Se il TCP viene utilizzato a livello di trasporto, il TCP recupera questa perdita facendo in modo che la sorgente ritrasmetta i dati del datagramma originale.

Abbiamo appena appreso che la frammentazione IP svolge un ruolo importante nell'incollare insieme le diverse tecnologie del livello di collegamento. Ma la frammentazione ha anche dei costi. In primo luogo, complica i router e i sistemi finali, che devono essere progettati per gestire la frammentazione e il riassemblaggio dei datagrammi. In secondo luogo, la frammentazione può essere utilizzata per creare attacchi DoS letali, in cui l'attaccante invia una serie di frammenti bizzarri e inaspettati. Un esempio classico è l'attacco Jolt2, in cui l'attaccante invia all'host di destinazione un flusso di piccoli frammenti, nessuno dei quali ha un offset pari a zero. L'obiettivo può collassare nel tentativo di ricostruire i datagrammi dai pacchetti degenerati. Un'altra classe di exploit invia frammenti IP sovrapposti, ovvero frammenti i cui valori di offset sono impostati in modo che i frammenti non si allineino correttamente. I sistemi operativi vulnerabili, non sapendo cosa fare con i frammenti sovrapposti, possono bloccarsi [Skoudis 2006]. Come vedremo alla fine di questa sezione, una nuova versione del protocollo IP, l'IPv6, elimina del tutto la frammentazione, semplificando così l'elaborazione dei pacchetti IP e rendendo l'IP meno vulnerabile agli attacchi.

Sul sito Web di questo libro è disponibile un'applet Java che genera frammenti. L'utente fornisce la dimensione del datagramma in arrivo, l'MTU e l'identificazione del datagramma in arrivo. L'applet genera automaticamente i frammenti. Vedere http:// www.awl.com/kurose-ross.

4.4.2 Indirizzamento IPv4

Ora ci occupiamo dell'indirizzamento IPv4. Sebbene si possa pensare che l'indirizzamento debba essere un argomento semplice, si spera che alla fine di questo capitolo ci si convinca che l'indirizzamento di Internet non è solo un argomento succoso, sottile e interessante, ma anche di importanza centrale per Internet. Eccellenti trattazioni dell'indirizzamento IPv4 sono [3Com Addressing 2012] e il primo capitolo di [Stewart 1999].

Prima di parlare dell'indirizzamento IP, tuttavia, è necessario spendere qualche parola su come gli host e i router sono collegati alla rete. Un host ha in genere un solo collegamento alla rete; quando IP nell'host vuole inviare un datagramma, lo fa attraverso questo collegamento. Il confine tra l'host e il collegamento fisico è chiamato **interfaccia**. Consideriamo ora un router e le sue interfacce. Poiché il compito di un router è ricevere un datagramma su un collegamento e inoltrarlo su un altro collegamento, un router ha necessariamente due o più collegamenti a cui è connesso. Il confine tra il router e uno qualsiasi dei suoi collegamenti è chiamato anche interfaccia. Un router ha quindi più interfacce, una per ciascuno dei suoi collegamenti. Poiché ogni host e router è in grado di inviare e ricevere datagrammi IP, il protocollo IP richiede che ogni interfaccia di host e router abbia un proprio

indirizzo IP. Pertanto, un indirizzo IP è tecnicamente associato a un'interfaccia, piuttosto che all'host o al router che la contiene.

Ogni indirizzo IP ha una lunghezza di 32 bit (equivalenti a 4 byte), quindi ci sono in totale ^{232} indirizzi IP possibili. Approssimando ^{210} per ^{103}, è facile vedere che ci sono

sono circa 4 miliardi gli indirizzi IP possibili. Questi indirizzi sono tipicamente scritti nella cosiddetta **notazione decimale punteggiata**, in cui ogni byte dell'indirizzo è scritto nella sua forma decimale ed è separato da un punto dagli altri byte dell'indirizzo. Ad esempio, consideriamo l'indirizzo IP 193.32.216.9. Il 193 è l'equivalente decimale dei primi 8 bit dell'indirizzo; il 32 è l'equivalente decimale dei secondi 8 bit dell'indirizzo e così via. Quindi, l'indirizzo 193.32.216.9 in notazione binaria è

11000001 00100000 11011000 00001001

Ogni interfaccia di ogni host e router nell'Internet globale deve avere un indirizzo IP unico a livello globale (ad eccezione delle interfacce dietro i NAT, come discusso alla fine di questa sezione). Questi indirizzi, tuttavia, non possono essere scelti in modo casuale. Una parte dell'indirizzo IP di un'interfaccia sarà determinata dalla sottorete a cui è collegata.

La Figura 4.15 fornisce un esempio di indirizzamento IP e di interfacce. In questa figura, un router (con tre interfacce) viene utilizzato per interconnettere sette host. Osservate attentamente gli indirizzi IP assegnati alle interfacce dell'host e del router, perché ci sono diverse cose da notare. I tre host nella parte superiore sinistra della Figura 4.15 e l'interfaccia del router a cui sono collegati hanno tutti un indirizzo IP della forma 223.1.1.xxx. Cioè, hanno tutti gli stessi 24 bit a sinistra nel loro indirizzo IP. Le quattro interfacce sono inoltre interconnesse tra loro da una rete *che non contiene router*. Questa rete

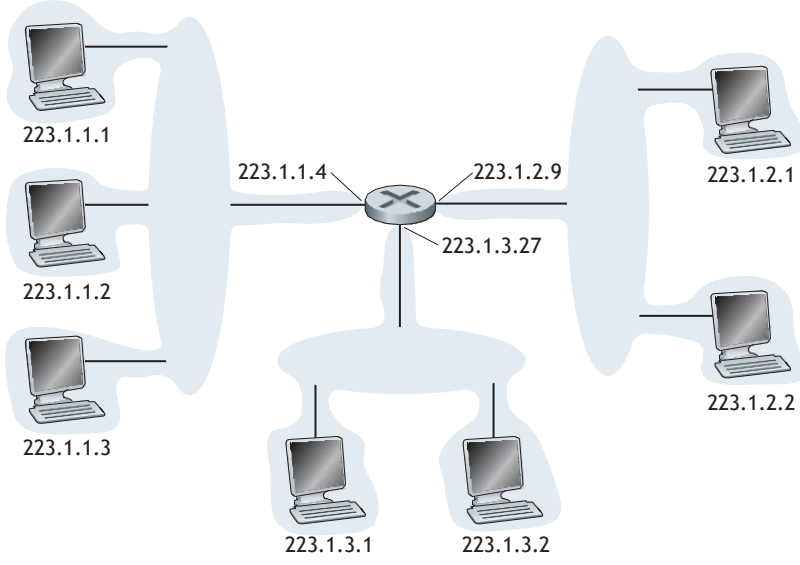

Figura 4.15 Indirizzi di interfaccia e sottoreti

anche in questo esempio: una sottorete, 223.1.9.0/24, per le interfacce che collegano i router R1 e R2; un'altra sottorete, 223.1.8.0/24, per le interfacce che collegano i router R2 e R3; e una terza sottorete, 223.1.7.0/24, per le interfacce che collegano i router R3 e R1. Per un sistema generale interconnesso di router e host, possiamo usare la seguente ricetta per definire le sottoreti del sistema:

> *Per determinare le sottoreti, staccare ogni interfaccia dal proprio host o router, creando isole di reti isolate, con le interfacce che terminano ai punti finali delle reti isolate. Ciascuna di queste reti isolate è chiamata* ***sottorete****.*

Se applichiamo questa procedura al sistema interconnesso della Figura 4.17, otteniamo sei isole o sottoreti.

