1. Qual é a diferença entre rotear e repassar (transmitir)?

R: Repasse refere-se à ação local realizada por um roteador para transferir um pacote da interface de um enlace de entrada para interface de enlace de saída apropriada.

Roteamento refere-se ao processo de âmbito geral da rede que determina os caminhos fim a fim que os pacotes percorrem desde a origem até o destino.

1. Explique como são configuradas as tabelas de repasse nos roteadores.

R: Um roteador repassa um pacote examinando o valor de um campo no cabeçalho do pacote que está chegando e então utiliza esse valor para indexar sua tabela de repasse. O resultado da tabela de repasse indica para qual das interfaces de enlace do roteador o pacote deve ser repassado. Dependendo do protocolo de camada de rede, o valor no cabeçalho do pacote pode ser o endereço de destino do pacote ou uma indicação da conexão à qual ele pertence. O algoritmo de roteamento determina os valores que são inseridos nas tabelas de repasse dos roteadores. Esse algoritmo pode ser centralizado (por exemplo, por um algoritmo que roda em um local central e descarrega informação de roteamento a cada um dos roteadores) ou descentralizado (com o algoritmo funcionando em cada roteador). Um roteador recebe mensagens de protocolo de roteamento que são utilizadas para configurar sua tabela de repasse.

1. Defina o modelo de serviço de rede.

R: O modelo de serviço de rede define as características dos transportes de dados fim a fim entre uma borda da rede e a outra, isto é, entre sistemas finais remetentes e destinatários.

1. Cite e explique alguns serviços possíveis que a camada de rede pode oferecer.

R: Entrega garantida: Esse serviço assegura que o pacote mais cedo ou mais tarde chegará a seu destino.

Entrega garantida com atraso limitado: Não somente assegura a entrega de um pacote, mas também a entrega com um atraso hospedeiro a hospedeiro limitado e especificado (por exemplo, dentro de 100ms).

Além disso, há outros serviços que podem ser providos a um fluxo de pacotes entre uma origem e um destino determinados, como os seguintes:

Entrega de pacotes na ordem: Garante que pacotes chegarão ao destino na ordem em que foram enviados.

Largura de banda mínima garantida: Esse serviço de camada de rede emula o comportamento de um enlace de transmissão com uma taxa de bits especificada entre hospedeiros remetentes e destinatários. Contanto que o hospedeiro remetente transmita bits (como parte de pacotes) a uma taxa abaixo da taxa de bits especificada, nenhum pacote será perdido e cada um chegará dentro de um atraso hospedeiro a hospedeiro previamente especificado (por exemplo, dentro de 40 ms).

Jitter máximo especificado: Assegura a quantidade de tempo entre a transmissão de dois pacotes sucessivos no remetente seja igual à quantidade de tempo entre o recebimento dos dois pacotes no destino (ou que esse espaçamento não mude mais do que algum valor especificado).

Serviços de segurança: Utilizando uma chave de sessão secreta conhecida somente por um hospedeiro de origem e de destino, a camada de rede no computador de origem pode codificar a carga útil de todos os datagramas que estão sendo enviados ao computador de destino. A camada de rede no computador de destino, então, seria responsável por decodificar as cargas úteis. Com esse serviço, o sigilo seria fornecido para todos os segmentos da camada de transporte (TCP e UDP) entre os computadores de origem e de destino. Além do sigilo, a camada de rede poderia prover integridade dos dados e serviços de autenticação na origem.

1. O que são redes de circuitos virtuais e rede de datagramas? Explique cada uma delas.

R: Redes de computadores que oferecem apenas um serviço orientado para conexão na camada de rede são denominadas rede de circuitos virtuais (redes cv); redes de computadores que oferecem apenas um serviço não orientado para conexão na camada de rede são denominadas redes de diagramas.

1. Cite e explique brevemente o que há dentro de um roteador

R**: Portas de entrada**: A porta de entrada tem diversas funções. Ela realiza as funções de camada física de terminar um enlace físico de entrada em um roteador. Executa também as de camada de enlace (representadas pelas caixas do meio nas portas de entrada e de saída) necessárias para interoperar com as funções da camada de enlace do outro lado do enlace de entrada. Talvez mais importante, a função de exame também é realizada na porta de entrada; isso ocorrerá na caixa mais à direita da porta de entrada.

