

Puede solicitar los archivos complementarios de este libro escribiendo
a **comercial@ediciones-eni.com**

Prólogo

Capítulo 1

Presentación de los conceptos de red

1. Antecedentes.....	19
1.1 Principios de la informática de redes.....	19
1.1.1 La informática centralizada.....	19
1.1.2 La primera red informática a gran escala.....	21
1.1.3 El desarrollo de una norma de hecho: TCP/IP.....	23
1.1.4 La informática descentralizada.....	25
1.2 Redes heterogéneas.....	27
1.3 Redes informáticas actuales.....	28
1.4 Interacción con las redes informáticas.....	29
2. Principales elementos de una red.....	36
2.1 Cliente/servidor.....	37
2.1.1 Principios.....	37
2.1.2 Definiciones.....	37
2.1.3 El sistema operativo de red.....	45
2.2 Desde la perspectiva del hardware.....	59
2.2.1 La interconexión.....	59
2.2.2 Los protocolos de comunicación.....	59
3. Tecnología de redes.....	59
3.1 Definición de una red informática.....	59
3.2 Topologías de redes informáticas.....	60
3.2.1 La red personal.....	60
3.2.2 La red local.....	61

2 **Redes informáticas**

Nociones fundamentales

3.2.3	La red metropolitana	61
3.2.4	La red extendida	61
3.3	Compartir recursos	61
3.3.1	Los servicios de archivos	62
3.3.2	Los servicios de gestión electrónica de documentos	66
3.3.3	Los servicios de base de datos	67
3.3.4	Los servicios de impresión	70
3.3.5	Los servicios de mensajería y de trabajo colaborativo	71
3.3.6	Los servicios de aplicaciones	73
3.3.7	Los servicios de almacenamiento	74
3.3.8	Los servicios de copia de seguridad	94
3.3.9	Los protocolos de replicación entre bahías	98
3.3.10	WAAS y compresión del flujo	100
3.4	Virtualización	103
3.4.1	Introducción	103
3.4.2	Algunos conceptos de virtualización	103
3.4.3	Soluciones de virtualización típicas	107
3.4.4	Resumen de tecnologías de virtualización	110
3.4.5	Desktop as a Service	113
3.5	Cloud Computing	118
4.	Plan de continuidad de la actividad	121
4.1	Disponibilidad	121
4.1.1	La fiabilización del sistema de almacenamiento	121
4.1.2	La fiabilización de los intercambios	124
4.2	Confidencialidad	125
4.2.1	La seguridad del sistema de archivos	125
4.2.2	La protección de los intercambios	127
4.3	Redundancia de datos	128
4.3.1	La tolerancia a fallos	128
4.3.2	El espejo de discos	133
4.3.3	El espejo de controladores y discos	135
4.3.4	Bloques de intervalo con paridad	136
4.3.5	La neutralización de los sectores defectuosos	139

4.4	Soluciones de redundancia en servidor	139
4.4.1	La tolerancia a fallos	140
4.4.2	La distribución de la carga de red	143
4.4.3	La configuración de las tarjetas de red en teaming	144
4.4.4	La virtualización como solución en sí misma	146
4.5	Política de respaldo	147
4.5.1	El respaldo completo	148
4.5.2	El respaldo incremental	148
4.5.3	El respaldo diferencial	148
4.5.4	Securización de las copias de seguridad	149
4.5.5	Respaldos inmutables	150
4.6	Continuidad y reanudación de la actividad en caso de siniestro	150
4.6.1	Principios	150
4.6.2	El plan de continuidad de la actividad (PCA)	151
4.6.3	El plan de reanudación de actividad (PRA)	152

Capítulo 2

Estandarización de protocolos

1.	Modelo OSI	153
1.1	Principios	154
1.2	Comunicación entre capas	155
1.3	Encapsulación y modelo OSI	157
1.4	Protocolos	163
1.5	Papel de las distintas capas	164
1.5.1	La capa física	164
1.5.2	La capa de Conexión (o Conexión de datos)	164
1.5.3	La capa de Red	165
1.5.4	La capa de Transporte	165
1.5.5	La capa de Sesión	166
1.5.6	La capa de Presentación	166
1.5.7	La capa de Aplicación	167

4 **Redes informáticas**

Nociones fundamentales

2. Enfoque pragmático del modelo de capas	167
2.1 Nivel 1: capa física	168
2.2 Nivel 2: capa de Conexión de datos	168
2.3 Nivel 3: capa de Red	172
2.3.1 Principios.	172
2.3.2 La dirección lógica	172
2.3.3 La salida de una red lógica	174
2.3.4 La transmisión de paquetes en la intranet	176
2.3.5 Distribución de paquetes en el router	179
2.4 Nivel 4: capa de Transporte	181
2.4.1 El modo conectado TCP	181
2.4.2 El modo no conectado UDP	183
2.5 Nivel 5 y superiores	183
3. Estándares y organismos	184
3.1 Tipos de estándares	184
3.2 Algunos organismos de estandarización para redes	184
3.2.1 American National Standards Institute (ANSI)	185
3.2.2 Unión internacional de las telecomunicaciones (UIT)	186
3.2.3 Electronic Component Industry Association (ecia)	187
3.2.4 Institute of Electrical and Electronics Engineers (IEEE)	188
3.2.5 ISO	189
3.2.6 Internet Engineering Task Force (IETF)	190

