

CONTENIDO

PREFACIO xix

1 INTRODUCCIÓN 1

- 1.1 USOS DE LAS REDES DE COMPUTADORAS 2
 - 1.1.1 Aplicaciones de negocios 3
 - 1.1.2 Aplicaciones domésticas 5
 - 1.1.3 Usuarios móviles 9
 - 1.1.4 Cuestiones sociales 12
- 1.2 HARDWARE DE RED 15
 - 1.2.1 Redes de área personal 15
 - 1.2.2 Redes de área local 17
 - 1.2.3 Redes de área metropolitana 20
 - 1.2.4 Redes de área amplia 20
 - 1.2.5 Interredes 23
- 1.3 SOFTWARE DE RED 25
 - 1.3.1 Jerarquías de protocolos 25
 - 1.3.2 Aspectos de diseño para las capas 29
 - 1.3.3 Comparación entre servicio orientado a conexión y servicio sin conexión 30
 - 1.3.4 Primitivas de servicios 32
 - 1.3.5 La relación entre servicios y protocolos 34
- 1.4 MODELOS DE REFERENCIA 35
 - 1.4.1 El modelo de referencia OSI 35
 - 1.4.2 El modelo de referencia TCP/IP 39
 - 1.4.3 El modelo utilizado en este libro 41

- *1.4.4 Comparación de los modelos de referencia OSI y TCP/IP 42
 - *1.4.5 Una crítica al modelo y los protocolos OSI 43
 - *1.4.6 Una crítica al modelo de referencia TCP/IP 45
 - 1.5 REDES DE EJEMPLO 46
 - 1.5.1 Internet 46
 - *1.5.2 Redes de teléfonos móviles de tercera generación 55
 - *1.5.3 Redes LAN inalámbricas: 802.11 59
 - *1.5.3 Redes RFID y de sensores 63
 - *1.6 ESTANDARIZACIÓN DE REDES 65
 - 1.6.1 Quién es quién en el mundo de las telecomunicaciones 66
 - 1.6.2 Quién es quién en el mundo de los estándares internacionales 67
 - 1.6.3 Quién es quién en el mundo de estándares de Internet 68
 - 1.7 UNIDADES MÉTRICAS 70
 - 1.8 ESQUEMA DEL RESTO DEL LIBRO 71
 - 1.9 RESUMEN 72
- ## 2 LA CAPA FÍSICA 77
- 2.1 BASES TEÓRICAS PARA LA COMUNICACIÓN DE DATOS 77
 - 2.1.1 Análisis de Fourier 78
 - 2.1.2 Señales de ancho de banda limitado 78
 - 2.1.3 La tasa de datos máxima de un canal 81
 - 2.2 MEDIOS DE TRANSMISIÓN GUIADOS 82
 - 2.2.1 Medios magnéticos 82
 - 2.2.2 Par trenzado 83
 - 2.2.3 Cable coaxial 84
 - 2.2.4 Líneas eléctricas 85
 - 2.2.5 Fibra óptica 86
 - 2.3 TRANSMISIÓN INALÁMBRICA 91
 - 2.3.1 El espectro electromagnético 91
 - 2.3.2 Radiotransmisión 94
 - 2.3.3 Transmisión por microondas 95
 - 2.3.4 Transmisión infrarroja 98
 - 2.3.5 Transmisión por ondas de luz 99
 - *2.4 SATÉLITES DE COMUNICACIÓN 100
 - 2.4.1 Satélites geoestacionarios 101
 - 2.4.2 Satélites de Órbita Terrestre Media (MEO) 104
 - 2.4.3 Satélites de Órbita Terrestre Baja (LEO) 105
 - 2.4.4 Comparación de los satélites y la fibra óptica 107
 - 2.5 MODULACIÓN DIGITAL Y MULTIPLEXIÓN 108
 - 2.5.1 Transmisión en banda base 108
 - 2.5.2 Transmisión pasa-banda 112

