um endereço IP), assim como o ARP convencional, em um mesmo enlace, porém o servidor que roda proxy ARP é o responsável pela requisição/resposta ARP de um subconjunto de máquinas. O principal o objetivo de um proxy ARP é a criação de sub-redes, sem a necessidade de maiores alterações na rede(endereços de ip, etc) em questão. Um servidor que roda proxy ARP ‘protege’ (ou esconde) as máquinas configuradas para utilizarem seu serviço(dando a idéia de uma sub-rede), respondendo por todas as requisições ARP(tanto request como reply) que chegam a qualquer uma de suas máquinas.

Resposta 4:

Ver a figura abaixo [FOROUZAN4PT, p.617]:



Resposta 5: (Material da cisco)

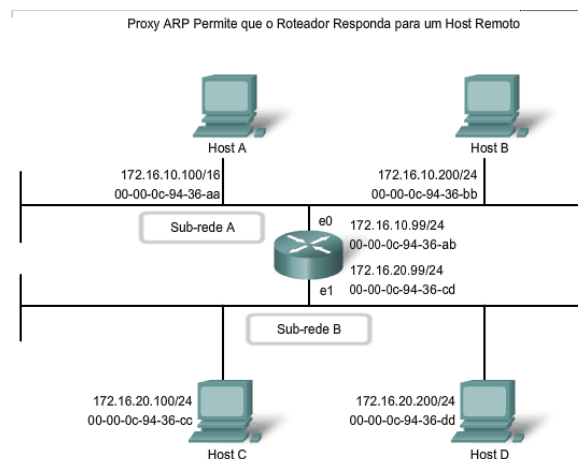
Proxy ARP

Existem circunstâncias sob as quais um host poderá enviar uma solicitação ARP buscando mapear um endereço IPv4 fora da faixa da rede local. Nesses casos, o dispositivo envia solicitações ARP para endereços IPv4 que não estão na rede local, em vez de solicitar o endereço MAC associado ao endereço IPv4 do gateway. Para fornecer um endereço MAC para esses hosts, uma interface do roteador poderá usar um proxy ARP para responder em nome desses hosts remotos. Isso significa que a cache ARP do dispositivo solicitante conterá o endereço MAC do gateway mapeado para quaisquer endereços IP que não estão na rede local. Usando proxy ARP, uma interface de roteador atua como se fosse o host com o endereço IPv4 solicitado pela solicitação ARP. Ao "fingir" sua identidade, o roteador aceita a responsabilidade por rotear pacotes ao destino "real".

Uma utilização desse processo ocorre quando uma implementação IPv4 mais antiga não puder determinar se o host de destino está na mesma rede lógica que o de origem. Nessas implementações, o ARP sempre envia solicitações para o endereço IPv4 de destino. Se o proxy ARP for desabilitado na interface do roteador, esses hosts não conseguem se comunicar fora da rede local.

Outro situação onde o proxy ARP é usado ocorre quando um host acredita que está diretamente conectado à mesma rede lógica que o host de destino. Isso geralmente ocorre quando um host é configurado com uma máscara inadequada.

Como mostra a figura, o Host A foi configurado de maneira inadequada com uma máscara de sub-rede /16. Esse host acredita estar diretamente conectado a toda a rede 172.16.0.0 /16 em vez da sub-rede 172.16.10.0 /24.



Quando são feitas tentativas de se comunicar com qualquer host IPv4 na faixa de 172.16.0.1 a 172.16.255.254, o Host A enviará uma solicitação ARP para o endereço IPv4. O roteador pode usar um proxy ARP para responder a solicitações para o endereço IPv4 do Host C (172.16.20.100) e do Host D (172.16.20.200). O Host A terá, então, entradas para esses endereços mapeadas para o endereço MAC da interface e0 do roteador (00-00-0c-94-36-ab).

Ainda, outra finalidade de um proxy ARP ocorre quando um host não é configurado com um gateway padrão. O Proxy ARP pode ajudar os dispositivos em uma rede a alcançarem sub-redes remotas sem a necessidade de configurar o roteamento ou um gateway padrão.

Por padrão, os roteadores Cisco têm o proxy ARP habilitado em interfaces LAN.

http://www.cisco.com/en/US/tech/tk648/tk361/technologies_tech_note09186a0080094adb.shtml

4. Qual é a explicação para a tabela ARP abaixo possuir em várias entradas um mesmo endereço MAC associado a diferentes endereços IPs? (Obs: a rede como um todo está corretamente configurada e funcional.)

| IP ADDRESS | | MAC ADDRESS |
|--------------|--|-------------------|
| 143.54.11.5 | | 00:21:A0:6B:12:11 |
| 143.54.11.20 | | 00:21:A0:AD:15:0A |
| 143.54.15.12 | | 00:20:A0:BF:12:C0 |
| 143.54.83.15 | | 00:20:A0:BF:12:C0 |
| 143.58.12.12 | | 00:20:A0:BF:12:C0 |

Resposta 2:

Pode ser que o dispositivo identificado pelo MAC 00:20:A0:BF:12:C0 seja um Roteador ligado em mais de uma Rede. Por exemplo, caso a máscara de rede seja /24, podemos dizer que esse mac tem IPs de 3 redes diferentes (143.54.15.x, 143.54.83.x e 143.58.12.x) e nesse caso o Roteador responde uma consulta ARP com um IP dessas redes com o seu próprio endereço MAC, e a máquina que fez a consulta vai encaminhar o pacote ethernet para o roteador que irá encaminhar para a respectiva rede. Essa situação também é conhecida como *proxy ARP*. Nesse caso o roteador está respondendo como o *default gateway* da rede.

[TANENBAUM5PT, Página 294; CISCO, [Proxy ARP](#)]

5. Uma máquina em uma rede TCP/IP é caracterizada pelo endereço IP 128.138.243.100 e máscara 255.255.255.192.

Determine o número da rede, o endereço de broadcast dessa rede, o primeiro e último endereços IPs válidos para máquinas nessa rede. Considere sistema classfull.

Resposta 1:

255.255.255.192 == máscara 26.

128.138.243.64 -> endereço da rede

128.138.243.127 -> endereço de broadcast

128.138.243.65 -> primeiro endereço válido

128.138.243.126 -> último endereço válido

Resposta 2 (binário):

255.255.255.192 = 11111111.11111111.11111111.11000000 = Máscara /26

128.138.243.100 = 10000000.10001010.11110011.01100100 = IP da máquina

Portanto:

10000000.10001010.11110011.01XXXXXX = 128.138.243.64 => Endereço da Rede

10000000.10001010.11110011.01111111 = 128.138.243.127 => Endereço de Broadcast

10000000.10001010.11110011.01000001 = 128.138.243.65 => Primeiro Endereço Válido

10000000.10001010.11110011.01111110 = 128.138.243.126 => Último Endereço Válido

6. Escreva tudo o que você sabe sobre hubs, switches e roteadores. Tópicos a serem abordados (lista não exaustiva): tecnologia, princípio de operação, utilização da banda passante, domínios de broadcast, domínios de colisão, protocolo spanning tree, etc.

HUB:

* Camada 1 (Nível Físico)

* 1 domínio de colisão

* 1 domínio de broadcast

- * Princípio de operação: o sinal elétrico recebido em uma das portas é replicado em todas as outras. Funciona como um repetidor.
- * Utilização da largura de banda: compartilham largura de banda limitada entre usuários

SWITCH:

- * Camada 2 (Nível de Enlace)
- * 1 domínio de broadcast (se não forem utilizadas VLANs)
- * 1 domínio de colisão por porta
- * Princípio de operação: encaminha seletivamente quadros individuais de uma porta receptora para a porta à qual o nó destino está conectado. Um switch fará buffer de um quadro que está entrando e, então, irá encaminhá-lo para a porta adequada quando estiver ociosa. Este processo é chamado de *store and forward* (armazenar e encaminhar). Com a comutação de armazenamento e encaminhamento, o switch recebe todo o quadro, verifica o FSC quando a erros e encaminha o quadro até a porta adequada para o nó de destino. Como os nós não têm que esperar o meio ficar ocioso, podem enviar e receber em velocidade total sem perdas devido a colisões ou processamento associado ao gerenciamento de colisões (Fonte: material da cisco). Há também os switches do tipo *cut-through*, que não fazem buferização dos pacotes (quadros), ao terminar de ler o endereço de destino eles imediatamente encaminham o quadro para a porta de destino, nesse caso o quadro é encaminhado diretamente antes, inclusive, de se fazer a verificação de erro com o CRC, o switch pode encaminhar quadros com erro para outros enlaces. [CARISSIMI, p. 202]

- * Utilização da largura de banda: fornecem a largura de banda total disponível para cada host: Fazem buffer dos quadros, mas com apenas um host em cada segmento, não há atraso quando cada host deseja transmitir.
- * Em switches gerenciáveis, é possível utilizar o protocolo SPT para prevenir loop. Com o SPT é possível criar uma topologia redundante de switches. O protocolo irá calcular qual o caminho mais eficiente e irá automaticamente desativar ou ativar portas para permitir o tráfego por este caminho e nenhum outro que cause loop.

ROTEADOR:

- * Camada 3 (Nível de Rede)
- ~~* Cada interface de um roteador define um domínio de colisão diferente~~
- ~~* Define um domínio de colisão para cada interface~~
- * 1 Domínio de broadcast por interface [Aula 13, Slide 22; Aula 19, Slide 2; WIKIPÉDIA, [Broadcast Domain](#)].
- * Realiza duas funções: encaminhamento e roteamento. O encaminhamento corresponde à maneira pela qual um pacote é entregue para a próxima estação. Roteamento diz respeito à maneira pela qual as tabelas de roteamento são criadas para auxiliar o encaminhamento.

7. Determine a seqüência de pacotes de ARPs envolvidos no envio de um datagrama, pela primeira vez, de uma máquina A (192.31.65.7) para uma máquina B (192.31.62.8). Especifique para cada mensagem quais são os endereços de hardware fonte (Ef) e destino (Ed), assim como os endereços IP fonte (IPf) e destino (IPd) . As máquinas estão configurados com uma máscara /24. No seu ponto de vista, está faltando alguma informação no enunciado ? Qual ? Faça as suposições necessárias.

Supondo um gateway por configuração, está faltando o IP do gateway.. Se for proxy ARP, não está faltando nada.

Suposições: Gateway por configuração. Redes diretamente conectadas.

No momento em que um datagrama é enviado, a máquina de origem faz uma operação E lógico entre o próprio endereço (192.31.65.7) com a máscara de rede (255.255.255.0). Esta operação resulta na rede 192.31.65.0. A mesma operação é realizada com o IP de destino (192.31.62.8) e a máscara de rede da origem. Isso resulta na rede 192.31.62.0. Como as redes são diferentes, a máquina de origem envia um ARP request perguntando qual é o MAC do gateway (Ef=MAC máquina A, Ed=broadcast, IPf=192.31.65.7, IPd=IP do Gateway). O gateway responde a requisição replay (Ef=MAC gateway, IPf=IP Gateway, Ed=MAC máquina A, IPd=máquina A). A máquina de origem entrega os dados para o gateway. O gateway tem que descobrir onde está a máquina com o IP 192.31.62.8. Supondo que está numa rede diretamente conectada, o gateway faz um ARP request (Ef=end MAC do gateway da interface da rede 192.31.62.0, IPf=IP do gateway nesta interface, Ed=broadcast, IPd=192.31.62.8). A máquina B responde com um pacote ARP: (Ef=MAC gateway, IPf=IP Gateway, Ed=MAC máquina B, IPd=máquina B). O roteador entrega o pacote.

8. Explique o funcionamento dos algoritmos de roteamento menor caminho (shortest path), vetor de distância, estado de enlace (link state). Comente suas diferenças, vantagens e desvantagens comparando-os entre si. Quais desses algoritmos estão relacionados com roteamento estático e quais são relacionados com roteamento dinâmico ?

Menor caminho:

Algoritmo global, distribuído e estático

Neste algoritmo, é construída uma matriz de conectividade com os custos para sair de um nó e chegar a outro. O algoritmo calcula qual é o caminho mais curto para entre dois nós. Um desses algoritmos é o Dijkstra. Ele define para cada par de nó um custo a partir de um predecessor (p) considerado o melhor caminho. Inicialmente, os caminhos para vizinhos não adjacentes é $C(i,j)=\infty$. O par custo-predecessor (c,p) de o rótulo de um nó, que pode ser provisório ou permanente .

..

Desvantagem: Matriz de custo é calculada na inicialização do sistema e não prevê a atualização de novos nós.

Vetor distância:

Teoricamente, pode ser estático (nó envia seu vetor distância para os vizinhos na inicialização) ou dinâmico (enviar periodicamente, tipicamente é o que acontece ou quando houver uma modificação).

Exemplo de protocolo dinâmico: RIPv1, RIPv2.

Vetor de distância significa que as rotas são anunciadas como vetores de distância e direção. A distância é definida em termos de uma métrica como contagem de saltos ou atraso e a direção é dada simplesmente pelo roteador do próximo salto ou pela interface de saída. Os protocolos do vetor de distância normalmente usam o algoritmo Bellman-Ford para determinar a melhor rota.

Algoritmo:

Inicialmente, cada nó só possui informações sobre suas redes diretamente conectadas. O nó envia sua tabela para todos os vizinhos diretamente conectados. O nó então verifica a existência de novas rotas e atualiza sua tabela de roteamento. Na maior parte dos casos, a tabela completa é enviada periodicamente para os vizinhos. O algoritmo compara as tabelas recebidas pelos vizinhos e sua própria e inclui em sua tabela atual qual é a rota com menor custo considerando todas as possibilidades.

Vantagens:

- Implementação e manutenção simples. O nível de conhecimento para implementar e manter uma rede com um protocolo de vetor distância não é alto.
- Requisitos de recursos baixos: Os protocolos do vetor de distância normalmente não precisam

de grandes quantidades de memória para armazenar as informações. Eles também não precisam de uma CPU avançada. Dependendo do tamanho da rede e o endereçamento IP implementado, geralmente eles também não precisam de um alto nível de largura de banda de link para enviar atualizações de roteamento. No entanto, isso poderá se tornar um problema se você implementar um protocolo do vetor de distância em uma rede grande.

Desvantagens:

- Convergência lenta. O uso de atualizações periódicas pode causar uma convergência mais lenta. Mesmo se algumas técnicas avançadas forem usadas, como atualizações disparadas, que serão discutidas posteriormente, a convergência geral ainda será mais lenta em comparação com os protocolos de roteamento link-state.
- Escalabilidade limitada. A convergência lenta pode limitar o tamanho da rede porque redes maiores requerem mais tempo para propagar informações de roteamento.
- Loops de roteamento. Os loops de roteamento podem ocorrer quando as tabelas de roteamento inconsistentes não são atualizadas devido a uma convergência lenta em uma rede variável.
- Contagem para o infinito

Estado de enlace:

Roteamento dinâmico, global e distribuído.

Algoritmo:

Cada nó obtém informações das suas redes diretamente conectadas e envia um pacote Hello para cada vizinho diretamente conectado. Os vizinhos respondem com um pacote Hello. Os pacotes Hello são enviados constantemente. Cada nó cria um pacote chamado LSP com informações dos links diretamente conectados e envia os LSP para os vizinhos, exceto para o vizinho que enviou o LSP. Essas informações incluem ID do vizinho, largura de banda, tipo de link. Os nós enviam seus LSPs para todos os vizinhos que armazenam cada LSP em um banco de dados. OS LSP não precisam ser enviados periodicamente, apenas na inicialização e quando há uma mudança na topologia. Os nós executam o algoritmo e criam uma topologia da rede a partir dos LSPs armazenados no banco de dados. O algoritmo cria uma árvore de rotas baseado no custo.

Vantagem:

- Convergência rápida: Ao receberem um pacote link-state, os protocolos de roteamento link-state imediatamente inundam o LSP em todas as interfaces com exceção da interface da qual o LSP foi recebido. No protocolo de vetor distância as informações recebidas pelos vizinhos precisam ser processadas para atualizar a tabela de roteamento e só assim ser propagadas.
- Atualizações baseadas em eventos: LSP são enviados só quando há uma atualização na topologia.
- Design hierárquico: Utilizam conceitos de áreas. Possibilita melhor agregação de rotas e isolamento de problemas.

Desvantagens:

- Requisitos de processamento: Necessita de mais tempo de CPU para calcular o algoritmo SPF.
- Requisitos de largura de banda: Embora as atualizações sejam enviadas apenas em caso de alterações na topologia, em caso de redes instáveis, a largura de banda pode ser comprometida.
- Requisitos de memória: exigem mais memória para guardar o banco de dados link-states e árvore do SPF.

Fonte: Material Cisco CCNA.

9. Uma máquina em uma rede TCP/IP é caracterizada pelo endereço IP 143.54.13.100 e máscara 255.255.255.192 (considere classfull). Determine o número da rede, o endereço de broadcast (direto) dessa rede, o primeiro e último endereços IPs válidos para máquinas nessa rede. Fornecer a resposta na forma decimal, isto é, a.b.c.d.

Resposta:

255.255.255.192 == máscara 26.

143.54.13.64 -> endereço da rede

143.54.13.127 -> endereço de broadcast

143.54.13.65 -> primeiro endereço válido

143.54.13.126 -> último endereço válido

10. Você está administrando uma faixa de endereços classes C utilizando CIDR. Uma faixa de endereços disponíveis corresponde a rede 200.61.00.00/18. Três entidades solicitam endereços IP, a entidade A precisa de 1800 endereços, a entidade B de 800 endereços, e a entidade C, de 600 endereços. Quais seriam os endereços de rede e as máscaras de sub-rede que você atribuiria a entidade A, a entidade B e a entidade C com o uso de CIDR ? Quais são, com as respectivas máscaras, as redes livres após essa alocação ? Fornecer a resposta na forma decimal, isto é, a.b.c.d.