Capítulo 3

Transmisión de datos en la capa física

1. Papel de una interfaz de red	191
1.1 Principios.	191
1.2 Preparación de los datos	192
2. Opciones y parámetros de configuración	193
2.1 Dirección física	193
2.2 Interrupción	197
2.3 Dirección de entrada/salida	198

2.4	Dirección de memoria base	198
2.5	Canal DMA (Direct Memory Access)	198
2.6	Bus	198
2.6.1	El bus PCI (Peripheral Component Interconnect)	200
2.6.2	El bus USB	203
2.7	Conectores de cable de red	207
2.7.1	El conector RJ45	208
2.7.2	El conector BNC	209
2.7.3	Los conectores de fibra óptica	209
2.7.4	Los conectores híbridos	212
2.8	Velocidad	213
2.9	Otras interfaces de red	213
3.	Arranque desde la red	214
3.1	Principios	214
3.2	Protocolos	215
3.2.1	La conexión entre las direcciones física y lógica	215
3.2.2	El protocolo BOOTP	216
3.2.3	El protocolo DHCP	216
3.2.4	PXE	217
3.2.5	Wake-On-LAN: WOL	219
4.	Codificación de los datos	223
4.1	Tipos de datos y de señales	223
4.1.1	La señal analógica	223
4.1.2	La señal digital	224
4.1.3	La utilización	225
4.2	Codificación de los datos	225
4.2.1	La codificación de los datos digitales como señales analógicas	225
4.2.2	La codificación de los datos digitales en señales digitales	227
4.2.3	La codificación en línea	227
4.2.4	La codificación completa	230

6 **Redes informáticas**

Nociones fundamentales

4.3	Multiplexado de señales	230
4.3.1	El sistema de banda básica	230
4.3.2	El sistema de banda ancha	231
4.3.3	El multiplexado	231
5.	Conversión de las señales	233
5.1	Definiciones	233
5.2	Módem	234
5.3	CODEC	235
6.	Soportes de transmisión	236
6.1	Soportes limitados	236
6.1.1	El par trenzado	237
6.1.2	El cable coaxial	244
6.1.3	La fibra óptica	247
6.1.4	Los criterios de elección de los diferentes medios	251
6.1.5	El Bucle Local Óptico Mutualizado	253
6.1.6	Cables submarinos intercontinentales	256
6.2	Soportes no limitados	257
6.2.1	Los infrarrojos	258
6.2.2	El láser	258
6.2.3	Las ondas de radio terrestres	258
6.2.4	Las ondas de radio por satélite	260
6.2.5	Órbita terrestre baja	261
6.2.6	Las ondas de radio según las frecuencias	264

Capítulo 4

Software de comunicación

1.	Configuración de la tarjeta de red	269
1.1	Configuración del hardware	270
1.2	Configuración de software	270
1.3	Especificaciones NDIS y ODI	273

2.	Instalación y configuración del controlador de la tarjeta de red . . .	275
2.1	Principios.	275
2.2	Utilización de una herramienta proporcionada por el fabricante.	276
2.3	Utilización del sistema operativo	277
2.3.1	En Windows	278
2.3.2	En Linux Red Hat	280
2.3.3	En un Mac OS X.	285
2.3.4	En un smartphone Android	289
2.3.5	Tethering.	299
2.3.6	En un iPhone.	309
3.	Pila de protocolos	314
4.	Detección de un problema de red	316
4.1	Conexión física de red	316
4.1.1	El tipo de cable	316
4.1.2	El tipo de componentes	317
4.2	Configuración del software de red.	318

Capítulo 5

Arquitectura de red e interconexión

1.	Topologías.	321
1.1	Principios.	321
1.2	Topologías estándar	321
1.2.1	El bus	321
1.2.2	La estrella	322
1.2.3	El anillo	323
1.2.4	El árbol.	324
1.2.5	Las topologías derivadas.	324
1.2.6	El caso de las redes inalámbricas	326
2.	Elección de la topología de red adaptada.	327

8 **Redes informáticas**

Nociones fundamentales

3. Gestión de la comunicación	328
3.1 Dirección del flujo de información	328
3.1.1 El modo simplex	328
3.1.2 El modo half-duplex	329
3.1.3 El modo full-duplex	329
3.2 Tipos de transmisión	329
3.3 Métodos de acceso al soporte.	330
3.3.1 La contención	330
3.3.2 La pregunta (polling)	332
3.3.3 El paso de testigo	332
3.4 Tecnologías de conmutación	333
3.4.1 La conmutación de circuitos	333
3.4.2 La conmutación de mensajes	334
3.4.3 La conmutación de paquetes	335
4. Interconexión de redes	336
4.1 Principios.	336
4.2 Componentes de interconexión y modelo OSI	337
4.3 Descripción funcional de los componentes.	338
4.3.1 El repetidor	338
4.3.2 El puente	340
4.3.3 El conmutador	352
4.3.4 El router.	368
4.3.5 La puerta de enlace	390
4.4 Elección de los dispositivos de conexión apropiados	390
4.4.1 El repetidor	391
4.4.2 El puente	391
4.4.3 El conmutador	391
4.4.4 El router.	392
4.4.5 La puerta de enlace	392
4.5 Ejemplo de topología de red local segura	392