- 2.5.3 Multiplexión por división de frecuencia 114
- 2.5.4 Multiplexión por división de tiempo 116
- 2.5.5 Multiplexión por división de código 117
- 2.6 LA RED TELEFÓNICA PÚBLICA CONMUTADA 120**
 - 2.6.1 Estructura del sistema telefónico 120
 - 2.6.2 La política de los teléfonos 123
 - 2.6.3 El lazo local: módems, ADSL y fibra óptica 124
 - 2.6.4 Troncales y multiplexión 131
 - 2.6.5 Conmutación 138
- *2.7 EL SISTEMA DE TELEFONÍA MÓVIL 142**
 - 2.7.1 Teléfonos móviles de primera generación (1G): voz analógica 143
 - 2.7.2 Teléfonos móviles de segunda generación (2G): voz digital 146
 - 2.7.3 Teléfonos móviles de tercera generación (3G): voz y datos digitales 150
- *2.8 TELEVISIÓN POR CABLE 154**
 - 2.8.1 Televisión por antena comunal 154
 - 2.8.2 Internet por cable 155
 - 2.8.3 Asignación de espectro 156
 - 2.8.4 Módems de cable 157
 - 2.8.5 Comparación de ADSL y cable 159
- 2.9 RESUMEN 160**
- 3 LA CAPA DE ENLACE DE DATOS 167**
 - 3.1 CUESTIONES DE DISEÑO DE LA CAPA DE ENLACE DE DATOS 168**
 - 3.1.1 Servicios proporcionados a la capa de red 168
 - 3.1.2 Entramado 170
 - 3.1.3 Control de errores 173
 - 3.1.4 Control de flujo 174
 - 3.2 DETECCIÓN Y CORRECCIÓN DE ERRORES 175**
 - 3.2.1 Códigos de corrección de errores 176
 - 3.2.2 Códigos de detección de errores 181
 - 3.3 PROTOCOLOS ELEMENTALES DE ENLACE DE DATOS 186**
 - 3.3.1 Un protocolo simplex utópico 190
 - 3.3.2 Protocolo simplex de parada y espera para un canal libre de errores 191
 - 3.3.3 Protocolo simplex de parada y espera para un canal ruidoso 193
 - 3.4 PROTOCOLOS DE VENTANA DESLIZANTE 196**
 - 3.4.1 Un protocolo de ventana deslizante de un bit 198
 - 3.4.2 Un protocolo que utiliza retroceso N 200
 - 3.4.3 Un protocolo que usa repetición selectiva 206
 - 3.5 EJEMPLOS DE PROTOCOLOS DE ENLACE DE DATOS 211**
 - 3.5.1 Paquetes sobre SONET 211
 - 3.5.2 ADSL 214
 - 3.6 RESUMEN 216**

