

CONTENIDO

PREFACIO

1 INTRODUCCIÓN

1

- 1.1 USOS DE LAS REDES DE COMPUTADORAS 3
 - 1.1.1 Aplicaciones de negocios 3
 - 1.1.2 Aplicaciones domésticas 6
 - 1.1.3 Usuarios móviles 9
 - 1.1.4 Temas sociales 12
- 1.2 HARDWARE DE REDES 14
 - 1.2.1 Redes de área local 16
 - 1.2.2 Redes de área metropolitana 18
 - 1.2.3 Redes de área amplia 19
 - 1.2.4 Redes inalámbricas 21
 - 1.2.5 Redes domésticas 23
 - 1.2.6 Interredes 25
- 1.3 SOFTWARE DE REDES 26
 - 1.3.1 Jerarquías de protocolos 26
 - 1.3.2 Aspectos de diseño de las capas 30
 - 1.3.3 Servicios orientados a la conexión y no orientados a la conexión 32
 - 1.3.4 Primitivas de servicio 34
 - 1.3.5 Relación de servicios a protocolos 36

- 1.4 MODELOS DE REFERENCIA 37
 - 1.4.1 El modelo de referencia OSI 37
 - 1.4.2 El modelo de referencia TCP/IP 41
 - 1.4.3 Comparación entre los modelos de referencia OSI y TCP/IP 44
 - 1.4.4 Crítica al modelo OSI y los protocolos 46
 - 1.4.5 Crítica del modelo de referencia TCP/IP 48
- 1.5 REDES DE EJEMPLO 49
 - 1.5.1 Internet 50
 - 1.5.2 Redes orientadas a la conexión: X.25, Frame Relay y ATM 59
 - 1.5.3 Ethernet 65
 - 1.5.4 LANs inalámbricas: 802.11 68
- 1.6 ESTANDARIZACIÓN DE REDES 71
 - 1.6.1 Quién es quién en el mundo de las telecomunicaciones 71
 - 1.6.2 Quién es quién en los estándares internacionales 74
 - 1.6.3 Quién es quién en el mundo de los estándares de Internet 75
- 1.7 UNIDADES MÉTRICAS 77
- 1.8 PANORAMA DEL RESTO DEL LIBRO 78
- 1.9 RESUMEN 80

2 LA CAPA FÍSICA

85

- 2.1 LA BASE TEÓRICA DE LA COMUNICACIÓN DE DATOS 85
 - 2.1.1 El análisis de Fourier 86
 - 2.1.2 Señales de ancho de banda limitado 86
 - 2.1.3 La tasa de datos máxima de un canal 89
- 2.2 MEDIOS DE TRANSMISIÓN GUIADOS 90
 - 2.2.1 Medios magnéticos 90
 - 2.2.2 Par trenzado 91
 - 2.2.3 Cable coaxial 92
 - 2.2.4 Fibra óptica 93
- 2.3 TRANSMISIÓN INALÁMBRICA 100
 - 2.3.1 El espectro electromagnético 100
 - 2.3.2 Radiotransmisión 103

2.3.3	Transmisión por microondas	104
2.3.4	Ondas infrarrojas y milimétricas	106
2.3.5	Transmisión por ondas de luz	107
2.4	SATÉLITES DE COMUNICACIONES	109
2.4.1	Satélites geoestacionarios	109
2.4.2	Satélites de Órbita Terrestre Media	113
2.4.3	Satélites de Órbita Terrestre Baja	114
2.4.4	Satélites en comparación con fibra óptica	117
2.5	LA RED TELEFÓNICA PÚBLICA CONMUTADA	118
2.5.1	Estructura del sistema telefónico	119
2.5.2	La política de los teléfonos	122
2.5.3	El circuito local: módems, ADSL e inalámbrico	124
2.5.4	Troncales y multiplexión	137
2.5.5	Conmutación	146
2.6	EL SISTEMA TELEFÓNICO MÓVIL	152
2.6.1	Teléfonos móviles de primera generación	153
2.6.2	Teléfonos móviles de segunda generación: voz digital	157
2.6.3	Teléfonos móviles de tercera generación: voz y datos digitales	166
2.7	TELEVISIÓN POR CABLE	169
2.7.1	Televisión por antena comunal	169
2.7.2	Internet a través de cable	170
2.7.3	Asignación de espectro	172
2.7.4	Módems de cable	173
2.7.5	ADSL en comparación con el cable	175
2.8	RESUMEN	177

3 LA CAPA DE ENLACE DE DATOS

183

3.1	CUESTIONES DE DISEÑO DE LA CAPA DE ENLACE DE DATOS	184
3.1.1	Servicios proporcionados a la capa de red	184
3.1.2	Entramado	187
3.1.3	Control de errores	191
3.1.4	Control de flujo	192

