A camada de aplicação

Capítulo 7

Depois de passarmos por todas as camadas preliminares, chegamos àquela em que são encontradas todas as aplicações. As camadas inferiores à camada de aplicação têm a função de oferecer um serviço de transporte confiável, mas, na verdade, elas não executam nenhuma tarefa para os usuários. Neste capítulo, estudaremos algumas aplicações reais em redes.

No entanto, mesmo na camada de aplicação, há necessidade de protocolos de suporte, a fim de permitir que as aplicações funcionem. Da mesma forma, examinaremos um desses protocolos antes de iniciarmos o estudo das aplicações em si. O item em questão é o DNS, que cuida da nomenclatura na Internet. Depois disso, examinaremos três aplicações reais: correio eletrônico, a World Wide Web e, por fim, multimídia. Terminaremos o capítulo explicando melhor a distribuição de conteúdo, incluindo as redes peer-to-peer.

7.1 DNS — Domain Name System (Sistema de Nomes de Domínio)

Embora os programas possam se referir em teoria a páginas Web, caixas de correio e outros recursos que utilizam os endereços de rede (por exemplo, endereços IP) dos computadores em que estão armazenados, esses endereços são difíceis para as pessoas memorizarem. Além disso, navegar pelas páginas Web de uma empresa a partir de *128.111.24.41* significa que, se a empresa mudar o servidor Web para uma máquina diferente, com um endereço IP diferente, todos precisam ser informados sobre o novo endereço IP. Por isso, foram introduzidos nomes de alto nível, legíveis, a fim de desassociar os nomes das máquinas dos endereços dessas máquinas. Desse modo, o servidor Web da empresa poderia ser conhecido como www.cs.washington.edu independentemente do seu endereço IP. Todavia, a rede somente reconhece endereços numéricos; portanto, é necessário algum tipo de mecanismo para converter as strings ASCII em endereços de rede. Nas seções a seguir estudaremos como esse mapeamento é feito na Internet.

Na ARPANET havia simplesmente um arquivo, *hosts.txt*, que listava todos os nomes de computador e seus endereços IP. Toda noite, esse arquivo era acessado por todos os hosts no local em que era mantido. Para uma rede de algumas centenas de grandes máquinas com tempo compartilhado, essa estratégia funcionava bastante bem.

No entanto, bem antes que milhões de PCs estivessem conectados à Internet, todos perceberam que essa estratégia não poderia continuar a ser utilizada para sempre. Em algum momento, o arquivo acabaria por se tornar grande demais. No entanto, a razão mais importante é que poderia haver conflitos de nomes de hosts constantemente, a menos que os nomes fossem gerenciados de uma forma centralizada — algo totalmente fora de cogitação em uma enorme rede internacional, devido à carga e à latência. Para resolver esses problemas, foi criado o sistema de nomes de domínios, ou **DNS (Domain Name System)**, em 1983. Ele tem sido uma parte fundamental da Internet desde então.

A essência do DNS é a criação de um esquema hierárquico de atribuição de nomes baseado no domínio e de um sistema de banco de dados distribuído para implementar esse esquema de nomenclatura. Ele é mais usado para mapear nomes de hosts em endereços IP, mas também pode servir para outros objetivos. O DNS é definido nas RFCs 1034, 1035, 2181 e elaborado com mais detalhes em muitas outras.

Em resumo, o DNS é utilizado da forma descrita a seguir. Para mapear um nome em um endereço IP, um programa aplicativo chama um procedimento de biblioteca denominado **resolvedor** e repassa a ele o nome como um parâmetro. Vimos um exemplo de resolvedor, *gethostbyname*, na Figura 6.6. O resolvedor envia uma consulta contendo o nome para um servidor DNS local, que procura o nome e retorna uma resposta contendo o endereço IP ao resolvedor. Este, em seguida, retorna o endereço IP ao programa aplicativo que fez a chamada. As mensagens de consulta e resposta são enviadas como pacotes UDP. Munido do endereço IP, o programa pode então estabelecer uma conexão TCP com o host ou enviar pacotes UDP até ele.

7.1.1 O ambiente de nomes do DNS

Gerenciar um grande conjunto de nomes que está em mudança constante não é um problema de fácil resolução. Em um sistema postal, o gerenciamento de nomes é feito por meio do uso de letras que especificam (implícita ou explicitamente) o país, o estado ou a província, a cidade e a rua do destinatário. Graças ao uso desse tipo de endereçamento hierárquico, não há confusão entre o João da Silva que mora na Rua Barata Ribeiro, em São Paulo, e o João da Silva que mora na Rua Barata Ribeiro, no Rio de Janeiro. O DNS funciona da mesma forma.