Capítulo 6

Capas bajas de las redes locales

1. Capas bajas e IEEE	395
1.1 Diferenciación de las capas	395
1.2 IEEE 802.1	396
1.3 IEEE 802.2	397
1.3.1 Principios de Logical Link Control (LLC)	397
1.3.2 Tipos de servicio	398
2. Ethernet e IEEE 802.3	398
2.1 Generalidades	398
2.2 Características de la capa física	399
2.2.1 Las especificidades de Ethernet	399
2.2.2 Las especificidades de Fast Ethernet	406
2.2.3 Gigabit Ethernet	408
2.2.4 10 Gigabit Ethernet	409
2.2.5 40/100 Gigabit Ethernet	410
2.2.6 Recapitulación	412
2.3 Encabezados de trama Ethernet	413
2.4 Las tarjetas híbridas Ethernet/SAN	414
3. Token Ring e IEEE 802.5	416
3.1 Configuración de la red	416
3.2 Autorreconfiguración del anillo	420
4. Wi-Fi e IEEE 802.11	421
4.1 Presentación	421
4.2 Normas de la capa física	422
4.2.1 802.11b	423
4.2.2 802.11a	424
4.2.3 802.11g	424
4.2.4 802.11n	424
4.2.5 802.11ac	425
4.2.6 802.11ad	428
4.2.7 802.11ah - Wi-Fi HaLow	429

4.2.8	802.11ax - High Efficiency WLAN (HEW)	430
4.2.9	802.11be - Extremely High Throughput (EHT)	431
4.2.10	Normas y logos Wi-Fi	432
4.3	Hardware	434
4.3.1	La tarjeta de red	434
4.3.2	El equipo de infraestructura	434
4.3.3	Los dispositivos Wi-Fi	436
4.4	Arquitectura	436
4.5	Seguridad	437
4.5.1	Introducción	437
4.5.2	WEP	440
4.5.3	WPA/WPA 2	441
4.5.4	WPA 3	443
4.6	Utilización	446
4.7	Encabezado de trama Wi-Fi	447
5.	Bluetooth e IEEE 802.15	448
5.1	Antecedentes	449
5.2	Estandarización	449
5.3	Red Bluetooth	453
5.4	Clases de equipos	454
6.	Otras tecnologías	455
6.1	Otros estándares de IEEE	455
6.1.1	802.16	456
6.1.2	802.17	456
6.1.3	802.18	457
6.1.4	802.19	457
6.1.5	802.21	457
6.1.6	802.22	457
6.1.7	802.24	458
6.2	Infrared Data Association (IrDA)	458
6.2.1	El protocolo IrDA DATA	459
6.2.2	El protocolo IrDA CONTROL	461

6.3	Bucle local eléctrico (BLE)	462
6.3.1	Principios	462
6.3.2	El funcionamiento	465
7.	El universo de los objetos conectados, IoT	467
7.1	Introducción	467
7.2	Evolución de los objetos conectados	469
7.3	Acceso a los objetos conectados	471
7.4	Problemas planteados por objetos conectados	472

Capítulo 7

Protocolos de redes MAN y WAN

1.	Interconexión de la red local	475
1.1	Utilización de la red telefónica	475
1.2	Red digital de servicios integrados (RDSI)	477
1.2.1	Principios	477
1.2.2	Correspondencia con el modelo OSI	478
1.2.3	Tipos de acceso disponibles	479
1.3	Línea dedicada (LD)	480
1.3.1	Los principios	480
1.3.2	Velocidades	480
1.4	Tecnologías xDSL	481
1.4.1	Principios	481
1.4.2	Los diferentes servicios	481
1.4.3	Las ofertas «Todo en uno»	483
1.5	Cable público	485
1.6	WiMax	486
1.6.1	El bucle local inalámbrico	486
1.6.2	La solución WiMax	486
1.7	Redes móviles	488
1.7.1	Inicios	488
1.7.2	El comienzo	490
1.7.3	La evolución hacia el transporte de datos	491

12 **Redes informáticas**

Nociones fundamentales

1.7.4	La tercera generación (3G) de telefonía móvil	493
1.7.5	La cuarta generación (4G)	494
1.7.6	La quinta generación (5G)	496
1.8	Fiber Distributed Data Interface (FDDI)	502
1.8.1	Principios.	503
1.8.2	Topología	503
1.8.3	Funcionamiento	504
1.9	Asynchronous Transfer Mode (ATM)	505
1.9.1	Principios.	505
1.9.2	El enlace de celdas.	506
1.9.3	Regulación del tráfico.	506
1.9.4	Tipos de servicios	507
1.9.5	Topología y velocidades	508
1.10	Synchronous Optical Network (SONET) y Synchronous Digital Hierarchy (SDH)	509
1.10.1	Antecedentes.	509
1.10.2	Las características de SDH	509
1.10.3	Velocidades	510
1.11	X.25	511
1.12	Frame Relay	512
1.13	MPLS	513
1.13.1	Origen	513
1.13.2	Principios.	515
1.13.3	El circuito virtual y el etiquetado	515
1.13.4	Enrutamiento	516
2.	Acceso remoto y redes privadas virtuales	516
2.1	Utilización y evolución	517
2.2	Protocolo de acceso remoto	517
2.3	Red privada virtual	518
2.3.1	Establecimiento de la conexión	518
2.3.2	Autenticación.	519
2.3.3	El cifrado	519

