Índice general

I Familia de protocolos **1**

1. Asociando una dirección de Internet con una dirección física (ARP) **3**
1.1. Introducción . . . 3
1.2. Resolución a través de la asociación dinámica . . . 3
1.3. ARP Cache . . . 4
1.4. Revalidación automática de la tabla ARP . . . 4
1.5. Protocolo de resolución de direccion reversa . . . 5
1.6. Revisar y manipular las tablas ARP . . . 5
1.6.1. El comando *arp* . . . 5
1.6.2. El comando *arping* . . . 6

2. Protocolo de Internet (IP) **7**
2.1. Introducción . . . 7
2.2. Ruteo IP . . . 7
2.3. CIDR y extensiones de red . . . 8
2.3.1. Proxy ARP . . . 8
2.3.2. Subredes . . . 9
2.3.3. Redes punto a punto anónimas . . . 12
2.3.4. Encaminamiento inter-dominios sin clases (CIDR) y supernetting . . . 12
2.4. Configurando TCP/IP en una interfaz de red . . . 13
2.4.1. El comando *ifconfig* . . . 13
2.4.2. El comando *route* . . . 15

3. Protocolo de datagramas de usuario (UDP) **19**
3.1. Introducción . . . 19
3.2. Identificar el destino final . . . 19
3.3. El protocolo UDP . . . 20
3.4. Formato de los mensajes UDP . . . 20
3.5. Pseudo encabezado UDP . . . 21
3.6. El encapsulado UDP y el cómputo del checksum . . . 22
3.7. Multiplexación, de-multiplexación y puertos . . . 22
3.8. Número de puertos UDP disponibles y reservados . . . 22

4. Protocolo UDP-Lite **25**
4.1. Introducción . . . 25
4.2. Formato de los mensajes UDP-Lite . . . 25
4.3. Pseudo encabezado UDP-Lite . . . 26
4.4. Consideraciones para las capas inferiores . . . 26
4.5. Compatibilidad con UDP . . . 26
4.6. Consideraciones de seguridad . . . 26
4.7. Programa UDP-Lite en Perl . . . 27

4.7.1. Cliente . . . 27
4.7.2. Servidor . . . 28
4.7.3. Modo de uso . . . 28

5. Servicio de transporte de datos confiable (TCP) 29
5.1. Propiedades de un servicio de transporte confiable . . . 29
5.2. Proveer fiabilidad . . . 30
5.3. La idea detrás de la ventana deslizante . . . 30
5.4. El protocolo TCP . . . 32
5.5. Puertos, conexiones y terminales . . . 32
5.6. Apertura pasiva y activa . . . 32
5.7. Segmentos, flujos y números de secuencia . . . 33
5.8. Ventana de tamaño variable y control de flujo . . . 33
5.9. Formato del segmento TCP . . . 33
5.10. Datos fuera de banda . . . 34
5.11. Estableciendo una conexión TCP . . . 34
5.12. Número de secuencia inicial (ISN) . . . 35
5.13. Terminando una conexión TCP . . . 35
5.14. Reiniciar una conexión TCP . . . 36
5.15. *Sockets*, clientes y servidores . . . 36
5.15.1. El comando *nc* . . . 36
5.15.2. El comando *netstat* . . . 38
5.15.3. El comando *ss* . . . 40

6. Protocolo de Internet: mensajes de error y control 43
6.1. Introducción . . . 43
6.2. Protocolo de mensages de control de Internet . . . 43
6.3. Reporte de errores vs. Corrección de errores . . . 43
6.4. Entrega de mensajes ICMP . . . 44
6.5. Cambio de rutas por los enrutadores . . . 44
6.6. Herramientas de diagnóstico . . . 44
6.6.1. El comando *ping* . . . 44
6.6.2. El comando *traceroute* . . . 47
6.6.3. El comando *mtr* . . . 49