Entidade A: 1800 endereços -> 2048 -> máscara 21

Endereço de rede: 200.61.0.0

Máscara: 255.255.248.0

Entidade B: 800 endereços -> 1024 -> máscara 22

Endereço de rede: 200.61.8.0

Máscara: 255.255.252.0

Entidade C: 600 endereços -> 1024 -> máscara 22

Endereço de rede: 200.61.12.0

Máscara: 255.255.252.0

Redes livres: 200.61.16.0/20 -> máscara: 255.255.240.0

200.61.32.0/19 -> máscara: 255.255.224.0

11. Uma rede emprega roteamento por vetor de distância (Bellman-Ford, Ford-Fulkerson). Determine a tabela de roteamento do roteador Y considerando que neste instante o roteador Y recebe os seguintes vetores de distância de seus 4 vizinhos imediatos (A, I, H e K).

| | A | B | C | D | E | F | G | H | I | Y | K | L |
|------------|----|----|----|----|----|----|----|----|----|----|----|----|
| Roteador A | 0 | 12 | 25 | 40 | 14 | 23 | 18 | 17 | 21 | 9 | 24 | 29 |
| Roteador I | 24 | 36 | 18 | 27 | 7 | 20 | 31 | 20 | 0 | 11 | 22 | 33 |
| Roteador H | 20 | 31 | 19 | 8 | 30 | 19 | 6 | 0 | 14 | 7 | 22 | 9 |

| | | | | | | | | | | | | |
|------------|----|----|----|----|----|----|----|----|----|----|---|---|
| Roteador K | 21 | 28 | 36 | 24 | 22 | 40 | 31 | 19 | 22 | 10 | 0 | 9 |
|------------|----|----|----|----|----|----|----|----|----|----|---|---|

TAB. 1 – Os tempos são fornecidos em milissegundos (msec)

Sabe-se ainda que o roteador Y mediu os seguintes atrasos em relação a seus vizinhos : 8 msec para o roteador A, 10 msec para o roteador I, 12 msec para o roteador H e 6 msec para o roteador K.

Resposta 1:

Resposta 2:

| Destino | A + 8 | I + 10 | H + 12 | K + 6 | Custo | Próximo |
|---------|-------|--------|--------|-------|-------|---------|
| A | 8 | 34 | 32 | 27 | 8 | A |
| B | 20 | 46 | 43 | 34 | 20 | A |
| C | 33 | 28 | 31 | 42 | 28 | I |
| D | 48 | 37 | 20 | 30 | 20 | H |
| E | 22 | 17 | 42 | 28 | 17 | I |
| F | 31 | 30 | 31 | 46 | 30 | I |
| G | 26 | 41 | 18 | 37 | 18 | H |
| H | 25 | 30 | 12 | 25 | 12 | H |
| I | 29 | 10 | 26 | 28 | 10 | I |
| Y | - | - | - | - | - | - |
| K | 32 | 32 | 34 | 6 | 6 | K |
| L | 37 | 43 | 21 | 15 | 15 | K |

[CARISSIMI, p.223, figura 5.6]

12. Considerando uma rede IEEE 802.3, explique o por quê do protocolo ARP não ser capaz de identificar o endereço MAC de uma máquina destino, caso esta pertença a uma rede diferente da rede da máquina que executou o ARP. A solução empregada para resolver esse problema passa pelo emprego de default gateway e de ARP proxies. Explique o funcionamento de cada uma dessas soluções identificando como ele resolve o problema mencionado anteriormente.

Roteador não encaminha pacotes ARP em nível de enlace.

A comunicação de fato entre duas máquinas ocorre em nível de enlace através dos endereços MACs que são escritos no quadro ethernet. A máquina de origem deve então fazer uma solicitação ARP questionando qual o MAC do IP de destino. Porém, máquinas em redes diferentes devem estar ligada por roteador(es) e um roteador não encaminha pacotes ARP em nível de enlace. A solução é utilizar uma default gateway ou um proxy ARP. Na primeira solução, a máquina de origem descobre (pela máscara de rede) que o destino não está na mesma rede e envia o pacote para o default gateway encaminhar para a rede de destino. Os roteadores modificam o quadro ethernet com o endereço MAC da interface de entrada como endereço de origem e o endereço MAC na interface de saída como endereço de destino. No enlace final, o roteador faz uma requisição ARP em broadcast para encontrar o destino. No caso do proxy ARP, a máquina de origem não tem um gateway default configurado e envia um ARP em broadcast. O roteador percebe que a rede de destino não é a mesma da origem e

responde a solicitação ARP como se fosse a máquina destino. O proxy ARP também modificará os campos do quadro Ethernet de endereço MAC de origem e destino, conforme descrito para o default gateway. Desta forma, a máquina de origem nunca saberá o MAC da máquina de destino.

13. Qual a quantidade máxima de bits do **sufixo de uma rede IP classe C que pode ser utilizada para definir sub-redes? JUSTIFIQUE sua resposta.**

Uma classe C contém 8 bits no sufixo. A quantidade máxima de bits utilizadas para definir subredes é

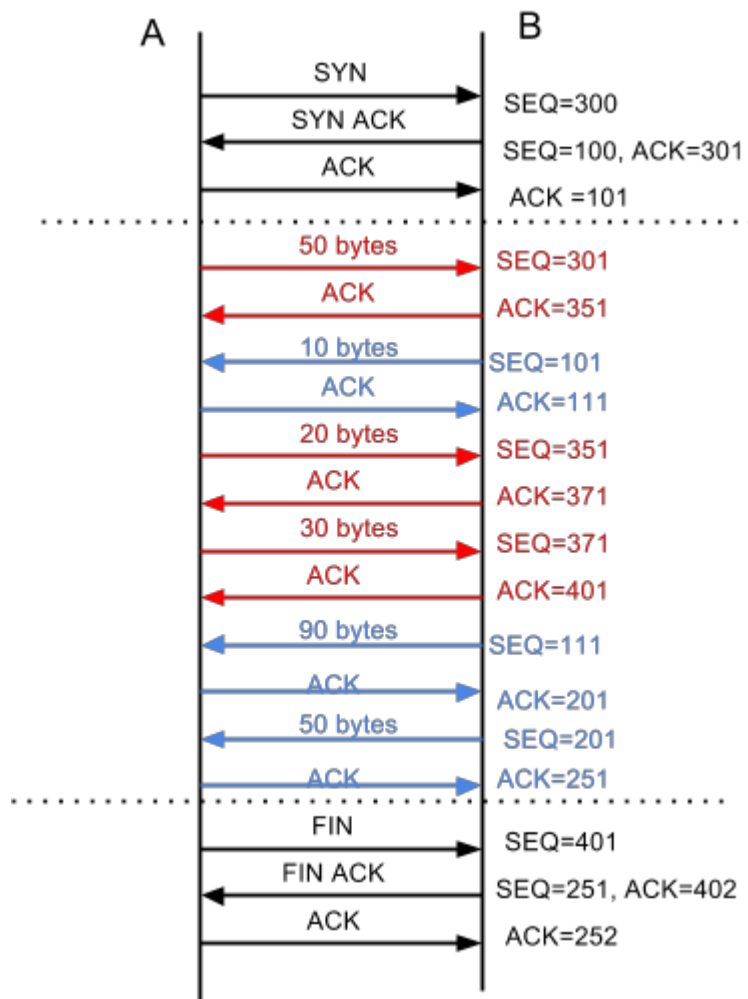
6. Sobram 2 bits para definir *hosts*. Isso resulta em 4 endereços: o de rede, o de broadcast e mais 2.

[\[http://pt.wikipedia.org/wiki/M%C3%A1scara_de_rede#M.C3.A1scaras_de_Subrede\]](http://pt.wikipedia.org/wiki/M%C3%A1scara_de_rede#M.C3.A1scaras_de_Subrede)

14. Supondo que duas máquinas, A e B, através de uma conexão TCP, desejam trocar entre si o conjunto de dados abaixo :

- Máquina A envia 50 bytes de dados para a máquina B ;
- Máquina B envia 10 bytes de dados para a máquina A ;
- Máquina A envia 20 bytes de dados para a máquina B ;
- Máquina A envia 30 bytes de dados para a máquina B ;
- Máquina B envia 90 bytes de dados para a máquina A ;
- Máquina B envia 50 bytes de dados para a máquina A ;

Desenhe de forma esquemática a sequência de mensagens trocados entre essas duas máquinas, incluindo as de abertura e encerramento de conexão. Supor que a máquina A solicita a abertura e o encerramento da conexão. Considere que o número de sequência proposto por A seja 300 e que o número de sequência proposto por B seja 100. Deixe claro, para cada mensagem trocada, incluindo o estabelecimento e o encerramento de conexão, o número de sequência dos dados (SEQ), o número de sequência do ACK, e os flags utilizados (SYN, ACK, FIN).



OBS:

1. O próximo SEQ (Número de Sequencia) do *transmissor* deve ser *igual* ao ACK recebido anteriormente. No exemplo: Como na primeira transmissão $SEQ_A = 301$, $ACK_B = 351$; então o próximo SEQ_A será 351.
2. Os pacotes SYN e FYN não tem dados no *payload*, mas consomem um número de sequência.
3. O ACK pode ser enviado via *piggybacking*, como foi feito durante o *3-way handshake* (SYN ACK) e durante a finalização (FYN ACK).

15. Explique como um processo cliente consegue localizar e acessar um processo servidor em uma máquina remota utilizando o protocolo TCP/IP. Em que sua resposta seria modificada caso o protocolo utilizado fosse UDP/IP ?

Inicialmente, o processo cliente utiliza o protocolo **DNS** para resolução do nome de host em um número de IP para localizar a **máquina** do servidor, caso o acesso seja por um nome de host (uma outra possibilidade seria o processo cliente fornecer diretamente o endereço de IP da máquina destino, não havendo assim a necessidade da utilização do protocolo **DNS**).

Juntamente com o endereço de IP do servidor, o processo cliente informa a **Porta** de destino para localização do **processo** servidor na **máquina** anteriormente obtida.

A partir da informação da **máquina** e da **porta** de destino, o processo cliente pode iniciar uma conexão com o processo servidor, utilizando-se do protocolo TCP/IP. Antes da criação da conexão, o processo cliente pode escolher uma porta de origem para a comunicação e, caso não o faça, o

sistema operacional, ao qual se encontra o processo cliente, escolhe aleatoriamente uma porta de origem a ser utilizada para a criação da conexão.

Definidas as portas de origem e destino, bem como os endereços de IPs de origem (IP da máquina cliente) e destino, o processo cliente inicia a conexão com o processo servidor e, a partir daí, apenas transfere os dados, com todas as garantias que um serviço orientado à conexão garante.

Caso fosse utilizado o UDP

Nessa situação, a principal diferença é o estabelecimento de conexão que, no UDP, **não ocorre**, já que ele é um protocolo dito não confiável e não fornece nenhuma garantia de entrega, sem duplicidade de pacotes, ou ainda, a manutenção da ordem de pacotes. No UDP, basta o processo cliente, a partir da obtenção das informações de IP e porta já descritas anteriormente, enviar e receber dados para o processo servidor.

16. Responda :

A) Em relação a fragmentação (no nível de rede), explique quais as razões que justificam a decisão da remontagem dos fragmentos ser feita no destino final e não nos nós intermediários.

Na remontagem nos nós intermediários, roteador precisa guardar fragmentos no buffer e saber quando recebeu todas as partes. Além disso, as rotas dos fragmentos não podem ser distintas causando uma perda considerável no desempenho.

A principal vantagem da remontagem no destino final é que os roteadores precisam realizar menos trabalho.

B) Se a remontagem fosse feita nos nós intermediários (roteadores) qual o impacto que isso traria para serviços de rede não orientados a conexão como o IP.

O maior problema da remontagem de serviços não orientados a conexão seria a perda desempenho, pois na remontagem nos nós intermediários os fragmentos precisam seguir a mesma rota e precisam ser guardados em um buffer.. Em aplicações como VOIP (voz sobre IP) poderia gerar atrasos que afetariam o serviço.

17. Compare o algoritmo de roteamento por vetor de distância com o algoritmo de estado de enlace. Aborde, entre outros pontos, questões relacionadas com o tipo de informação trocada, quantidade de dados transmitidos, forma com que o caminho (roteamento) é escolhido, problemas de convergência. Forneça ainda exemplos de protocolos que utilizam cada um desses algoritmos.

| | Vetor distância | Estado de Enlace |
|-------------------------------------|--|---|
| Tipo de informações trocadas | Tabelas de roteamento inteiras são trocadas apenas entre vizinho adjacentes, geralmente, periodicamente. A informação enviada é o custo | Além dos pacotes Hello, os pacotes LSP com o estado das redes conectadas diretamente são enviadas para todos os vizinho que repassam de |

| | | |
|---|---|--|
| | (estimado) $v(i, d)$ para todos os nós. | vizinho em vizinho sempre que há uma alteração na topologia da rede. A informação enviada é o custo do nó para cada um de seus vizinhos imediatos |
| Quantidade de dados transmitidos | Muitos. Toda a tabela de roteamento é transmitida | Poucos, apenas na inicialização ou quando há uma mudança de topologia. Apenas a alteração é transmitida. |
| Como caminho é escolhido | Roteador compara rotas com rotas aprendidas por vizinhos e escolhe a com menor número de saltos (geralmente é essa a métrica) executando o algoritmo de <i>Bellman-Ford</i> . | Roteadores guardam LSP recebidos em um banco de dados. O Algoritmo SPF é executado para escolher a rota com melhor métrica (geralmente o custo) e constroi árvore SPF. |
| Convergência | Lenta. Os roteadores recebem a tabela de roteamento dos vizinhos e tem que executar o algoritmo para escolher o melhor caminho para atualizar a tabela de roteamento. Envio geralmente é periódico. | Rápido. LSPs são enviados e repassados assim que chegam ao roteador. |
| Exemplos | RIPv1, RIPv2, IGRP, EIGRP (dois últimos proprietários da Cisco) | OSPF e IS-IS |

18. Qual a quantidade máxima de sub-redes que se pode definir para uma rede IP classe C? JUSTIFIQUE sua resposta.

Uma rede classe C tem 256 endereços. Cada rede tem que ter, no mínimo, 4 endereços. $256/4 = 64$ sub-redes.

19. Compare o algoritmo de roteamento por vetor de distância com o algoritmo de estado de enlace. Aborde, entre outros pontos, questões relacionadas com o tipo de informação trocada, quantidade de dados transmitidos, forma com que o caminho (roteamento) é escolhido, problemas de convergência. Caracterize se é tipo global ou local, centralizado ou distribuído e discuta quais os principais problemas e soluções.

Olhar 17

| | Vetor distância | Estado de Enlace |
|-------------------------------|---|--|
| Caracterização | Local (cálculo a partir do conhecimento parcial da rede) Distribuído | Global (Conhece toda a topologia da rede) Distribuído |
| Principais problemas e | Contagem ao infinito. Solução: | Grande uso de CPU e memória. |

| | | |
|----------|--|--|
| soluções | métrica infinita. Horizonte dividido e inversão envenenada. Convergência lenta | Roteadores podem receber LSPs duplicados. Solução: usar número de sequência e idade. Elimina também laços de roteamento. |
|----------|--|--|

20. Uma máquina A se deseja comunicar com uma máquina B que está em uma sub-rede diferente. Existe apenas um roteador R separando essas duas sub-redes. Dê a sequência de trocas de PDUs, incluindo as requisições ARP, envolvidas nessa comunicação. Para cada PDU especificar os endereços MAC e IP de origem e de destino. Os equipamentos dessa rede (máquinas A e B) estão configuradas para empregar default gateway e não há nenhuma informação mantida em caches ARP.

IP route 1: IP da interface na rede que liga máquina A

IP route 2: IP da interface na rede que liga máquina B

MAC route 1: MAC da interface na rede que liga máquina A

MAC route 2: MAC da interface na rede que liga máquina B

1) ARP request:

| MAC ORIGEM | IP ORIGEM | MAC DESTINO | IP DESTINO |
|------------------|-----------------|-------------|------------|
| MAC _A | IP _A | BROADCAST | IP route 1 |

2) ARP reply:

| MAC ORIGEM | IP ORIGEM | MAC DESTINO | IP DESTINO |
|-------------|------------|------------------|-----------------|
| MAC route 1 | IP route 1 | MAC _A | IP _A |

2) Pacote:

| MAC ORIGEM | IP ORIGEM | MAC DESTINO | IP DESTINO |
|------------------|-----------------|-------------|-----------------|
| MAC _A | IP _A | MAC route 1 | IP _B |

3) ARP request:

| MAC ORIGEM | IP ORIGEM | MAC DESTINO | IP DESTINO |
|-------------|------------|-------------|-----------------|
| MAC route 2 | IP route 2 | BROADCAST | IP _B |

4) ARP reply:

| MAC ORIGEM | IP ORIGEM | MAC DESTINO | IP DESTINO |
|------------------|-----------------|-------------|------------|
| MAC _B | IP _B | MAC route 2 | IP route 2 |

5) Pacote:

| MAC ORIGEM | IP ORIGEM | MAC DESTINO | IP DESTINO |
|-------------|-----------------|------------------|-----------------|
| MAC route 2 | IP _A | MAC _B | IP _B |

21. Responda :

A) Por que é necessário usar um mecanismo do tipo three way handshake invés de two way handshake para estabelecer conexões TCP? Quais são os problemas que o three way handshake resolve que o two way handshake não resolve?

Resposta 1:

a) O problema do two way handshake é que quando chega um segmento CONNECTION REQUEST contendo um número de sequência inicial, se é uma duplicata de uma conexão recente. No mecanismo three way handshake, os dois pares verificam se a conexão está realmente ativa.

O three way handshake resolve o problema dos pacotes duplicados atrasados. Também há o problema da segurança...

Problema que three way handshake resolve: duplicatas atrasadas.

[TANENBAUM5PT] pág 323

Resposta 2:

a) É necessário o 3-way handshake pois nesse método ambas as partes confirmam a conexão, no 2-way handshake, as partes não precisam confirmar a conexão, e cada uma assume que a conexão está ativa após o envio do seu próprio SYN.