Dalla discussione precedente, è chiaro che un'organizzazione (come un'azienda o un'istituzione accademica) con più segmenti Ethernet e collegamenti punto a punto avrà più sottoreti, con tutti i dispositivi di una determinata sottorete aventi lo stesso indirizzo di sottorete. In linea di principio, le diverse sottoreti potrebbero avere indirizzi di sottorete molto diversi. In pratica, però, i loro indirizzi di sottorete hanno spesso molto in comune. Per capire il perché, vediamo come viene gestito l'indirizzamento nell'Internet globale.

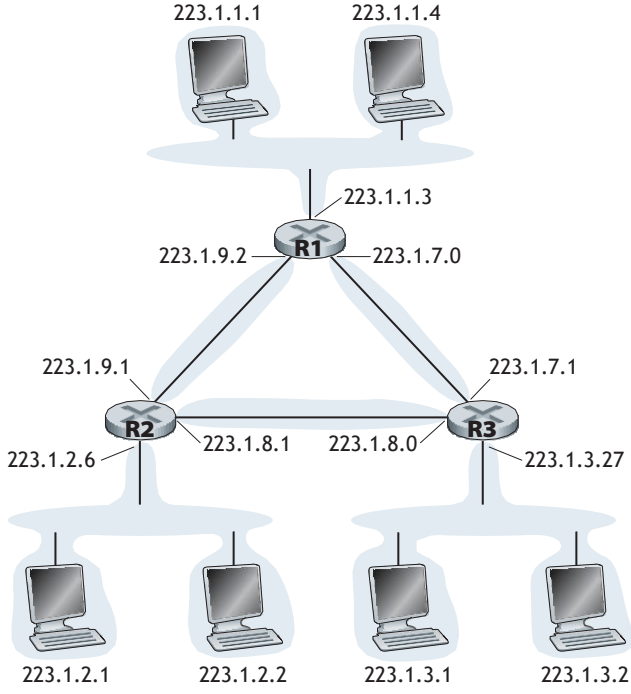

Figura 4.17 Tre router che interconnettono sei sottoreti

La strategia di assegnazione degli indirizzi di Internet è nota come **Classless Interdomain Routing** (**CIDR - pronunciato** *sidro*) [RFC 4632]. Il CIDR generalizza la nozione di indirizzamento di sottorete. Come nel caso dell'indirizzamento di sottorete, l'indirizzo IP a 32 bit è diviso in due parti e ha ancora una volta la forma decimale punteggiata *a.b.c.d/x*, dove *x* indica il numero di bit nella prima parte dell'indirizzo.

Gli *x* bit più significativi di un indirizzo della forma *a.b.c.d/x* costituiscono la parte di rete dell'indirizzo IP e sono spesso indicati come il **prefisso** (o *prefisso di rete*) dell'indirizzo. A un'organizzazione viene tipicamente assegnato un blocco di indirizzi contigui, cioè una serie di indirizzi con un prefisso comune (vedere la barra laterale Principi in pratica). In questo caso, gli indirizzi IP dei dispositivi all'interno dell'organizzazione condivideranno il prefisso comune. Quando si tratta del BGP di Internet

PRINCIPI IN PRATICA

L'esempio di un ISP che collega otto organizzazioni a Internet illustra bene come gli indirizzi CIDRized assegnati con cura facilitino l'instradamento. Supponiamo, come mostrato nella Figura 4.18, che l'ISP (che chiameremo Fly-By-Night-ISP) pubblicizzi al mondo esterno che gli vengano inviati tutti i datagrammi i cui primi 20 bit dell'indirizzo corrispondono a 200.23.16.0/20. Il resto del mondo non deve sapere che all'interno del blocco di indirizzi 200.23.16.0/20 non ci sia alcun indirizzo CIDR. Il resto del mondo non deve sapere che all'interno del blocco di indirizzi 200.23.16.0/20 ci sono in realtà altre otto organizzazioni, ciascuna con le proprie sottoreti. Questa capacità di utilizzare un singolo indirizzo per pubblicizzare più reti viene spesso definita **aggregazione di indirizzi** (anche **aggregazione di percorsi** o **sommarizzazione di percorsi**).

L'aggregazione degli indirizzi funziona molto bene quando gli indirizzi sono assegnati in blocchi agli ISP e poi dagli ISP alle organizzazioni clienti. Ma cosa succede quando gli indirizzi non vengono assegnati in modo così gerarchico? Cosa succederebbe, ad esempio, se Fly-By-Night-ISP acquisisse ISP-R-Us e poi l'Organizzazione 1 si collegasse a Internet attraverso i suoi ISP-R-Us sussidiari? Come mostrato nella Figura 4.18, la filiale ISPs-R-Us possiede il blocco di indirizzi 199.31.0.0/16, ma gli indirizzi IP dell'Organizzazione 1 sono purtroppo al di fuori di questo blocco di indirizzi. Cosa si deve fare in questo caso? Certamente, l'Organizzazione 1 potrebbe rinumerare tutti i suoi router e host in modo che abbiano indirizzi all'interno del blocco di indirizzi ISPs-R-Us. Ma questa è una soluzione costosa e l'Organizzazione 1 potrebbe essere riassegnata a un'altra filiale in futuro. La soluzione tipicamente adottata è che l'Organizzazione 1
per mantenere i suoi indirizzi IP in 200.23.18.0/23. In questo caso, come illustrato nella Figura 4.19, Fly-By-Night-ISP continua a pubblicizzare il blocco di indirizzi 200.23.16.0/20 e ISPs-R-Us continua a pubblicizzare 199.31.0.0/16. Tuttavia, ISP-R-Us ora pubblicizza anche il blocco di indirizzi per l'Organizzazione 1, 200.23.18.0/23. Quando altri router nella grande Internet vedono i blocchi di indirizzi 200.23.16.0/20 (da Fly-By-Night-ISP) e 200.23.18.0/23 (da ISP-R-Us) e vogliono instradare verso un indirizzo nel blocco 200.23.18.0/23, useranno la corrispondenza del prefisso più lungo (si veda la Sezione 4.2.2) e instraderanno verso ISP-R-

Us, che pubblicizza il prefisso più lungo (più specifico) che corrisponde all'indirizzo di destinazione.