Capítulo 8

Protocolos de capas medias y altas

1. Principales familias de protocolos	521
1.1 IPX/SPX.....	521
1.1.1 Antecedentes.....	521
1.1.2 Protocolos	522
1.2 NetBIOS	523
1.2.1 Antecedentes.....	523
1.2.2 Principio	524
1.2.3 Los nombres NetBIOS	525
1.3 TCP/IP.....	529
1.3.1 Antecedentes.....	529
1.3.2 La suite de protocolos.....	530
1.3.3 Correspondencia con el modelo OSI.....	531
1.3.4 La implementación en las empresas	531
2. Protocolo IP versión 4.....	532
2.1 Principios.....	532
2.2 Direccionamiento	532
2.2.1 La dirección IPv4.....	532
2.2.2 La máscara.....	533
2.2.3 Clases de direcciones	534
2.2.4 Direcciones privadas.....	538
2.2.5 Las direcciones APIPA	538
2.3 El direccionamiento sin clase.....	539
2.3.1 Principios.....	539
2.3.2 La notación CIDR.....	540
2.3.3 El papel de la máscara de red	542
2.3.4 La descomposición en subredes	548
2.3.5 Factorización de las tablas de enrutamiento.....	556
3. Protocolo IP versión 6.....	558
3.1 Introducción	558
3.2 Principios.....	558

3.3	Estructura de una dirección IP	559
3.3.1	Categorías de direcciones	559
3.3.2	Ámbito de una dirección	561
3.3.3	Dirección unicast	561
3.3.4	Notación	562
3.3.5	Identificador EUI-64	564
3.3.6	Direcciones reservadas	567
3.3.7	Descomposición de rangos para la IETF	568
3.3.8	Segmentación de las categorías	572
3.3.9	Autoconfiguración de las direcciones IPv6	577
3.4	Túneles	580
3.4.1	Introducción	580
3.4.2	Tipos de túneles	581
3.5	Organismos de asignación de direcciones	587
3.6	Cabecera IPv6	589
4.	Otros protocolos de la capa Internet	590
4.1	Internet Control Message Protocol (ICMP)	590
4.2	Internet Group Management Protocol (IGMP)	593
4.3	Address Resolution Protocol (ARP) y Reverse Address Resolution Protocol (RARP)	593
4.4	Internet Protocol Security (IPsec)	594
4.5	Lista de los números de protocolos de la capa internet	595
5.	Voz sobre IP (VoIP)	596
5.1	Principios	596
5.2	Algunas definiciones importantes	597
5.3	Ventajas	598
5.4	Funcionamiento	600
5.4.1	El protocolo H323	600
5.4.2	Los elementos terminales	600
5.4.3	Las aplicaciones	601
6.	Protocolos de transporte TCP y UDP	602
6.1	Transmission Control Protocol (TCP)	602
6.2	User Datagram Protocol (UDP)	603

7.	Capa de aplicación TCP/IP	603
7.1	Servicios de mensajería	603
7.1.1	Simple Mail Transfer Protocol (SMTP)	603
7.1.2	Post Office Protocol 3 (POP3)	605
7.1.3	Internet Message Access Protocol (IMAP)	606
7.2	Servicios de transferencia de archivos	607
7.2.1	HyperText Transfer Protocol (HTTP)	607
7.2.2	File Transfer Protocol (FTP) y Trivial FTP (TFTP)	611
7.2.3	Network File System (NFS)	615
7.3	Servicios de administración y de gestión de red	618
7.3.1	Domain Name System (DNS)	618
7.3.2	Dynamic Host Configuration Protocol v.4 (DHCPv4) .	630
7.3.3	Telnet	644
7.3.4	Network Time Protocol (NTP)	645
7.3.5	Simple Network Management Protocol (SNMP).	648
7.4	Servicios de autenticación	657
7.4.1	Métodos de autenticación	657
7.4.2	NTLM	658
7.4.3	Kerberos	661
7.4.4	SAML 2.0	668
7.4.5	OpenID Connect	669

Capítulo 9

Principios de protección de una red

1.	Comprensión de la necesidad de la seguridad	671
1.1	Garantías exigidas	671
1.2	Peligros latentes	672
1.2.1	La circulación de los datos	672
1.2.2	Protocolos de Red y Transporte	673
1.2.3	Protocolos aplicativos estándares	673
1.2.4	Protocolos de capas bajas	674
1.2.5	Riesgos a nivel de software	674