Para a Internet, o topo da hierarquia de nomes é controlado por uma organização chamada **ICANN** (**Internet Corporation for Assigned Names and Numbers**). A ICANN foi criada para essa finalidade em 1998, como parte do amadurecimento da Internet para uma abrangência mundial, econômica. Conceitualmente, a Internet é dividida em mais de 250 **domínios de nível superior**, em que cada domínio cobre muitos hosts. Um domínio é dividido em subdomínios, e estes são partidos ainda mais, e assim por diante. Todos esses domínios podem ser representados por uma árvore, como mostra a Figura 7.1. As folhas representam domínios que não possuem subdomínios (mas contêm máquinas, é claro). Um domínio de folha pode conter um único host, ou então pode representar uma empresa e conter milhares de hosts.

Existem dois tipos de domínios de nível superior: genéricos e de países. Os genéricos, listados na Tabela 7.1, incluem domínios originais da década de 80 e domínios introduzidos por meio de solicitações à ICANN. Outros domínios genéricos de alto nível serão acrescentados no futuro.

Os domínios de países incluem uma entrada para cada país, conforme a definição da ISO 3166. Os nomes de domínio de país internacionalizado que usa alfabeto não latino foram introduzidos em 2010. Esses domínios permitem que as pessoas nomeiem hosts em árabe, cirílico, chinês ou outros idiomas.

É fácil obter um domínio de segundo nível, como nome-da-empresa.com. Os domínios de nível superior são controlados pelos **registradores** apontados pela ICANN. Para obter um nome, basta ir até um registrador correspondente (nesse caso, *com*) para verificar se o nome desejado está disponível e não é marca registrada de outra pessoa. Se não houver nenhum problema, o solicitante pagará uma pequena taxa anual e conseguirá o nome.

Porém, à medida que a Internet se torna mais comercial e mais internacional, ela também passa a ser mais disputada, especialmente em questões relacionadas a nomes. Essa controvérsia inclui a própria ICANN. Por exemplo, a criação do domínio *xxx* levou vários anos e exigiu a solução de vários casos em tribunal. Colocar conteúdo adulto voluntariamente em seu próprio domínio é uma coisa boa ou ruim? (Algumas pessoas não queriam conteúdo adulto disponível de forma alguma na Internet, enquanto outras queriam colocá-lo em um domínio, de modo que filtros pudessem facilmente localizá-lo e impedir seu uso por crianças.) Alguns dos domínios são auto-organizados, enquanto outros têm restrições sobre quem pode obter um nome, conforme indicado na Tabela 7.1. Mas que restrições são apropriadas? Pense no domínio *pro*, por exemplo. Ele é adotado por profissionais qualificados. Mas quem é um profissional? Médicos e advogados sem dúvida são profissionais. Mas e fotógrafos autônomos, professores de música, mágicos, bombeiros hidráulicos, barbeiros, exterminadores, tatuadores, mercenários e prostitutas? Essas profissões são válidas? De acordo com quem?

Também há dinheiro envolvido nos nomes. Tuvalu (o país) vendeu uma licença em seu domínio *tv* por US$ 50 milhões, tudo porque o código do país é bastante adequado para anunciar sites de televisão. Praticamente toda palavra comum (em inglês) é usada no domínio *com*, além dos erros de grafia mais usuais. Experimente pesquisar utensílios domésticos, animais, plantas, partes do corpo etc. A prática de registrar um domínio apenas para esperar e vendê-lo a uma parte interessada por um preço muito mais alto tem até mesmo um nome. Isso se chama **cybersquatting**. Muitas empresas que foram lentas quando a era da Internet começou descobriram que seus nomes de domínio óbvios já haviam sido usados quando tentaram adquiri-los. Em geral, desde que nenhuma marca registrada esteja sendo violada e nenhuma fraude seja envolvida, os nomes são atribuídos a quem chegar primeiro. Apesar disso, políticas para resolver disputas de nomenclatura ainda estão sendo preparadas.

Cada domínio tem seu nome definido pelo caminho ascendente entre ele e a raiz (sem nome). Esses componentes são separados por pontos. Dessa forma, o departamento de engenharia da Cisco poderia ser eng.cisco.com, em vez de um nome no estilo UNIX, como /com/sun/eng. Observe que essa nomenclatura hierárquica significa que eng.cisco.com.