3.2	DETECCIÓN Y CORRECCIÓN DE ERRORES	192
3.2.1	Códigos de corrección de errores	193
3.2.2	Códigos de detección de errores	196
3.3	PROTOCOLOS ELEMENTALES DE ENLACE DE DATOS	200
3.3.1	Un protocolo simplex sin restricciones	204
3.3.2	Protocolo simplex de parada y espera	206
3.3.3	Protocolo simplex para un canal con ruido	208
3.4	PROTOCOLOS DE VENTANA CORREDIZA	211
3.4.1	Un protocolo de ventana corrediza de un bit	214
3.4.2	Protocolo que usa retroceso N	216
3.4.3	Protocolo que utiliza repetición selectiva	223
3.5	VERIFICACIÓN DE LOS PROTOCOLOS	229
3.5.1	Modelos de máquinas de estado finito	229
3.5.2	Modelos de red de Petri	232
3.6	EJEMPLOS DE PROTOCOLOS DE ENLACE DE DATOS	234
3.6.1	HDLC—Control de Enlace de Datos de Alto Nivel	234
3.6.2	La capa de enlace de datos en Internet	237
3.7	RESUMEN	242
4	LA SUBCAPA DE CONTROL DE ACCESO AL MEDIO	247
4.1	EL PROBLEMA DE ASIGNACIÓN DEL CANAL	248
4.1.1	Asignación estática de canal en LANs y MANs	248
4.1.2	Asignación dinámica de canales en LANs y MANs	249
4.2	PROTOCOLOS DE ACCESO MÚLTIPLE	251
4.2.1	ALOHA	251
4.2.2	Protocolos de acceso múltiple con detección de portadora	255
4.2.3	Protocolos libres de colisiones	259
4.2.4	Protocolos de contención limitada	261
4.2.5	Protocolos de acceso múltiple por división de longitud de onda	265
4.2.6	Protocolos de LANs inalámbricas	267

- 4.3 ETHERNET 271
 - 4.3.1 Cableado Ethernet 271
 - 4.3.2 Codificación Manchester 274
 - 4.3.3 El protocolo de subcapa MAC de Ethernet 275
 - 4.3.4 Algoritmo de retroceso exponencial binario 278
 - 4.3.5 Desempeño de Ethernet 279
 - 4.3.6 Ethernet conmutada 281
 - 4.3.7 Fast Ethernet 283
 - 4.3.8 Gigabit Ethernet 286
 - 4.3.9 Estándar IEEE 802.2: control lógico del enlace 290
 - 4.3.10 Retrospectiva de Ethernet 291
- 4.4 LANS INALÁMBRICAS 292
 - 4.4.1 La pila de protocolos del 802.11 292
 - 4.4.2 La capa física del 802.11 293
 - 4.4.3 El protocolo de la subcapa MAC del 802.11 295
 - 4.4.4 La estructura de trama 802.11 299
 - 4.4.5 Servicios 301
- 4.5 BANDA ANCHA INALÁMBRICA 302
 - 4.5.1 Comparación entre los estándares 802.11 y 802.16 303
 - 4.5.2 La pila de protocolos del estándar 802.16 305
 - 4.5.3 La capa física del estándar 802.16 306
 - 4.5.4 El protocolo de la subcapa MAC del 802.16 307
 - 4.5.5 La estructura de trama 802.16 309
- 4.6 BLUETOOTH 310
 - 4.6.1 Arquitectura de Bluetooth 311
 - 4.6.2 Aplicaciones de Bluetooth 312
 - 4.6.3 La pila de protocolos de Bluetooth 313
 - 4.6.4 La capa de radio de Bluetooth 314
 - 4.6.5 La capa de banda base de Bluetooth 315
 - 4.6.6 La capa L2CAP de Bluetooth 316
 - 4.6.7 Estructura de la trama de Bluetooth 316
- 4.7 CONMUTACIÓN EN LA CAPA DE ENLACE DE DATOS 317
 - 4.7.1 Puentes de 802.x a 802.y 319
 - 4.7.2 Interconectividad local 322
 - 4.7.3 Puentes con árbol de expansión 323
 - 4.7.4 Puentes remotos 325
 - 4.7.5 Repetidores, concentradores, puentes, conmutadores, enrutadores y puertas de enlace 326
 - 4.7.6 LANs virtuales 328
- 4.8 RESUMEN 336

5 LA CAPA DE RED**343**

- 5.1 ASPECTOS DE DISEÑO DE LA CAPA DE RED 343
 - 5.1.1 Conmutación de paquetes de almacenamiento y reenvío 344
 - 5.1.2 Servicios proporcionados a la capa de transporte 344
 - 5.1.3 Implementación del servicio no orientado a la conexión 345
 - 5.1.4 Implementación del servicio orientado a la conexión 347
 - 5.1.5 Comparación entre las subredes de circuitos virtuales y las de datagramas 348