O principal problema que o 3-way handshake resolve é o de *conexões duplicadas*, por exemplo, sejam duas máquinas A e B realizando uma conexão através do 2-way handshake, a máquina A envia um SYN_A X para B, B recebe e envia um SYN_B Y para A, B agora encontra-se com a conexão aberta, mas o pacote SYN_B Y é perdido e A “pensa” que não houve conexão, então por timeout reenvia SYN_A X novamente, então B assume uma nova conexão. Outro problema resolvido é o de *perda de pacotes*: usando o mesmo exemplo anterior, caso B começasse a enviar dados para A os mesmos seriam perdidos, pois B considera que há conexão ativa, enquanto A não possui conexão.

B) Descreva as T-PDUs trocadas no encerramento de conexões de forma simétrica, assimétrica e abrupta?

b) “No encerramento **assimétrico**, qualquer um dos lados pode emitir uma primitiva DISCONNECT, fazendo com que uma TPDU DISCONNECT seja enviada à entidade de transporte remota. Quando essa TPDU chega a seu destino, a conexão é encerrada

No encerramento **simétrico**, cada direção da comunicação é encerrada em separado e de forma independente da outra. Quando uma das partes executa uma primitiva DISCONNECT, isso significa que não há mais dados para enviar, mas ainda é possível receber dados enviados pela outra parte. Nesse modelo, a conexão só é encerrada quando os dois lados tiverem executado uma primitiva DISCONNECT.” <http://pt.scribd.com/doc/96361211/69/Encerramento-de-uma-Conexao>

No encerramento **abrupto**, uma TPDU ABORT é enviada e quem abortou a conexão não recebe mais dados.

C) O que é TSAP? Para que serve?

c) TSAP (Transport Service Access Point) são portas utilizadas para definir endereços na camada de transporte para identificar um processo de aplicação que deseja estabelecer uma conexão com outro.

[TANENBAUM5PT] pág 319

22. Qual a quantidade máxima de bits de um sufixo que pode ser empregado para definir sub-redes em uma rede IP? JUSTIFIQUE sua resposta.

Resposta 1:

30 bits. Precisa de, no mínimo 1 endereço IP para identificar a rede, 1 endereço de broadcast e 1 endereço para o host. Isso é conseguido com uma máscara 30 que resulta em 4 endereços.

Resposta 2:

Como estamos interessados em *subredes* estamos trabalhando com o sistema *classfull*. Desse modo só podemos definir subredes a partir da Classe A, a qual possui um prefixo com 8 bits. Também é necessário para subredes que, além do endereçamento de hosts, tenhamos, pelo menos, 1 endereço de rede e 1 endereço de broadcast, ou seja, precisamos de mais de 2+ endereços para hosts (contabilizados o de rede e o de broadcast), para isso temos que usar 2 bits do endereço IP (4 endereços). Desse modo o sufixo para definir subredes, a partir da Classe A, com 2 bits reservados para os endereços de rede e broadcast, deve ser de, no máximo 22 bits, resultando em $2^{22} - 2$ subredes.

23. O que é CIDR ? Como esse esquema auxilia na solução do problema de esgotamento de endereços IP ? Faça um exemplo de alocação de blocos de endereço IP baseado em CIDR.

Explique ainda o que se entende por máscara mais e menos restritiva ? Como essas máscaras são empregadas ?

CIDR (Roteamento Inter-Domínio sem Classes) é um esquema de atribuição de IPs que , diferentemente do Classfull, aloca endereços por demanda, utilizando-se a noção de blocos de endereços. Ele auxilia na redução de desperdício de endereços de IP (se comparado ao classfull) ,porém necessita de mecanismo diferentemente de roteamento que, basicamente, consiste na utilização de uma máscara de tamanho variável , para cada bloco de endereços.

Exemplo de alocação: Alocação de um bloco com 10 endereços.

A alocação de um bloco de 10 endereços consiste na utilização de 4 bits para a numeração de cada endereço. Sendo assim, temos a alocação dos 10 endereços, porém com uma sobra de $16 - 2 - 10 = 4$ endereços. Observe que esse esquema sem classe não garante 100% de aproveitamento dos blocos, podendo gerar desperdício de endereços na rede. Obviamente , o desperdício é muito menor se comparado ao *Classfull*, que , nesse exemplo, seria de $256 - 2 - 10 = 244$ endereços.

Uma máscara mas restritiva, restringe um endereço de rede à uma quantidade menor de bits, sendo útil num esquema de roteamento hierárquico, pois auxilia na definição de rotas, 'roteando' pacotes para destinos ao qual possui informação sobre rotas mais específicas para o destino real do pacote.

Uma máscara menos restritiva funciona de maneira oposta, ela permite identificar com mais precisão o destino de um determinado pacote. Por exemplo, uma máscara /32, presente em uma tabela de roteamento da internet, para um dado IP_A permite identificar diretamente a rota para a máquina A.

Resposta 2

O CIDR é uma convenção global para atribuição de endereços, que define como a IANA, suas agências membro e os ISPs devem atribuir o espaço de endereçamento IPv4 global e único a organizações individuais. Tem dois objetivos principais: Primeiro: sua política diz que as opções para atribuição de endereços deve ajudar no processo de sumarização de múltiplos números de redes em uma única

entidade de roteamento, reduzindo o tamanho das tabelas de roteamento. O segundo objetivo é permitir que os ISPs atribuam a seus clientes faixas de IPv4 em tamanhos diferentes de redes classes A, B e C inteiras, reduzindo o desperdício.

Fonte: CCNA cisco

24. No estabelecimento de uma conexão foi visto em aula o por quê da necessidade de se realizar um three way handshake ao invés de empregar um esquema two way handshake. Explique COM CLAREZA o problema que existe no two way handshake e como ele é resolvido no three way handshake. Comente ainda em sua resposta a importância do tempo de vida do número de sequência de um segmento e como ele pode afetar o estabelecimento de uma conexão e a fase de transferência de dados.

Resposta 1:

No *two way handshake*, uma máquina A, ao iniciar uma conexão com a máquina B, solicita um início de conexão. A máquina B, ao receber a solicitação de A, envia uma confirmação para A e assume o início da conexão. A máquina A, por sua vez, ao receber a confirmação, assume o início da conexão, e, a partir daí, a conexão entre as máquinas A e B está estabelecida.

O principal problema desse mecanismo é que a máquina B assume o início da conexão sem confirmação de que a máquina A recebeu a sua primeira confirmação. Sendo assim, caso a confirmação ACK da máquina B fosse perdida, ela estaria com uma conexão aberta com A, enquanto A, por não receber o ACK de B, assumiria que a conexão foi encerrada.

A correção desse problema é realizada com o *three way handshake*, o qual difere justamente na necessidade de uma segunda confirmação por parte de A para B. Sendo assim, A, assim como no *two way*, continua assumindo o início da confirmação somente após o recebimento da confirmação por B, porém, B só assume o início da conexão, somente após receber uma segunda confirmação por A.

O tempo de vida de um determinado segmento é importante no sentido que o atraso de um segmento com número X em uma conexão não chegue atrasado em uma segunda conexão (mesma máquina de origem e destino, nas mesmas portas de origem e destino da conexão anterior), sendo aceito erroneamente pela máquina receptora (uma vez que ela espera segmentos pela mesma origem que originou o segmento X). A diminuição do tempo de vida do segmento X evitará que ele seja roteado entre diversas máquinas e chegue atrasado ao seu destino, pois esse será decrementado a cada novo salto de roteamento, sendo descartado assim que o tempo atingir seu limite.

No que diz respeito ao estabelecimento da conexão, o número de sequência inicial dessa conexão é definido aleatoriamente. Cada segmento ao ser enviado possui um tempo de vida que, junto com a aleatoriedade da escolha dos números de segmento inicial, evitam o recebimento de um pacote 'fantasma' por parte de um receptor.

25. O que é proxy ARP? Como funciona o proxy ARP? Qual(ais) a(s) opção(ões) que existe(m) em uma rede caso não se use proxy ARP?

Resposta:

O *proxy ARP* é um método do protocolo ARP (pertencente à *Camada de Rede*) que faz resolução de endereços MAC (descobre o endereço MAC a partir de um endereço IP). Este método é usado principalmente na *entrega indireta*, ou seja, ele é usado para descobrir um endereço MAC de um IP de destino que não está na mesma rede do endereço de origem usando um gateway.

No método proxy ARP, o sistema de origem, após não encontrar uma correspondência de mapeamento entre o *Endereço IP-Endereço MAC* em sua cache ARP, envia em broadcast um *ARP Request*. Todos os dispositivos da rede, incluindo o gateway da rede, recebem essa requisição e analisam o endereço IP de destino. Aquele cujo endereço IP for igual ao endereço IP destino da requisição responde com

seu endereço MAC com um *ARP Reply*. Porém, se o endereço IP de destino não pertencer à mesma rede que a origem, quem responde com seu endereço MAC é o gateway. Portanto, qualquer requisição ARP com endereço IP de destino diferente da rede de origem será resolvida para o endereço MAC do gateway da rede. É importante ressaltar que esse método não realiza o procedimento do “E” lógico para determinar se origem e destino estão na mesma rede (como no caso de uma *entrega direta*).

Caso não se use o *proxy ARP*, podemos usar a *entrega direta* e, no caso de uma *entrega indireta*, podemos usar os métodos ARP *por anúncio* e *por configuração*. Na *entrega direta* a máquina de origem verifica se está na mesma rede que a máquina de destino, comparando o resultado do “E” lógico entre a máscara e seu próprio endereço IP é igual ao resultado do “E” lógico entre a máscara e o endereço IP de destino, se ambas as máquinas estiverem na mesma rede a máquina de origem faz um *ARP Request* então a máquina de destino faz um *ARP Reply* informando qual o seu MAC. A *entrega indireta* ocorre quando o endereço IP da origem não está na mesma rede do endereço IP do destino, nesse caso a máquina de origem deve fazer um *ARP Request* para o gateway da rede e encaminhar o datagrama para ele. No método ARP *por anúncio* o gateway da rede envia periodicamente uma mensagem a todos os dispositivos informando sua existência e seu endereço MAC (pode ser usado para isso o *ARP Reply*), se a máquina de origem determinar que o endereço IP de destino pertence à outra rede (aplicando a máscara, conforme explicado na entrega direta) ele envia o datagrama usando o endereço MAC do gateway. No método ARP *por configuração* cada dispositivo da rede deve ser configurado com o *endereço IP* do gateway, desse modo, o equipamento de origem, ao descobrir que o IP de destino pertence a outra rede, realiza um *ARP Request* usando o endereço IP do gateway pré-configurado.

[CARISSIMI, Páginas 243 e 244]

26. Porque o tempo máximo de duração de um segmento (tempo de vida) deve ser longo o suficiente para assegurar que não apenas o segmento mas também todas as suas confirmações tenham desaparecido da rede? Comente CLARAMENTE como ele pode afetar o estabelecimento de uma conexão e a fase de transferência de dados.

(Exercício 6.5 Tanenbauh 4 ed.)

É a mesma idéia dos pacotes fantasmas, mas aplicado ao pacote SYN. Por exemplo o problema que pode ocorrer com um tempo de vida muito curto pode afetar conexões muito longas (com mais de um dia, por exemplo). Com um tempo de vida muito longo poderemos ter um problema de dupla conexão, da seguinte maneira: sejam duas máquinas A e B, A inicia a conexão com B enviando um SYN⁽¹⁾, esse pacote se “perde” na rede e fica tráfegando; então é acionado o *timeout* de A e ela reenvia o SYN⁽²⁾, B responde, é feito o 3-way handshake e a conexão inicia, como a troca de informações é muito longa o número de sequência acaba reiniciando, a conexão é encerrada normalmente; depois do encerramento da conexão, o pacote SYN⁽¹⁾ que estava “perdido” na rede acaba chegando na máquina B e é aberta uma nova conexão, que não deveria ser aberta. O *tempo de vida* do pacote deve ser calculado de forma a evitar que essas situações aconteçam.

27. A fragmentação e a remontagem de datagramas são tratados pelo IP e são invisíveis para o TCP. Isso significa que o TCP não tem que se preocupar com a chegada de dados na ordem correta? JUSTIFIQUE CLARAMENTE seu ponto de vista.

(Exercício 6.20 Tanenbauh 4 ed.)

Embora cada datagrama chegue intacto, é possível que os datagramas cheguem na ordem errada; assim, o TCP tem de estar preparado para montar novamente as peças de uma mensagem de maneira apropriada.

28. Um roteador tem as seguintes entradas (CIDR) em sua tabela de roteamento :
Rede destino máscara Next hop

135.46.56.0 255.255.252.0 Interface 0 135.46.56.0 - 135.46.59.255

135.46.60.0 255.255.252.0 Interface 1 135.46.60.0 - 135.46.63.255

192.53.40.0 255.255.254.0 Interface 2 192.53.40.0 - 192.53.41.255

Padrão (default) 0.0.0.0 Interface 3

Para qual "próximo hop" o roteador encaminhará os datagramas que apresentam como destino os seguintes endereços IP :

135.46.63.10, -> interface 1

135.46.57.14, -> interface 0

135.46.52.2, -> interface 3

192.53.40.7 -> interface 2

192.53.56.7. -> interface 3

29. Explique DETALHADAMENTE o funcionamento do roteamento por estado de enlace? Que vantagens ele apresenta em relação ao vetor de distância? Ele é do tipo global ou local? Forneça CLARAMENTE qual a razão de haver os campos número de sequência e idade em PDUs de um protocolo estado de enlace. Porque um ou outro, isoladamente, não é suficiente?

Funcionamento: vide questão 8.

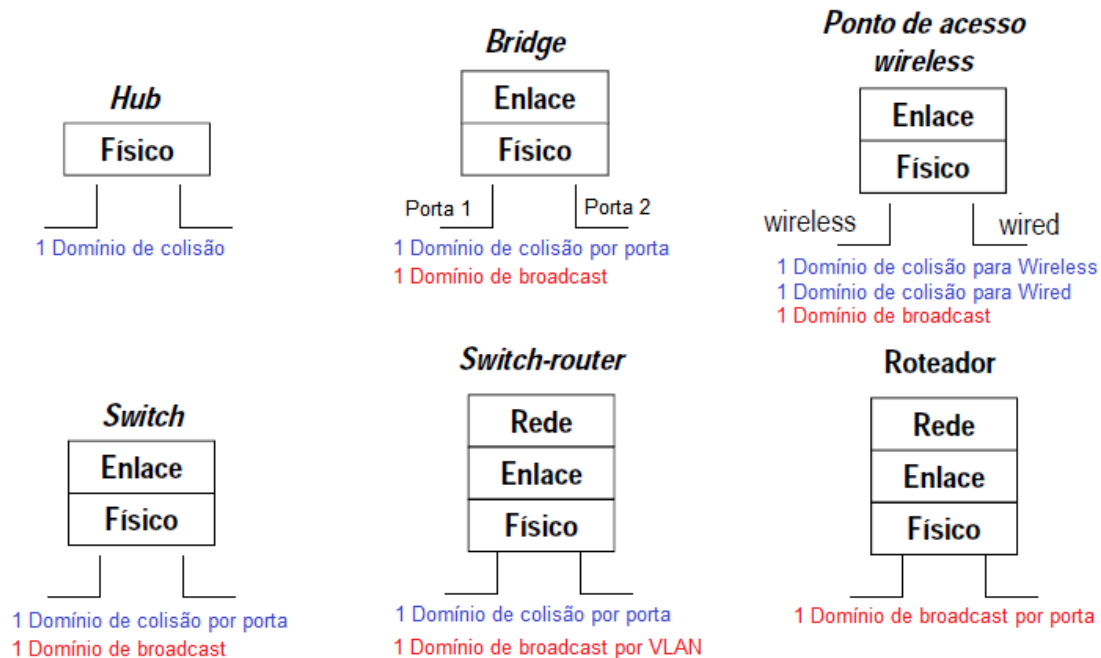
Global.

Os roteadores executando o algoritmo de estado de enlace enviam pacotes informando o estado de enlace por inundação, broadcast ou multicast. Esses pacotes recebidos de outros roteadores são reenviados para todas as outras interfaces. Em algum momento, pode ocorrer a chegada de pacotes duplicados. O problema da duplicação pode ser resolvido identificando o pacote com um número de sequência que é incrementado pelo roteador que o gerou a cada novo pacote gerado. Desta forma, o roteador que recebeu o pacote guarda a informação {origem, número de sequência} e descarta pacotes com número de sequência menor. O problema é que esse número de sequência é finito e ao atingir o último número, retorna a contagem inicial. Os roteadores então descartariam o pacote com a informação mais atual porque ele possui um número de sequência menor. Um roteador, quando é inicializado, também numera os pacotes a partir do zero. A solução adotada para evitar o descarte errado de pacotes é incluir uma data de validade para o armazenamento do pacote, por exemplo, o pacote vale por 10 segundos. Após esse tempo, o próximo pacote será aceito até que apareça um pacote com um número de sequência maior ou que seu tempo de validade expire. [CARISSIMI] pág 226-228

30. Existem 20 PCs na sua rede, sendo que 18 deles possuem interfaces IEEE 802.3 e dois possuem IEEE 802.11. Os equipamentos de interconexão de redes (hub, switches, roteadores etc) possuem interfaces IEEE 802.3. Cinco PCs estão conectados em um hub e cinco estão conectados em outro hub. Cada hub está conectado a um switch diferente e ambos switches estão conectados a diferentes roteadores. Os roteadores estão ligados entre si por uma ponte (bridge). Dois PCs são equipados apenas com placas wireless e usam um ponto de acesso (access point) que está ligado em uma porta de um dos switches. Os restantes 8 PCs estão distribuídos em portas dos switches. Quantos domínios de colisão e de broadcast existem nessa configuração, respectivamente?