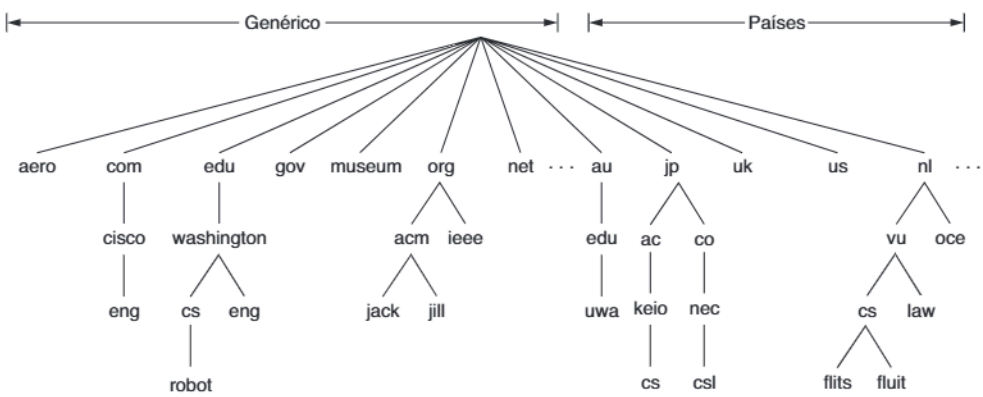

Figura 7.1 | Uma parte do espaço de nomes de domínios da Internet.

Domínio	Uso intencionado	Data de início	Restrito?
com	Comercial	1985	Não
edu	Instituições educacionais	1985	Sim
gov	Governo	1985	Sim
int	Organizações internacionais	1988	Sim
mil	Militares	1985	Sim
net	Provedores de rede	1985	Não
org	Organizações não lucrativas	1985	Não
aero	Transporte aéreo	2001	Sim
biz	Empresas	2001	Não
coop	Cooperativas	2001	Sim
info	Informativos	2002	Não
museum	Museus	2002	Sim
name	Pessoas	2002	Não
pro	Profissionais	2002	Sim
cat	Catalão	2005	Sim
jobs	Empregos	2005	Sim
mobi	Dispositivos móveis	2005	Sim
tel	Detalhes de contato	2005	Sim
travel	Indústria de viagens	2005	Sim
xxx	Indústria do sexo	2010	Não

Tabela 7.1 | Domínios genéricos de nível superior.

não entra em conflito com um possível uso de *eng* em eng.washington.edu., que poderia ser usado pelo departamento de língua inglesa da Universidade de Washington.

Os nomes de domínios podem ser absolutos ou relativos. Um nome de domínio absoluto sempre termina com um ponto (por exemplo, eng.sun.com.), ao contrário de um nome de domínio relativo. Os nomes relativos têm de ser interpretados em algum contexto para determinar exclusivamente seu verdadeiro significado. Em ambos os casos, um nome de domínio se refere a um nó específico da árvore e a todos os nós abaixo dele.

Os nomes de domínios não fazem distinção entre letras maiúsculas e minúsculas. Os nomes de componentes podem ter até 63 caracteres, e os nomes de caminhos completos não podem exceder 255 caracteres.

Em princípio, os domínios podem ser inseridos na árvore em domínios genéricos ou de país. Por exemplo, cs.washington.edu poderia ser igualmente listado sob o domínio de país *us* como cs.washington.wa.us. Contudo, na prática, quase todas as organizações dos Estados Unidos estão sob um domínio genérico e, praticamente, todas fora dos Estados Unidos estão sob o domínio de seu país. Não existe regra contra o registro sob dois domínios de nível superior. Grandes empresas normalmente fazem isso (por exemplo, sony.com, sony.net e sony.nl).

Cada domínio controla como serão alocados todos os domínios abaixo dele. Por exemplo, o Japão tem os domínios *ac.jp* e *co.jp*, que espelham *edu* e *com*. A Holanda não faz essa distinção e coloca todas as organizações diretamente sob *nl*. Assim, os três domínios a seguir representam departamentos de ciência da computação de universidades:

1. cs.washington.edu (Universidade de Washington, nos Estados Unidos);
2. cs.vu.nl (Vrije Universiteit, na Holanda);
3. cs.keio.ac.jp (Keio University, no Japão).

Para que um novo domínio seja criado, é necessária a permissão do domínio no qual ele será incluído. Por exemplo, se o grupo VLSI tiver começado na Universidade de Washington e quiser ser conhecido como vlsi.cs.washington.edu, ele precisará da permissão de quem gerencia cs.washington.edu. Da mesma forma, se uma nova universidade for licenciada, digamos a University of Nor-

thern South Dakota, ela terá de solicitar ao gerente do domínio *edu* que lhe atribua o domínio unsd.edu (se estiver disponível). Dessa forma, os conflitos de nomes são evitados e cada domínio pode controlar seus subdomínios. Uma vez que um novo domínio tenha sido criado e registrado, ele poderá criar subdomínios, tais como cs.unsd.edu, sem que seja necessária a permissão de alguém que esteja em um nível mais alto na árvore.

A atribuição de nomes leva em consideração as fronteiras organizacionais, e não as redes físicas. Por exemplo, mesmo que os departamentos de ciência da computação e de engenharia elétrica estejam no mesmo prédio e compartilhem a mesma LAN, eles poderão ter domínios distintos. Da mesma forma, mesmo que o departamento de ciência da computação esteja dividido em dois prédios, normalmente todos os hosts instalados em ambos pertencerão ao mesmo domínio.

