asíncronamente (a través de retrollamadas a procesos escucha, por ejemplo cuando cambia el estado de la red).

- *Núcleo distribuido.* El estado de los enlaces, hosts y dispositivos de la red se mantiene en el núcleo distribuido de ONOS. ONOS se implanta como un servicio en un conjunto de servidores interconectados, ejecutándose en cada servidor una copia idéntica del software ONOS; a mayor número de servidores, mayor capacidad de servicio. El núcleo de ONOS proporciona los mecanismos de replicación y coordinación del servicio entre instancias, proporcionando a las aplicaciones situadas por encima y a los dispositivos de red situados por debajo la abstracción de unos servicios del núcleo lógicamente centralizados.
- *Protocolos y abstracciones sur.* Las abstracciones sur enmascaran la heterogeneidad de los hosts, enlaces, conmutadores y protocolos subyacentes, permitiendo que el núcleo distribuido sea independiente de los dispositivos y de los protocolos. Debido a esta abstracción, la interfaz sur situada por debajo del núcleo distribuido está a un nivel lógico superior que en nuestro controlador canónico de la Figura 5.15 o en el controlador ODL de la Figura 5.17.

5.6 Protocolo de mensajes de control de Internet (ICMP)

Los hosts y los routers utilizan ICMP (*Internet Control Message Protocol*, protocolo de mensajes de control de Internet), especificado en [RFC 792], para intercambiarse información acerca de la capa de red. El uso más típico de ICMP es la generación de informes de error. Por ejemplo, al ejecutar una sesión HTTP podemos encontrarnos con un mensaje de error como "Red de destino inalcanzable". Este mensaje tiene su origen en ICMP. En algún punto, un router IP no ha podido encontrar una ruta hasta el host especificado en la solicitud HTTP, y dicho router ha creado y enviado un mensaje ICMP a nuestro host para informarle del error.

ICMP a menudo se considera parte de IP pero, en sentido arquitectónico, se encuentra justo encima de IP, ya que los mensajes ICMP son transportados dentro de datagramas IP. Es decir, los mensajes ICMP son transportados como carga útil de IP, al igual que los segmentos TCP o UDP son transportados como carga útil de IP. De forma similar, cuando un host recibe un datagrama IP con ICMP especificado como el protocolo de la capa superior (número de protocolo de la capa superior igual a 1), demultiplexa el contenido del datagrama hacia ICMP, al igual que demultiplexaría el contenido de un datagrama hacia TCP o UDP.

Los mensajes ICMP tienen un campo de tipo y un campo de código, y contienen la cabecera y los 8 primeros bytes del datagrama IP que ha dado lugar a la generación del mensaje ICMP (para que el emisor pueda determinar qué datagrama ha producido el error). En la Figura 5.19 se muestra una serie de tipos de mensajes ICMP seleccionados. Observe que los mensajes ICMP no solo se emplean para señalizar condiciones de error.

El famoso programa ping envía un mensaje ICMP de tipo 8 y código 0 al host especificado. El host de destino, al ver la solicitud de eco, devuelve una respuesta de eco ICMP de tipo 0 y código 0. La mayoría de las implementaciones de TCP/IP soportan el servidor ping directamente en el sistema operativo; es decir, el servidor no es un proceso. El Capítulo 11 de [Stevens 1990] proporciona el código fuente del programa cliente ping. Observe que el programa cliente necesita poder instruir al sistema operativo para generar un mensaje ICMP de tipo 8 y código 0.

Otro interesante mensaje ICMP es el mensaje de regulación del origen. Este mensaje rara vez se emplea en la práctica. Su propósito original era llevar a cabo el control de congestión (permitir a un router congestionado enviar un mensaje ICMP de este tipo a un host para forzarle a reducir su velocidad de transmisión). Hemos visto en el Capítulo 3 que TCP dispone de su propio mecanismo control de congestión que opera en la capa de transporte, sin utilizar ninguna realimentación de la capa de red, como el mensaje ICMP de regulación del origen.

Tipo ICMP	Código	Descripción
0	0	respuesta de eco (para ping)
3	0	red de destino inalcanzable
3	1	host de destino inalcanzable
3	2	protocolo de destino inalcanzable
3	3	puerto de destino inalcanzable
3	6	red de destino desconocida
3	7	host de destino desconocido
4	0	regulación del origen (control de congestión)
8	0	solicitud de eco
9	0	anuncio de router
10	0	descubrimiento de router
11	0	TTL caducado
12	0	Cabecera IP errónea

Figura 5.19 ♦ Tipos de mensajes ICMP.

En el Capítulo 1 hemos introducido el programa Traceroute, el cual nos permite trazar una ruta desde un host a cualquier otro host del mundo. Merece la pena resaltar que Traceroute se implementa con mensajes ICMP. Para determinar los nombres y las direcciones de los routers existentes entre el origen y el destino, el programa Traceroute del origen envía una serie de datagramas IP ordinarios al destino. Cada uno de estos datagramas transporta un segmento UDP con un número de puerto UDP poco probable. El primero de estos datagramas tiene un TTL de 1, el segundo de 2, el tercero de 3, y así sucesivamente. El origen también inicia sendos temporizadores para cada uno de los datagramas. Cuando el datagrama *n*-ésimo llega al router *n*-ésimo, este observa que el TTL del datagrama acaba de caducar. De acuerdo con las reglas del protocolo IP, el router descarta el datagrama y envía al origen un mensaje de advertencia ICMP (tipo 11, código 0). Este mensaje de advertencia incluye el nombre del router y su dirección IP. Cuando este mensaje ICMP llega de vuelta al origen, este obtiene el tiempo de ida y vuelta del temporizador, y obtiene también del propio mensaje ICMP el nombre y la dirección IP del router *n*-ésimo.