- 5.2 ALGORITMOS DE ENRUTAMIENTO 350
 - 5.2.1 Principio de optimización 352
 - 5.2.2 Enrutamiento por la ruta más corta 353
 - 5.2.3 Inundación 355
 - 5.2.4 Enrutamiento por vector de distancia 357
 - 5.2.5 Enrutamiento por estado del enlace 360
 - 5.2.6 Enrutamiento jerárquico 366
 - 5.2.7 Enrutamiento por difusión 368
 - 5.2.8 Enrutamiento por multidifusión 370
 - 5.2.9 Enrutamiento para *hosts* móviles 372
 - 5.2.10 Enrutamiento en redes *ad hoc* 375
 - 5.2.11 Búsqueda de nodos en redes de igual a igual 380

- 5.3 ALGORITMOS DE CONTROL DE CONGESTIÓN 384
 - 5.3.1 Principios generales del control de congestión 386
 - 5.3.2 Políticas de prevención de congestión 388
 - 5.3.3 Control de congestión en subredes de circuitos virtuales 389
 - 5.3.4 Control de congestión en subredes de datagramas 391
 - 5.3.5 Desprendimiento de carga 394
 - 5.3.6 Control de fluctuación 395

- 5.4 CALIDAD DEL SERVICIO 397
 - 5.4.1 Requerimientos 397
 - 5.4.2 Técnicas para alcanzar buena calidad de servicio 398
 - 5.4.3 Servicios integrados 409
 - 5.4.4 Servicios diferenciados 412
 - 5.4.5 Conmutación de etiquetas y MPLS 415

- 5.5 INTERCONECTIVIDAD 418
 - 5.5.1 Cómo difieren las redes 419
 - 5.5.2 Conexión de redes 420
 - 5.5.3 Circuitos virtuales concatenados 422
 - 5.5.4 Interconectividad no orientada a la conexión 423

- 5.5.5 Entunelamiento 425
- 5.5.6 Enrutamiento entre redes 426
- 5.5.7 Fragmentación 427
- 5.6 LA CAPA DE RED DE INTERNET 431
 - 5.6.1 El protocolo IP 433
 - 5.6.2 Direcciones IP 436
 - 5.6.3 Protocolos de Control en Internet 449
 - 5.6.4 OSPF—Protocolos de Enrutamiento de Puerta de Enlace Interior 454
 - 5.6.5 BGP—Protocolo de Puerta de Enlace de Frontera 459
 - 5.6.6 Multidifusión de Internet 461
 - 5.6.7 IP móvil 462
 - 5.6.8 IPv6 464
- 5.7 RESUMEN 473

6 LA CAPA DE TRANSPORTE

481

- 6.1 EL SERVICIO DE TRANSPORTE 481
 - 6.1.1 Servicios proporcionados a las capas superiores 481
 - 6.1.2 Primitivas del servicio de transporte 483
 - 6.1.3 *Sockets* de Berkeley 487
 - 6.1.4 Un ejemplo de programación de *sockets*: un servidor de archivos de Internet 488
- 6.2 ELEMENTOS DE LOS PROTOCOLOS DE TRANSPORTE 492
 - 6.2.1 Direccionamiento 493
 - 6.2.2 Establecimiento de una conexión 496
 - 6.2.3 Liberación de una conexión 502
 - 6.2.4 Control de flujo y almacenamiento en búfer 506
 - 6.2.5 Multiplexión 510
 - 6.2.6 Recuperación de caídas 511
- 6.3 UN PROTOCOLO DE TRANSPORTE SENCILLO 513
 - 6.3.1 Las primitivas de servicio de ejemplo 513
 - 6.3.2 La entidad de transporte de ejemplo 515
 - 6.3.3 El ejemplo como máquina de estados finitos 522
- 6.4 LOS PROTOCOLOS DE TRANSPORTE DE INTERNET: UDP 524
 - 6.4.1 Introducción a UDP 525
 - 6.4.2 Llamada a procedimiento remoto 526
 - 6.4.3 El protocolo de transporte en tiempo real 529

6.5 LOS PROTOCOLOS DE TRANSPORTE DE INTERNET: TCP 532

- 6.5.1 Introducción a TCP 532
- 6.5.2 El modelo del servicio TCP 533
- 6.5.3 El protocolo TCP 535
- 6.5.4 El encabezado del segmento TCP 536
- 6.5.5 Establecimiento de una conexión TCP 539
- 6.5.6 Liberación de una conexión TCP 541
- 6.5.7 Modelado de administración de conexiones TCP 541
- 6.5.8 Política de transmisión del TCP 543
- 6.5.9 Control de congestión en TCP 547
- 6.5.10 Administración de temporizadores del TCP 550
- 6.5.11 TCP y UDP inalámbricos 553
- 6.5.12 TCP para Transacciones 555