7.1.2 Registros de recursos (RRs)

Todo domínio, seja um único host, seja um domínio de nível superior, pode ter um conjunto de **registros de recursos** associado a ele. Esses registros são o banco de dados DNS. Para um único host, o registro de recurso mais comum é apenas seu endereço IP, mas também existem muitos outros tipos. Quando um resolvedor repassa um nome de domínio ao DNS, o que ele obtém são os registros de recursos associados àquele nome. Portanto, a principal função do DNS é mapear nomes de domínios em registros de recursos.

Um registro de recurso é uma tupla de cinco campos. Apesar de serem codificados em binário para proporcionar maior eficiência, na maioria das exposições os registros de recursos são mostrados como texto ASCII, uma linha para cada registro de recurso. O formato que utilizaremos é:

Nome_domínio Tempo_de_vida Classe Tipo Valor

Nome_domínio informa o domínio ao qual esse registro se aplica. Normalmente, existem muitos registros para cada domínio, e cada cópia do banco de dados armazena informações sobre vários domínios. Assim, esse campo é a chave de pesquisa primária utilizada para atender às consultas. A ordem dos registros no banco de dados não é significativa.

Tempo_de_vida fornece uma indicação da estabilidade do registro. As informações muito estáveis são definidas com um número alto, como 86.400 (o número de segundos em 1 dia). As informações muito voláteis recebem um número baixo, como 60 (1 minuto). Voltaremos a esse ponto mais adiante, quando discutirmos o caching.

O terceiro campo de cada registro de recurso é *Classe*. No caso de informações relacionadas à Internet, ele é sempre *IN*. Para informações não relacionadas à Internet, podem ser empregados outros códigos; porém, estes raramente são encontrados na prática.

O campo *Tipo* informa qual é o tipo do registro. Os tipos mais importantes estão listados na Tabela 7.2.

Um registro *SOA* fornece o nome da principal fonte de informações sobre a zona do servidor de nomes (descrita a seguir), o endereço de correio eletrônico do administrador, um número de série exclusivo e diversos flags e timeouts.

O tipo de registro mais importante é o *A* (Address). Ele contém um endereço IPv4 de 32 bits de algum host. O registro *AAAA* correspondente, ou 'A quádruplo', mantém um endereço IPv6 de 128 bits. Cada host da Internet deve ter pelo menos um endereço IP, de forma que outras máquinas possam se comunicar com ele. Alguns hosts têm duas ou mais interfaces de rede; nesse caso, eles terão dois ou mais registros de recurso do tipo *A* ou *AAAA*. Consequentemente, o DNS pode retornar vários endereços para um único nome.

Tipo	Significado	Valor
SOA	Início de autoridade	Parâmetros para essa zona
A	Endereço IPv4 de um host	Inteiro de 32 bits
AAAA	Endereço IPv6 de um host	Inteiro de 128 bits
MX	Troca de mensagens de correio	Prioridade, domínio disposto a aceitar correio eletrônico
NS	Servidor de nomes	Nome de um servidor para este domínio
CNAME	Nome canônico	Nome de domínio
PTR	Ponteiro	Nome alternativo de um endereço IP
SPF	Estrutura de política do transmissor	Codificação de texto da política de envio de mensagens de correio
SRV	Serviço	Host que o oferece
TXT	Texto	Texto ASCII descritivo

Tabela 7.2 | Os principais tipos de registros de recursos.

Um tipo de registro comum é o *MX*. Ele especifica o nome do host preparado para aceitar mensagens de correio eletrônico para o domínio especificado. O registro *MX* é utilizado porque nem toda máquina está preparada para aceitar correio eletrônico. Se alguém quiser enviar correio eletrônico para bill@microsoft.com, o host transmissor precisará encontrar um servidor de correio em microsoft.com que esteja disposto a aceitar correio eletrônico. O registro *MX* pode fornecer essa informação.

Outro tipo de registro importante é o *NS*. Ele especifica um servidor de nomes para o domínio ou subdomínio. Ele é um host que tem uma cópia do banco de dados para um domínio e é usado como parte do processo de pesquisa de nomes, o que veremos adiante.