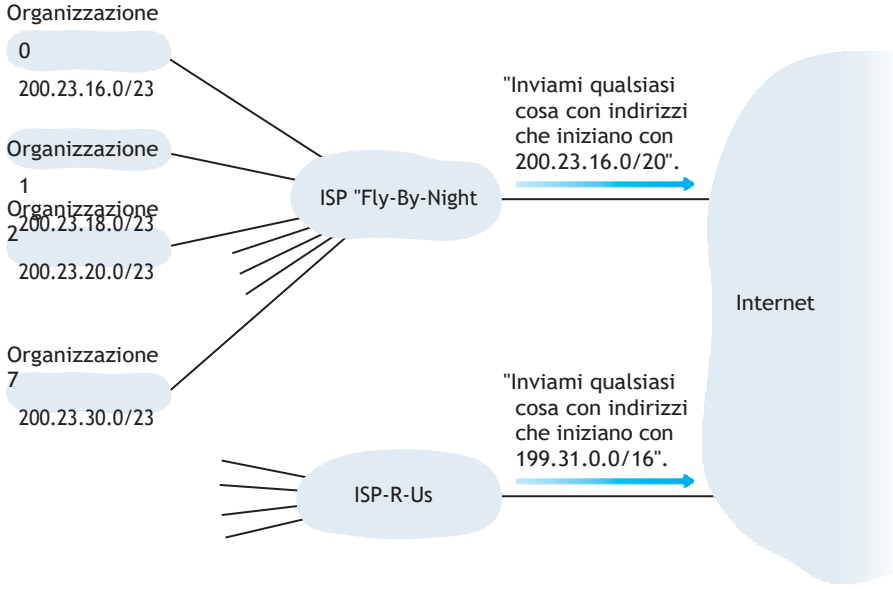

Figura 4.18 Indirizzamento gerarchico e aggregazione di percorsi

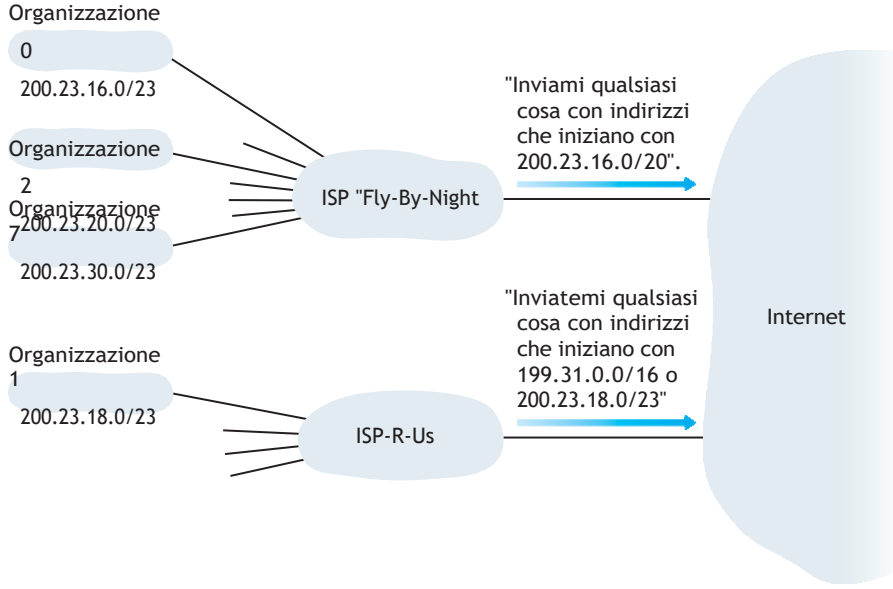

Figura 4.19 ISP-R-Us ha un percorso più specifico verso l'Organizzazione 1

Nella Sezione 4.6 vedremo che i router esterni alla rete dell'organizzazione considerano solo gli *x* bit iniziali del prefisso. In altre parole, quando un router esterno all'organizzazione inoltra un datagramma il cui indirizzo di destinazione si trova all'interno dell'organizzazione, devono essere considerati solo gli *x* bit iniziali dell'indirizzo. Ciò riduce notevolmente le dimensioni della tabella di inoltro in questi router, poiché una *sola* voce della forma *a.b.c.d/x* sarà sufficiente per inoltrare i pacchetti verso *qualsiasi* destinazione all'interno dell'organizzazione.

I restanti 32-x bit di un indirizzo possono essere considerati come una distinzione tra i dispositivi *all'interno dell'*organizzazione, che hanno tutti la stessa prefissazione di rete. Questi sono i bit che verranno presi in considerazione per l'inoltro dei pacchetti ai router *dell'*organizzazione. Questi bit di ordine inferiore possono avere (o meno) una struttura di subnetting aggiuntiva, come quella discussa in precedenza. Ad esempio, supponiamo che i primi 21 bit dell'indirizzo CIDRized a.b.c.d/21 specifichino il prefisso di rete dell'organizzazione e siano comuni agli indirizzi IP di tutti i dispositivi dell'organizzazione. Gli 11 bit rimanenti identificano gli host specifici dell'organizzazione. La struttura interna dell'organizzazione potrebbe essere tale da utilizzare gli 11 bit più a destra per la subnettizzazione all'interno dell'organizzazione, come discusso in precedenza. Ad esempio, a.b.c.d/24 potrebbe riferirsi a una sottorete specifica dell'organizzazione.

Prima dell'adozione del CIDR, le porzioni di rete di un indirizzo IP dovevano avere una lunghezza di 8, 16 o 24 bit, uno schema di indirizzamento noto come **indirizzamento di classe**, poiché le sottoreti con indirizzi di sottorete a 8, 16 e 24 bit erano note rispettivamente come reti di classe A, B e C. Il requisito per cui la porzione di sottorete di un indirizzo IP deve essere lunga esattamente 1, 2 o 3 byte si è rivelato problematico per la gestione del numero crescente di organizzazioni con sottoreti di piccole e medie dimensioni. Una sottorete di classe C (/24) può ospitare solo fino a $2^8 - 2 = 254$ host (due dei $2^8 = 256$ indirizzi sono riservati per uso speciale) - troppo piccola per molte organizzazioni. Tuttavia, una sottorete di classe B (/16), che supporta fino a 65.634 host, era troppo grande. Con l'indirizzamento di classe, a un'organizzazione con, ad esempio, 2.000 host veniva tipicamente assegnato un indirizzo di sottorete di classe B (/16). Questo portava a un rapido esaurimento dello spazio di indirizzi di classe B e a uno scarso utilizzo dello spazio di indirizzi assegnato. Ad esempio, all'organizzazione che utilizzava un indirizzo di classe B per i suoi 2.000 host veniva assegnato uno spazio di indirizzi sufficiente per 65.534 interfacce, lasciando più di 63.000 indirizzi che non potevano essere utilizzati da altre organizzazioni.

Saremmo negligenti se non menzionassimo un altro tipo di indirizzo IP, l'indirizzo IP broadcast 255.255.255.255. Quando un host invia un datagramma con indirizzo di destinazione 255.255.255.255, il messaggio viene recapitato a tutti gli host della stessa sottorete. I router possono inoltrare il messaggio anche nelle sottoreti vicine (anche se di solito non lo fanno).

Dopo aver studiato in dettaglio l'indirizzamento IP, dobbiamo sapere come gli host e le sottoreti ottengono i loro indirizzi. Cominciamo a vedere come un'organizzazione ottiene un blocco di indirizzi per i suoi dispositivi e poi vediamo come a un dispositivo (ad esempio un host) viene assegnato un indirizzo all'interno del blocco di indirizzi dell'organizzazione.

Ottenere un blocco di indirizzi

Per ottenere un blocco di indirizzi IP da utilizzare all'interno della sottorete di un'organizzazione, l'amministratore di rete potrebbe innanzitutto contattare il proprio ISP, che fornirebbe gli indirizzi da un blocco di indirizzi più ampio già assegnato all'ISP. Ad esempio, all'ISP potrebbe essere stato assegnato il blocco di indirizzi 200.23.16.0/20. L'ISP, a sua volta, potrebbe fornire indirizzi da un blocco più grande di indirizzi già assegnato all'ISP. L'ISP, a sua volta, potrebbe dividere il suo blocco di indirizzi in otto blocchi di indirizzi contigui di uguali dimensioni e distribuire uno di questi blocchi di indirizzi a ciascuna delle otto organizzazioni supportate dall'ISP, come mostrato di seguito. (Per comodità abbiamo sottolineato la parte di sottorete di questi indirizzi).

Blocco dell'ISP	200.23.16.0/20	11001000 00010111 00010000	00000000
Organizzazione 0	200.23.16.0/23	11001000 00010111 00010000	00000000
Organizzazione 1	200.23.18.0/23	11001000 00010111 00010010	00000000
Organizzazione 2	200.23.20.0/23	11001000 00010111 00010100	00000000
		. . .	
. . .. . .			
Organizzazione 7	200.23.30.0/23	11001000 00010111 00011110	00000000

Ottenere una serie di indirizzi da un ISP è un modo per ottenere un blocco di indirizzi, ma non è l'unico. È chiaro che deve esistere anche un modo per l'ISP stesso di ottenere un blocco di indirizzi. Esiste un'autorità globale che ha la responsabilità ultima di gestire lo spazio degli indirizzi IP e di assegnare blocchi di indirizzi agli ISP e ad altre organizzazioni? Certo che esiste! Gli indirizzi IP sono gestiti sotto l'autorità dell'Internet Corporation for Assigned Names and Numbers (ICANN) [ICANN 2012], sulla base delle linee guida stabilite in [RFC 2050]. Il ruolo dell'organizzazione non profit ICANN [NTIA 1998] non è solo quello di assegnare gli indirizzi IP, ma anche di gestire i root server DNS. Ha anche il compito, molto controverso, di assegnare i nomi di dominio e di risolvere le controversie sui nomi di dominio. L'ICANN assegna gli indirizzi ai registri Internet regionali (ad esempio ARIN, RIPE, APNIC e LACNIC, che insieme formano l'Address Supporting Organization dell'ICANN [ASO-ICANN 2012]) e si occupano dell'assegnazione/gestione degli indirizzi all'interno delle loro regioni.