Colisão: 15

Broadcast: 3 domínios (S1-R1, R1-R2, R2-S2-AP)



Fonte: [Aula 13, Slide 23]

Ilustração do exercício:

https://docs.google.com/drawings/d/19ZsTd37yx_Oj1PfiPA7K6431d-slRMeHljR9lawB5W8/edit

31. Quais problemas do algoritmo de vetor de distância são resolvidos ou deixam de existir com um algoritmo de estado de enlace? EXPLIQUE como esses problemas são resolvidos.

- **Convergência lenta:** Ao receberem um pacote link-state, os protocolos de roteamento link-state imediatamente inundam o LSP em todas as interfaces com exceção da interface da qual o LSP foi recebido. No protocolo de vetor distância as informações recebidas pelos vizinhos precisam ser processadas para atualizar a tabela de roteamento e só assim ser processadas para atualizar a tabela de roteamento e só assim ser propagadas.

A rápida convergência também resolve os seguintes problemas

- **Escalabilidade limitada.** A convergência lenta pode limitar o tamanho da rede porque redes maiores requerem mais tempo para propagar informações de roteamento.
- **Loops de roteamento.** Os loops de roteamento podem ocorrer quando as tabelas de roteamento inconsistentes não são atualizadas devido a uma convergência lenta em uma rede variável.

O conhecimento da topologia da rede resolve o seguinte problema.

- **Contagem ao infinito:** Deixa de existir.

32. No mínimo, quais parâmetros de uma rede TCP/IP devem estar corretamente configurados em um computador para que este tenha acesso a serviços de redes em redes externas a sua ? JUSTIFIQUE a necessidade de cada um desses parâmetros.

- **IP:** Para ter uma identificação na rede
- **Máscara de rede:** para poder comparar se o IP de destino pertence ou não a mesma rede.
- **Gateway default:** para enviar os pacotes ao endereço externo e assim ele possa ser roteado até chegar a rede do destinatário. Se estive utilizando um proxy ARP, não é necessário

- **Servidor de DNS:** Para resolver IP em nomes simbólicos. Sem ele, a rede externa vai continuar acessível, mas somente com o uso de IPs.

33. Por que os computadores de uso pessoal (desktop) de uma rede possuem tabelas de roteamento se eles normalmente têm apenas uma interface de rede ? JUSTIFIQUE a sua resposta.

Qualquer dispositivo de rede TCP/IP toma decisões de roteamento. A tabela de roteamento é criada automaticamente baseada nas configurações de rede do pc. Uma entrada muito importante nesta tabela é o gateway default, que é para onde o tráfego que não pertence a rede local é encaminhado.

Exemplo:

Tabela de Roteamento IP do Kernel

| Destino | Roteador | MáscaraGen. | Opções | Métrica | Ref | Uso | Interface |
|---------|---------------|-------------|--------|---------|-----|-----|-----------|
| 0.0.0.0 | 192.168.1.254 | 0.0.0.0 | UG | 0 | 0 | 0 | wlan0 |

34. Um aluno de INF01154 estudando para a prova se deparou com o seguinte dilema : "se tanto o UDP como o IP oferecem serviços não orientados a conexão, porque o UDP existe?". Esse mesmo aluno defende a tese que teria sido suficiente deixar os programas de usuário (aplicativos) enviarem seus dados usando diretamente datagramas IP. Esse colega hipotético está certo ou errado em sua tese? Responda porque o UDP deve ou não existir? JUSTIFIQUE sua resposta.

Errado. Os pacotes IP contêm endereços IP que especificam uma máquina de destino. Quando o pacote chegasse ao destino seria preciso saber a qual processo entregar. O UDP contém em seu cabeçalho a informação qual porta de destino e assim o processo remoto é identificado. O protocolo UDP é responsável pela comunicação fim-a-fim entre dois processos. O IP não permite a troca de dados entre processos, pois, como já dito seus datagramas possuem apenas o endereço IP do host, não tendo a indicação do endereço do processo (que é a porta).

35. Um administrador de rede está configurando regras em um firewall de filtro de pacotes para evitar que máquinas externas abram conexões TCP em máquinas internas a rede. Que tipo de PDUs TCP devem ser descartadas por esse conjunto de regras? Por tipo de PDU TCP entende-se: (a) se elas são provenientes da rede interna ou da rede externa desse firewall e (b) qual, ou quais flags do cabeçalho estão posicionados. Responda na forma {IP origem, IP Destino, Porta origem, Porta destino, flags}. Considere que a rede interna a ser protegida é a 200.20.20.0/24 e use o caractere "*" para denotar qualquer endereço, qualquer porta etc.

Para que máquinas externas à rede não possam abrir conexões TCP para a rede interna deve-se bloquear as PDUs entrantes no Firewall (que vem da rede externa) com apenas a flag de SYN, pois uma PDU apenas com SYN indica a abertura de conexão. No 3-way handshake, no estabelecimento de conexão por uma máquina da rede interna (envio de SYN), a máquina da rede externa irá responder com uma PDU com SYN+ACK, que no caso não será bloqueada pelo firewall.

{*, 200.20.20.0/24, *, *, SYN}

Flag SYN: Pedido de abertura de conexão.

36. Um administrador de redes necessita dividir uma faixa de endereçamento classe C (200.30.40.0/24) em cinco sub-redes. Qual, ou quais, máscara(s) deve(m) ser configurado(s) nas máquinas de cada uma dessas cinco sub-redes? Defina ainda o endereço de broadcast de cada uma dessas redes. Considere classless.

Resposta:

Rede 1: 200.30.40.0/27 - mask: 255.255.255.224 - broadcast: 200.30.40.31
Rede 2: 200.30.40.32/27 - mask: 255.255.255.224 - broadcast: 200.30.40.63
Rede 3: 200.30.40.64/27 - mask: 255.255.255.224 - broadcast: 200.30.40.95
Rede 4: 200.30.40.96/27 - mask: 255.255.255.224 - broadcast: 200.30.40.127
Rede 5: 200.30.40.128/25 - mask: 255.255.255.128 - broadcast: 200.30.40.255

37. Um roteador tem as seguintes rotas em sua tabela de roteamento :

| Rota | interface |
|-------------|-----------|
| 0.0.0.0/0 | e1 |
| 10.0.0.0/8 | e0 |
| 10.0.0.0/16 | e1 |
| 10.0.1.0/24 | s0 |
| 10.1.1.0/24 | s1 |
| 10.1.0.0/16 | s0 |
| 10.1.0.0/24 | e1 |
| 10.1.1.1/32 | s2 |

TAB. 2 – Tabela de roteamento

Um datagrama chega ao roteador com um endereço de destino igual a 10.0.4.1. Considerando que todas as redes de destino estão diretamente conectadas a este roteador, qual é a interface que o roteador usará para transmitir esse datagrama?

e1. Máscara /16 mais restritiva que /8.

38. Considere a Internet e seus diferentes protocolos. Uma máquina cliente está em uma rede A e solicita um serviço a um servidor que está em uma rede B. A máquina A possui todos os parâmetros mínimos necessários corretamente configurados mais o endereço IP do servidor de DNS de seu domínio. Supondo que você esteja capturando o tráfego na rede do cliente com um sniffer, liste, NA ORDEM CORRETA em que são capturados, TODOS os protocolos da camada de rede, de transporte e de aplicação quando o cliente for :

A) Um browser web em que se insere uma URL na forma http://www.fifa.com. Considere que este é o primeiro acesso que a máquina está realizando a rede e que não existe nenhuma informação armazenada em nenhum tipo de cache.

Aplicação:

DNS e HTTP

Transporte:

TCP/UDP, para cada conversa, tanto DNS como HTTP

Rede:

ARP e IP, para cada uma das solicitações da camada de transporte

Na ordem:

ARP: para resolver endereço do servidor de DNS. O servidor de DNS tem que resolver o nome www.fifa.com.

DNS: para resolver nome www.fifa.com

ARP: para encontrar o end MAC do default gateway

TCP: Para abrir uma conexão na porta 80 na máquina www.fifa.com

HTTP: para solicitar objetos no site www.fifa.com

B) Um MUA (Mail User Agent) que está sendo usado para enviar uma mensagem eletrônica para um destinatário que está no mesmo domínio administrativo do remetente da mensagem. O MUA possui configurado como servidor de e-mail a máquina smtp.acme.com e como servidor POP a máquina pop.acme.com. Considere que este é o primeiro acesso que a máquina está realizando a rede e que não existe nenhuma informação armazenada em nenhum tipo de cache.

Aplicação:

1)DNS: obtém IP do host smtp.acme.com

5)SMTP: transfere a mensagem para o servidor de envio

Transporte:

2)TCP/UDP: utilizado para a solicitação **DNS** anterior

6)TCP: Transferência da mensagem solicitada pelo SMTP

Rede:

3)ARP para obtenção do MAC do DNS especificado

4)IP para envio da mensagem de DNS para o servidor de DNS

7)ARP para obtenção do MAC do servidor de email

8)IP para envio da mensagem de para o servidor de email

Na Ordem....

ARP para obter o MAC do IP do servidor de DNS

DNS: obtém IP do host smtp.acme.com

ARP para obtenção do MAC do servidor de smtp.

TCP para abrir conexão com o servidor de e-mails

SMTP para enviar o e-mail.

39. Qual a razão da criação do ftp ativo ? Que problema do modo passivo ele resolve ?

Resposta 1:

O FTP necessita de duas conexões, uma para controle e outra para os dados. A conexão de controle é aberta sempre pelo cliente, geralmente, na porta 21 do servidor. No modo passivo, o servidor responde informando uma porta (aleatória) que o cliente deve abrir a conexão de dados e o cliente abre outra conexão com o servidor nessa porta especificada. No modo ativo, o cliente informa ao servidor uma porta e a conexão de dados é aberta pelo servidor nessa porta especificada pelo cliente. O problema do modo passivo é que o firewall que protege o servidor terá que desbloquear a porta aleatória escolhida pelo servidor (escolhida pelo Sistema Operacional), já no modo ativo como o servidor é quem abre a

conexão, o firewall não necessitará ser reconfigurado para abertura de portas aleatórias.

Fontes:

<http://www.juliobattisti.com.br/tutoriais/gersonkonnus/iis6004.asp>

http://www.pop-rs.rnp.br/~berthold/etcom/redes2-2000/trabalhos/FTP_EltonMarques.htm

<http://www.openbsd.org/faq/pf/pt/ftp.html>

40. Quais são as duas funções mais importantes da camada de rede em uma rede de datagramas como o IP?

Endereçamento lógico e roteamento.

41. Em um roteamento por estado de enlace, os pacotes de estado de enlace são distribuídos através de inundação (flooding). Explique como um roteador determina se um pacote é uma nova informação ou se ele é obsoleto.

São utilizados dois parâmetros: número de sequência, que é incrementado quando um novo pacote é criado e tempo de vida de um pacote, para evitar que o número se esgote ou que o roteador seja reiniciado e comece a contagem do 0, fazendo com que um pacote com a informação mais atual mas com o número de sequência menor seja erroneamente descartado.

Mais detalhes, vide questão 29.

42. Qual a diferença de procedimentos executados durante a resolução de endereços, isto é, tradução de endereços IP para endereços MAC, quando uma máquina está configurada em uma rede que utiliza default gateway e quando está em uma rede que usa proxy ARP?

Resposta 1:

Quando se usa o *default gateway*, o host tem em sua configuração o endereço IP deste gateway. Quando o host quer enviar um pacote para outro IP ele faz um AND binário com seu IP e máscara e compara com o AND binário com o IP do destino e máscara. Se não pertencerem a mesma rede, o host encaminha para o *gateway default*. No caso do proxy ARP não há essa configuração de gateway no host. Quando o host quer enviar um pacote para uma rede distinta neste caso, o proxy ARP responde com seu MAC, como se fosse o host de destino.

Resposta 2:

Com o uso do default gateway a requisição ARP é feita perguntando-se qual é o endereço MAC associado ao endereço IP do default gateway. Com proxy ARP a requisição ARP é feita perguntando-se qual é o endereço MAC associado ao endereço IP da máquina destino. (resposta do professor).

43. Um administrador de redes necessita dividir a faixa de endereçamento 192.168.30.0/24 em cinco sub-redes. Qual, ou quais, máscara(s) deve(m) ser configurado(s) nas máquinas de cada uma dessas cinco sub-redes? Ainda, para cada sub-rede, defina o endereço de broadcast de rede, o primeiro e o último endereços IPs válidos. Considere **classless.**

Rede 1:

| | |
|--------------------|--|
| Rede/Mask: | 192.168.30.0/27 ou 192.168.30.0/255.255.255.224 |
| Broadcast: | 192.168.30.31 |
| Primeiro endereço: | 192.168.30.1 |
| Último endereço: | 192.168.30.30 |

Rede 2:

Rede/Mask: 192.168.30.32/27
192.168.30.32/255.255.255.224
Broadcast: 192.168.30.63
Primeiro endereço: 192.168.30.33
Último endereço: 192.168.30.62

Rede 3:
Rede/Mask: 192.168.30.64/27 ou
192.168.30.64/255.255.255.224

Broadcast: 192.168.30.95
Primeiro endereço: 192.168.30.65
Último endereço: 192.168.30.94

Rede 4:
Rede/Mask: 192.168.30.96/27 ou
192.168.30.96/255.255.255.224
Broadcast: 192.168.30.127
Primeiro endereço: 192.168.30.97
Último endereço: 192.168.30.126

Rede 5:
Rede/Mask: 192.168.30.128/25 ou
192.168.30.128/255.255.255.128
Broadcast: 192.168.30.255
Primeiro endereço: 192.168.30.129
Último endereço: 192.168.30.254

44. Quais são as diferenças entre confidencialidade de mensagem e integridade de mensagem? É possível ter uma sem a outra? JUSTIFIQUE sua resposta.

Confidencialidade: a mensagem só está acessível para pessoas devidamente autorizadas (que possuem a chave para decodificar).

Integridade: a mensagem não foi alterada antes de chegar no destinatário.

Uma está ligada a permissão de leitura e a outra a permissão de escrita.

É possível ter integridade apenas, confidencialidade apenas ou ambas. Para garantir a

45. Considere a Internet e seus diferentes protocolos. Um cliente MUA (Mail User Agent) envia uma mensagem para um servidor de e-mail dentro de seu próprio domínio administrativo, por exemplo, para coioote@acme.com. A máquina cliente e o servidor estão na mesma sub-rede e ambos estão com todos seus parâmetros de redes corretamente configurados. Supondo que você esteja capturando o tráfego nessa rede com um sniffer, liste, NA ORDEM CORRETA em que são capturados, TODOS os protocolos da camada de rede, de transporte e de aplicação. JUSTIFIQUE brevemente o que cada um dos protocolos faz quando acionado.

IMPORTANTE: Desconsidere que informações estão sendo lidas em qualquer tipo de cache, isto é, as informações necessárias não estão armazenadas em nenhum tipo cache.

ARP: Para obter o MAC do servidor de DNS partir do IP do servidor de DNS e assim identificar máquina

servidor de e-mails.

IP: encapsula o UDP do servidor DNS

UDP: Encapsula a requisição DNS

DNS: Para consultar o IP do servidor de e-mails

ARP: Para obter MAC do servidor de e-mails

IP: para encapsular o TCP

TCP para fazer a conexão no servidor de e-mails

SMTP (Simple Mail Transfer Protocol) para entregar a mensagem

(melhorar)

46. Qual a principal diferença entre estabelecer um circuito virtual e estabelecer uma conexão?

Resposta 1:

No estabelecimento de um circuito virtual é fixado um caminho envolvendo os sistemas finais e os nós intermediários,

No estabelecimento da conexão é criado um canal lógico e nenhum caminho é pré fixado. Apenas os dois sistemas finais estão envolvidos. Os nós intermediários não ficam sabendo da existência da conexão. [CARISSIMI, pg211]

Tabela comparativa [TANENBAUM5, pg.361]:

| Questão | Rede orientada a Datagramas (IP) | Circuito Virtual |
|--|--|--|
| Configuração dos Circuitos | Desnecessária | Requerida |
| Endereçamento | Cada pacote contém os endereços completos de Origem e Destino | Cada pacote contém o número do Circuito Virtual |
| Informação de Estado | Os roteadores não armazenam informações sobre o estado das conexões. | Cada Circuito Virtual precisa ser armazenado na tabela do roteador a cada conexão. |
| Roteamento | Cada pacote é roteado independentemente. | A rota é escolhida quando o Circuito Virtual é estabelecido, todos os pacotes devem seguir essa rota previamente acertada. |
| Efeito de uma falha no roteador | Nenhum efeito, apenas serão perdidos alguns pacotes durante a falha. | Todos os Circuitos Virtuais que passaram pelo roteador durante a falha serão encerrados. |
| QoS | Difícil de ser feito. | Fácil, se for possível alocar recursos suficientes com antecedência para cada Circuito Virtual. |
| Controle de congestionamento | Difícil de ser feito. | Fácil, se for possível alocar recursos suficientes com antecedência para cada Circuito |

| | | |
|--|--|----------|
| | | Virtual. |
|--|--|----------|

Resposta do Professor:

A comunicação via circuito virtual envolve os sistemas finais e intermediários, enquanto que uma conexão envolve apenas os sistemas finais. Além disso, uma comunicação sobre uma conexão tem-se garantia de entrega, ordem e não duplicação, ao passo que sobre um circuito virtual não fornece essas garantias.

Quais os passos envolvidos em cada caso ?

Passos para estabelecer um circuito virtual:

*Denificar caminho

*Negociação tanto os sistemas finais como intermediários

Passos para estabelecer uma conexão:

*Sistemas finais via software criam um canal lógico

É possível estabelecer uma sem a outra? JUSTIFIQUE sua resposta.

Sim, são sistemas distintos.

47. Um dos problemas do algoritmo de roteamento por vetor de distância é a contagem para o infinito. Qual a razão desse problema? Por que ele acontece? Como o estado de enlace resolve esse problema?

A origem deste problema está no fato de que, quando um nó x informa a um nó y que tem um caminho para um nó z, o nó y não tem como saber se ele próprio está nesse caminho para o nó z.

Ele acontece porque no algoritmo de roteamento vetor distância há apenas a informação da métrica e do próximo salto. Não há informação de quem está enviando a informação das rotas na tabela de roteamento.