4 LA SUBCAPA DE CONTROL DE ACCESO AL MEDIO 221

4.1 EL PROBLEMA DE ASIGNACIÓN DEL CANAL 222

4.1.1 Asignación estática de canal 222

4.1.2 Supuestos para la asignación dinámica de canales 223

4.2 PROTOCOLOS DE ACCESO MÚLTIPLE 225

4.2.1 ALOHA 225

4.2.2 Protocolos de acceso múltiple con detección de portadora 229

4.2.3 Protocolos libres de colisiones 232

4.2.4 Protocolos de contención limitada 235

4.2.5 Protocolos de LAN inalámbrica 238

4.3 ETHERNET 240

4.3.1 Capa física de Ethernet clásica 241

4.3.2 El protocolo de subcapa MAC de la Ethernet clásica 242

4.3.3 Desempeño de Ethernet 245

4.3.4 Ethernet conmutada 247

4.3.5 *Fast Ethernet* 249

4.3.6 Gigabit Ethernet 251

4.3.7 10 Gigabit Ethernet 254

4.3.8 Retrospectiva de Ethernet 255

4.4 REDES LAN INALÁMBRICAS 257

4.4.1 La arquitectura de 802.11 y la pila de protocolos 257

4.4.2 La capa física del estándar 802.11 258

4.4.3 El protocolo de la subcapa MAC del 802.11 260

4.4.4 La estructura de trama 802.11 265

4.4.5 Servicios 267

***4.5 BANDA ANCHA INALÁMBRICA 268**

4.5.1 Comparación del estándar 802.16 con 802.11 y 3G 269

4.5.2 La arquitectura de 802.16 y la pila de protocolos 270

4.5.3 La capa física del estándar 802.16 271

4.5.4 Protocolo de la subcapa MAC del estándar 802.16 273

4.5.5 La estructura de trama del estándar 802.16 274

4.6 BLUETOOTH* 275

4.6.1 Arquitectura de Bluetooth 275

4.6.2 Aplicaciones de Bluetooth 276

4.6.3 La pila de protocolos de Bluetooth 277

4.6.4 La capa de radio de Bluetooth 278

4.6.5 Las capas de enlace de Bluetooth 278

4.6.6 Estructura de la trama de Bluetooth 279

4.7 RFID* 281

4.7.1 Arquitectura EPC Gen 2 281

4.7.2 Capa física de EPC Gen 2 282

4.7.3 Capa de identificación de etiquetas de EPC Gen 2 283

4.7.4 Formatos de los mensajes de identificación de etiquetas 284

- 4.8 CONMUTACIÓN DE LA CAPA DE ENLACE DE DATOS 285
 - 4.8.1 Usos de los puentes 286
 - 4.8.2 Puentes de aprendizaje 287
 - 4.8.3 Puentes con árbol de expansión 290
 - 4.8.4 Repetidores, hubs, puentes, switches, enrutadores y puertas de enlace (gateways) 292
 - 4.8.5 Redes LAN virtuales 294
- 4.9 RESUMEN 300
- 5 LA CAPA DE RED 305**
 - 5.1 ASPECTOS DE DISEÑO DE LA CAPA DE RED 305
 - 5.1.1 Conmutación de paquetes de almacenamiento y reenvío 305
 - 5.1.2 Servicios proporcionados a la capa de transporte 306
 - 5.1.3 Implementación del servicio sin conexión 307
 - 5.1.4 Implementación del servicio orientado a conexión 309
 - 5.1.5 Comparación entre las redes de circuitos virtuales y las redes de datagramas 310
 - 5.2 ALGORITMOS DE ENRUTAMIENTO 311
 - 5.2.1 Principio de optimización 313
 - 5.2.2 Algoritmo de la ruta más corta 314
 - 5.2.3 Inundación 317
 - 5.2.4 Enrutamiento por vector de distancia 318
 - 5.2.5 Enrutamiento por estado del enlace 320
 - 5.2.6 Enrutamiento jerárquico 325
 - 5.2.7 Enrutamiento por difusión 326
 - 5.2.8 Enrutamiento multidifusión 328
 - 5.2.9 Enrutamiento anycast 331
 - 5.2.10 Enrutamiento para hosts móviles 332
 - 5.2.11 Enrutamiento en redes *ad hoc* 334
 - 5.3 ALGORITMOS DE CONTROL DE CONGESTIÓN 337
 - 5.3.1 Métodos para el control de la congestión 338
 - 5.3.2 Enrutamiento consciente del tráfico 339
 - 5.3.3 Control de admisión 340
 - 5.3.4 Regulación de tráfico 341
 - 5.3.5 Desprendimiento de carga 344
 - 5.4 CALIDAD DEL SERVICIO 347
 - 5.4.1 Requerimientos de la aplicación 347
 - 5.4.2 Modelado de tráfico 349
 - 5.4.3 Programación de paquetes 353
 - 5.4.4 Control de admisión 356
 - 5.4.5 Servicios integrados 359
 - 5.4.6 Servicios diferenciados 361
 - 5.5 INTERCONEXIÓN DE REDES 364
 - 5.5.1 Cómo difieren las redes 365
 - 5.5.2 Cómo se pueden conectar las redes 366
 - 5.5.3 Tunelización 368
 - 5.5.4 Enrutamiento entre redes 370
 - 5.5.5 Fragmentación de paquetes 371