Ottenere un indirizzo host: il protocollo di configurazione dinamica degli host

Una volta ottenuto un blocco di indirizzi, un'organizzazione può assegnare i singoli indirizzi IP alle interfacce host e router della propria organizzazione. Un amministratore di sistema in genere configura manualmente gli indirizzi IP nel router (spesso in remoto, con uno strumento di gestione della rete). Anche gli

indirizzi degli host possono essere configurati manualmente, ma più spesso questo compito viene svolto utilizzando il **Dynamic Host Configu- ration Protocol (DHCP)** [RFC 2131]. Il DHCP consente a un host di ottenere (assegnare) un indirizzo IP automaticamente. L'amministratore di rete può configurare il DHCP in modo tale che un host

Un host riceve lo stesso indirizzo IP ogni volta che si connette alla rete, oppure può essergli assegnato un **indirizzo IP temporaneo** che sarà diverso ogni volta che si connetterà alla rete. Oltre all'assegnazione dell'indirizzo IP dell'host, il DHCP consente a un host di apprendere ulteriori informazioni, come la maschera di sottorete, l'indirizzo del router first-hop (spesso chiamato gateway predefinito) e l'indirizzo del server DNS locale.

Per la capacità di DHCP di automatizzare gli aspetti di rete relativi alla connessione di un host a una rete, viene spesso definito un **protocollo plug-and-play**. Questa capacità lo rende *molto* interessante per l'amministratore di rete che altrimenti dovrebbe eseguire queste operazioni manualmente! Il DHCP è molto utilizzato anche nelle reti residenziali di accesso a Internet e nelle LAN wireless, dove gli host entrano ed escono frequentemente dalla rete. Si consideri, ad esempio, lo studente che trasporta un lap- top da una stanza del dormitorio a una biblioteca a una classe. È probabile che in ogni luogo lo studente si connetta a una nuova sottorete e quindi abbia bisogno di un nuovo indirizzo IP in ogni luogo. Il DHCP è ideale per questa situazione, poiché ci sono molti utenti che vanno e vengono e gli indirizzi sono necessari solo per un periodo di tempo limitato. Il DHCP è altrettanto utile nelle reti di accesso ISP residenziali. Si consideri, ad esempio, un ISP residenziale con 2.000 clienti, ma con non più di 400 clienti online contemporaneamente. In questo caso, invece di avere bisogno di un blocco di 2.048 indirizzi, un server DHCP che assegna gli indirizzi dinamicamente ha bisogno solo di un blocco di 512 indirizzi (ad esempio, un blocco della forma a.b.c.d/23). Man mano che gli host si aggiungono e se ne vanno, il server DHCP deve aggiornare l'elenco degli indirizzi IP disponibili. Ogni volta che un host si unisce, il server DHCP assegna un indirizzo arbitrario dal suo pool attuale di indirizzi disponibili; ogni volta che un host se ne va, il suo indirizzo viene restituito al pool.

Il DHCP è un protocollo client-server. Un client è tipicamente un host appena arrivato che vuole ottenere informazioni sulla configurazione della rete, compreso un indirizzo IP per sé. Nel caso più semplice, ogni sottorete (nel senso di indirizzamento della Figura 4.17) avrà un server DHCP. Se nella sottorete non è presente alcun server, è necessario un agente di relay DHCP (tipicamente un router) che conosca l'indirizzo di un server DHCP per quella rete. La Figura 4.20 mostra un server DHCP collegato alla sottorete 223.1.2/24, con il router che funge da agente relay per i client in arrivo collegati alle sottoreti 223.1.1/24 e 223.1.3/24. Nella discussione che segue, assumeremo che un server DHCP sia disponibile sulla sottorete.

Per un nuovo host in arrivo, il protocollo DHCP è un processo in quattro fasi, come mostrato nella Figura 4.21 per l'impostazione di rete mostrata nella Figura 4.20. In questa figura, yiaddr (come "il vostro indirizzo Internet") indica l'indirizzo che viene assegnato al nuovo client. In questa figura, `yiaddr` (come "il vostro indirizzo Internet") indica l'indirizzo che viene assegnato al client appena arrivato. Le quattro fasi sono:

- *Individuazione del server DHCP.* Il primo compito di un host appena arrivato è trovare un server DHCP con cui interagire. Ciò avviene tramite un **messaggio di scoperta DHCP**, che un client invia all'interno di un pacchetto UDP alla porta

67. Il pacchetto UDP è incapsulato in un datagramma IP. Il pacchetto UDP viene incapsulato in un datagramma IP. Ma a chi deve essere inviato questo datagramma? L'host non conosce nemmeno l'indirizzo IP della rete a cui si sta collegando, tanto meno l'indirizzo IP della rete a cui si sta collegando.

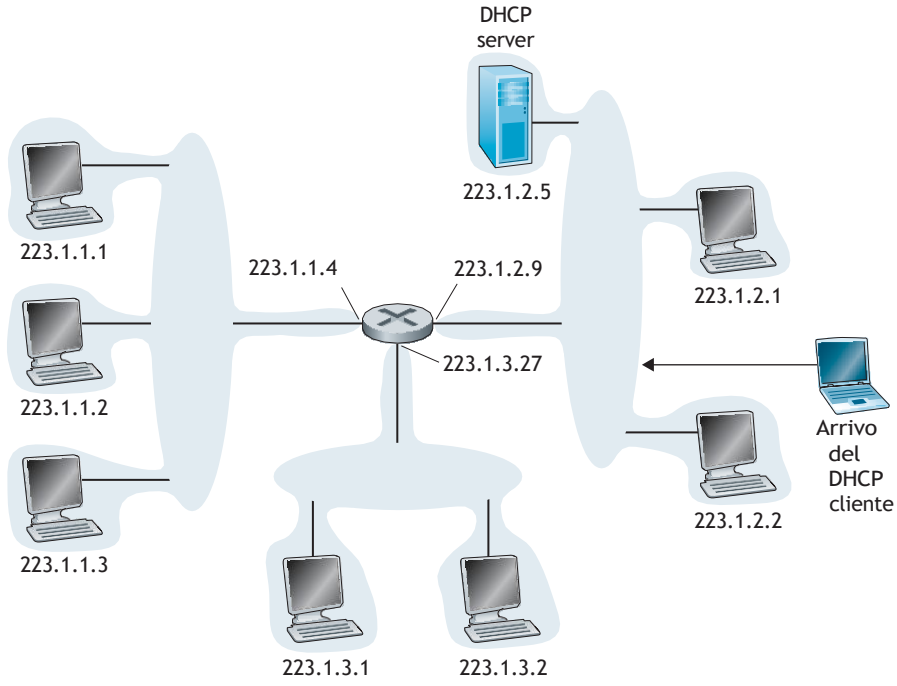

Figura 4.20 Scenario client-server DHCP

meno l'indirizzo di un server DHCP per questa rete. A questo punto, il client DHCP crea un datagramma IP contenente il suo messaggio di scoperta DHCP insieme all'indirizzo IP di destinazione broadcast di 255.255.255.255 e all'indirizzo IP di origine "questo host" di 0.0.0.0. Il client DHCP passa il datagramma IP al livello di collegamento, che trasmette questo frame a tutti i nodi collegati alla sottorete (i dettagli del broadcasting del livello di collegamento sono illustrati nella Sezione 5.4).