No algoritmo de roteamento estado de enlace, quando um link cai, o roteador enviar imediatamente a informação em um pacote LSP. Os pacotes LSP são repassados de roteador para roteador atingindo uma rápida convergência da informação. O LSP também possuem uma validade. Isso elimina laços no roteamento.

48. Quais parâmetros de uma rede TCP/IP devem estar corretamente configurados em um computador para que este tenha acesso a serviços de redes em redes externas a sua? Considere a necessidade de acessar máquinas externas a partir de seus nomes simbólicos. JUSTIFIQUE a necessidade de cada um desses parâmetros dizendo, para cada um deles, que tipo de erro/problema acontece se ele estiver não-configurado ou mal configurado.

IP do Gateway padrão para acessar redes externas. Caso não esteja configurado, não consegue ter acesso à redes externas.

IP do servidor de DNS para a resolução de nomes. Caso não esteja configurado, não é possível resolver os nomes em endereços IPs e vice-versa, apesar de ser possível efetuar a conexão utilizando diretamente o endereço IP.

IP da máquina, para que a mesma tenha um endereço válido na rede para o protocolo TCP/IP. Caso não esteja configurado não será possível enviar dados para esta máquina.

Máscara de Rede, é usada para definir qual a rede que a máquina pertence. Caso não esteja configurado não é possível saber se o IP de destino faz parte ou não da rede dessa máquina.

49. Você é o administrador de uma grande empresa e necessita definir qual o protocolo de

roteamento a ser usado internamente (IRP - Interior Router Protocol) nesta sua organização (Autonomos System). A dúvida é entre usar um protocolo baseado em vetor de distância (RIP, por exemplo) ou um protocolo baseado em estado de enlace (OSPF, por exemplo). Sabendo-se que a rede dessa organização sofre pouquíssimas alterações em sua topologia, qual dos dois protocolos você adotaria? JUSTIFIQUE sua escolha, citando pelo menos dois argumentos favoráveis a sua recomendação.

OSPF

* Convergência mais rápida, pois RIP converge proporcionalmente ao número de nós. OSPF converge em uma proporção logarítmica ao número de enlaces.

* Menos ocupação de largura de banda, pois o OSPF manda atualizações somente quando há mudança na rede, apesar do processo de inundação de pacotes LSP em toda a rede usado pelo OSPF (gerando uma carga alta de dados nesse momento), como o número de alterações na rede é muito baixo, esse processo de inundação irá ocorrer com pouquíssima frequência. O RIP manda atualizações periódicas (30s). Também cabe lembrar que o pacote LSP, em geral, é menor que o vetor de distância.

* Escalabilidade, pois o RIP demora muito para convergir em redes muito grandes, o que pode ser um problema.

50. Um administrador de redes necessita dividir a faixa de endereçamento privativo 10.1.2.0/24 em cinco sub-redes. Qual, ou quais, máscara(s) deve(m) ser configurado(s) nas máquinas de cada uma dessas cinco sub-redes? Ainda, para cada sub-rede, defina o endereço de broadcast de rede, o primeiro e o último endereços IPs válidos. Considere classfull e depois refaça o exercício considerando classless.

Classfull:

| Rede | End rede/mask | End. Broadcast | Faixa de endereços |
|---------------|---------------|----------------|-----------------------|
| Não utilizada | 10.1.2.0/27 | 10.1.2.31 | 10.1.2.1-10.1.2.32 |
| N1 | 10.1.2.32/27 | 10.1.2.63 | 10.1.2.33-10.1.2.62 |
| N2 | 10.1.2.64/27 | 10.1.2.95 | 10.1.2.65-10.1.2.94 |
| N3 | 10.1.2.96/27 | 10.1.2.127 | 10.1.2.97-10.1.2.126 |
| N4 | 10.1.2.128/27 | 10.1.2.159 | 10.1.2.129-10.1.2.158 |
| N5 | 10.1.2.160/27 | 10.1.2.191 | 10.1.2.161-10.1.2.190 |

Classless:

Várias possibilidade.

5 redes /27 (sobram 3 redes /27)

3 redes /26 e 2 redes /27

4 redes /27 e 1 rede /25

2 redes /26 e 3 redes /27 (sobra 1 rede /27)

51. O analista de TI (tecnologia da informação) de um órgão público está com o seguinte problema: é preciso divulgar publicamente o resultado de uma licitação, mas é necessário impedir que esse documento eletrônico seja alterado e difundido na Internet como se fosse o original. Responda, JUSTIFICANDO seu ponto de vista:

A) Entre as propriedades da segurança da informação, qual(ais) deve(m) ser preservada(s) nesse caso?

Autenticidade para garantir a autoria.

Integridade para garantir que não será modificado.

B) Que tipo de solução você daria a esse analista? JUSTIFIQUE a sua resposta.

Assinatura digital, pois a mesma garante a integridade (que os dados não foram alterados antes de serem entregues ao destinatário) e a autenticidade (que o documento foi assinado com o certificado válido e emitido por uma autoridade certificadora para o emissor do documento, que pode ser uma pessoa ou empresa).

52. Considere a Internet e seus diferentes protocolos. A máquina asterix.inf.ufrgs.br roda um cliente HTTP (ou seja, um navegador ou browser) e o usuário solicita uma URL para um servidor web que está fora de seu domínio administrativo. Por exemplo, o cliente estando no domínio inf.ufrgs.br solicita uma página ao servidor web www.acme.com. O servidor de DNS do domínio inf.ufrgs.br não está na mesma sub-rede da máquina cliente (inf.ufrgs.br).

Supondo que você esteja capturando o tráfego nessa rede com um sniffer, liste, NA ORDEM CORRETA em que são capturados os quadros de TODOS os protocolos da camada de rede, de transporte e de aplicação envolvidos nesta requisição. JUSTIFIQUE brevemente o porquê dessa ordem e o que cada um dos protocolos faz quando acionado. Importante: Desconsidere a existência de informações em qualquer tipo/nível de cache, ou seja, toda e qualquer informação necessária deve ser buscada via requisições na rede.

Camada de Aplicação:

DNS: obtenção do endereço de IP correspondente ao nome www.acme.com

HTTP: Solicitações de acesso ao conteúdo do servidor web localizado nessa máquina

Camada de transporte:

UDP(maior parte das solicitações utilizam UDP): Encapsulamento do pacote DNS a ser enviado para a porta de destino padrão do DNS

TCP: Tráfego HTTP, em geral, na porta padrão do protocolo (80).

Camada de Rede:

Para o DNS:

ARP: Consulta ao endereço MAC do servidor DNS da máquina cliente(pré-configurado pelo administrador do sistema)

IP: Encapsulamento e envio do pacote DNS para o endereço de IP do servidor DNS(ou de alguma máquina intermediária, dependendo da resposta ARP).

Para o HTTP:

ARP: Consulta ao endereço MAC da máquina de destino.

IP: Encapsulamento e envio do pacote DNS para o endereço de IP da máquina de destino(ou de alguma máquina intermediária, dependendo da resposta ARP).

(Deixar a ordem mais clara)

53. Quando se usa NAT e quando se usa VPN? Para embasar a sua resposta dê, para cada um desses mecanismos, um exemplo de "caso de uso" e justifique o emprego de um em detrimento do outro.

Resposta 1:

Inicialmente a solução proposta pelo uso de NAT estava focada em combater a escassez de endereços IP, pois constatou-se que nem todos os equipamentos com endereços IP têm a necessidade de serem “visíveis” na Internet. Os endereços IPs válidos só são necessários para a rede externa, já que para a rede interna é possível usar um esquema de endereçamento que desvincule os números de IPs válidos do número de usuários. Por exemplo, podemos usar na rede interna a rede 10.0.0.0, que não é roteável na internet, e todas as máquinas dessa rede podem acessar a internet através de um servidor NAT, que só usará um IP válido na internet. Essa tradução é a base do NAT. Como IPs válidos estão cada vez mais escassos, usa-se apenas 1 para acessar a Internet, e os clientes na rede interna poderão usar um esquema de endereçamento próprio, inclusive usando faixas de IPs válidas na Internet, já que os IPs dessa rede não serão “visíveis” externamente. Um outro aspecto do NAT é que as empresas tem utilizado ele não somente devido à escassez de endereços IPs, mas como forma de prevenir ataques externos às máquinas internas da organização, já que apenas o servidor NAT estará “exposto” na Internet. Um exemplo prático de utilização do NAT é uma empresa usar um esquema de endereçamento próprio da rede interna e permitir que as máquinas com esses endereços possam acessar a Internet usando um único IP válido distribuído, por exemplo, pelo <http://registro.br> [CARÍSSIMI, p250-252].

O propósito da VPN é interligar os computadores de diversas unidades (filiais, por exemplo) de uma organização em uma mesma rede interna (privativa) independente da localização geográfica (muitas vezes dispersa) dessas unidades usando a infraestrutura pública da Internet para trafegar dados. Uma outra maneira de se fazer isso seria alugando linhas privadas dedicadas de empresas de telecomunicações, mas o custo é extremamente elevado e as velocidades, na maioria das vezes, não são satisfatórias. O uso da Internet para trafegar dados entre redes dispersas tem uma série de vantagens, as quais podemos citar o custo (se a empresa já possui acesso à Internet, não é necessário pagar nenhum valor adicional para se criar uma VPN), a versatilidade (para ter acesso à rede interna da empresa, basta o usuário ter um acesso à Internet e se conectar à VPN). A VPN permite a criação de uma rede que, ao mesmo tempo, é privativa (garante a confidencialidade dos dados que trafegam através dela, fazendo uso do IPSec) e virtual (pois não possui nenhum meio físico próprio). A rede fisicamente é pública (os pacotes IPSec trafegam e são acessíveis publicamente na Internet) e é virtualmente privada (os datagramas IP da rede interna estão criptografados dentro dos pacotes IPSec, ou seja, os dados que trafegam na rede interna não podem ser acessados). Como exemplo prático podemos citar como exemplo um executivo que está em Porto Alegre, no aeroporto aguardando seu voo (dispõe de uma conexão WiFi pública do aeroporto para acessar a Internet) e deseja acessar a rede interna da empresa, cujos servidores estão localizados em São Paulo, para ele acessar a rede interna da empresa, usando o acesso WiFi público do aeroporto, não expondo a rede interna da empresa à ataques externos, ele pode acessar através de uma VPN, que, depois de estabelecida a conexão, ele terá um acesso seguro à rede interna da empresa como se estivesse na matriz com seu computador lá conectado diretamente [CARÍSSIMI, p.377-379].

Palavras-chave:

* NAT: computadores da rede interna acessam a Internet através de um mesmo IP válido, passando pelo servidor de NAT.

* VPN: um computador externo pode acessar a rede interna da empresa com garantia de confidencialidade, usando a Internet como meio de infraestrutura.

54. Um estudante está aprendendo o funcionamento do protocolo ARP e descobre que com o comando `arp -a` ele pode ver o conteúdo da cache ARP de seu PC. Entretanto, após realizar o comando `ping` para uma série de máquinas externas a sua rede ele viu que a cache ARP tinha apenas uma entrada. Você acha que ele fez corretamente a experiência ? Explique a ele o que aconteceu ou o que ele fez de errado. Diga o porquê dessa única entrada.

IMPORTANTE: os parâmetros de rede da máquina desse estudante estão corretamente configurados e o comando `arp -a` lista o conteúdo de todas as entradas da tabela ARP (cache ARP) da máquina que executa o comando.

A única entrada na tabela ARP pertence ao gateway padrão.

55. (Prova 2 2008/1, questão 1A). Sobre sockets, considere que um processo servidor oferece um serviço X na porta Y, usando UDP, responda:

A) Outro processo, também usando UDP, pode oferecer o mesmo serviço X em outra porta Z ? JUSTIFIQUE.

Sim, basta ser uma instância de processo diferente sendo executada em outra porta (que é justamente o caso da questão). Basicamente, teremos dois servidores rodando o mesmo serviço na mesma máquina, porém em portas diferentes.

B) É possível um outro processo oferecer o mesmo serviço X na mesma porta Y (UDP)? JUSTIFIQUE dizendo o porquê de uma negativa ou dando as condições necessárias, em caso afirmativo.

Resposta 1:

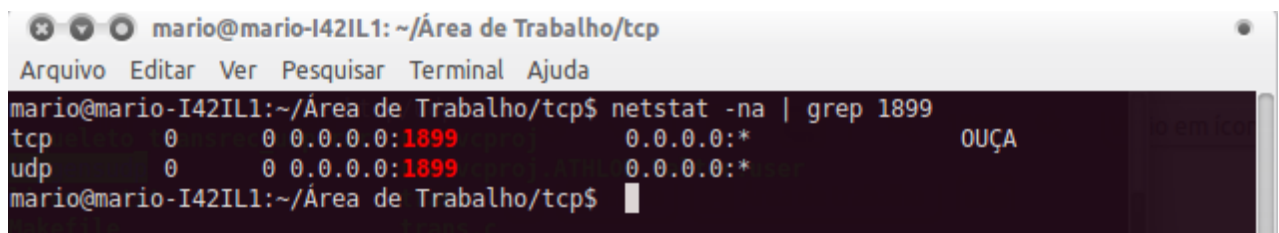
Não é possível. A porta é uma forma de comunicação fim-a-fim, em outras palavras, processo a processo, de modo que a forma de se executar essa idéia é separando-os de alguma forma, no caso, por portas.

Resposta 2:

Para identificar uma conexão na camada de transporte usamos uma 5-upla { IP Origem, Porta Origem, IP Destino, Porta Destino, Protocolo }. Quando falamos em “serviço” presume-se que estamos permitindo conexões vindas de vários clientes (modo *listen*), desse modo, no caso de termos um serviço UDP, teremos como origem a porta Y e o IP do servidor e como destino qualquer IP e qualquer porta (0.0.0.0:*), assim nossa 5-upla seria { 0.0.0.0, *, IP Servidor, Y, UDP } para as conexões desse serviço. Nessa mesma porta Y, usando o protocolo UDP, nesse mesmo servidor, não poderemos ter outro serviço escutando nessa porta para qualquer máquina e porta de origem.

Resposta 3:

Para identificar uma conexão na camada de transporte usamos uma 5-upla { IP Origem, Porta Origem, IP Destino, Porta Destino, Protocolo }. Caso o serviço atenda apenas um IP de Origem, ou seja, uma conexão entre duas máquinas, podemos ter dois serviços UDP no mesmo servidor, na mesma porta Y, desde que atendam máquinas diferentes.



```
mario@mario-I42IL1: ~/Área de Trabalho/tcp
Arquivo Editar Ver Pesquisar Terminal Ajuda
mario@mario-I42IL1:~/Área de Trabalho/tcp$ netstat -na | grep 1899
tcp        0      0 0.0.0.0:1899          0.0.0.0:*             OUÇA
udp        0      0 0.0.0.0:1899          0.0.0.0:*
```

C) É possível um outro processo, usando TCP, oferecer o mesmo serviço X na mesma porta Y ? JUSTIFIQUE.

É possível, desde que o processo utilize um protocolo diferente do UDP. Como é o TCP, isso pode ser feito sem problemas.

56. (Prova 2 2008/1, questão 1B). Por quais razões, em que momento e para quê, o SSL usa criptografia assimétrica e simétrica ?

O SSL consiste em dois subprotocolos, um para estabelecer uma conexão segura e outro para usa-la.

A criptografia de chaves assimétricas é utilizada para o compartilhamento da chave secreta (neste caso, também chamada de chave de sessão), pois seria necessário um canal de comunicação seguro para promover o compartilhamento da chave secreta simétrica entre as partes, além da dificuldade de gerenciamento de grandes quantidades de chaves simétricas.

A criptografia de chave simétrica é usada para a codificação da informação. Ela é a mais indicada para garantir a confidencialidade de grandes volumes de dados, pois seu processamento (codificação e decodificação) é mais rápido.

Fonte: <http://cartilha.cert.br/criptografia/>

57. Uma empresa possui o seguinte conjunto de blocos: 150.10.0.0/19, 150.10.32.0/19 e 150.10.96.0/19. Esses blocos podem ser agregados? EXPLIQUE. Caso possam ser agregados, indique o endereço do bloco agregado. Caso contrário, determine os blocos que estão faltando e, em seguida, determine o endereço do bloco agregado.

Como só podemos agregar blocos contíguos e está faltando o bloco 150.10.64.0/19, não é possível agregar as rotas. Neste caso, o bloco agregado seria 150.10.0.0/17, pois temos 4 blocos, logo 2^2 então diminuímos 2 da máscara, pegando o menor endereço dos blocos (150.10.0.0)

58. Um usuário, em casa, em seu computador corretamente configurado, acessa a página <http://www.euro2008.uefa.com>. Considerando que não há nenhuma informação armazenada em nenhum tipo de cache, liste todos os protocolos envolvidos nesse acesso, na ordem que são acionados, a partir da camada de rede (inclusive). Para cada protocolo forneça, com o auxílio de um desenho (como o posto no quadro) todos os encapsulamentos a partir da camada do protocolo até a camada de rede (inclusive). IMPORTANTE : o usuário, em sua casa, não tem nenhum serviço Internet instalado em seu computador ou em sua rede local. Desconsidere qualquer suposição relativa a NAT em sua resposta. O endereço IP do usuário é um endereço fornecido por seu provedor de acesso a Internet (ISP).

* ARP para o default gateway para se obter o seu MAC. Isso é necessário para poder enviar a consulta ao servidor de DNS (que está fora da rede).

* DNS para resolver www.uefa.com.

* ARP, pois é preciso se comunicar com o servidor da uefa (fora da rede).

* TCP com o servidor uefa.

* HTTP.

O ARP é encapsulado apenas na camada de enlace.

O DNS é encapsulado em UDP, que por sua vez é encapsulado em IP.

O TCP é encapsulado no IP e o http é encapsulado em TCP, que é encapsulado em IP.

Fonte: Lista anterior.