7. Protocolo de manejo de red simple (SNMP) 51
7.1. Introducción . . . 51
7.2. El modelo de SNMP . . . 51
7.2.1. La MIB y SMI . . . 53
7.3. La operación SNMP . . . 57
7.4. Mejoras de SNMPv2 . . . 60
7.5. SNMPv3 . . . 60
7.6. Aplicaciones para manejo de SNMP en Linux . . . 61
7.6.1. Instalando Net-SNMP . . . 61
7.6.2. Configurando el agente SNMP . . . 61
7.6.3. Explorando con SNMP . . . 61
7.6.4. Registrando nuevas MIB . . . 62
7.6.5. MIB-2: La tabla TCP Connection . . . 64
7.6.6. MIB-2: la tabla UDP . . . 65
7.6.7. El contenido de la MIB-2 . . . 65
7.6.8. Escribiendo valores con SNMP . . . 66
7.6.9. El navegador MIB . . . 69

II Herramientas para el administrador de red **71**

8. Captura de tráfico **73**
8.1. Analizadores de paquetes . . . 73
8.1.1. Introducción . . . 73
8.1.2. Acceder al tráfico . . . 73
8.2. El programa TCPDump . . . 75
8.2.1. Introducción . . . 75
8.2.2. Guardar las capturas . . . 75
8.2.3. Opciones de tcpdump . . . 77
8.2.4. Filtros de tcpdump . . . 85

9. Escaneadores de red **91**
9.1. Introducción . . . 91
9.2. Técnicas para escanear redes . . . 91
9.2.1. Host discovery . . . 91
9.2.2. Escaneo de puertos y servicios . . . 92
9.2.3. Detección de sistema operativo . . . 93
9.2.4. Optimización . . . 93
9.2.5. Evasión y suplantación de identidad . . . 93
9.2.6. ¿Quién usa escaneadores de red? . . . 94
9.3. NMAP . . . 94
9.3.1. Introducción . . . 94
9.3.2. Usando NMAP . . . 95
9.3.3. Técnicas de escaneo avanzadas con NMAP . . . 100

10. Herramientas de monitoreo **103**
10.1. Introducción . . . 103
10.2. Cacti . . . 103
10.2.1. ¿Qué es Cacti? . . . 103
10.2.2. Cómo opera Cacti . . . 103
10.2.3. Conocimientos básicos de RRDtool . . . 104
10.2.4. Instalando Cacti . . . 104
10.2.5. Actualizando Cacti . . . 110
10.3. NAGIOS: NAGIOS Ain't Gonna Insist On Sainthood . . . 111
10.3.1. Instalando NAGIOS . . . 111
10.3.2. Configurando NAGIOS . . . 112

III Apendices **123**

A. Protocolos **125**
A.1. Ethernet . . . 125
A.2. ARP . . . 126
A.3. IP . . . 127
A.4. TCP . . . 128
A.5. UDP . . . 130
A.6. ICMP . . . 130

B. Tutorial de Linux **133**
B.1. Ingresando al sistema . . . 133
B.2. Crear una cuenta de usuario . . . 133
B.3. Documentación y ayuda . . . 134
B.3.1. Páginas Man . . . 134
B.3.2. El comando man . . . 134
B.4. Saliendo de la sesión . . . 135
B.5. Apagando el sistema . . . 135
B.6. Determinar el directorio actual . . . 135
B.7. Cambiando de directorio . . . 136
B.8. Ver el contenido del directorio . . . 136
B.9. Manipulando archivos . . . 137
B.9.1. Redireccionar la salida estandar . . . 138
B.9.2. Anexar la salida estandar . . . 138
B.9.3. Redireccionar la entrada estandar . . . 138
B.10. Sobre pipes y pagers . . . 139
B.11. Más comandos para leer archivos de texto . . . 139
B.11.1. El comando `head` . . . 139
B.11.2. El comando `tail` . . . 139
B.11.3. El comando `grep` . . . 139
B.11.4. Comodines y expresiones regulares . . . 139
B.12. Permisos y propiedades . . . 139
B.12.1. El comando `chmod` . . . 140
B.12.2. El comando `chown` . . . 141
B.13. Crear archivos . . . 141
B.14. Copiando archivos . . . 142
B.15. Mover archivos . . . 142
B.16. Eliminar archivos y directorios . . . 142

C. Instalando NAGIOS desde el Código Fuente **143**
C.1. Instalando NAGIOS . . . 143
C.2. Instalando los plug-ins de NAGIOS . . . 144
C.3. Configurando Apache . . . 144
C.4. Configurando la autenticación de usuarios . . . 145

Índice Alfabético **147**

Bibliografía **150**