16 **Redes informáticas**

Nociones fundamentales

2. Herramientas y tipos de ataques	675
2.1 Ingeniería social	675
2.2 Escuchas de red	683
2.3 Análisis de los puertos	684
2.4 Códigos maliciosos	686
2.5 Programas furtivos	687
2.6 Ransomware	688
3. Conceptos de protección en la red local	689
3.1 Servicios de seguridad	689
3.1.1 El control de acceso al sistema	689
3.1.2 La gestión de permisos	690
3.1.3 La integridad	690
3.1.4 La no denegación	691
3.2 Autenticación	691
3.2.1 La identificación	692
3.2.2 La autenticación por contraseña	696
3.2.3 La autenticación con soporte físico	697
3.2.4 La autenticación por biometría	698
3.3 Confidencialidad	699
3.3.1 El cifrado con claves simétricas	700
3.3.2 El cifrado de claves asimétricas	701
3.4 Protección de los datos de usuario	704
3.4.1 Protección de la inicialización del disco	706
3.4.2 Cifrado de los discos locales	710
3.4.3 Cifrado de discos USB	712
3.5 Herramientas de investigación relacionadas con la seguridad	714
3.5.1 Verificación de URL	714
3.5.2 Verificación de un archivo adjunto	718
3.5.3 Obtención de información adicional	720
4. Protección de la interconexión de redes	726
4.1 Router de filtrado	727
4.2 Traductor de direcciones	727
4.3 Cortafuegos	728

4.4 Proxy	729
4.5 Zona desmilitarizada	730

Capítulo 10

Reparación de una red

1. Método de enfoque.	733
2. Ejemplos de diagnóstico en capas bajas.	734
2.1 Dispositivos.	735
2.1.1 El téster de cables	735
2.1.2 El reflectómetro	736
2.1.3 El multímetro digital	737
2.2 Análisis de tramas.	737
2.3 Otros problemas con Ethernet.	739
2.3.1 La unicidad de la dirección MAC.	739
2.3.2 La configuración física de la tarjeta de red	739
2.3.3 Parámetros de comunicación	739
2.4 IPX y Ethernet	740
2.5 Otros problemas ligados a la fibra	740
3. Utilización de herramientas TCP/IP adaptadas	741
3.1 Principios.	741
3.2 Ejemplo de utilización de las herramientas.	741
3.2.1 arp	741
3.2.2 Neighbor Discovery Table	744
3.2.3 ping	744
3.2.4 tracert/traceroute	746
3.2.5 ipconfig/ip address	748
3.2.6 netstat	750
3.2.7 Identificación de una dirección IP	752
3.2.8 Geolocalización de una dirección IP	754
3.2.9 nbtstat	754
3.2.10 nslookup	756

4. Herramientas de análisis de capas altas	759
4.1 La herramienta sysinternals	759
4.2 Análisis de peticiones de aplicaciones	766
4.3 Análisis de peticiones web	767

Capítulo 11

Anexos

1. Conversión de decimal (base 10) a binario (base 2)	771
1.1 Vocabulario utilizado	771
1.2 Conversión a partir de base 10	772
2. Conversión de binario (base 2) a decimal (base 10)	774
3. Conversión de hexadecimal (base 16) a decimal (base 10)	775
4. Conversión de hexadecimal (base 16) a binario (base 2)	777
5. Glosario	778
Índice	801

Prólogo

1. Introducción	15
2. Público objetivo y enfoque	18
3. Contenido	19
4. Organización	22
5. Agradecimientos	23

Capítulo 1

Evolución de las profesiones en torno a las redes

1. Evolución de la informática y las redes	25
1.1 Los primeros ordenadores	25
1.2 Redes de conmutación de circuitos	26
1.3 Redes de conmutación de paquetes	27
1.4 La aparición de las redes LAN y del protocolo TCP/IP	29
1.5 La evolución hacia las redes ATM	30
1.6 El surgimiento de la virtualización de servidores	31
1.7 Desarrollo de Internet y de la WAN	32
1.8 El cloud computing	33
2. La profesión de administrador de redes	34
2.1 Tareas y funciones del administrador de redes	34
2.2 Ampliación y evolución de la profesión	35
2.3 Nuevos ámbitos que hay que dominar	36
2.3.1 Movimiento DevOps	36
2.3.2 El contexto de la virtualización	37
2.3.3 Certificaciones y herramientas de autoformación	38
2.3.4 ¿Una profesión puramente técnica?	43

2 Las redes informáticas

Guía práctica para la administración, la seguridad y la supervisión

Capítulo 2

Diseño de una red local

1. Ethernet y las conexiones físicas	45
1.1 Historia	45
1.2 Principales estándares Ethernet y evoluciones	46
1.3 Corriente de alta intensidad por Ethernet: el PoE	51
1.3.1 Principios de la norma	51
1.3.2 Rendimiento y uso en la práctica	53
1.4 Conexiones de fibra óptica en una red local	55
2. Segmentación de una red	59
2.1 ¿Por qué segmentar una red?	59
2.1.1 Segmentación geográfica	59
2.1.2 Segmentación funcional y de seguridad	61
2.1.3 Segmentación por motivos de rendimiento	64
2.2 Segmentación de la red mediante la implementación de VLAN	69
2.2.1 Principio de las VLAN	69
2.2.2 Tipos de VLAN	70
2.2.3 Norma 802.1Q	71
2.2.4 Configuración de enlaces entre conmutadores y etiquetado de VLAN	73
2.2.5 Gestión del etiquetado por parte de los equipos de red	75
2.3 Diseño avanzado de redes a partir de VLAN	83
2.3.1 El estándar QinQ o 802.3ad: VLAN dentro de una VLAN	83
2.3.2 Ampliación de las VLAN con VXLAN	87
2.3.3 VLAN privada	90