59. Aquela vizinha (ou vizinho, se for o caso) que você espera uma oportunidade para conversar, sabendo que você é estudante de computação, vem lhe pedir auxílio por que a sua rede em casa não funciona. Os sintomas relatados são : – Ao tentar acessar a web, dá erro que não consegue encontrar nenhum site fornecido na forma de URL com nome simbólico (como www.exemplo.com.br). – Não está conseguindo "baixar" e enviar e-mails a partir de

seu provedor de acesso Internet (ISP). – Consegue imprimir via rede na impressora de rede, instalada na rede local de casa. – Consegue "enxergar" os outros computadores da rede local através de "vizinhança da rede" ou compartilhamento de pastas. Qual ou quais seriam as prováveis causas do problema? Como você procederia para comprovar as suas suspeitas e resolver o problema? Que testes e verificações você faria? REFLITA: Quão efetiva sua solução é? Sabe-se ainda que a configuração da rede da casa é composta por 4 PCs e uma impressora de rede, todos conectados em uma mesma rede local e interconectados através de um roteador ADSL. Esse roteador possui suporte a DHCP e NAT.

Resposta 1:

As causas possíveis podem ser DNS, Rede Externa (site e servidor de e-mail que ela está tentando acessar), NAT, na companhia telefônica (GVT) ou no roteador ADSL. Como a rede interna está OK (consegue acessar outras máquinas e imprimir via rede) o DHCP está funcionando

Eu comporaria essas suspeitas com os seguintes testes:

1. *ping* no roteador ADSL para testar se o roteador está funcionando, como o roteador é o *default gateway*, verifica se o mesmo está OK, como o roteador também faz NAT, verifica se o mesmo está acessível.
2. *ping* em um IP externo para verificar se a rede externa está acessível, nesse caso verificamos que o problema não está na companhia telefônica (ISP da GVT).
3. *ping* no IP do DNS, para verificar se está ativo.
 - a. Se estiver ativo *nslookup* para verificar se o DNS está respondendo à consultas
4. *ping* no endereço do site, para verificar se o servidor web está acessível
5. *ping* no endereço do servidor de email para verificar se o servidor de email está acessível.

60. Uma determinada instituição possui o endereço de classe C 200.10.10.0. Essa instituição possui 7 redes físicas (N1 a N7), cada uma com 10, 5, 8, 12, 7, 9 e 4 estações, respectivamente. Forneça as possíveis máscaras de sub-redes que podem ser adotadas usando a notação decimal e a de contagem de bits. Indique os endereços de sub-redes criados, os endereços de broadcast direto e os intervalos de endereços válidos destas sub-redes. Considerar alocação classful.

Sendo a rede Classfull:

Todas as sub-redes derivadas da mesma rede devem ter a mesma máscara.

Alocação Classfull:

Não utilizar redes com bits em 0 e em 1.

Número de redes: $x^2 - 2 \geq 7 \rightarrow x = 14$

Máscara 28:.

Rede 1: 200.10.10.0.16/255.255.255.240 broadcast:200.10.10.31 end: 200.10.10.17-30

Rede 2: 200.10.10.0.32/255.255.255.240 broadcast:200.10.10.47 end: 200.10.10.31-46

Rede 3: 200.10.10.0.48/255.255.255.240 broadcast:200.10.10.63 end: 200.10.10.49-62

Rede 4: 200.10.10.0.64/255.255.255.240 broadcast:200.10.10.79 end: 200.10.10.65-78

Rede 5: 200.10.10.0.80/255.255.255.240 broadcast:200.10.10.95 end: 200.10.10.81-94

Rede 6: 200.10.10.0.96/255.255.255.240 broadcast:200.10.10.111 end: 200.10.10.97-110

Rede 7: 200.10.10.0.112/255.255.255.240 broadcast:200.10.10.127 end: 200.10.10.113-126

Redes que não são usadas:

200.10.0.0 e 200.10.10.240

61. Uma instituição recebeu um bloco de 4096 endereços e o subdividiu em dois blocos de 1024 endereços e em quatro blocos de 512 endereços. Sabe-se que os endereços 192.168.2.5 e 192.168.4.1 pertencem aos blocos de 1024 endereços, enquanto que os 192.168.9.20, 192.168.10.1, 192.168.12.1 e 192.168.15.50 pertencem, respectivamente, aos blocos de 512 endereços. Identifique o bloco alocado a essa instituição e todos os sub- blocos de 1024 e 512 endereços criados.

idem a 69.

62. (PROVA 2008/1 - Questão 5B). Ao se consultar a cache ARP de um computador se obteve o seguinte :

IP MAC IP M AC

| | |
|----------------|------------------------|
| 192.168.20.4 | 00 :18 :8B :DF :49 :77 |
| 143.15.30.12 | 00 :18 :8B :DF :49 :77 |
| 192.168.20.120 | 08 :81 :8B :FD :04 :67 |
| 169.12.12.15 | 00 :18 :8B :DF :49 :77 |
| 192.168.20.200 | 02 :12 :8B :DF :90 :77 |
| 61.15.6.1 | 00 :18 :8B :DF :49 :77 |
| 192.168.23.15 | 08 :11 :B8 :A0 :49 :65 |
| 150.100.24.5 | 00 :18 :8B :DF :49 :77 |

O que se pode afirmar quanto a rede (endereço de rede e máscara) que esse computador pertence? Como se explica as múltiplas entradas do endereço MAC 00 :18 :8B :DF :49 :77 ? Há mais alguma informação que se pode obter dessa tabela?

Resposta 1:

Rede 192.168.20.0/22.

Há um proxy ARP que responde para endereços na mesma rede que se entram atrás do proxy arp (end 192.168.20.4 ou 192.168.20.100). O proxy arp também responde para endereços consultados fora da rede, por isso a quantidade de MACs iguais. O endereço do Proxy arp é 192.168.20.4 ou 192.168.20.100.

Resposta 2:

Rede: 192.168.20.0 e máscara /22 (para ser coerente com o endereço local 192.168.23.15)

As múltiplas entradas do mesmo MAC correspondem ao MAC do default gateway, que , nesse caso, é acionado para todos os IPs externos a nossa rede. Sendo assim, todos os datagramas a serem encaminhados para uma rede externa são direcionados ao default gateway.

Há mais alguma informação? Sim, a primeira entrada corresponde a um IP local com o MAC do default gateway, o que significa que esse é o IP do default gateway, já que esse se encontra na nossa rede.

63. Um determinado roteador suporta roteamento classless e possui uma tabela de roteamento que é indicada abaixo. Forneça todas as rotas possíveis e a rota selecionada para encaminhar datagramas para os endereços 150.100.92.1, 150.100.94.1 e 150.100.128.1. JUSTIFIQUE, para cada caso, qual o critério a ser usado para selecionar a rota.

| Destino | Next-hop | Máscara |
|--------------|------------|---|
| 150.100.92.1 | 200.10.1.1 | 255.255.255.255 |
| 150.100.80.0 | 192.10.2.1 | 255.255.240.0 150.100.80.0 - 150.100.95.255 |

150.100.64.0 192.10.2.2 255.255.192.0 150.100.64.0 - 150.100.127.255
0.0.0.0 (default) 200.10.1.2 0.0.0.0

150.100.92.1 ->

Possíveis:

200.10.1.1, 192.10.2.1 , 192.10.2.2 ,200.10.1.2

Selecionada: 200.10.1.1

Motivo: Máscara mais restritiva

150.100.94.1 ->

Possíveis:

192.10.2.1 , 192.10.2.2 ,200.10.1.2

Selecionada: 200.10.2.1

Motivo: Máscara mais restritiva

150.100.128.1 ->

Possíveis:

200.10.1.2

Selecionada: 200.10.1.2

Motivo: Rota default. Nenhuma outra "bateu"

64. Uma determinada instituição possui o endereço de classe C 200.10.10.0. Essa instituição possui APENAS 6 redes físicas (N1 a N6), cada uma com 10, 5, 8, 12, 7 e 9 estações, respectivamente. Forneça as possíveis máscaras de sub-redes que podem ser adotadas usando a notação decimal e a de contagem de bits. Indique os endereços de sub-redes criados, os endereços de broadcast direto e os intervalos de endereços válidos destas sub-redes. ATENÇÃO : considerar alocação **classfull !**

Rede não utilizada: 200.10.10.0/27 255.255.255.224

N1: 200.10.10.32/27 255.255.255.224 end.sub:200.10.10.32 intervalo: 200.10.10.33-62 broadcast: 200.10.10.63

N2: 200.10.10.64/27 255.255.255.224 end.sub:200.10.10.64 intervalo: 200.10.10.65-94 broadcast: 200.10.10.95

N3: 200.10.10.96/27 255.255.255.224 end.sub:200.10.10.96 intervalo: 200.10.10.97-126 broadcast: 200.10.10.127

N4: 200.10.10.128/27 255.255.255.224 end.sub:200.10.10.128 intervalo: 200.10.10.129-158 broadcast: 200.10.10.159

N5: 200.10.10.160/27 255.255.255.224 end.sub:200.10.10.160 intervalo: 200.10.10.161-190 broadcast: 200.10.10.191

N6: 200.10.10.192/27 255.255.255.224 end.sub:200.10.10.192 intervalo: 200.10.10.193-222 broadcast: 200.10.10.223

Rede não utilizada: 200.10.10.224/27 255.255.255.224

65. Uma máquina para acessar adequadamente a Internet tem que ter um endereço IP, uma máscara de rede, um default gateway e o IP de servidor DNS corretamente configurados. DESCREVA: quais são os problemas que podem acontecer se, INDIVIDUALMENTE, cada um desses parâmetros estiver mal configurado ou ausente (ATENÇÃO: essa resposta tem quatro situações diferentes, um parâmetro com problema e os outros três corretos). RESPONDA ainda porque deve ser informado o IP do servidor DNS e não seu nome simbólico?

IP: A máquina não recebe adequadamente um ARP Reply, comprometendo a comunicação de toda a pilha superior ao nível de enlace. Na visão do nível de rede, um IP duplicado gera ambiguidade e , consequentemente , um comportamento inesperado durante a comunicação entre as máquinas com IP duplicado.

Máscara de Rede: A rede é identificada erroneamente, levando a erros no roteamento dos pacotes IP.

Uma máscara mais restritiva fará com que o host pense que computadores que na verdade pertençam a sua rede, estejam em uma rede externa. Uma máscara menos restritiva fará com que o host pense que computadores que na verdade estão em uma rede externa pertençam a sua rede.

Default gateway: A não possui uma rota padrão. Sendo assim, no caso de um gateway inatingível, solicitações não poderão ser enviadas para IPs externos à rede(outras sub-redes).

Servidor DNS: Não será possível descobrir IPs a partir de nomes de hosts. Talvez esse seja, dentre os erros possíveis na rede, o menos grave, pois as máquinas, mesmo não estando acessíveis a partir dos seus nomes, podem ser acessadas diretamente pelo seu número de IP

O servidor DNS precisa ter seu IP configurado na máquina cliente, pois como já dito, o cliente não consegue resolver nomes de hosts em endereços IPs, com base nisso, sabendo o IP do servidor DNS basta fazer uma consulta DNS para descobrir o endereço IP dos outros hosts. O protocolo IP não utiliza nomes de hosts, apenas endereços IPs.

OBS: Nos primórdios da Internet, quando ainda não existia a aplicação DNS, os clientes armazenavam localmente uma tabela contendo um mapeamento de nomes de hosts para endereços IPs e toda a tradução era feita por esta tabela. Esta tabela ainda está presente, mas é pouco usada, caso colocássemos os nomes de todos os hosts nela, até poderíamos não utilizar o DNS para resolver nomes.

66. Dois usuários A e B querem se comunicar na rede de forma que a confidencialidade das informações seja garantida. Responda:

A) Que tipo de criptografia esses usuários podem empregar para isso? Simétrica? Assimétrica? Ou ambas?JUSTIFIQUE.

Ambas. As duas conseguem criptografar as mensagens e manter a confidencialidade da mesma. Na criptografia Simétrica ambos usuários precisam ter a mesma chave para descriptografar as informações, esta chave não pode ser enviada pela rede. A diferença será no desempenho dos algoritmos de decodificação, na gerência e distribuição de chaves.

B) De acordo com sua resposta, diga quais tipos de chaves são empregados pelos usuários A e B nessa comunicação. EXPLICITE qual, ou quais, chaves são empregadas no envio de uma mensagem de A para B e de B para A.

Na simétrica, ambas as chaves são iguais e foram previamente trocadas, usa-se a mesma chave para criptografar e decodificar as mensagens.

Envio de mensagem de A para B: A criptografa a mensagem com a chave k e envia a mensagem para B, B recebe a mensagem criptografada de A e decodifica usando a chave k.

Envio de mensagem de B para A: análogo ao processo anterior.

Na assimétrica, um lado pega a chave pública do outro para cifrar a mensagem.

Envio de mensagem de A para B: A criptografa a mensagem com a chave pública de B e envia a mensagem para B, B recebe a mensagem criptografada de A e decodifica com sua chave privada.

Envio de mensagem de B para A: B criptografa a mensagem com a chave pública de A e envia a mensagem para A, A recebe a mensagem criptografada de B e decodifica com sua chave privada.

67. Uma determinada instituição possui 5000 estações distribuídas uniformemente em 100 redes físicas diferentes. Aloque um endereço de bloco (CIDR) para essa instituição (considere uma faixa de endereço IP qualquer). Compare o desperdício de endereços entre a alocação

do bloco e a situação em que essa instituição alocasse uma classe B e criasse sub-redes. **EXPLIQUE** claramente sua resposta e **EXPLICITE** todas as suposições que foram feitas.

Bloco: 10.0.0.0/19 (cabem 128 redes /26 dentro)

50 estações por rede.

Cada rede -> /26 (64 endereços)

100 redes de 64 endereços = 6400 endereços

Dispersão de 6400-5000 = 1400 endereços

Rede classe B: $2^{16} = 65536$ endereços

Dispersão classe B = 60536 endereços

68. O protocolo HTTP, em sua versão 1.1, suporta conexões persistentes e não persistentes. Dependendo do cliente web, as conexões não persistentes podem ser estabelecidas de forma serial ou paralela. No caso das conexões persistentes, as mensagens de requisição podem ser enviadas com ou sem paralelismo. Considere que uma página web (documento web) faça referência internamente a outros 15 objetos. Quantas conexões são estabelecidas, no mínimo, por um cliente web que adotam a abordagem não persistente serial, não persistente paralela, persistente não paralela e persistente paralela ? **EXPLIQUE** como se chegou a cada um desses números de conexões. Considere que o browser não tem número ilimitado de conexões possíveis.

Não persistente serial:

1 p/ página + 15 p/ objetos = 16 conexões, em série.

Não persistente paralela:

1 p/ página + 15 p/ objetos = 16 conexões, simultâneas, nesse caso.

Persistente serial:

1 p/ página e objetos = 1 conexão, com uma requisição de página e objetos sendo realizada por vez, esperando a confirmação a cada requisição.

Persistente paralela

1 p/ página e objetos = 1 conexão, com várias requisições de página e objetos podendo ser realizadas sem a necessidade de esperar confirmação

69. Uma instituição recebeu um bloco de 4096 endereços e o subdividiu em dois blocos de 1024 endereços e em quatro blocos de 512 endereços. Sabe-se que os endereços IPs 192.168.2.5 e 192.168.4.1 pertencem aos blocos de 1024 endereços, enquanto que os endereços IPs 192.168.9.20, 192.168.10.1, 192.168.12.1 e 192.168.15.50 pertencem aos blocos de 512 endereços. Identifique o bloco alocado a essa instituição e todos os sub-blocos de 1024 e 512 endereços criados.

Bloco da instituição: 192.168.0.0/20

Bloco 1: 192.168.0.0 - 192.168.3.255/22

Bloco 2: 192.168.4.0 - 192.168.7.255/22

Bloco 3: 192.168.8.0 - 192.168.9.255/23

Bloco 4: 192.168.10.0 - 192.168.11.255/23

Bloco 5: 192.168.12.0 - 192.168.13.255/23

Bloco 6: 192.168.14.0 - 192.168.15.255/23

70. Comumente, os usuários utilizam a interface webmail para acessar suas caixas de mensagens através da web. Nesse cenário, o usuário utiliza um browser que se conecta e

interage com um servidor web. Por sua vez, o servidor web acessa localmente os arquivos que contêm as caixas de mensagens dos usuários e a devolve na forma de uma página HTML.

A) Considerando o browser e o servidor web, quem desempenha o papel de cliente e de servidor? Quem abre o socket ativo e o socket passivo ?

O browser desempenha um papel de **cliente**, já que inicia a conexão com o servidor web, realizando as solicitações de páginas, etc.

O servidor web desempenha um papel de **servidor** para o browser (pois espera solicitações do browser, fornecendo as respostas), mas ao mesmo tempo desempenha um papel de **cliente** para o servidor de email (pois ele inicia uma conexão com o servidor de email, realizando de maneira indireta as solicitações de informações de cada usuário de email, caixa de entrada, etc.).

O servidor de email, por sua vez, desempenha um papel de **servidor**, esperando e respondendo as solicitações enviadas pelo servidor web.

De acordo com as situações descritas acima, podemos verificar que o browser abre um socket ativo para a conexão com o servidor web. O servidor web abre um socket passivo para o recebimento de conexões de browser, e também um ativo para cada conexão de browser para o acesso ao servidor de emails. O servidor de emails abre um socket passivo para o recebimento de novas conexões dos servidores web.