Os registros *CNAME* permitem a criação de nomes alternativos. Por exemplo, uma pessoa familiarizada com a Internet em geral que deseja enviar uma mensagem para alguém cujo nome de login seja *paul* no departamento de ciência da computação do MIT poderá imaginar que paul@cs.mit.edu seja o endereço correto. Na realidade, esse endereço não servirá, pois o domínio do departamento de ciência da computação do MIT é csail.mit.edu. No entanto, o MIT poderia criar uma entrada *CNAME* para orientar pessoas e programas na direção correta. Uma entrada como essa poderia executar essa função:

```
cs.mit.edu    86400    IN    CNAME    csail.mit.edu
```

A exemplo de *CNAME*, *PTR* indica outro nome. No entanto, ao contrário de *CNAME*, que, na verdade, é apenas um apelido de um nome atribuído originalmente [ou seja, CNAME permite substituir uma string (apelido) por outra (um nome canônico)], *PTR* é um tipo de dado comum do DNS, cuja interpretação depende do contexto no qual se encontra. Na prática, essa entrada é quase sempre usada para associar um nome a um endereço IP, a fim de permitir pesquisas de endereços IP e retornar o nome da máquina correspondente. Essas pesquisas são chamadas **pesquisas inversas**.

SRV é um tipo de registro mais novo, que permite que um host seja identificado para determinado serviço em um domínio. Por exemplo, o servidor Web para cs.washington.edu poderia ser identificado como cockatoo.cs.washington.edu. Esse registro generaliza o registro *MX* que realiza a mesma tarefa, mas é apenas para servidores de correio eletrônico.

SPF também é um tipo de registro mais novo. Ele permite que um domínio codifique informações sobre quais máquinas no domínio enviarão correio eletrônico ao restante da Internet. Isso ajuda as máquinas receptoras a verificar se o correio é válido. Se ele estiver sendo recebido de uma máquina que se chama *dodgy*, mas os registros de domínio disserem que o correio só será enviado do domínio por uma máquina chamada *smtp*, é provável que esse correio seja forjado.

Por fim, os registros *TXT* foram fornecidos originalmente para permitir que os domínios se identificassem de forma arbitrária. Hoje em dia, eles normalmente codificam informações legíveis à máquina, em geral a informação *SPF*.

Por fim, chegamos ao campo *Valor*. Esse campo pode ser um número, um nome de domínio ou uma string ASCII. A semântica dependerá do tipo de registro. Na Tabela 7.2, é mostrada uma breve descrição dos campos *Valor* de cada um dos principais tipos de registros.

Como exemplo do tipo de informação que se pode encontrar no banco de dados DNS de um domínio, observe o Quadro 7.1. Esse quadro ilustra parte de um banco de dados (hipotético) para o domínio cs.vu.nl mostrado na Figura 7.1. O banco de dados contém sete tipos de registros de recursos.

A primeira linha destinada a comentários do Quadro 7.1 apresenta algumas informações básicas sobre o domínio, que não nos interessarão em detalhes. As duas linhas seguintes mostram a primeira e a segunda opções para a entrega de mensagens de correio eletrônico enviadas para pessoa@cs.vu.nl. A entrada *zephyr* (uma máquina específica) deve ser a primeira opção a ser experimentada. Se ela não servir, *top* será a próxima opção. A próxima linha identifica o servidor de nomes para o domínio como *star*.

Depois da linha em branco (que foi incluída para facilitar a leitura) há outras informando os endereços IP para *star*, *zephyr* e *top*. Em seguida, há um nome alternativo, www.cs.vu.nl, ou seja, um endereço que pode ser usado sem a necessidade de especificar uma máquina. A criação desse nome alternativo permite que cs.vu.nl modifique seu servidor da World Wide Web sem invalidar o endereço que as pessoas utilizam para acessá-lo. Há um argumento semelhante para ftp.cs.vu.nl.

A seção para a máquina *flits* lista dois endereços IP e três escolhas são dadas para o tratamento de correio eletrônico enviado a flits.cs.vu.nl. A primeira escolha é naturalmente o próprio *flits*, mas se ele estiver fora do ar, *zephyr* e *top* são a segunda e a terceira opções, respectivamente.

As três linhas seguintes contêm uma entrada típica para um computador — nesse caso, rowboat.cs.vu.nl. As informações fornecidas contêm o endereço IP e as caixas de correio principal e secundária. Em seguida, vem uma entrada para um computador que não é capaz de receber correio por si só, seguida de uma entrada para uma impressora conectada à Internet.

7.1.3 Servidores de nomes

Pelo menos em teoria, um único servidor de nomes poderia conter o banco de dados DNS inteiro e responder a todas as consultas referentes ao banco. Na prática, esse servidor ficaria tão sobrecarregado que seria inútil. Além disso, caso ele ficasse fora do ar, toda a Internet seria atingida.