**Elemento de comutação:** O elemento de comutação conecta as portas de entrada do roteador às suas portas de saída. Ele está integralmente contido no interior do roteador — uma rede dentro de um roteador da rede!

Portas de saída: Uma porta de saída armazena os pacotes que foram repassados a ela através do elemento de comutação e, então, os transmite até o enlace de saída, realizando as funções necessárias da camada de enlace e da camada física. Quando um enlace é bidirecional (isto é, carrega um trafego em ambas as direções), uma porta de saída para o enlace será emparelhada com a porta de entrada para esse enlace na mesma placa de linha (uma placa de circuito impresso contendo uma ou mais portas de entrada, e que está conectada ao elemento de comutação).

**Processador de roteamento**: O processador de roteamento executa os protocolos de roteamento, mantém as tabelas de roteamento e as informações de estado do enlace, e calcula a tabela de repasse para o roteador. Ele também realiza funções de gerenciamento de rede

1. Explique a fragmentação do datagrama IP.

R: Alguns protocolos podem transportar datagramas grandes, ao passo que outros apenas pacotes pequenos. Por exemplo, quadros Ethernet não podem conter mais do que 1.500 bytes de dados, enquanto quadros para alguns enlaces de longa distância não podem conter mais do que 576 bytes. A quantidade máxima de dados que um quadro de camada de enlace pode carregar é denominada unidade máxima de transmissão (maximum transmission unit — MTU). Como cada datagrama IP é encapsulado dentro do quadro de camada de enlace para ser transportado de um roteador até o roteador seguinte, a MTU do protocolo de camada de enlace estabelece um limite estrito para o comprimento de um datagrama IP. Ter uma limitação estrita para o tamanho de um datagrama IP não é grande problema. O problema é que cada um dos enlaces da rota entre remetente e destinatário pode usar diferentes protocolos de camada de enlace, e cada um desses protocolos pode ter diferentes MTUs. Para entender melhor a questão do repasse, imagine que você é um roteador que está interligando diversos enlaces, cada um rodando diferentes protocolos de camada de enlace com diferentes MTUs. Suponha que você receba um datagrama IP de um enlace, verifique sua tabela de repasse para determinar o enlace de saída e perceba

Kurose\_menor.indb 247 01/08/13 20:57

 Redes de computadores e a InteRnet248

que este tem uma MTU menor do que o comprimento do datagrama IP. É hora de entrar em pânico — como você vai comprimir esse datagrama IP de tamanho excessivo no campo de carga útil do quadro da camada de enlace? A solução para esse problema é fragmentar os dados do datagrama IP em dois ou mais datagramas IP menores, encapsular cada um em um quadro separado na camada de enlace e, então, enviá- los pelo enlace de saída. Cada um desses datagramas menores é denominado um fragmento. Fragmentos precisam ser reconstruídos antes que cheguem à camada de transporte no destino. Na verdade, tanto o TCP quanto o UDP esperam receber da camada de rede segmentos completos, não fragmentados. Os projetistas do IPv4 perceberam que a reconstrução de datagramas nos roteadores introduziria uma complicação significativa no protocolo e colocaria um freio no desempenho do roteador. (Se você fosse um roteador, ia querer reconstruir fragmentos além de tudo mais que tem de fazer?) Seguindo o princípio de manter a simplicidade do núcleo da rede, os projetistas do IPv4 decidiram alocar a tarefa de reconstrução de datagramas aos sistemas finais, e não aos roteadores da rede. Quando um hospedeiro destinatário recebe uma série de datagramas da mesma origem, ele precisa determinar se alguns deles são fragmentos de um datagrama original de maior tamanho. Se alguns forem fragmentos, o hospedeiro ainda deverá determinar quando recebeu o último fragmento e como os fragmentos recebidos devem ser reconstruídos para voltar à forma do datagrama original. Para permitir que o hospedeiro destinatário realize essas tarefas de reconstrução, os projetistas do IP (versão 4) criaram campos de identificação, flag e deslocamento de fragmentação no cabeçalho do datagrama IP. Quando um datagrama é criado, o hospedeiro remetente marca o datagrama com um número de identificação, bem como com os endereços de origem e de destino. Em geral, o hospedeiro remetente incrementa o número de identificação para cada datagrama que envia. Quando um roteador precisa fragmentar um datagrama, cada datagrama resultante (isto é, cada fragmento) é marcado com o endereço de origem, o endereço do destino e o número de identificação do datagrama original. Quando o destinatário recebe uma série de datagramas do mesmo hospedeiro remetente, pode examinar os números de identificação para determinar quais deles são, na verdade, fragmentos de um mesmo datagrama de tamanho maior. Como o IP é um serviço não confiável, é possível que um ou mais fragmentos jamais cheguem ao destino. Por essa razão, para que o hospedeiro de destino fique absolutamente seguro de que recebeu o último fragmento do datagrama original, o último datagrama tem um bit de flag ajustado para 0, ao passo que todos os outros têm um bit de flag ajustado para 1. Além disso, para que o hospedeiro destinatário determine se falta algum fragmento (e possa reconstruí-los na ordem correta), o campo de deslocamento é usado para especificar a localização exata do fragmento no datagrama IP original.