B) Em um determinado instante, o servidor web está atendendo um único cliente webmail. O cliente está acessando apenas o webmail e nada mais. Considere que o servidor e o cliente estão sendo executados nas estações 192.168.10.1 e 192.168.20.2, respectivamente. Além disso, considere que o servidor adota a porta TCP 80 e o cliente a porta TCP efêmera 65432. Nesse cenário, identifique os endpoints (local e remoto) e os estados de TODOS os sockets usados pelo servidor e pelo cliente.

cliente (Endpoint local)

IP: 192.168.10.1

Porta Origem: 65432, Porta Destino: 80

IP destino: 192.168.20.2

Estado corrente do Socket: Established

Servidor (Endpoint Remoto)

IP: 192.168.20.2

Porta Origem: 80, Porta Destino: 65432

IP destino: 192.168.10.1

Estado corrente do Socket: Established

71. Um determinado roteador suporta roteamento classless e possui uma tabela de roteamento que é indicada abaixo. Forneça TODAS as rotas possíveis E a ROTA SELECIONADA para encaminhar datagramas para os endereços 195.112.92.1, 195.112.94.1, 195.112.96.1 e 195.112.130.1 JUSTIFIQUE, para cada caso, qual o critério a ser usado para selecionar a rota.

| Destino | Next-hop | Máscara |
|-------------------|------------|-----------------|
| 195.112.92.1 | 200.10.1.1 | 255.255.255.255 |
| 195.112.80.0 | 192.10.2.1 | 255.255.240.0 |
| 195.112.64.0 | 192.10.2.2 | 255.255.192.0 |
| 0.0.0.0 (default) | 200.10.1.2 | 0.0.0.0 |

195.112.92.1

Rota possível: 200.10.1.1 (rota direta)

195.112.94.1

Rota possível: 195.112.80.0 192.10.2.1 255.255.240.0

195.112.96.1

Rota possível: 195.112.64.0 192.10.2.2 255.255.192.0

195.112.130.1

Rota possível: 200.10.1.2 (rota parão)

0.0.0.0 (default) 200.10.1.2 0.0.0.0

72. Uma pessoa possui uma conta de usuário e uma conta de e-mail no domínio acme.com. Essa pessoa possui o seu MUA corretamente configurado para o seu servidor de SMTP (smtp.acme.com) e servidor POP (pop.acme.com). Todos os demais parâmetros de rede necessários a utilização da Internet estão corretamente configurados. Tudo está funcionando adequadamente. Agora, considere que essa pessoa envie um e-mail para dacomp@inf.ufrgs.br. Liste, na ordem CORRETA em que são acionados, TODOS os protocolos das camadas de REDE, TRANSPORTE e APLICAÇÃO envolvidos nesse envio por parte da máquina cliente. Para cada um dos protocolos usados ponha os seus encapsulamentos conforme o desenho fornecido no quadro. JUSTIFIQUE brevemente o porquê dessa ordem e o que cada um dos protocolos está fazendo.

IMPORTANTE : Desconsidere a existência de NAT e de informações em qualquer tipo de cache. Considere ainda que a máquina cliente está em uma rede e os demais servidores/serviços necessários estão em outras redes.

OBSERVAÇÃO : responda esta questão imaginando que você tem um analisador de protocolos (sniffer) instalado na máquina do usuário. A resposta esperada é a listagem dos protocolos que apareceriam nesse analisador e uma frase dizendo o porquê e o quê esse protocolo está fazendo.

- 1) ARP para consultar o endereço IP do servidor de DNS configurado na máquina cliente. ARP é encapsulado dentro de um quadro da camanha 2.
- 2) DNS. Para consultar o endereço IP do servidor de e-mails do cliente associado ao nome smtp.acme.com. O DNS é encapsulado dentro do UDP, que, por sua vez, é encapsulado dentro do IP.
- 3) ARP para o end. IP do servidor de e-mails. Como o servidor de e-mails é externo, o ARP será para o endereço IP do gateway padrão configurado na máquina cliente.
- 4) DNS para consultar o end. IP do servidor de e-mails do destino.
- 5) ARP para end. IP do servidor de e-mails a ser enviado. Será para o default gateway.
- 6) TCP para estabelecer conexão entre o cliente e o servidor de e-mails. O TCP é encapsulado dentro do IP.
- 7)SMTP para enviar a mensagem para o servidor de e-mails. O SMTP é encapsulado dentro do TCP, que é encapsulado dentro do IP.

73. Qual o prefixo e a máscara mais restritiva adequada para uma rede IP na qual existe um servidor com o endereço 192.168.1.5 e um único roteador com endereço 192.168.2.1 ? JUSTIFIQUE sua resposta.

Máscara 22

Rede 192.168.0.0 - 192.168.3.255

Máscara 23 não daria, pois p servidor e o roteador ficariam em redes separadas. Essas redes seriam: 192.168.0.0 - 192.168.1.255 e 192.168.2.0 - 192.168.2.255

74. Uma organização possui 7 redes identificadas de N1 a N7. Os prefixos de cada uma dessas rede são 200.10.0.0/26 (N1), 200.10.0.64/26 (N2), 200.10.0.128/26 (N3), 200.10.0.192/26 (N4), 200.10.1.0/26 (N5), 200.10.1.64/26 (N6) e 200.10.1.128/25 (N7). Qual é o bloco de endereços

alocado para a instituição ?

Bloco da instituição: 200.10.0.0/23

Agrupamentos:

$N1+N2+N3+N4 \rightarrow 24$

$N5+N6 \rightarrow 25$

$(N5+N6) + N7 \rightarrow 24$

$(N1+N2+N3+N4) + [(N5+N6) (N7)] \rightarrow 23$

75. Um usuário baixa arquivos de um servidor remoto na Internet usando FTP a partir de seu computador corretamente configurado em sua casa. Considerando que não há nenhuma informação armazenada em nenhum tipo de cache, liste TODOS os protocolos envolvidos nessa consulta, na ORDEM em que são acionados, a partir da camada de rede (inclusive). Para cada UM dos protocolos listados, forneça todos os encapsulamentos a partir da camada deste protocolo até a camada de rede (inclusive). EXPLICITE ainda o porquê que cada protocolo está sendo acionado em um dado momento. Considerações adicionais : o usuário não tem nenhum serviço Internet instalado em seu computador ou em sua rede local. Há apenas o computador do usuário nesta casa. Responda a questão imaginando que você tem um analisador de protocolos (sniffer) instalado na máquina de usuário. A resposta esperada é a listagem dos protocolos que apareceriam nesse analisador.

1) ARP para o end. IP do servidor de DNS. ARP é encapsulado na camada 2.

2) DNS para obter endereço IP associado ao nome do servidor de FTP. DNS é encapsulado dentro do UDP que, por sua vez é encapsulado dentro do IP

3) ARP para obter o end. IP do default gateway

4) TCP abrir conexão com porta 21 do servidor de FTP. TCP é encapsulado dentro do IP.

5) FTP para transferência de dados. FTP é encapsulado dentro do TCP, que é encapsulado dentro do IP.

76. Que vantagens o roteamento hierárquico traz para o procedimento de roteamento ? EXPLIQUE claramente o impacto dessas vantagens.

A medida que as redes aumentam, as tabelas de roteamento no roteadores também aumentam. Tabelas maiores consomem recursos dos roteadores (memória, CPU para a busca e mais largura de banda para enviar tabelas) até que se torne inviável cada roteador saber uma rota para qualquer outro roteador.

Com o roteamento hierárquico, os roteadores são divididos em regiões. Os roteadores sabem rotear pacotes para roteadores de sua região.

Por exemplo, considerando uma rede com 720 roteadores. Sem hierarquia, seriam necessárias 720 entradas na tabela de roteamento de cada roteador. Se a rede for dividida em 24 regiões de 30 roteadores cada, cada roteador precisará de 30 entradas locais e mais 23 remotas. De 720 entradas em cada roteador, diminuiria para 53 entradas. Aumentando a quantidade de níveis, reduz ainda mais a quantidade de entradas na tabela. Mamoun e Kleinrock descobriram que o número ideal de níveis para uma rede com N roteadores é $\ln N$, exigindo um total de $e \ln N$ entradas. [TANENBAUM5PT, pág. 237-238]

Outras vantagens do roteamento hierárquico são: escalabilidade (as redes podem crescer, porém basta colocar poucas novas entradas na tabela de roteamento) e autonomia administrativa (evitar tráfego de redes um nível superior em um nível inferior, internamente o próprio nível faz o seu controle). Para isto acontecer deve-se definir um roteamento padrão para a rede interna (*estado de enlace* ou *vetor de distância*), de modo que esta rede irá se comunicar com uma rede em outro nível (superior) a partir do roteador de borda.

77. Um provedor possui uma faixa de endereços IP válidos (195.168.0.0/16) para distribuir entre seus clientes empresariais. Ele oferece pacotes de até 30, até 62 e até 126 endereços IPs. As empresas A,B e C desejam adquirir o pacote de 30 endereços; a empresa D, o pacote de 62 endereços e as empresas E e F o pacote de 126 endereços. Considerando que a distribuição inicia a partir do endereço de base do bloco, você, como administrador da rede do provedor, defina as configurações a serem passadas para cada um dos administradores de rede das empresas A,B,C,D,E e F.

REDE A: 195.168.0.0/27 máscara 255.255.255.224 (IPs de 195.168.0.0 - 195.168.0.31)

REDE B: 195.168.0.32/27 máscara 255.255.255.224 (IPs de 195.168.0.32 - 195.168.0.63)

REDE C: 195.168.0.64/27 máscara 255.255.255.224 (IPs de 195.168.0.64 - 195.168.0.95)

REDE LIVRE: 195.168.0.192/27 máscara 255.255.255.224 (IPs de 195.168.0.96 - 195.168.0.127)

REDE D: 195.168.0.128/26 máscara 255.255.255.192 (IPs de 195.168.0.128 - 195.168.0.191)

REDE LIVRE: 195.168.0.192/26 máscara 255.255.255.192 (IPs de 195.168.0.192 - 195.168.0.255)

REDE E: 195.168.1.0/25 máscara 255.255.255.128 (IPs de 195.168.1.0 - 195.168.0.127)

REDE F: 195.168.1.128/25 máscara 255.255.255.128 (IPs de 195.168.1.128 - 195.168.0.255)

78. Um administrador recém-contratado está tentando identificar os serviços que estão sendo oferecidos em uma determinada máquina. Para tal, ele executou o comando netstat, cuja saída é fornecida abaixo :

```
>netstat -tuan
```

| Proto | Recv-Q | Send-Q | Local Address | Foreign Address | State |
|-------|--------|--------|----------------|-------------------|-------------|
| tcp | 0 | 0 | 0.0.0.0:25 | 0.0.0.0:* | LISTEN |
| tcp | 0 | 0 | 0.0.0.0:80 | 0.0.0.0:* | LISTEN |
| tcp | 0 | 0 | 192.10.1.33:21 | 0.0.0.0:* | LISTEN |
| tcp | 0 | 0 | 192.10.1.65:25 | 192.10.1.1:55120 | ESTABLISHED |
| tcp | 0 | 0 | 192.10.1.33:21 | 200.20.1.1:63472 | ESTABLISHED |
| tcp | 0 | 0 | 192.10.1.65:80 | 150.10.50.1:54387 | ESTABLISHED |
| udp | 0 | 0 | 0.0.0.0:7 | 0.0.0.0:* | |
| udp | 0 | 0 | 192.10.1.97:53 | 0.0.0.0:* | |

IMPORTANTE:

O endereço 0.0.0.0 tem a seguinte semântica: em **Local Address** significa "para qualquer interface", em **Foreign Address** significa "de qualquer IP".

Responda :

a) Quantos serviços estão em execução nessa máquina ?

5 serviços (ou portas abertas), cujos serviços estão nas portas: 25 (ftp), 80 (http), 21 (smtp), 53 (dns) e 7 (echo).

Os serviços das portas 25, 80 e 21 são TCP e os serviços 53 e 7 são UDP.

Quais os protocolos de transporte que estão sendo usados por esses serviços?

UDP e TCP

Quantos serviços de cada tipo de protocolo de transporte existem? JUSTIFIQUE.

3 TCP e 2 UDP.

b) Identifique quais os sockets que são usados para aguardar requisições de pedidos de

conexão (segmentos com flag SYN ativo). JUSTIFIQUE.

Os 3 sockets no estado LISTEN. Somente esses são capazes de processar segmentos com a flag SYN ligada.

c) Quantos clientes estão usando os serviços no momento que o comando foi executado? JUSTIFIQUE.

tcp 0 0 192.10.1.65:25 192.10.1.1:55120 ESTABLISHED

tcp 0 0 192.10.1.33:21 200.20.1.1:63472 ESTABLISHED

tcp 0 0 192.10.1.65:80 150.10.50.1:54387 ESTABLISHED

3 clientes com conexão estabelecidas (estado ESTABLISHED).

No protocolo UDP não existem clientes com conexão estabelecida.

d) É possível deduzir o(s) endereço(s) IP dessa máquina? Qual ou quais é(são) ele(s)? JUSTIFIQUE.

Sim, é possível deduzir os IPs da máquina onde o comando foi executado, os IPs são:

192.10.1.33 (ftp porta 21)

192.10.1.65 (smtp porta 25)

192.10.1.97 (requisições de DNS)

Estão sendo usadas 3 interfaces de rede.

e) Essa máquina recebeu um segmento de SYN cujas portas de origem e destino são 55120 e 25. Para qual socket este segmento foi encaminhado? JUSTIFIQUE.

Será encaminhado para o primeiro socket que está escutando na porta 25 (smtp), identificado por: tcp 0 0 0.0.0.0:25 0.0.0.0:* LISTEN. Esse é o socket que atende às conexões da porta 25 em todas as interfaces da máquina e aceita conexões de qualquer IP e qualquer porta de uma máquina remota.

f) Na saída desse comando, os sockets udp não estão com nenhum estado assinalado. Isso significa algum tipo de problema na máquina? Sim ou Não? JUSTIFIQUE. OBS.: os parâmetros -tuan e as colunas Recv-Q e Send-Q são totalmente irrelevantes para responder a questão. Da mesma forma, não é preciso saber qual serviço Internet está associado a cada número de porta. Basta dizer, por exemplo, "o serviço da porta 80".

Não, o protocolo UDP é não orientado a conexão, por esse motivo não é especificado o IP das máquinas de origem dos datagramas..

79. Considere a linha abaixo, extraída da saída do resultado do comando "netstat -na", no Windows XP :

TCP 127.0.0.1:2222 0.0.0.0:* LISTENING

EXPLIQUE o quê ela representa (obs: o comando "netstat" fornece, entre outras coisas, informações sobre os sockets do sistema).

Resposta Oficial:

A linha significa que há um serviço orientado à conexão (TCP) na porta 2222, e que só aceita conexões provenientes da interface de rede 127.0.0.1, ou seja, da própria máquina em que o serviço está sendo executado.

Resposta 1:

Significa que a máquina está aceitando conexões TCP no endereço de loopback (127.0.0.1) na porta 2222 de qualquer endereço e qualquer porta remota.

Resposta 2:

Função do comando netstat: mostrar as conexões TCP ativas, quais portas estão recebendo conexões (listening), estatísticas da Ethernet, tabela de roteamento IP, estatísticas do IPv4 (IP, ICMP, TCP, UDP)

e estatísticas do IPv6 (IPv6, ICMPv6, TCP over IPv6 e UDP over IPv6).

Parâmetros usados na questão:

- **-n:** mostra as conexões TCP ativas, entretanto os endereços e portas são espessos numericamente, não sendo possível determinar os nomes.
- **-a:** mostra todas as conexões TCP ativas e as portas TCP e UDP que o computador está aceitando conexões (listening)

Retorno do comando:

- Protocolo
- Endereço Local:Porta
 - se a porta não foi estabelecida, ela é mostrada como um asterisco (*)
- Endereço Remoto:Porta
 - se a porta não foi estabelecida, ela é mostrada como um asterisco (*)
- Estado da conexão TCP
 - CLOSE_WAIT, CLOSED, ESTABLISHED, FIN_WAIT_1, FIN_WAIT_2, LAST_ACK, LISTEN, SYN_RECEIVED, SYN_SEND, TIMED_WAIT

Aplicando os dados do comando sobre o retorno do mesmo passado no exercício temos:

- Protocolo = TCP
- Endereço Local:Porta = 127.0.0.1:2222 (loopback)
- Endereço Remoto:Porta = 0.0.0.0:* (qualquer máquina, porta não estabelecida ainda)
- Estado da conexão TCP = LISTENING (aceitando conexões)

Portando o comando nos indica que a máquina local (endereço IP 127.0.0.1) está aceitando conexões TCP (serviço orientado a conexão) na porta 2222 provenientes de qualquer endereço IP e qualquer porta. Porém como o endereço IP 127.0.0.1 que representa a máquina local não é roteável, não serão aceitas conexões de IPs externos à máquina local, portanto *só serão aceitas conexões de processos da própria máquina local.*

[MICROSOFT, [Microsoft Windows XP Product Documentation](#); WIKIPEDIA, [netstat](#); VIVA O LINUX, [Netstat a Fundo](#); COMMANDWINDOWS.COM, [Netstat](#)]

80. Ao se dividir uma faixa de endereços IP como 200.30.40.0 com uma máscara 255.255.255.0 (/24) em sete sub-redes, há diferenças entre se considerar um sistema classfull ou um sistema classless? Se sim, quais são elas e quais parâmetros de rede são afetados? Se não, defina os endereços de cada uma das sub-redes.

Resposta 1:

Sim. Um sistema classfull não aceita as redes 0 e a rede de broadcast. Se fossem necessárias 7 redes, no sistema classful teria que utilizar uma máscara 28 (14 redes "úteis") e no sistema classless uma máscara 27 serviria (8 redes úteis).