6.6 ASPECTOS DEL DESEMPEÑO 557

- 6.6.1 Problemas de desempeño en las redes de cómputo 557
- 6.6.2 Medición del desempeño de las redes 560
- 6.6.3 Diseño de sistemas para un mejor desempeño 562
- 6.6.4 Procesamiento rápido de las TPDU's 566
- 6.6.5 Protocolos para redes de gigabits 569

6.7 RESUMEN 573

7 LA CAPA DE APLICACIÓN

579

7.1 DNS—EL SISTEMA DE NOMBRES DE DOMINIO 579

- 7.1.1 El espacio de nombres del DNS 580
- 7.1.2 Registros de recursos 582
- 7.1.3 Servidores de nombres 586

7.2 CORREO ELECTRÓNICO 588

- 7.2.1 Arquitectura y servicios 590
- 7.2.2 El agente de usuario 591
- 7.2.3 Formatos de mensaje 594
- 7.2.4 Transferencia de mensajes 602
- 7.2.5 Entrega final 605

7.3 WORLD WIDE WEB 611

- 7.3.1 Panorama de la arquitectura 612
- 7.3.2 Documentos Web estáticos 629

7.3.3	Documentos Web dinámicos	643
7.3.4	HTTP—Protocolo de Transferencia de Hipertexto	651
7.3.5	Mejoras de desempeño	656
7.3.6	La Web inalámbrica	662
7.4	MULTIMEDIA	674
7.4.1	Introducción al audio digital	674
7.4.2	Compresión de audio	676
7.4.3	Audio de flujo continuo	679
7.4.4	Radio en Internet	683
7.4.5	Voz sobre IP	685
7.4.6	Introducción al vídeo	692
7.4.7	Compresión de vídeo	696
7.4.8	Vídeo bajo demanda	704
7.4.9	Mbone—Red dorsal de multidifusión	711
7.5	RESUMEN	714

8 SEGURIDAD EN REDES

721

8.1	CRIPTOGRAFÍA	724
8.1.1	Introducción a la criptografía	725
8.1.2	Cifrados por sustitución	727
8.1.3	Cifrados por transposición	729
8.1.4	Rellenos de una sola vez	730
8.1.5	Dos principios criptográficos fundamentales	735
8.2	ALGORITMOS DE CLAVE SIMÉTRICA	737
8.2.1	DES—El Estándar de Encriptación de Datos	738
8.2.2	AES—El Estándar de Encriptación Avanzada	741
8.2.3	Modos de cifrado	745
8.2.4	Otros cifrados	750
8.2.5	Criptoanálisis	750
8.3	ALGORITMOS DE CLAVE PÚBLICA	752
8.3.1	El algoritmo RSA	753
8.3.2	Otros algoritmos de clave pública	755

- 8.4 FIRMAS DIGITALES 755
 - 8.4.1 Firmas de clave simétrica 756
 - 8.4.2 Firmas de clave pública 757
 - 8.4.3 Compendios de mensaje 759
 - 8.4.4 El ataque de cumpleaños 763

- 8.5 ADMINISTRACIÓN DE CLAVES PÚBLICAS 765
 - 8.5.1 Certificados 765
 - 8.5.2 X.509 767
 - 8.5.3 Infraestructuras de clave pública 768

- 8.6 SEGURIDAD EN LA COMUNICACIÓN 772
 - 8.6.1 Ipsec 772
 - 8.6.2 *Firewalls* 776
 - 8.6.3 Redes privadas virtuales 779
 - 8.6.4 Seguridad inalámbrica 780

- 8.7 PROTOCOLOS DE AUTENTICACIÓN 785
 - 8.7.1 Autenticación basada en una clave secreta compartida 786
 - 8.7.2 Establecimiento de una clave compartida: el intercambio de claves de Diffie-Hellman 791
 - 8.7.3 Autenticación que utiliza un centro de distribución de claves 793
 - 8.7.4 Autenticación utilizando Kerberos 796
 - 8.7.5 Autenticación utilizando criptografía de clave pública 798

- 8.8 SEGURIDAD DE CORREO ELECTRÓNICO 799
 - 8.8.1 PGP—Privacidad Bastante Buena 799
 - 8.8.2 PEM—Correo con Privacidad Mejorada 803
 - 8.8.3 S/MIME 804

- 8.9 SEGURIDAD EN WEB 805
 - 8.9.1 Amenazas 805
 - 8.9.2 Asignación segura de nombres 806
 - 8.9.3 SSL—La Capa de Sockets Seguros 813
 - 8.9.4 Seguridad de código móvil 816

- 8.10 ASPECTOS SOCIALES 819
 - 8.10.1 Privacidad 819
 - 8.10.2 Libertad de expresión 822
 - 8.10.3 Derechos de autor 826

- 8.11 RESUMEN 828