1. Explique o que é “Máscara de Subrede”.

R: A máscara de Subrede é utilizada para determinar por exemplo se uma rede é pertencente à classe A/B/ ou C, por exemplo a máscara 255.255.255.0 refere-se a uma rede classe C onde os últimos 8 bits referem-se ao host, nos possibilitando 254 diferentes endereços IPs na rede. Numa rede de classe B com máscara 255.255.0.0 os dois últimos conjuntos de 8 bit são reservados para host. Nós podemos também usar máscara de complexa para criar sub-redes e dividir os endereços ip entre elas. As máscaras de tamanho variável permitem dividir em uma única faixa de endereços(seja de classe A, B ou C) em duas ou mais redes distintas, cada uma recebendo parte dos endereços disponíveis.

Um endereço IP de Um ou Mais Servidores Cisco ICM NT é um endereço usado a fim identificar excepcionalmente um dispositivo em uma rede IP. O endereço é composto de 32 bit binários, que podem ser divisíveis em uma porção de rede e hospedar a parcela com a ajuda de uma máscara de sub-rede. Os 32 bits binários estão divididos em quatro octetos (1 octeto = 8 bits). Cada octeto é convertido em decimal e separado por um ponto final (ponto). Por esse motivo, um endereço IP deve ser expressado no formato decimal pontuado (por exemplo, 172.16.81.100). O valor em cada octeto varia de 0 a 255 decimais ou de 00000000 a 11111111 binários.

Fonte: <http://www.cisco.com/cisco/web/support/BR/104/1045/1045524_3.html>

1. Explique o que é Roteamento Interdomínio sem Classes.

R: A estratégia de atribuição de endereços da Internet é conhecida como roteamento interdomínio sem classes (Classless Interdomain Routing — CIDR), que se pronuncia “sáider”, como a palavra cider (cidra) em inglês [RFC 4632]. O CIDR generaliza a noção de endereçamento de sub-rede. Como acontece com o endereçamento de sub-redes, o endereço IP de 32 bits é dividido em duas partes e, mais uma vez, tem a forma decimal com pontos de separação a.b.c.d/x, em que x indica o número de bits da primeira parte do endereço.

1. .O que é DHCP? Explique seu funcionamento.