Para evitar os problemas associados à presença de uma única fonte de informações, o espaço de nomes do DNS é dividido em **zonas** não superpostas. Uma forma possível

; Dados oficiais para cs.vu.nl				
cs.vu.nl.	86400	IN	SOA	star boss (9527,7200,7200,241920,86400)
cs.vu.nl.	86400	IN	MX	1 zephyr
cs.vu.nl.	86400	IN	MX	2 top
cs.vu.nl.	86400	IN	NS	star
star	86400	IN	A	130.37.56.205
zephyr	86400	IN	A	130.37.20.10
top	86400	IN	A	130.37.20.11
www	86400	IN	CNAME	star.cs.vu.nl
ftp	86400	IN	CNAME	zephyr.cs.vu.nl
flits	86400	IN	A	130.37.16.112
flits	86400	IN	A	192.31.231.165
flits	86400	IN	MX	1 flits
flits	86400	IN	MX	2 zephyr
flits	86400	IN	MX	3 top
rowboat		IN	A	130.37.56.201
		IN	MX	1 rowboat
		IN	MX	2 zephyr
little-sister		IN	A	130.37.62.23
laserjet		IN	A	192.31.231.216

Quadro 7.1 | Uma parte de um possível banco de dados DNS para *cs.vu.nl*.

de dividir o espaço de nomes da Figura 7.1 é mostrada na Figura 7.2. Cada zona contém uma parte da árvore.

A localização das fronteiras de uma zona fica a cargo de seu administrador. Essa decisão é tomada principalmente com base no número de servidores de nomes desejados, e onde. Por exemplo, na Figura 7.2, a Universidade de Washington tem uma zona para washington.edu que trata de eng.washington.edu, mas não de cs.washington.edu, que é uma zona separada com seus próprios servidores de nomes. Tal decisão pode ser tomada quando um departamento como língua inglesa não deseja ter seu próprio servidor de nomes, mas um departamento como ciência da computação sim.

Cada zona também está associada a um ou mais servidores de nomes. Estes são hosts que mantêm o banco de dados para a zona. Normalmente, uma zona terá um servidor de nomes primário, que recebe sua informação de um arquivo em seu disco, e um ou mais servidores de nomes secundários, que recebem suas informações do servidor de nomes primário. Para melhorar a confiabilidade, alguns dos servidores de nomes podem estar localizados fora da zona.

O processo de pesquisa de um nome e localização de um endereço é chamado **resolução de nomes**. Quando um resolvedor tem uma consulta sobre um nome de domínio, ele passa a consulta para um servidor de nomes local. Se o domínio buscado cair sob a jurisdição do servidor de nomes, como top.cs.vu.nl caindo sob cs.vu.nl, ele retornará os registros de recursos oficiais. Um **registro oficial** é aquele que vem da autoridade que controla o registro e, portanto, sempre está correto. Os registros oficiais contrastam com os **registros em cache**, que podem estar desatualizados.

O que acontece quando o domínio é remoto, como quando flits.cs.vu.nl deseja encontrar o endereço IP de robot.cs.washington.edu em UW (Universidade de Washington)? Nesse caso, e se não houver informações sobre o domínio disponíveis localmente em cache, o servidor de nomes inicia uma consulta remota. Essa consulta segue o processo mostrado na Figura 7.3. A etapa 1 mostra a consulta que é enviada ao servidor de nomes local. Ela contém o nome de domínio buscado, o tipo (*A*) e a classe (*IN*).

A próxima etapa é começar no topo da hierarquia de nomes pedindo a um dos **servidores de nomes raiz**. Esses servidores de nomes têm informações sobre cada domínio de alto nível. Isso pode ser visto na etapa 2 da Figura 7.3. Para entrar em contato com um servidor-raiz, cada servidor

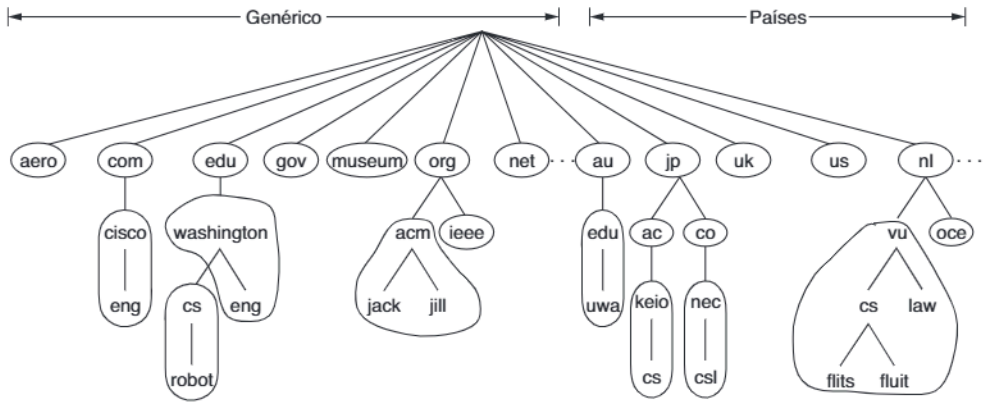

Figura 7.2 | Parte do espaço de nomes do DNS dividido em zonas (que estão circuladas).

de nomes precisa ter informações sobre um ou mais servidores de nomes raiz. Essa informação normalmente está presente em um arquivo de configuração do sistema que é carregado no cache DNS quando o servidor DNS é iniciado. Essa é simplesmente uma lista de registros *NS* para a raiz e os registros *A* correspondentes.