Capítulo 3

Arquitecturas de operador y WAN

1. Marco general de los operadores	95
1.1 Definición	95
1.2 Los diferentes tipos de operadores	95
1.2.1 Los FAI: proveedores de acceso a Internet	95
1.2.2 Operadores de infraestructuras	96
1.2.3 Operadores de telefonía	96
2. Organización técnica de los proveedores de servicios de Internet. . .	97
2.1 Registros de Internet regionales (RIR)	97
2.2 Bloques de IP y número de AS (ASN)	98
2.3 Relaciones de enrutamiento de tráfico entre operadores: peering y tránsito	98
2.3.1 Relaciones de tránsito IP	98
2.3.2 Relaciones de peering	100
2.4 Jerarquía entre operadores: los tres niveles Tiers	105
3. Gestión del bucle local y conexión física al proveedor de servicios de Internet	107
3.1 Visión general del enrutamiento del tráfico del usuario final hacia Internet	107
3.2 Bucle local óptico	109
3.3 Red de recogida y backbone	113
3.3.1 Enlace PMZ - NCO	113
3.3.2 La conexión NCO - punto de presencia del operador (PoP)	116
3.4 La elección de una oferta de acceso WAN para una empresa .	117
3.4.1 Criterios de elección del acceso WAN	117
3.4.2 Acceso de fibra para empresas: FTTO	120
3.4.3 Acceso de fibra reservado a los profesionales	122
3.4.4 Conclusión: MultiWAN	124

4 Las redes informáticas

Guía práctica para la administración, la seguridad y la supervisión

Capítulo 4

Gestión de activos y alta disponibilidad

1. Gestión de conmutadores y enrutadores	127
1.1 Herramientas e interfaces de administración	127
1.1.1 Interfaces CLI	127
1.1.2 Interfaces web.	132
1.1.3 Gestión a través de una aplicación pesada	137
1.1.4 Gestión de los equipos mediante API REST para la automatización.	139
1.1.5 Herramientas de desarrollo para la gestión de configuraciones: consulta de un API	143
1.1.6 Herramientas de desarrollo para la gestión de configuraciones: gestión de versiones con Git	144
1.2 Gestión de las configuraciones de los elementos activos	146
1.2.1 Memorias de un equipo y sincronización	146
1.2.2 Sincronización de la configuración	147
1.2.3 Copia de seguridad y restauración de la configuración ..	150
1.3 Gestión de los sistemas operativos de los elementos activos. .	152
1.3.1 Inventario	152
1.3.2 Homogeneidad del hardware	155
1.3.3 Actualización de los equipos de red.	158
2. Alta disponibilidad	161
2.1 Introducción	161
2.2 Redundancia de enlaces físicos y agregación	162
2.2.1 Principio del spanning tree.	162
2.2.2 Protocolos de agregación de interfaces	164
2.3 Stacking de conmutadores	169
2.3.1 Stacking tradicional	169
2.3.2 Capacidad de conmutación de un conmutador	171
2.3.3 Particularidades de la implementación del stack	173
2.3.4 Stacking virtual y MLAG	175

2.4	Redundancia y clustering de nivel 3	185
2.4.1	Principio de clustering de los routers.	185
2.4.2	El protocolo VRRP y su funcionamiento	186
2.4.3	Soluciones propietarias.	191
2.4.4	Redundancia de enlaces de operadores	192

Capítulo 5

Principios de seguridad en una red local

1.	Seguridad a nivel de los conmutadores	201
1.1	Las debilidades del protocolo ARP.	201
1.2	Mecanismo de seguridad de puerto o port-security	206
1.3	Seguridad en torno a los mecanismos de direccionamiento IP.	207
1.3.1	Direccionamiento estático o dinámico mediante DHCP	207
1.3.2	DHCP Snooping	209
1.4	Políticas de acceso a la red	212
1.4.1	Principio del NAC: Control de acceso a la red	212
1.4.2	Autenticación 802.1x en el puerto del conmutador	213
1.5	Salto de VLAN: hopping	216
2.	Los cortafuegos	219
2.1	Características de un firewall.	219
2.1.1	Función y ubicación en una red	219
2.1.2	Análisis hasta la capa de transporte	222
2.1.3	Análisis hasta la capa de aplicación.	225
2.2	Las soluciones del mercado y cómo elegir.	228
2.2.1	Soluciones comerciales NGFW (Next Generation Firewall).	228
2.2.2	Soluciones libres	230
2.2.3	Inteligencia artificial y cortafuegos	232
2.2.4	Criterios de selección y métricas	234
2.2.5	¿Cortafuegos físico o virtual?	237

6 Las redes informáticas

Guía práctica para la administración, la seguridad y la supervisión

2.3	Probar su firewall	239
2.3.1	Utilizar escáneres de vulnerabilidades para probar el análisis de aplicaciones	239
2.3.2	Comprobar el estado de un puerto o simular un puerto abierto en un equipo	240
2.3.3	Determinar los puertos abiertos a la salida de un firewall	243
3.	Los ataques de denegación de servicio	245
3.1	Principio del ataque	245
3.2	Ataques distribuidos de denegación de servicio	247
3.3	Medidas de protección	249