Resposta 2:

Há diferenças entre ambos os sistemas. No sistema *classfull* existem algumas limitações para as subredes: as máscaras de subredes devem ter o mesmo tamanho e não se pode usar as subredes que contenham os endereços onde todos os bits do sufixo são 0 (endereço de subrede, no caso do enunciado não podemos usar a subrede que contém o IP 200.30.40.0) nem as subredes onde todos os bits do sufixo são 1 (endereço de broadcast, no caso do enunciado não podemos usar a subrede que contém o IP 200.30.40.255). Com essa reserva de endereços feita pelo padrão há uma "perda" de 2 subredes. Nesse caso o número total de subredes é limitado a $2^n - 2$, onde n é o número de bits usados na subrede. No sistema *classfull* caso precisássemos de 7 redes teríamos que usar uma máscara /28

(16 subredes, onde apenas 14 podem ser utilizadas) e poderíamos escolher 7 das 14 redes disponíveis, cada rede com 14 IPs válidos. Com o sistema *classless* não há mais a reserva dos endereços cujos bits do sufixo são 0 (no caso do enunciado, o endereço 200.30.40.0) e 1 (no caso do enunciado, o endereço 200.30.40.255), eles podem ser utilizados normalmente e representarão os endereços da primeira subrede (no caso de 200.30.40.0) e o endereço de broadcast da última subrede (no caso de 200.30.40.255), no sistema *classless* as subredes também podem ter diferentes tamanhos de máscaras. Nesse sistema o número total de subredes é limitado a 2^n , onde n é o número de bits usados na subrede. No caso do *classfull* podemos dividir em uma subrede /26 e seis subredes /27.

Podemos ter os seguintes endereços de subredes no padrão *classfull* /28 (4 bits para subrede):

| Binário | Rede | Broadcast | Range | OBS |
|---|---------------|---------------|----------|-----------|
| 1100 1000.0001 1110.0010 1000.0000 0000 | 200.30.40.0 | 200.30.40.15 | 1..14 | Inválido |
| 1100 1000.0001 1110.0010 1000.0001 0000 | 200.30.40.16 | 200.30.40.31 | 17..30 | Rede 1 |
| 1100 1000.0001 1110.0010 1000.0010 0000 | 200.30.40.32 | 200.30.40.47 | 33..46 | Rede 2 |
| 1100 1000.0001 1110.0010 1000.0011 0000 | 200.30.40.48 | 200.30.40.63 | 49..62 | Rede 3 |
| 1100 1000.0001 1110.0010 1000.0100 0000 | 200.30.40.64 | 200.30.40.79 | 65..78 | Rede 4 |
| 1100 1000.0001 1110.0010 1000.0101 0000 | 200.30.40.80 | 200.30.40.95 | 81..94 | Rede 5 |
| 1100 1000.0001 1110.0010 1000.0110 0000 | 200.30.40.96 | 200.30.40.111 | 97..110 | Rede 6 |
| 1100 1000.0001 1110.0010 1000.0111 0000 | 200.30.40.112 | 200.30.40.127 | 113..126 | Rede 7 |
| 1100 1000.0001 1110.0010 1000.1000 0000 | 200.30.40.128 | 200.30.40.143 | 129..142 | Não Usado |
| 1100 1000.0001 1110.0010 1000.1001 0000 | 200.30.40.144 | 200.30.40.159 | 145..158 | Não Usado |
| 1100 1000.0001 1110.0010 1000.1010 0000 | 200.30.40.160 | 200.30.40.175 | 161..174 | Não Usado |
| 1100 1000.0001 1110.0010 1000.1011 0000 | 200.30.40.176 | 200.30.40.191 | 177..190 | Não Usado |
| 1100 1000.0001 1110.0010 1000.1100 0000 | 200.30.40.192 | 200.30.40.207 | 193..206 | Não Usado |
| 1100 1000.0001 1110.0010 1000.1101 0000 | 200.30.40.208 | 200.30.40.223 | 209..222 | Não Usado |
| 1100 1000.0001 1110.0010 1000.1110 0000 | 200.30.40.224 | 200.30.40.239 | 225..238 | Não Usado |
| 1100 1000.0001 1110.0010 1000.1111 0000 | 200.30.40.240 | 200.30.40.255 | 241..254 | Inválido |

Podemos ter os seguintes endereços de subredes no padrão *classless* (bits para subrede podem ser diferentes):

| Binário | Máscara | Rede | Broadcast | Range |
|---|---------|---------------|---------------|----------|
| 1100 1000.0001 1110.0010 1000.0000 0000 | /26 | 200.30.40.0 | 200.30.40.63 | 1..62 |
| 1100 1000.0001 1110.0010 1000.0100 0000 | /27 | 200.30.40.64 | 200.30.40.95 | 65..94 |
| 1100 1000.0001 1110.0010 1000.0110 0000 | /27 | 200.30.40.96 | 200.30.40.127 | 97..126 |
| 1100 1000.0001 1110.0010 1000.1000 0000 | /27 | 200.30.40.128 | 200.30.40.159 | 129..158 |
| 1100 1000.0001 1110.0010 1000.1010 0000 | /27 | 200.30.40.160 | 200.30.40.191 | 161..190 |

| | | | | |
|---|-----|---------------|---------------|----------|
| 1100 1000.0001 1110.0010 1000.1100 0000 | /27 | 200.30.40.192 | 200.30.40.223 | 193..222 |
| 1100 1000.0001 1110.0010 1000.1110 0000 | /27 | 200.30.40.224 | 200.30.40.255 | 225..255 |

[WIKIPÉDIA, Máscara de Rede; RFC 950; RFC 1812; Aula 17, Slides 5-15]

81. Em uma rede é usado roteamento com vetor de distância. Nessa rede existem seis roteadores A, B, C, D, E e F. Em um dado momento os vetores de distância a seguir chegam no roteador C : de B(5, 0, 8, 12, 6, 2), de D :(16, 12, 6, 0, 9, 10), e de E :(7, 6, 3, 9, 0, 4). Da esquerda para a direita, cada um dos valores desses vetores correspondem, respectivamente, aos roteadores A, B, C, D, E e F. Os retardos (custo) medidos de C para B, D e E são 6, 3 e 5, respectivamente. Qual é a nova tabela de roteamento de C ? Forneça, para cada destino, a linha de saída a ser usada e o retardo esperado.

| | Custo | Next hop |
|---|-------|----------|
| A | 11 | B |
| B | 6 | B |
| C | 0 | - |
| D | 3 | D |
| E | 5 | E |
| F | 8 | B |

82. Supondo uma máquina com capacidade de processamento e memória infinitos, qual seria o número máximo teórico de conexões TCP estabelecidas que essa máquina poderia suportar ao mesmo tempo? JUSTIFIQUE.

Resposta 1:

2^{16} conexões, que é o número máximo de portas disponíveis, tanto para recebimento como envio de dados, no TCP.

Resposta 2:

2^{16} (portas de origem) * 2^{32} (IPs de origem)

Resposta 3 (gabarito):

O número máximo teórico de conexões é limitado pela capacidade de endereçamento dos números de portas (2^{16}), o que permite 65536 conexões simultâneas em uma máquina. (No contexto exposto na questão foi aceito “infinitas”, SE considerasse infinitas máquinas se conectando em uma porta. ENTRETANTO, nessa lógica, o mais correto seria 2^{16} (nro de portas) * 2^{32} (nro de end. IP). Nesse caso, o recurso consumido seriam as estruturas de dados que representam os sockets e não a capacidade de endereçamento).

83. Que vantagens os sistemas autônomos trazem para o roteamento ? EXPLIQUE claramente o impacto delas no procedimento de roteamento.

Um sistema autônomo é um grupo de redes e roteadores sob regência de uma única administração. A vantagens dos sistemas autônomos para o roteamento é autonomia administrativa e a escalabilidade.

- 1) Escalabilidade. Grupos de roteadores reduzem tabela de roteamento.
- 2) Autonomia. Podem escolher o protocolo IRP que quiserem.

84. Uma determinada instituição possui o bloco 192.50.32.0/19. Essa instituição tem quatorze redes, cada uma delas com certo número máximo de máquinas, de acordo com a tabela abaixo. Considerando que cada máquina possua um único endereço IP, aloque blocos de endereços IP para cada uma das redes (N1 a N14).

Qtd. de sub-redes Nome da sub-redes Nro. máximo de máquinas

- 1 N1 800 -> 1024 endereços /22
- 2 N2, N3 400 -> 512 endereços /23
- 1 N4 350 -> 512 endereços /23
- 2 N5, N6 200 -> 256 endereços /24
- 5 N7, N8, N9, N10, N11 100 -> 128 endereços /25
- 3 N12, N13, N14 80 -> 128 endereços /25

N1: 192.50.32.0 - 192.50.35.255 máscara /22 ou 255.255.252.0
N2: 192.50.36.0 - 192.50.37.255 máscara /23 ou 255.255.254.0
N3: 192.50.38.0 - 192.50.39.255 máscara /23 ou 255.255.254.0
N4: 192.50.40.0 - 192.50.41.255 máscara /23 ou 255.255.254.0
N5: 192.50.42.0 - 192.50.42.255 máscara /24 ou 255.255.255.0
N6: 192.50.43.0 - 192.50.43.255 máscara /24 ou 255.255.255.0
N7: 192.50.44.0 - 192.50.44.127 máscara /25 ou 255.255.255.128
N8: 192.50.44.128 - 192.50.44.255 máscara /25 ou 255.255.255.128
N9: 192.50.45.0 - 192.50.44.127 máscara /25 ou 255.255.255.128
N10: 192.50.45.128 - 192.50.44.255 máscara /25 ou 255.255.255.128
N11: 192.50.46.0 - 192.50.46.127 máscara /25 ou 255.255.255.128
N12: 192.50.46.128 - 192.50.46.255 máscara /25 ou 255.255.255.128
N13: 192.50.47.0 - 192.50.47.127 máscara /25 ou 255.255.255.128
N14: 192.50.47.128 - 192.50.47.255 máscara /25 ou 255.255.255.128

Sobrou o bloco: 192.50.48.0/20

85. O protocolo UDP usa apenas a porta de destino para demultiplexar os datagramas recebidos, ao passo que o protocolo TCP utiliza a identificação da conexão, ou seja, um par de endpoints (ou sockets). Porque o TCP não pode utilizar apenas a porta de destino para demultiplexação ?

Pois o TCP é um protocolo orientado a conexão, unicast. Caso utilizássemos apenas a porta de destino, permitiríamos que qualquer destino (inclusive os sem conexão estabelecida) enviassem pacotes para um receptor, fato que não está de acordo com o processo de conexão (pois uma conexão depende, também, da porta de origem) e também viola a idéia do TCP ser um protocolo unicast, onde é necessário identificar os pares (origem e destino).

86. O que são sistemas autônomos (SA) ? Qual a principal motivação para a criação e uso desse conceito ? Exemplifique seu emprego na Internet.

Um sistema autônomo é um grupo de redes e roteadores sob regência de uma única administração. O roteamento dentro de um sistema autônomo é chamado de roteamento intradomínio. O roteamento entre sistemas autônomos é chamado de interdomínio.

A principal motivação para a criação e uso dos sistemas autônomos é a independência na

administração. Cada sistema autônomo pode escolher um ou mais protocolos de roteamento intradomínio para tratar do roteamento dentro do sistema autônomo, pode querer rotear utilizando métricas diferentes, como menor atraso, custo monetário, etc.

Na internet, um SA seria uma rede de ISP (embora uma ISP possa ter mais de um SA). Um grande fator de determinante são os arranjos comerciais entre os ISPs. Cada ISP pode cobrar ou receber dinheiros de outros ISPs para transportar tráfego. Há também a questão política. Os dados podem estar trafegando em territórios com leis distintas. Todas estas questões não técnicas são incluídas no conceito de política de roteamento.

Exemplos de protocolos utilizados para roteamento intradomínio: RIP e OSPF

Exemplo de protocolo utilizado para roteamento interdomínio: BGP. O BGP pode ainda ser dividido em IBGP e EBGP. O IBGP é utilizado para trocar informações entre roteadores dentro de um mesmo sistema autônomo. O EBGP é utilizado para trocar informações entre roteadores pertencentes a sistemas autônomos diferentes.

[TANENBAUM5PT] pág 270-271 [FOROUZAN4PT] pág 659

87. O TCP inicializa o estabelecimento de uma conexão realizando um protocolo de apresentação de três vias (three-way hand- shake) onde os pares negociam entre si os números de sequência que cada um utilizará até o final da conexão. Que tipo(s) de problema(s) ocorreria(m) se a numeração de sequência fosse iniciada a partir de zero ?

Iniciando uma conexão a partir do zero (ou a partir de qualquer outro número fixo), teríamos o problema com pacotes 'fantasmas'.

Essa situação pode acontecer da seguinte maneira, imagine duas máquinas A e B:

1. 'A' inicia uma conexão com 'B', definindo seu número de sequência inicial em 0.
2. 'A' envia segmentos para 'B', porém um segmento qualquer, por exemplo, de número 600 é enviado, mas, por algum motivo, demora para chegar em 'B'.
3. O timeout desse segmento é excedido e A retransmite o segmento 600, que chega em 'B' e é confirmado pelo receptor. Nesse momento, o segmento 600 da primeira transmissão ainda está 'flutuando na rede, tentando atingir o seu destino 'B'.
4. 'A' finaliza a conexão com 'B'.
5. 'A' cria uma nova conexão com B, definindo seu número de sequência inicial, novamente em 0, a conexão é iniciada..
6. Antes do envio do primeiro pacote de dados de 'A', nessa nova conexão, o pacote 'fantasma' da conexão anterior chega em 'B'. 'B' identifica ele como um número de sequência válido, armazena seus dados e envia um ACK 601, confirmando o recebimento de 600 bytes de 'A', o que é um problema, uma vez que esses dados pertenciam a uma conexão anterior e estão fora do contexto da conexão atual.

A solução para esse problema (além do esquema de 'sorteio' de porta de origem para o envio dos dados, que é adotado por algumas implementações de software de aplicação e permite que uma porta de uma conexão anterior não seja a mesma de uma nova conexão, fazendo com que o receptor identifique o pacote fantasma pelo número da porta de origem) é sortear um número aleatório para o número de sequência inicial. Sendo assim, o segmento com número 600 na primeira conexão teria chances pequenas de ser recebido por 'B' na nova conexão, uma vez que o número de sequência utilizado provavelmente seria consideravelmente diferente, a ponto do receptor 'B' poder detectar que o

segmento trata-se de um segmento 'fantasma'.

Explicação do Prof. Caríssimi:

https://picasaweb.google.com/lh/photo/dkYq_U9mSe0hJIF89I2u45tFo3m1WbVwYzWK7sSPCXU?feat=directlink

88. Um software MUA, como o outlook, Mozilla-Thunderbird, Eudora, etc, executa que protocolos tipicamente? Descreva o que cada um desses protocolos faz e suas principais características? (OBS. : não é para mostrar a PDU de cada protocolo e suas mensagens, mas sim as suas funcionalidades).

Os protocolos executados em um software MUA tipicamente são:

POP: Para acessar as mensagens no servidor de e-mails e baixa-las localmente. A cada momento que o usuário acessar sua caixa postal, as mensagens atuais são baixadas para a estação de trabalho usada para acesso.

IMAP: manipular emails em pastas que podem estar localizadas no servidor de email. Em uma conexão IMAP, todas as mensagens do usuários residem no servidor de email. As mensagens são transmitidas somente para serem mostradas na tela da estação de trabalho.

SMTP: Protocolo para envio de e-mails.

Fonte: http://www.gta.ufrj.br/grad/01_2/qmail/page2.html

89. Um provedor de acesso a Internet alocou para um cliente a rede 200.231.15.240 (CIDR) com 16 endereços IP (incluindo os endereços especiais). Quais são os primeiro e último endereços válidos para interfaces de redes, a máscara de rede e o endereço de broadcast desta rede ?

16 Endereços: 4 bits para subrede, ou ainda, 28 bits para máscara.

Endereço da rede: 200.231.15.240

Endereço Broadcast: 200.231.15.255

Primeiro endereço válido: 200.231.15.241

Último endereço válido: 200.231.15.254

90. Uma organização detém a rede 200.15.20.0/24 e a organiza em sub-redes. Uma máquina configurada com endereço IP 200.15.20.131, com default gateway 200.15.20.158 e servidor de DNS 200.15.20.33, executa um cliente HTTP (browser) para acessar a página www.uefa.com (IP 72.246.216.26). Sabe-se ainda que o default gateway é o último endereço válido da sub-rede onde se encontra a máquina que executa o cliente HTTP.

Supondo que você esteja capturando o tráfego nessa rede com um sniffer, liste, NA ORDEM

CORRETA em que são capturados, **TODOS** os protocolos da camada de rede, de transporte e de aplicação. **JUSTIFIQUE** brevemente o que cada um dos protocolos faz quando acionado e o porquê da ordem fornecida. **IMPORTANTE:** Desconsidere que as informações são lidas de qualquer tipo de cache, isto é, as informações necessárias não estão armazenadas em nenhum tipo de cache e todas devem ser buscadas através de requisições.

ARP request: consulta a MAC do servidor de DNS

ARP replay: resposta com o MAC do servidor de DNS

DNS para fazer a consulta no servidor de DNS

UDP para transportar requisições e respostas do servidor DNS

ARP request para encontrar IP do Gateway

ARP replay do Gateway

Resolução recursiva de DNS

UDP para transportar requisições e respostas do DNS externo

TCP para abrir a conexão

HTTP para fazer requisições da página

91. Descreva o que acontece em uma rede IP quando uma máquina possui :

A) um endereço IP duplicado.

Inconsistência/Ambiguidade na rede, levando a um comportamento inesperado.

Com relação ao ARP, duas máquinas responderão pelo mesmo IP, não sendo possível determinar qual responderá e será atendida primeiro.

B) a máscara de sub-rede é mais restritiva do que deveria ser.

Endereço da rede obtido com a aplicação da máscara não será correto. O IP a ser acessado pode estar na rede e o host identificar que está em uma rede externa.

C) a máscara de sub-rede é menos restritiva do que deveria ser.

Endereço da rede obtido com a aplicação da máscara não será correto, podendo ser roteado para uma rede diferente.

D) o default gateway não está configurado e não há proxy arp na rede.

Rede não consegue alcançar rede externa.

E) o endereço do servidor de DNS não está corretamente configurado.

Hosts não conseguem resolver nomes. A rede interna e externa continuam funcionando pelos seus IPs.

Seja bastante **CLARO** e **EXPLÍCITO** na sua resposta ressaltando os protocolos afetados e/ou o comportamento apresentado pela máquina cliente e seus aplicativos em cada uma das situações listadas anteriormente.