- *Offerta/i del server DHCP.* Un server DHCP che riceve un messaggio di scoperta DHCP risponde al client con un **messaggio di offerta DHCP** che viene trasmesso a tutti i nodi della sottorete, utilizzando ancora una volta l'indirizzo IP di trasmissione 255.255.255.255 (si potrebbe riflettere sul motivo per cui anche la risposta del server deve essere trasmessa). Poiché nella sottorete possono essere presenti più server DHCP, il client può trovarsi nell'invidiabile posizione di poter scegliere tra più offerte. Ogni messaggio di offerta del server contiene l'ID di transazione del messaggio di scoperta ricevuto, l'indirizzo IP proposto per il client, la maschera di rete e il **tempo di locazione dell'indirizzo** IP**, ovvero il** periodo di tempo in cui l'indirizzo IP sarà valido. È normale che il server imposti il tempo di locazione a diverse ore o giorni [Droms 2002].

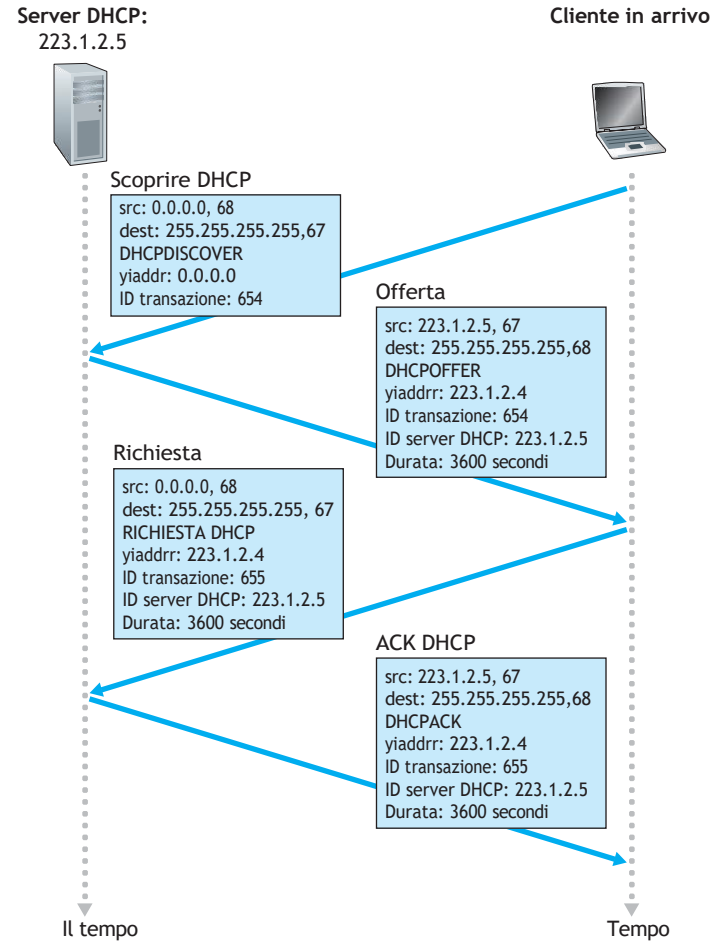

Figura 4.21 Interazione client-server DHCP

- *Richiesta DHCP.* Il nuovo client in arrivo sceglierà tra una o più offerte di server e risponderà all'offerta selezionata con un **messaggio di richiesta DHCP**, che riporterà i parametri di configurazione.
- *DHCP ACK.* Il server risponde al messaggio di richiesta DHCP con un **messaggio DHCP ACK**, confermando i parametri richiesti.

Quando il client riceve l'ACK DHCP, l'interazione è completa e il client può utilizzare l'indirizzo IP assegnato dal DHCP per la durata del lease. Poiché un client

Il DHCP fornisce anche un meccanismo che consente a un client di rinnovare il lease di un indirizzo IP.

Il valore della capacità plug-and-play di DHCP è evidente, considerando che l'alternativa è configurare manualmente l'indirizzo IP di un host. Si pensi allo studente che si sposta da un'aula all'altra, da una biblioteca a un dormitorio con un portatile, si unisce a una nuova sottorete e quindi ottiene un nuovo indirizzo IP in ogni luogo. È inimmaginabile che un amministratore di sistema debba riconfigurare i portatili in ogni luogo e pochi studenti (tranne quelli che frequentano un corso di computer networking!) hanno l'esperienza necessaria per configurare manualmente i loro portatili. Dal punto di vista della mobilità, tuttavia, il DHCP presenta delle lacune. Poiché un nuovo indirizzo IP viene ottenuto da DHCP ogni volta che un nodo si connette a una nuova sottorete, una connessione TCP a un'applicazione remota non può essere mantenuta mentre un nodo mobile si sposta tra le sottoreti. Nel Capitolo 6 esamineremo l'IP mobile, una recente estensione dell'infrastruttura IP che consente a un nodo mobile di utilizzare un unico indirizzo permanente mentre si sposta tra le sottoreti. Ulteriori dettagli su DHCP sono disponibili in [Droms 2002] e [dhc 2012]. Un'implementazione di riferimento open source di DHCP è disponibile presso l'Internet Systems Consor- tium [ISC 2012].

Traduzione degli indirizzi di rete (NAT)

Alla luce della nostra discussione sugli indirizzi Internet e sul formato dei datagrammi IPv4, siamo ormai consapevoli che ogni dispositivo in grado di funzionare su IP ha bisogno di un indirizzo IP. Con la proliferazione delle sottoreti per piccoli uffici e uffici domestici (SOHO), questo sembrerebbe implicare che ogni volta che un SOHO vuole installare una LAN per collegare più macchine, l'ISP deve assegnare una serie di indirizzi per coprire tutte le macchine del SOHO. Se la sottorete si allarga (ad esempio, i ragazzi a casa non hanno solo i loro computer, ma anche smartphone e Game Boy collegati in rete), è necessario assegnare un blocco di indirizzi più grande. Ma cosa succede se l'ISP ha già assegnato le porzioni contigue dell'attuale gamma di indirizzi della rete SOHO? E quale proprietario di casa vuole (o dovrebbe) sapere come gestire gli indirizzi IP? Fortunatamente, esiste un approccio più semplice all'assegnazione degli indirizzi che ha trovato un uso sempre più diffuso in questi scenari: la **traduzione degli indirizzi di rete** (**NAT**) [RFC 2663; RFC 3022; Zhang 2007].

La Figura 4.22 mostra il funzionamento di un router abilitato NAT. Il router NAT-enabled, che risiede in casa, ha un'interfaccia che fa parte della rete domestica, sulla destra della Figura 4.22. L'indirizzamento all'interno della rete domestica è esattamente quello che abbiamo visto in precedenza: tutte e quattro le interfacce della rete domestica hanno lo stesso indirizzo di sottorete 10.0.0/24. Lo spazio di indirizzi 10.0.0.0/8 è una delle tre porzioni dello spazio di indirizzi IP riservate in [RFC 1918] a una rete privata o a un **reame** con indirizzi privati, come la rete domestica della Figura 4.22. Un *regno con indirizzi privati* si riferisce a una rete i cui indirizzi hanno significato solo per i dispositivi all'interno della rete stessa. Per capire perché questo è importante, si consideri il fatto che esistono centinaia di