¿Cómo sabe un origen Traceroute cuándo dejar de enviar segmentos UDP? Recuerde que el origen incrementa el valor del campo TTL cada vez que envía un datagrama. Por tanto, uno de los datagramas terminará recorriendo el camino completo hasta el host de destino. Dado que ese datagrama contiene un segmento UDP con un número de puerto improbable, el host de destino devuelve al origen un mensaje ICMP de puerto inalcanzable (tipo 3, código 3). Cuando el host de origen recibe este mensaje ICMP, sabe que no tiene que enviar más paquetes de sondeo. (Realmente, el programa estándar Traceroute envía conjuntos de tres paquetes con el mismo TTL; es por ello que la salida de Traceroute proporciona tres resultados para cada TTL.)

De esta forma, el host de origen obtiene el número y la identidad de los routers que existen entre él y el host de destino, así como el tiempo de ida y vuelta entre los dos hosts. Observe que el programa cliente Traceroute tiene que poder instruir al sistema operativo para generar datagramas UDP con valores TTL específicos, y que el sistema operativo también tiene que ser capaz de notificarle la llegada de mensajes ICMP. Ahora que comprende cómo funciona Traceroute, puede volver atrás y practicar con él un poco más.

En RFC 4443 se ha definido una nueva versión de ICMP para IPv6. Además de reorganizar las definiciones existentes de tipos y códigos ICMP, ICMPv6 también añade nuevos tipos y códigos, requeridos por la nueva funcionalidad IPv6. Entre estos se incluyen el tipo "Packet too big" (paquete demasiado grande) y un código de error "unrecognized IPv6 options" (opciones IPv6 no reconocidas).

5.7 Gestión de red y SNMP

Habiendo finalizado nuestro estudio de la capa de red, y cuando ya solo nos queda por delante la capa de enlace, sabemos que una red está compuesta por muchos elementos hardware y software complejos, que interactúan unos con otros: elementos que van desde los enlaces, switches, routers, hosts y otros dispositivos que constituyen los componentes físicos de la red, hasta los muchos protocolos que controlan y coordinan estos dispositivos. Cuando una organización junta centenares o miles de esos componentes para formar una red, se vuelve todo un desafío el trabajo del administrador de la red, que no es otro que mantener la red funcionando. Hemos visto en la Sección 5.5 que el controlador lógicamente centralizado puede ayudar con este proceso, en un contexto SDN. Pero el desafío representado por la gestión de la red ha existido desde bastante antes que SDN, existiendo un rico conjunto de herramientas y técnicas de gestión de red que ayudan al administrador de la red a monitorizarla, gestionarla y controlarla. En esta sección estudiaremos esas herramientas y técnicas.

A menudo suele plantearse la pregunta de "¿Qué es la gestión de red?". Una definición de la gestión de red muy bien concebida, en una sola frase (aunque hay que reconocer que un poco larga), es la que da [Saydam 1996]:

> *La gestión de red incluye la implantación, integración y coordinación del hardware, el software y los elementos humanos para monitorizar, probar, sondear, configurar, analizar, evaluar y controlar los elementos y recursos de la red, con el fin de satisfacer los requisitos de tiempo real, de rendimiento operativo y de Calidad de Servicio, a un coste razonable.*

Dada esta amplia definición, vamos a cubrir en esta sección únicamente los rudimentos de la gestión de red: la arquitectura, los protocolos y la base de información que un administrador de red utiliza para llevar a cabo su tarea. No hablaremos de los procesos de toma de decisiones de los administradores, en los que hay que tener en cuenta la identificación de fallos [Labovitz 1997; Steinder 2002; Feamster 2005; Wu 2005; Teixeira 2006], la detección de anomalías [Lakhina 2005; Barford 2009], el diseño/ingeniería de la red para satisfacer los acuerdos de nivel de servicio (SLA, *Service Level Agreement*) contratados [Huston 1999a] y otros temas. Nuestro enfoque será, por tanto, deliberadamente reducido; el lector interesado puede consultar las referencias indicadas, el excelente libro de gestión de red de Subramanian [Subramanian 2000] y el tratamiento más detallado de la gestión de red disponible en el sitio web del presente libro.

5.7.1 El marco conceptual de la gestión de red

La Figura 5.20 muestra los componentes clave de la gestión de red:

- El **servidor de gestión** es una aplicación, normalmente con intervención humana, que se ejecuta en una estación central de gestión de red situada en el centro de operaciones de red (NOC, *Network Operations Center*). El servidor de gestión es el punto focal de la actividad de administración de la red; controla la recopilación, procesamiento, análisis y/o visualización de la información de gestión de la red. Es aquí donde se inician las acciones para el control del comportamiento de la red y donde el administrador interactúa con los dispositivos que forman la red.
- Un **dispositivo gestionado** es un equipo de red (incluyendo su software) que forma parte de una red gestionada. Un dispositivo gestionado puede ser un host, un router, un switch, un dispositivo