- 5.6 LA CAPA DE RED DE INTERNET 374
 - 5.6.1 El protocolo IP versión 4 376
 - 5.6.2 Direcciones IP 379
 - 5.6.3 IP versión 6 390
 - 5.6.4 Protocolos de control en Internet 398
 - 5.6.5 Conmutación mediante etiquetas y MPLS 403
 - 5.6.6 OSPF: un protocolo de enrutamiento de puerta de enlace interior 405
 - 5.6.7 BGP: el protocolo de enrutamiento de Puerta de Enlace Exterior 410
 - 5.6.8 Multifusión de Internet 414
 - 5.6.9 IP móvil 415
- 5.7 RESUMEN 418
- 6 LA CAPA DE TRANSPORTE 425**
 - 6.1 EL SERVICIO DE TRANSPORTE 425
 - 6.1.1 Servicios que se proporcionan a las capas superiores 425
 - 6.1.2 Primitivas del servicio de transporte 427
 - 6.1.3 Sockets de Berkeley 430
 - 6.1.4 Un ejemplo de programación de sockets: un servidor de archivos de Internet 432
 - 6.2 ELEMENTOS DE LOS PROTOCOLOS DE TRANSPORTE 436
 - 6.2.1 Direccionamiento 437
 - 6.2.2 Establecimiento de una conexión 439
 - 6.2.3 Liberación de una conexión 444
 - 6.2.4 Control de errores y almacenamiento en búfer 448
 - 6.2.5 Multiplexión 452
 - 6.2.6 Recuperación de fallas 453
 - 6.3 CONTROL DE CONGESTIÓN 455
 - 6.3.1 Asignación de ancho de banda deseable 455
 - 6.3.2 Regulación de la tasa de envío 459
 - 6.3.3 Cuestiones inalámbricas 462
 - 6.4 LOS PROTOCOLOS DE TRANSPORTE DE INTERNET: UDP 464
 - 6.4.1 Introducción a UDP 464
 - 6.4.2 Llamada a procedimiento remoto 466
 - 6.4.3 Protocolos de transporte en tiempo real 469
 - 6.5 LOS PROTOCOLOS DE TRANSPORTE DE INTERNET: TCP 474
 - 6.5.1 Introducción a TCP 474
 - 6.5.2 El modelo del servicio TCP 474
 - 6.5.3 El protocolo TCP 477
 - 6.5.4 El encabezado del segmento TCP 478
 - 6.5.5 Establecimiento de una conexión TCP 481
 - 6.5.6 Liberación de una conexión TCP 482
 - 6.5.7 Modelado de administración de conexiones TCP 482
 - 6.5.8 Ventana deslizante de TCP 485
 - 6.5.9 Administración de temporizadores de TCP 488
 - 6.5.10 Control de congestión en TCP 490
 - 6.5.11 El futuro de TCP 499

- *6.6 ASPECTOS DEL DESEMPEÑO 500
 - 6.6.1 Problemas de desempeño en las redes de computadoras 500
 - 6.6.2 Medición del desempeño de las redes 501
 - 6.6.3 Diseño de hosts para redes rápidas 503
 - 6.6.4 Procesamiento rápido de segmentos 506
 - 6.6.5 Compresión de encabezado 509
 - 6.6.6 Protocolos para redes de alto desempeño 511
 - *6.7 REDES TOLERANTES AL RETARDO 515
 - 6.7.1 Arquitectura DTN 516
 - 6.7.2 El protocolo Bundle 518
 - 6.8 RESUMEN 520
- ## 7 LA CAPA DE APLICACIÓN 525
- 7.1 DNS: EL SISTEMA DE NOMBRES DE DOMINIO 525
 - 7.1.1 El espacio de nombres del DNS 526
 - 7.1.2 Registros de recursos de dominio 529
 - 7.1.3 Servidores de nombres 532
 - *7.2 CORREO ELECTRÓNICO 535
 - 7.2.1 Arquitectura y servicios 536
 - 7.2.2 El agente de usuario 538
 - 7.2.3 Formatos de mensaje 541
 - 7.2.4 Transferencia de mensajes 548
 - 7.2.5 Entrega final 553
 - 7.3 WORLD WIDE WEB 555
 - 7.3.1 Panorama de la arquitectura 556
 - 7.3.2 Páginas web estáticas 569
 - 7.3.3 Páginas web dinámicas y aplicaciones web 577
 - 7.3.4 HTTP: el Protocolo de Transferencia de HiperTexto 587
 - 7.3.5 La web móvil 596
 - 7.3.6 Búsqueda web 598
 - 7.4 AUDIO Y VIDEO DE FLUJO CONTINUO 599
 - 7.4.1 Audio digital 601
 - 7.4.2 Video digital 605
 - 7.4.3 Medios almacenados de flujo continuo (*streaming*) 612
 - 7.4.4 Transmisión en flujo continuo de medios en vivo 619
 - 7.4.5 Conferencia en tiempo real 623
 - 7.5 ENTREGA DE CONTENIDO 631
 - 7.5.1 Contenido y tráfico de Internet 632
 - 7.5.2 Granjas de servidores y proxies web 635
 - 7.5.3 Redes de entrega de contenido 639
 - 7.5.4 Redes de igual a igual 643
 - 7.6 RESUMEN 651