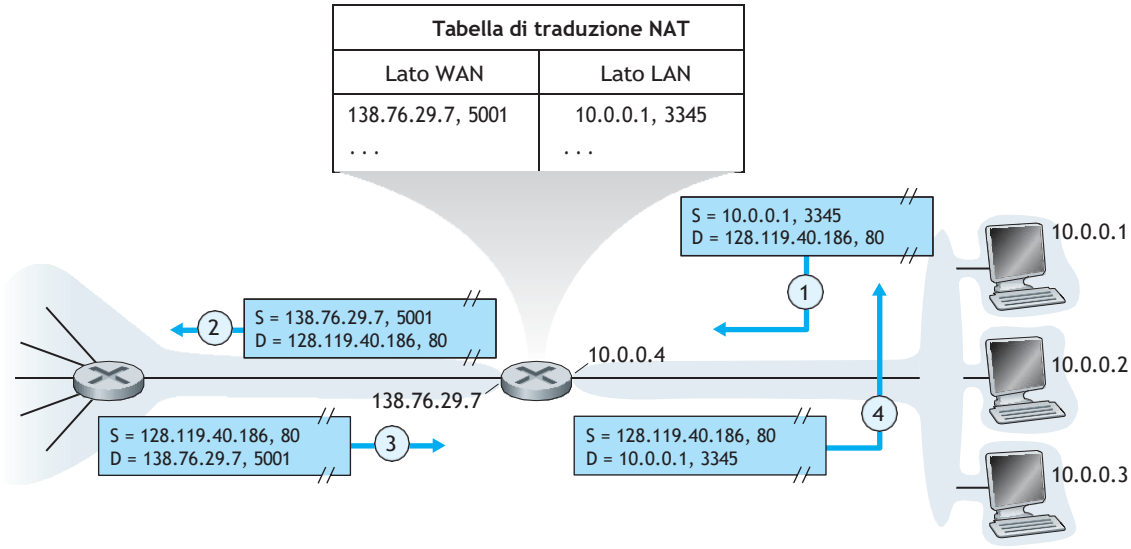

Figura 4.22 Traduzione degli indirizzi di rete

migliaia di reti domestiche, molte delle quali utilizzano lo stesso spazio di indirizzamento, 10.0.0.0/24. I dispositivi all'interno di una determinata rete domestica possono inviare pacchetti l'uno all'altro utilizzando l'indirizzo 10.0.0.0/24. Tuttavia, i pacchetti inoltrati *al di fuori della* rete domestica nella più ampia Internet globale non possono chiaramente utilizzare questi indirizzi (né come indirizzo di origine né come indirizzo di destinazione) perché ci sono centinaia di migliaia di reti che utilizzano questo blocco di indirizzi. In altre parole, gli indirizzi 10.0.0.0/24 possono avere un significato solo all'interno della rete domestica. Ma se gli indirizzi privati hanno significato solo all'interno di una determinata rete, come viene gestito l'indirizzamento quando i pacchetti vengono inviati o ricevuti da Internet globale, dove gli indirizzi sono necessariamente unici? La risposta sta nella comprensione del NAT.

Il router abilitato NAT non *appare* come un router al mondo esterno. Il router NAT si comporta invece con il mondo esterno come un *singolo* dispositivo con un *unico* indirizzo IP. Nella Figura 4.22, tutto il traffico che lascia il router domestico per la grande rete Internet ha un indirizzo IP di origine 138.76.29.7 e tutto il traffico che entra nel router domestico deve avere un indirizzo di destinazione 138.76.29.7. In sostanza, il router NAT-enabled nasconde il router all'esterno. In sostanza, il router abilitato al NAT nasconde i dettagli della rete domestica al mondo esterno. (A parte questo, ci si potrebbe chiedere dove i computer della rete domestica ottengano i loro indirizzi e dove il router ottenga il suo singolo indirizzo IP. Spesso la risposta è la stessa: l'HCP! Il router ottiene il suo indirizzo dal server DHCP dell'ISP e il router gestisce un server DHCP per fornire indirizzi ai computer all'interno dello spazio di indirizzi della rete domestica controllato dal router NAT-

DHCP).

Se tutti i datagrammi che arrivano al router NAT dalla WAN hanno lo stesso indirizzo IP di desti- nazione (in particolare, quello dell'interfaccia lato WAN del router NAT), come fa il router a sapere quale host interno deve inoltrare un dato datagramma? Il trucco consiste nell'utilizzare una **tabella di traduzione NAT** presso il router NAT e nell'includere i numeri di porta e gli indirizzi IP nelle voci della tabella.

Considerate l'esempio della Figura 4.22. Supponiamo che un utente seduto in una rete domestica dietro l'host 10.0.0.1 richieda una pagina Web su un server Web (porta 80) con indirizzo IP 128.119.40.186. L'host 10.0.0.1 assegna il numero di porta sorgente (arbitrario) 3345 e invia il datagramma nella LAN. Il router NAT riceve il dato, genera un nuovo numero di porta sorgente 5001 per il datagramma, sostituisce l'indirizzo IP sorgente con il suo indirizzo IP lato WAN 138.76.29.7 e sostituisce il numero di porta sorgente originale 3345 con il nuovo numero di porta sorgente 5001. Quando si genera un nuovo numero di porta sorgente, il router NAT può selezionare qualsiasi numero di porta sorgente che non sia attualmente presente nella tabella di traduzione NAT. (Si noti che, poiché il campo del numero di porta è lungo 16 bit, il protocollo NAT può supportare oltre 60.000 connessioni simultanee con un singolo indirizzo IP del router sul lato WAN). Il NAT nel router aggiunge anche una voce alla sua tabella di traduzione NAT. Il server Web, beatamente ignaro del fatto che il datagramma in arrivo contenente la richiesta HTTP sia stato manipolato dal router NAT, risponde con un datagramma il cui indirizzo di destinazione è l'indirizzo IP del router NAT e il cui numero di porta di destinazione è 5001. Quando questo datagramma arriva al router NAT, il router indicizza la tabella di traduzione NAT usando l'indirizzo IP di destinazione e il numero di porta di destinazione per ottenere l'indirizzo IP appropriato (10.0.0.1) e il numero di porta di destinazione (3345) per il browser nella rete domestica. Il router riscrive quindi l'indirizzo di destinazione e il numero di porta di destinazione del datagramma e lo inoltra nella rete domestica.

Negli ultimi anni il NAT si è diffuso in modo capillare. Tuttavia, è bene ricordare che molti puristi della comunità IETF si oppongono a gran voce al NAT. In primo luogo, sostengono che i numeri di porta devono essere usati per indirizzare i processi, non per indirizzare gli host. (Questa violazione può effettivamente causare problemi ai server in esecuzione sulla rete domestica, poiché, come abbiamo visto nel Capitolo 2, i processi server attendono le richieste in arrivo su numeri di porta noti). In secondo luogo, sostengono che i router dovrebbero elaborare i pacchetti solo fino al livello 3. In terzo luogo, il protocollo NAT viola la cosiddetta argomentazione end-to-end: gli host dovrebbero parlare direttamente tra loro, senza che i nodi interferenti modifichino gli indirizzi IP e i numeri di porta. E in quarto luogo, sostengono, dovremmo usare l'IPv6 (si veda la Sezione 4.4.4) per risolvere la carenza di indirizzi IP, piuttosto che rattoppare incautamente il problema con una soluzione provvisoria come il NAT. Ma, volenti o nolenti, il NAT è diventato un componente importante di Internet.

Un altro problema importante dei NAT è che interferiscono con le applicazioni P2P, comprese le applicazioni P2P di condivisione di file e le applicazioni P2P Voice-over-IP. Ricordiamo dal Capitolo 2 che in un'applicazione P2P, qualsiasi Peer A partecipante dovrebbe essere in grado di avviare una connessione TCP a

qualsiasi altro Peer B partecipante. L'essenza del problema è che se il Peer B si trova dietro un NAT, non può agire come server e accettare connessioni TCP.

connessioni. Come vedremo nei problemi a casa, questo problema NAT può essere aggirato se il Peer A non si trova dietro un NAT. In questo caso, il Peer A può prima contattare il Peer B attraverso un Peer C intermedio, che non si trova dietro una NAT e con cui B ha stabilito una connessione TCP in corso. Il Peer A può quindi chiedere al Peer B, tramite il Peer C, di avviare una connessione TCP direttamente al Peer A. Una volta stabilita la connessione TCP P2P diretta tra i Peer A e B, i due peer possono scambiarsi messaggi o file. Questo hack, chiamato **inversione della connessione**, è in realtà utilizzato da molte applicazioni P2P per l'**attraversamento del NAT**. Se sia il Peer A che il Peer B si trovano dietro i propri NAT, la situazione è un po' più complicata, ma può essere gestita utilizzando i relè dell'applicazione, come abbiamo visto con i relè di Skype nel Capitolo 2.