R: Tão logo tenha obtido um bloco de endereços, uma organização pode atribuir endereços IP individuais às interfaces de hospedeiros e roteadores. Em geral, um administrador de sistemas configurará de modo manual os endereços IP no roteador (muitas vezes remotamente, com uma ferramenta de gerenciamento de rede). Os endereços dos hospedeiros podem também ser configurados manualmente, mas essa tarefa costuma ser feita usando o Protocolo de Configuração Dinâmica de Hospedeiros (DHCP) [RFC 2131]. O DHCP permite que um hospedeiro obtenha (seja alocado a) um endereço IP de maneira automática. Um administrador de rede pode configurar o DHCP para que determinado hospedeiro receba o mesmo endereço IP toda vez que se conectar, ou um hospedeiro pode receber um endereço IP temporário diferente sempre que se conectar. Além de receber um endereço IP temporário, o DHCP também permite que o hospedeiro descubra informações adicionais, como a máscara de sub-rede, o endereço do primeiro roteador (em geral chamado de roteador de borda padrão — default gateway) e o endereço de seu servidor DNS local. Por causa de sua capacidade de automatizar os aspectos relativos à rede da conexão de um hospedeiro, o DHCP é em geral denominado um protocolo plug and play. Essa capacidade o torna muito atraente para o administrador de rede que, caso contrário, teria de executar essas tarefas manualmente! O DHCP também está conquistando ampla utilização em redes residenciais de acesso à Internet e em LANs sem fio, nas quais hospedeiros entram e saem da rede com frequência. Considere, por exemplo, um estudante que leva seu laptop do quarto para a biblioteca, para a sala de aula. É provável que ele se conecte a uma nova sub-rede em cada um desses lugares e, por conseguinte, precisará de um novo endereço IP em cada um deles. O DHCP é ideal para essa situação, pois há muitos usuários em trânsito e os endereços são utilizados apenas por um tempo limitado. O DHCP é, de maneira semelhante, útil em redes domésticas de acesso. Como exemplo, considere um ISP residencial que tem dois mil clientes, porém, nunca mais de 400 estão on-line ao mesmo tempo. Nesse caso, em vez de precisar de um bloco de 2.048 endereços, um servidor DHCP que designa endereços dinamicamente só precisa de um bloco de 512 endereços (por exemplo, um bloco da forma a.b.c.d/23). À medida que hospedeiros entram e saem da rede, o servidor DHCP precisa atualizar sua lista de endereços IP disponíveis. Toda vez que um hospedeiro se conecta à rede, o servidor DHCP designa a ele um endereço arbitrário do seu reservatório de endereços disponíveis; toda vez que um hospedeiro sai, o endereço é devolvido ao reservatório. O DHCP é um protocolo cliente-servidor. Em geral o cliente é um hospedeiro recém-chegado que quer obter informações sobre configuração da rede, incluindo endereço IP, para si mesmo. Em um caso mais simples, cada sub-rede (no sentido de endereçamento da Figura 4.17) terá um servidor DHCP. Se não houver um servidor na sub-rede, é necessário um agente relé DHCP (normalmente um roteador) que sabe o endereço de um servidor DHCP para tal rede.

1. .O que é NAT? Explique seu funcionamento.

R: Network Address Translation serve para traduzir endereços ip internos para ips externos, por exemplo na sua rede interne temos o ip 10.0.0.1 e o ip externo 138.28.5.90, o roteador direciona os pacotes enviados e recebidos através da NAT.