Capítulo 6

Gestión del acceso remoto a los recursos

1.	Conexión remota segura: VPN móvil	251
1.1	Principio	251
1.2	Soluciones móviles libres	255
1.3	Soluciones comerciales gratuitas para un uso limitado	259
2.	Conexión de sitio a sitio: VPN IPSec	261
2.1	Introducción	261
2.2	Las fases y la negociación de un túnel VPN IPSec	262
2.3	Los problemas del NAT	265
2.4	Problemas de direccionamiento IP	266
2.5	Guía para una configuración IPSec sitio a sitio rápida y sencilla	268
3.	Otros tipos de VPN y ZTNA	269
3.1	VPN de operadores: MPLS, VXLAN y EVPN	269
3.2	El enfoque Zero Trust Network Access (ZTNA): la "VPN inversa por servicio"	271

Capítulo 7

Ciberataques en la red

1. Contexto y fases de un ataque.	275
2. Recopilación activa de información en la red	277
2.1 Introducción	277
2.2 Recopilación de máquinas de una red	277
2.3 Enumeración de servicios: escaneo de puertos	280
2.4 Enumeración de servicios y versiones	282
3. Recopilación pasiva de información	286
3.1 Información relativa a un nombre de dominio.	286
3.2 Open Source Intelligence (OSINT)	289
3.2.1 Principios.	289
3.2.2 Los Google Dorks	290
3.2.3 Reconocimiento de servicios mediante herramientas en línea	291
3.3 Ingeniería social (social engineering)	292
4. Fase de explotación.	295
4.1 Vulnerabilidades y exploits	295
4.1.1 Tipos de vulnerabilidades.	295
4.1.2 Concepto de exploit	298
4.2 La carga útil o payload	298
4.3 Acciones posteriores a la intrusión	300
4.3.1 Persistencia, elevación de privilegios y lateralización.	300
4.3.2 Anonimización y SIEM	301
5. Caso práctico: intrusión en una red empresarial mediante el aprovechamiento de una vulnerabilidad en una pasarela VPN SSL	304
5.1 Introducción	304
5.2 Contexto	304
5.3 Reconocimiento del objetivo	305
5.4 Obtención de un exploit e intrusión	306
5.5 Uso directo del framework Metasploit	309
5.6 Epílogo.	311

8 Las redes informáticas

Guía práctica para la administración, la seguridad y la supervisión

Capítulo 8

Enfoque global de la supervisión con SNMP

1. Definición de la supervisión.	313
1.1 Contexto de la DSI.	313
1.2 ¿Cómo detectar un problema técnico?	314
1.3 ¿Cómo abordar un problema técnico?	315
1.4 Mejorar la disponibilidad efectiva	316
2. Enfoque ISO	317
2.1 Pliego de condiciones inicial.	317
2.2 Gestión de incidencias	318
2.3 Gestión de configuraciones	319
2.4 Gestión del rendimiento.	323
2.4.1 Medición del rendimiento	323
2.4.2 Las políticas de calidad de servicio.	324
2.5 Gestión de la seguridad	326
2.6 Gestión de la contabilidad	326
3. Lanzar un proyecto de supervisión	328
3.1 Errores que hay que evitar	328
3.2 ¿Qué supervisar a nivel de red?	330
3.2.1 Disponibilidad de los activos	330
3.2.2 Variables que se deben controlar según el tipo de equipo de red	334
4. Supervisión de red mediante el protocolo SNMP.	336
4.1 Principios del protocolo SNMP	336
4.1.1 Características del protocolo SNMP	336
4.1.2 Modelización de un elemento activo: la MIB.	337
4.1.3 Primera aproximación a la estructura de la MIB mediante un caso práctico	339
4.2 Las MIB públicas y privadas.	343
4.2.1 Principio general de la MIB I y la MIB II.	343
4.2.2 Organización de la MIB I.	346
4.2.3 Organización de la MIB II	352

4.2.4 MIB privadas e integración en el gestor	354
4.3 Configurar SNMP	355
4.3.1 Las comunidades y los permisos	355
4.3.2 Tipos de mensajes	359
4.3.3 Consultas en la MIB según la comunidad y los permisos sobre el OID	363
4.3.4 Pasos para la configuración mínima de SNMP	365

Capítulo 9

Otros protocolos de supervisión de redes

1. Gestión de registros con Syslog	367
1.1 Objetivos del registro de eventos	367
1.1.1 Funciones iniciales de los registros	367
1.1.2 Cuestiones jurídicas	368
1.1.3 Necesidad de una gestión centralizada	370
1.2 Principios del protocolo Syslog	371
1.2.1 Funcionamiento general	371
1.2.2 Clasificación de los registros generados	373
1.2.3 Formato de la trama	376
1.3 Configuración de Syslog	378
1.4 Soluciones de recopilación y análisis de registros	382
1.4.1 Criterios para elegir el colector	382
1.4.2 Recopiladores basados en código abierto o gratuitos	384
1.4.3 Otros recopiladores	389
2. Los protocolos de supervisión del flujo de red	395
2.1 Introducción a NetFlow	395
2.1.1 Orígenes del protocolo	395
2.1.2 Caso de uso	396
2.1.3 Características y contenido de un flujo NetFlow	397
2.1.4 Funcionamiento y arquitecturas	400
2.2 Configuración en un dispositivo de red	401