UPnP

Il NAT traversal è sempre più spesso fornito da Universal Plug and Play (UPnP), un protocollo che consente a un host di scoprire e configurare un NAT nelle vicinanze [UPnP Forum 2012]. UPnP richiede che sia l'host che il NAT siano compatibili con UPnP. Con UPnP, un'applicazione in esecuzione in un host può richiedere una mappatura NAT tra il suo (*indirizzo IP privato, numero di porta privato*) e il (*indirizzo IP pubblico, numero di porta pubblico*) per un numero di porta pubblico richiesto. Se il NAT accetta la richiesta e crea la mappatura, i nodi dall'esterno possono avviare connessioni TCP a (*indirizzo IP pubblico, numero di porta pubblica*). Inoltre, UPnP consente all'applicazione di conoscere il valore di (*indirizzo IP pubblico, numero di porta pubblica*), in modo che l'applicazione possa pubblicizzarlo all'esterno.

A titolo di esempio, supponiamo che il vostro host, dietro un NAT abilitato UPnP, abbia l'indirizzo privato 10.0.0.1 e stia eseguendo BitTorrent sulla porta 3345. Si supponga inoltre che l'indirizzo IP pubblico del NAT sia 138.76.29.7. L'applicazione BitTorrent vuole naturalmente essere in grado di accettare connessioni da altri host, in modo da poter scambiare chunk con loro. A tal fine, l'applicazione BitTorrent dell'host chiede al NAT di creare un "buco" che mappa (10.0.0.1, 3345) su (138.76.29.7, 5001). (L'applicazione BitTorrent nell'host potrebbe anche annunciare al suo tracker che è disponibile a (138.76.29.7, 5001). In questo modo, un host esterno che esegue BitTorrent può contattare il tracker e sapere che l'applicazione BitTorrent è in esecuzione a (138.76.29.7, 5001). L'host esterno può inviare un pacchetto TCP SYN a (138.76.29.7, 5001). Quando il NAT riceve il pacchetto SYN, cambia l'indirizzo IP di destinazione e il numero di porta del pacchetto in (10.0.0.1, 3345) e inoltra il pacchetto attraverso il NAT.

In sintesi, UPnP consente agli host esterni di avviare sessioni di comunicazione con host NATed, utilizzando TCP o UDP. I NAT sono stati a lungo una nemesi per le applicazioni P2P; UPnP, fornendo una soluzione efficace e robusta per l'attraversamento dei NAT, potrebbe essere il loro salvatore. La nostra discussione su NAT e UPnP è stata necessariamente breve. Per una discussione più dettagliata sui NAT si veda [Huston 2004, Cisco NAT 2012].

4.4.3 Protocollo messaggio di controllo Internet (ICMP)

Ricordiamo che il livello di rete di Internet ha tre componenti principali: il protocollo IP, discusso nella sezione precedente; i protocolli di routing di Internet (tra cui RIP, OSPF e BGP), trattati nella sezione 4.6; e ICMP, oggetto di questa sezione.

ICMP, specificato in [RFC 792], è utilizzato da host e router per comunicare informazioni di livello rete tra loro. L'uso più tipico di ICMP è la segnalazione di errori. Ad esempio, durante l'esecuzione di una sessione Telnet, FTP o HTTP, si può incontrare un messaggio di errore del tipo "Rete di destinazione non raggiungibile". Questo messaggio ha origine in ICMP. A un certo punto, un router IP non è riuscito a trovare un percorso verso l'host specificato nell'applicazione Telnet, FTP o HTTP. Il router ha creato e inviato un messaggio ICMP di tipo 3 all'host, indicando l'errore.

ICMP è spesso considerato parte di IP, ma dal punto di vista architetturale si trova appena al di sopra di IP, in quanto i messaggi ICMP sono trasportati all'interno dei datagrammi IP. In altre parole, i messaggi ICMP sono trasportati come carico utile IP, proprio come i segmenti TCP o UDP sono trasportati come carico utile IP. Analogamente, quando un host riceve un datagramma IP con ICMP specificato come proto-collo di livello superiore, demultiplexa il contenuto del datagramma in ICMP, proprio come demultiplexerebbe il contenuto di un datagramma in TCP o UDP.

I messaggi ICMP hanno un tipo e un campo codice e contengono l'intestazione e i primi 8 byte del datagramma IP che ha causato la generazione del messaggio ICMP (in modo che il mittente possa determinare il datagramma che ha causato l'errore). La Figura 4.23 mostra alcuni tipi di messaggi ICMP. Si noti che i messaggi ICMP non sono utilizzati solo per segnalare condizioni di errore.

Il noto programma ping invia un messaggio ICMP di tipo 8 codice 0 all'host specificato. L'host di destinazione, vedendo la richiesta di eco, invia una risposta di tipo 0 codice 0 ICMP. La maggior parte delle implementazioni TCP/IP supporta il server `ping` direttamente nel sistema operativo; in altre parole, il server non è un processo. Il capitolo 11 di [Stevens 1990] fornisce il codice sorgente del programma client ping. Si noti che il programma client deve essere in grado di istruire il sistema operativo a generare un messaggio ICMP di tipo 8 codice 0.

Un altro messaggio ICMP interessante è il messaggio di quench della sorgente. Questo messaggio è raramente utilizzato nella pratica. Il suo scopo originale era quello di eseguire il controllo della congestione, ovvero consentire a un router congestionato di inviare un messaggio ICMP source quench a un host per costringerlo a ridurre la sua velocità di trasmissione. Nel Capitolo 3 abbiamo visto che il TCP ha un proprio meccanismo di controllo della congestione che opera a livello di trasporto, senza l'uso di feedback a livello di rete come il messaggio ICMP source quench.

Nel Capitolo 1 abbiamo introdotto il programma Traceroute, che ci permette di tracciare un percorso da un host a qualsiasi altro host nel mondo. È interessante notare che Traceroute è implementato con i messaggi ICMP. Per determinare i nomi e gli indirizzi dei router tra la sorgente e la destinazione, Traceroute invia una

serie di normali datagrammi IP alla destinazione. Ciascuno di questi datagrammi contiene un segmento UDP con un numero di porta UDP improbabile. Il primo di questi datagrammi ha un TTL pari a 1, il secondo ha un TTL pari a 1, il terzo ha un TTL pari a 1.

Tipo ICMP	Codice	Descrizione
0	0	risposta eco (al ping)
3	0	rete di destinazione non raggiungibile
3	1	host di destinazione non raggiungibile
3	2	protocollo di destinazione non raggiungibile
3	3	porta di destinazione non raggiungibile
3	6	rete di destinazione sconosciuta
3	7	host di destinazione sconosciuto
4	0	source quench (controllo della congestione)
8	0	richiesta di eco
9	0	pubblicità del router
10	0	scoperta del router
11	0	TTL scaduto
12	0	Intestazione IP errata

Figura 4.23 Tipi di messaggi ICMP

il secondo di 2, il terzo di 3 e così via. La sorgente avvia anche dei timer per ciascuno dei datagrammi. Quando l'*ennesimo* datagramma arriva all'*ennesimo* router, quest'*ultimo* osserva che il TTL del datagramma è appena scaduto. Secondo le regole del protocollo IP, il router scarta il datagramma e invia un messaggio di avviso ICMP alla sorgente (tipo 11 codice 0). Questo messaggio di avviso include il nome del router e il suo indirizzo IP. Quando questo messaggio ICMP arriva alla sorgente, questa ottiene il tempo di andata e ritorno dal timer e il nome e l'indirizzo IP dell'*ennesimo* router dal messaggio ICMP.