8 SEGURIDAD EN REDES 657

- 8.1 **CRIPTOGRAFÍA 660**
 - 8.1.1 Introducción a la criptografía 660
 - 8.1.2 Sistemas de cifrado por sustitución 662
 - 8.1.3 Sistemas de cifrado por transposición 663
 - 8.1.4 Rellenos de una sola vez 664
 - 8.1.5 Dos principios criptográficos fundamentales 668
- 8.2 **ALGORITMOS DE CLAVE SIMÉTRICA 670**
 - 8.2.1 DES: Estándar de Encriptación de Datos 671
 - 8.2.2 AES: Estándar de Encriptación Avanzada 674
 - 8.2.3 Modos de sistema de cifrado 677
 - 8.2.4 Otros sistemas de cifrado 681
 - 8.2.5 Criptoanálisis 682
- 8.3 **ALGORITMOS DE CLAVE PÚBLICA 683**
 - 8.3.1 RSA 684
 - 8.3.2 Otros algoritmos de clave pública 685
- 8.4 **FIRMAS DIGITALES 686**
 - 8.4.1 Firmas de clave simétrica 686
 - 8.4.2 Firmas de clave pública 687
 - 8.4.3 Resúmenes de mensaje 689
 - 8.4.4 El ataque de cumpleaños 692
- 8.5 **ADMINISTRACIÓN DE CLAVES PÚBLICAS 694**
 - 8.5.1 Certificados 694
 - 8.5.2 X.509 696
 - 8.5.3 Infraestructuras de clave pública 697
- 8.6 **SEGURIDAD EN LA COMUNICACIÓN 700**
 - 8.6.1 IPsec 700
 - 8.6.2 *Firewalls* 703
 - 8.6.3 Redes privadas virtuales 706
 - 8.6.4 Seguridad inalámbrica 707
- 8.7 **PROTOCOLOS DE AUTENTIFICACIÓN 711**
 - 8.7.1 Autenticación basada en una clave secreta compartida 712
 - 8.7.2 Establecimiento de una clave compartida: el intercambio de claves de Diffie-Hellman 716
 - 8.7.3 Autenticación mediante el uso de un centro de distribución de claves 718
 - 8.7.4 Autenticación mediante el uso de Kerberos 720
 - 8.7.5 Autenticación mediante el uso de criptografía de clave pública 722
- *8.8 **SEGURIDAD DE CORREO ELECTRÓNICO 723**
 - 8.8.1 PGP: Privacidad Bastante Buena 723
 - 8.8.2 S/MIME 727
- 8.9 **SEGURIDAD EN WEB 727**
 - 8.9.1 Amenazas 727
 - 8.9.2 Asignación segura de nombres 728

8.9.3 SSL: la capa de sockets seguros 733

8.9.4 Seguridad de código móvil 736

8.10 ASPECTOS SOCIALES 739

8.10.1 Privacidad 739

8.10.2 Libertad de expresión 742

8.10.3 Derechos de autor 745

8.11 RESUMEN 747

9 LISTA DE LECTURAS Y BIBLIOGRAFÍA 753

***9.1 SUGERENCIAS DE LECTURAS ADICIONALES 753**

9.1.1 Introducción y obras generales 754

9.1.2 La capa física 755

9.1.3 La capa de enlace de datos 755

9.1.4 La subcapa de control de acceso al medio 756

9.1.5 La capa de red 756

9.1.6 La capa de transporte 757

9.1.7 La capa de aplicación 757

9.1.8 Seguridad en redes 758

***9.2 BIBLIOGRAFÍA 759**

ÍNDICE 775