Existem 13 servidores de nomes raiz, de um modo pouco criativo chamados a-root-servers.net a m.root-servers.net. Cada servidor-raiz poderia ser logicamente um único computador. Porém, como a Internet inteira depende dos servidores-raiz, eles são computadores poderosos e altamente replicados. A maioria dos servidores está presente em vários locais geográficos e alcançados por meio de roteamento anycast, em que um pacote é entregue para a próxima instância de um endereço de destino; descrevemos o anycast no Capítulo 5. A replicação melhora a confiabilidade e o desempenho.

O servidor de nomes raiz provavelmente não saberá o endereço de uma máquina em UW, e provavelmente também não conhece o servidor de nomes para UW. Mas ele precisa conhecer o servidor de nomes para o domínio *edu*, em que cs.washington.edu está localizado. Ele retorna o nome e endereço IP para a parte da resposta na etapa 3.

O servidor de nomes local, então, continua sua busca. Ele envia a consulta inteira para o servidor de nomes edu (a.edu-servers.net). Esse servidor de nomes retorna um servidor de nomes para UW. Isso é visto nas etapas 4 e 5. Mais próximo agora, o servidor de nomes local envia a consulta para o servidor de nomes UW (etapa 6). Se o nome de domínio que está sendo buscado estivesse no departamento de língua inglesa, a resposta seria encontrada, pois a zona UW inclui o departamento de língua inglesa. Mas o departamento de ciência da computação decidiu manter seu próprio servidor de nomes. A consulta retorna o nome e endereço IP do servidor de nomes de ciência da computação de UW (etapa 7).

Finalmente, o servidor de nomes local consulta o servidor de nomes de ciência da computação de UW (etapa 8). Esse servidor é oficial para o domínio cs.washington.edu, de modo que deve ter a resposta. Ele retorna a resposta final (etapa 9), que o servidor de nomes local encaminha como resposta para flits.cs.vu.nl (etapa 10). O nome foi resolvido.

Você pode explorar esse processo usando ferramentas-padrão como o programa *dig* que está instalado na maioria dos sistemas UNIX. Por exemplo, digitar

```
dig@a.edu-servers.net robot.cs.washington.edu
```

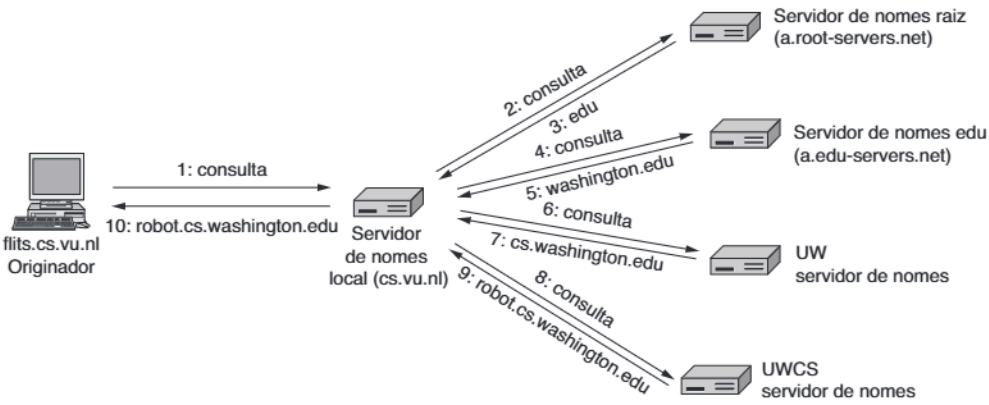

Figura 7.3 | O modo como um resolvedor procura um nome remoto em dez etapas.

motivará o envio de uma consulta para robot.cs.washington.edu ao servidor de nomes a.edu-servers.net e a impressão do resultado. Isso lhe mostrará a informação obtida na etapa 4 no exemplo anterior, e você aprenderá o nome e o endereço IP dos servidores de nomes UW.

Há três pontos técnicos a discutir sobre esse longo cenário. Primeiro, dois mecanismos de consulta estão em ação na Figura 7.3. Quando o host *flits.cs.vu.nl* envia sua consulta ao servidor de nomes local, o servidor de nomes trata a resolução em favor de *flits* até que tenha a resposta desejada para retornar. Ele *não* retorna respostas parciais. Elas poderiam ser úteis, mas não representam o que a consulta estava procurando. Esse mecanismo é chamado **consulta recursiva**.