Come fa una sorgente di Traceroute a sapere quando smettere di inviare segmenti UDP? Ricordiamo che la sorgente incrementa il campo TTL per ogni datagramma che invia. Pertanto, uno dei datagrammi arriverà fino all'host di destinazione. Poiché questo datagramma contiene un segmento UDP con un numero di porta improbabile, l'host di destinazione invia un messaggio ICMP di porta irraggiungibile (tipo 3 codice 3) alla sorgente. Quando l'host sorgente riceve questo particolare messaggio ICMP, sa di non dover inviare altri pacchetti di probe. (Il programma Traceroute standard invia in realtà serie di tre pacchetti con lo stesso TTL; pertanto l'output di Traceroute fornisce tre risultati per ogni TTL).

ATTENZIONE ALLA SICUREZZA

ISPEZIONARE I DATAGRAMMI: FIREWALL E SISTEMI DI RILEVAMENTO DELLE INTRUSIONI

Supponiamo che vi venga assegnato il compito di amministrare una rete domestica, dipartimentale, universitaria o aziendale. Gli aggressori, conoscendo l'intervallo di indirizzi IP della rete, possono facilmente inviare datagrammi IP agli indirizzi del vostro intervallo. Questi datagrammi possono fare ogni sorta di cose subdole, tra cui mappare la rete con ping e scansioni delle porte, bloccare gli host vulnerabili con pacchetti malformati, inondare i server con un diluvio di pacchetti ICMP e infettare gli host includendo malware nei pacchetti. In qualità di amministratore di rete, cosa farete contro tutti i malintenzionati là fuori, ognuno in grado di inviare pacchetti dannosi nella vostra rete? Due meccanismi di difesa popolari contro gli attacchi di pacchetti dannosi sono i firewall e i sistemi di rilevamento delle intrusioni (IDS).

L'amministratore di rete può innanzitutto provare a installare un firewall tra la rete e Internet (la maggior parte dei router di accesso è oggi dotata di funzionalità firewall). (I firewall ispezionano i campi dell'intestazione dei datagrammi e dei segmenti, negando l'accesso alla rete interna ai dati sospetti. Ad esempio, un firewall può essere configurato in modo da bloccare tutti i pacchetti di richiesta di eco ICMP, impedendo così a un aggressore di eseguire una tradizionale ricerca di ping sul vostro intervallo di indirizzi IP. I firewall possono anche bloccare i pacchetti in base agli indirizzi IP di origine e di destinazione e ai numeri di porta. Inoltre, i firewall possono essere configurati per tracciare le connessioni TCP, consentendo l'ingresso solo ai dati che appartengono a connessioni approvate.

Una protezione aggiuntiva può essere fornita da un IDS. Un IDS, tipicamente situato al confine della rete, esegue una "deep packet inspection", esaminando non solo i campi dell'intestazione ma anche i payload del datagramma (compresi i dati del livello applicativo). Un IDS dispone di un database di firme di pacchetti noti per essere parte di attacchi. Questo database viene aggiornato automaticamente quando vengono scoperti nuovi attacchi. Quando i pacchetti passano attraverso l'IDS, quest'ultimo cerca di far corrispondere i campi delle intestazioni e i payload alle firme presenti nel suo database di firme. Se viene trovata una corrispondenza, viene creato un allarme. Un sistema di prevenzione delle intrusioni (IPS) è simile a un IDS, ma blocca effettivamente i pacchetti oltre a creare avvisi. Nel Capitolo 8 verranno approfonditi i firewall e gli IDS.

I firewall e gli IDS possono proteggere completamente la rete da tutti gli attacchi? La risposta è chiaramente no, poiché gli aggressori trovano continuamente nuovi attacchi per i quali non sono ancora disponibili le firme. Tuttavia, i firewall e gli IDS tradizionali basati sulle firme sono utili per proteggere la rete dagli attacchi noti.

In questo modo, l'host sorgente apprende il numero e l'identità dei router che si trovano tra lui e l'host di destinazione e il tempo di andata e ritorno tra i due host. Si noti che il programma client di Traceroute deve essere in grado di istruire il sistema operativo a generare datagrammi UDP con valori TTL specifici e deve anche essere in grado di ricevere una notifica dal sistema operativo quando arrivano messaggi

ICMP. Ora che avete capito come funziona Traceroute, potete tornare a giocarci ancora un po'.

4.4.4 IPv6

All'inizio degli anni '90, l'Internet Engineering Task Force ha iniziato a sviluppare un successore del protocollo IPv4. Una delle motivazioni principali di questo sforzo è stata la consapevolezza che lo spazio di indirizzi IP a 32 bit stava iniziando a esaurirsi, con nuove sottoreti e nodi IP che venivano collegati a Internet (e a cui venivano assegnati indirizzi IP unici) a un ritmo mozzafiato. Per rispondere a questa esigenza di un ampio spazio di indirizzi IP, è stato sviluppato un nuovo protocollo IP, l'IPv6. I progettisti dell'IPv6 hanno colto l'occasione per modificare e migliorare altri aspetti dell'IPv4, sulla base dell'esperienza operativa accumulata con l'IPv4.

Il momento in cui gli indirizzi IPv4 sarebbero stati completamente allocati (e quindi nessuna nuova rete avrebbe potuto collegarsi a Internet) è stato oggetto di un notevole dibattito. Secondo le stime dei due leader del gruppo di lavoro Address Lifetime Expecta- tions dell'IETF, gli indirizzi sarebbero stati esauriti rispettivamente nel 2008 e nel 2018 [Solensky 1996]. Nel febbraio 2011, la IANA ha assegnato l'ultimo pool di indirizzi IPv4 non assegnati a un registro regionale. Anche se questi registri hanno ancora indirizzi IPv4 disponibili all'interno del loro pool, una volta che questi indirizzi sono esauriti, non ci sono più blocchi di indirizzi disponibili che possono essere assegnati da un pool centrale [Huston 2011a]. Sebbene le stime della metà degli anni Novanta sull'esaurimento degli indirizzi IPv4 suggerissero che poteva mancare ancora molto tempo all'esaurimento dello spazio di indirizzi IPv4, ci si rese conto che sarebbe stato necessario un tempo considerevole per implementare una nuova tecnologia su una scala così ampia, e così fu avviato lo sforzo di Next Generation IP (IPng) [Bradner 1996; RFC 1752]. Il risultato di questo sforzo è stata la specifica della versione 6 di IP (IPv6) [RFC 2460], di cui parleremo qui di seguito. (Una domanda che ci si pone spesso è: che fine ha fatto l'IPv5? Inizialmente si pensava che il protocollo ST-2 sarebbe diventato IPv5, ma ST-2 è stato poi abbandonato). Ottime fonti di informazioni su IPv6 sono [Huitema 1998, IPv6 2012].

Formato del datagramma IPv6

Il formato del datagramma IPv6 è mostrato nella Figura 4.24. I cambiamenti più importanti introdotti nel protocollo IPv6 sono evidenti nel formato del datagramma:

- *Capacità di indirizzamento ampliate.* L'IPv6 aumenta la dimensione dell'indirizzo IP da 32 a 128 bit. Questo garantisce che il mondo non esaurirà gli indirizzi IP. Ora ogni granello di sabbia del pianeta può essere indirizzato tramite IP. Oltre agli indirizzi unicast e multicast, l'IPv6 ha introdotto un nuovo tipo di indirizzo, chiamato **indirizzo anycast**, che consente di consegnare un datagramma a uno qualsiasi di un gruppo di host. (Questa funzione potrebbe essere utilizzata, ad esempio, per inviare un HTTP GET al più vicino di un certo numero di siti mirror che contengono un determinato documento).
- *Un'intestazione semplificata di 40 byte.* Come illustrato di seguito, una serie di campi IPv4 sono stati eliminati o resi opzionali. L'intestazione a lunghezza fissa

di 40 byte che ne risulta permette di