O roteador NAT recebe o datagrama, gera um novo número de porta de origem, 5001, para o datagrama, substitui o endereço IP de origem por seu endereço IP do lado da WAN, 138.76.29.7, e substitui o número de porta de origem original, 3345, pelo novo número de porta de origem, 5001. Ao gerar um novo número de porta de origem, o roteador NAT pode selecionar qualquer número de porta de origem que não esteja correntemente na tabela de tradução NAT. (Note que, como o comprimento de um campo de número de porta é 16 bits, o protocolo NAT pode suportar mais de 60 mil conexões simultâneas com um único endereço IP do lado da WAN para o roteador!) A NAT no roteador também adiciona um registro à sua tabela de tradução NAT. O servidor Web, totalmente alheio ao fato de que o datagrama que está chegando com uma requisição HTTP foi manipulado pelo roteador NAT, responde com um datagrama cujo endereço de destino é o endereço IP do roteador NAT, e cujo número de porta de destino é 5001. Quando esse datagrama chega ao roteador NAT, ele indexa a tabela de tradução NAT usando o endereço IP de destino e o número de porta de destino para obter o endereço IP (10.0.0.1) e o número de porta de destino (3345) adequados para o navegador na rede residencial. O roteador então reescreve o endereço de destino e o número de porta de destino do datagrama e o repassa para a rede residencial. A NAT conquistou ampla aceitação nos últimos anos. Mas devemos mencionar que muitos puristas da comunidade da IETF têm grandes restrições à NAT. Primeiro, argumentam, a finalidade dos números de portas é endereçar processos, e não hospedeiros. (De fato, a violação dessa regra pode causar problemas para servidores que rodam em redes residenciais, pois, como vimos no Capítulo 2, processos servidores esperam pela chegada de requisições em números de portas bem conhecidos.) Segundo, alegam que roteadores devem processar pacotes apenas até a camada 3. Terceiro, discutem, o protocolo NAT viola o argumento denominado fim a fim; isto é, hospedeiros devem falar diretamente uns com os outros, sem a interferência de nós que modifiquem endereços IP e números de portas. Quarto, argumentam que deveríamos usar o IPv6 (veja Seção 4.4.4) para resolver a escassez de endereços IP, e não tentar resolver o problema imprudentemente com uma solução temporária como a NAT. Mas, gostemos ou não, a NAT tornou-se um componente importante da Internet.

1. O que são algoritmos de roteamento? Quais são as principais “famílias” de algoritmos de roteamento?

R: São algoritmos que podem ser usados para buscar o melhor caminho para o trafego de dados em certa rede, podem analisar o custo do envio através dos nós. A tarefa deles é determinar o caminho tomado por um datagrama entre a origem e o destino.

Portanto, a finalidade de um algoritmo de roteamento é simples: dado um conjunto de roteadores conectados por enlaces, um algoritmo de roteamento descobre um “bom” caminho entre o roteador de origem e o de destino. Em geral, um “bom” caminho é aquele que tem o “menor custo”.

Familias de algoritmos de roteamento: Algoritmo de roteamento de estado de enlace(ls), algoritmo de roteamento de vetor de distâncias (dv), algoritmo de roteamento global, algoritmo de roteamento descentralizado, algoritmos de roteamento estáticos, Algoritmos de roteamento dinâmicos.

1. .Explique o funcionamento do algoritmo de Djikstra.

R: O Algoritmo de Dijkstra ([E.W. Dijkstra](http://net.cs.utexas.edu/users/UTCS/report/1994/profiles/dijkstra.html)) é um dos algoritmos que calcula o caminho de custo mínimo entre vértices de um grafo. Escolhido um vértice como raiz da busca, este algoritmo calcula o custo mínimo deste vértice para todos os demais vértices do grafo. Ele é bastante simples e com um bom nível de performance. Ele não garante, contudo, a exatidão da solução caso haja a presença de arcos com valores negativos.

1. O que são Sistemas Autônomos (autonomous systems – AS)?

R: Um sistema autônomo compreende a rede e todo o conjunto de computadores que ela conecta.

Para que uma rede seja considerada um sistema autônomo (Autonomous System –AS), ela precisa ser organizada de forma a seguir alguns princípios fundamentais: 1. Ela deve ser capaz de divulgar suas rotas (os blocos de endereço dos computadores que pertencem ao AS) para outras redes (AS) da Internet. 2. Ela deve possuir os seus próprios endereços IP públicos (registrados). Observe que mesmo uma rede de grande porte, como a rede de um banco, pode não ser um sistema autônomo. Por exemplo, se o banco se conecta a um backbone de uma operadora e utiliza os endereços IP da operadora, ele não é um sistema autônomo, mas sim parte do sistema autônomo que representa a operadora. Um AS é uma rede (coleção de roteadores e computadores) que segue uma arquitetura WAN. Para que a rede de uma instituição possa ser transformada em AS, ela primeiro, precisa obter um conjunto mínimo de endereços IP públicos (registrados) junto as autoridades da Internet. Quando uma instituição se torna um AS, ela passa a ter seus próprios endereços IP, isto é, os endereços utilizados na rede não são obtidos de provedores, mas pertencem a própria instituição. A topologia de uma rede AS possui dois tipos de roteadores: internos e de borda.