Por outro lado, o servidor de nomes raiz (e cada servidor de nomes subsequente) não continua recursivamente a consulta para o servidor de nomes local. Ele apenas retorna uma resposta parcial e prossegue para próxima consulta. O servidor de nomes local é responsável por continuar a resolução emitindo outras consultas. Esse mecanismo é chamado **consulta iterativa**.

Uma resolução de nome pode envolver os dois mecanismos, como esse exemplo mostrou. Uma consulta recursiva sempre pode parecer preferível, mas muitos servidores de nomes (especialmente o raiz) não cuidarão disso. Eles são muito ocupados. As consultas iterativas colocam o peso sobre o originador. O raciocínio para o servidor de nomes local que dá suporte a uma consulta recursiva é que ele está fornecendo um serviço para os hosts em seu domínio. Esses hosts não precisam ser configurados para usar um servidor de nomes completo, apenas alcançar o servidor local.

O segundo ponto é o caching. Todas as respostas, incluindo todas as parciais retornadas, são mantidas em cache. Desse modo, se outro host cs.vu.nl procurar robot.cs.washington.edu, a resposta já será conhecida. Melhor ainda, se um host consultar um host diferente no mesmo domínio, digamos, galah.cs.washington.edu, a consulta poderá ser enviada diretamente para o servidor de nomes oficial. De modo semelhante, as consultas por outros domínios em washington.edu podem começar diretamente do servidor de nomes washington.edu. O uso de respostas em cache reduz bastante as etapas de uma consulta e melhora o desempenho. O cenário original que esboçamos é, de fato, o pior caso que ocorre quando nenhuma informação útil é mantida em cache.

Porém, as respostas em cache não são oficiais, pois as mudanças feitas em cs.washington.edu não serão propagadas para todos os caches no mundo que podem conhecê-la. Por esse motivo, as entradas em cache não devem ter vida longa. Esse é o motivo para o campo *Tempo_de_vida* ser incluído em cada registro de recurso. Ele diz aos servidores de nomes remotos por quanto tempo manter os registros em cache. Se determinada máquina tiver tido o mesmo endereço IP por anos, pode ser seguro manter essa informação em cache por um dia. Para informações mais voláteis, pode ser mais seguro eliminar os registros após alguns segundos ou minutos.

A terceira questão é o protocolo de transporte usado para consultas e respostas. Ele é o UDP. As mensagens DNS são enviadas em pacotes UDP com um formato simples para consultas, respostas e servidores de nomes que podem ser usados para continuar a resolução. Não entraremos nos detalhes desse formato. Se nenhuma resposta chegar em um curto período de tempo, o cliente DNS repetirá a consulta, escolhendo outro servidor para o domínio após um pequeno número de tentativas. Esse processo é criado para lidar com o caso do servidor que ficou inoperante, bem como com o do pacote de consulta ou resposta que se perdeu. Um identificador de 16 bits é incluído em cada consulta e copiado para a resposta, de modo que um servidor de nomes pode combinar as respostas com a consulta correspondente, mesmo que várias consultas estejam pendentes ao mesmo tempo.

Embora sua finalidade seja simples, deve ficar claro que o DNS é um sistema distribuído, grande e complexo, que compreende milhões de servidores de nomes que trabalham juntos. Ele forma um elo importante entre os nomes de domínio legíveis aos humanos e os endereços IP das máquinas. E inclui replicação e caching para ganhar desempenho e confiabilidade, sendo projetado para ser altamente robusto.

Não abordamos a segurança, mas, como você poderia imaginar, a capacidade de mudar o mapeamento entre nome e endereço pode ter consequências devastadoras se isso for feito de forma maliciosa. Por esse motivo, extensões de segurança, chamadas DNSSEC, foram desenvolvidas para DNS. Vamos descrevê-las no Capítulo 8.

Há também demanda da aplicação para usar nomes de maneiras mais flexíveis, por exemplo, dando nome ao conteúdo e resolvendo para o endereço IP do host próximo que possui o conteúdo. Isso se encaixa no modelo de busca e downloading de um filme. É o filme que importa, e não o computador que tem uma cópia dele, de modo que tudo o que é necessário é o endereço IP de qualquer computador próximo que tenha uma cópia do filme. As redes de distribuição de conteúdo são uma forma de realizar esse mapeamento. Vamos descrever como elas se baseiam no DNS mais adiante neste capítulo, na Seção 7.5.

7.2 Correio eletrônico

O correio eletrônico, ou **e-mail**, como é chamado por muitos, já existe há mais de duas décadas. Mais rápido e mais barato que o correio tradicional, o e-mail tem sido uma aplicação popular desde os primeiros dias da Internet. Antes de 1990, ele era empregado principalmente nos meios acadêmicos. Durante os anos 1990, ficou conhecido para o público em geral e seu uso cresceu exponencialmente, até alcançar um número de mensagens de correio eletrônico en-