10 **Las redes informáticas**

Guía práctica para la administración, la seguridad y la supervisión

2.3	Los colectores NetFlow y las aplicaciones de análisis.	405
2.3.1	El mercado.	405
2.3.2	Recopiladores basados en código abierto o gratuitos . . .	405
2.3.3	Soluciones de pago y propietarias	409
2.4	El protocolo sFlow	413
2.4.1	Principios de sFlow.	413
2.4.2	NetFlow frente a sFlow	414
2.5	Las sondas RMON	416
2.5.1	Aspectos principales de RMON.	416
2.5.2	Funcionalidades aportadas por RMON.	418
2.5.3	Exploración de las MIB RMON 1 y 2	419
2.5.4	Configuración de RMON.	424

Capítulo 10

Metrología y medición del rendimiento

1.	Metrología y métricas de red	427
1.1	Definición de metrología	427
1.2	Las métricas de red	429
1.3	Metodología de pruebas de rendimiento.	431
2.	Medición de la velocidad y optimización	433
2.1	Velocidad bruta y velocidad de aplicación	433
2.2	Herramientas Iperf/Jperf	435
2.3	Ajustar los parámetros de red para aumentar el rendimiento .	439
2.4	Velocidades superiores al gigabit y tramas jumbo	442
2.5	Importancia del rendimiento en una red SAN	448
2.6	Comunicación directa entre memoria y la tarjeta de red: el RDMA	452

2.7	Dimensionamiento del ancho de banda de aplicaciones	455
2.7.1	Características de las redes IP en materia de ancho de banda	455
2.7.2	Medición del ancho de banda en el servidor o en el puesto de usuario	456
2.7.3	Captura de tramas y mediciones a través de SPAN	458
3.	Medición de los tiempos de respuesta	460
3.1	Medición de la latencia y la fluctuación	460
3.1.1	Ping	460
3.1.2	Traceroute	462
3.1.3	Calcular el jitter	463
3.2	Pérdida de paquetes y disponibilidad	464
3.2.1	Evaluación de la pérdida de paquetes	464
3.2.2	Índice de disponibilidad de un servicio	465
3.2.3	Disponibilidad de un servicio en "número de nueves"	466
3.2.4	Análisis de los servicios accesibles	467
3.3	Tiempo de respuesta de la aplicación	469
3.3.1	Concepto de experiencia de usuario (UX)	469
3.3.2	Scripts de supervisión	469
3.3.3	Monitorización de usuarios en tiempo real (RUM)	471
3.4	Tiempo de respuesta de una aplicación web	473
3.4.1	Introducción	473
3.4.2	Responsabilidades técnicas del rendimiento de una aplicación web alojada	473
3.4.3	Tiempo de respuesta y escalabilidad	478
3.4.4	Métricas específicas para caracterizar una aplicación web	478
3.5	Rendimiento de una red de telefonía IP	482
3.5.1	Gestión de la telefonía por parte del equipo de red	482
3.5.2	Requisitos de las redes en tiempo real en comparación con las redes de datos	483
3.5.3	Ancho de banda para telefonía IP y códecs	485
3.5.4	Adaptación de la red para transmitir flujos de VoIP	487

12 Las redes informáticas

Guía práctica para la administración, la seguridad y la supervisión

4. Herramientas de supervisión especializadas en metrología	488
4.1 Almacenar las mediciones	488
4.1.1 Problemas relacionados con el almacenamiento de datos de metrología	488
4.1.2 Herramientas habituales para el almacenamiento de datos de metrología	489
4.2 Visualización de los datos medidos	490
4.2.1 Representación de los datos	490
4.2.2 Herramientas habituales y diseñadas para la visualización de datos metrológicos	491
4.3 Recopilar las mediciones	493
4.3.1 Métodos de recopilación	493
4.3.2 Herramientas libres de recopilación multiprotocolo	494
4.4 Soluciones completas de código abierto	495
4.4.1 Funciones que se deben cubrir	495
4.4.2 InfluxDB/Telegraf/Graphana	495
4.4.3 ELK con agentes Beat	496
4.4.4 Cacti	497
4.4.5 LibreNMS	498
4.4.6 Graphite	499

Capítulo 11

Virtualización de la red y SDN

1. Virtualización de la red	501
1.1 Virtualización y cloud computing	501
1.1.1 Historia y principio de la virtualización	501
1.1.2 Servicios de computación en la nube ofrecidos en los datacenters	503
1.2 Cloud computing y redes de datacenters	506
1.2.1 Arquitectura de red tradicional	506
1.2.2 Modificaciones de la arquitectura de red de los datacenters	507
1.2.3 Incorporación de una capa virtual dentro de la red	512

1.3	Virtualización de funciones de red: NFV	513
1.3.1	Tecnologías de virtualización de red	513
1.3.2	Problemas de los dispositivos de hardware	514
1.3.3	Ventajas de la NFV	514
1.3.4	Soluciones propuestas por editores y fabricantes de equipos	516
1.3.5	Rendimiento de los dispositivos de red virtuales	517
1.4	Gestión de activos de red de un centro de datos	518
2.	Enfoque de la SDN (Software Defined Network)	519
2.1	Arquitectura de conmutación y enrutamiento	519
2.1.1	La conmutación de paquetes	519
2.1.2	Planos de datos, control y gestión	519
2.2	Características de la SDN	523
2.2.1	Definición de SDN	523
2.2.2	Tecnologías pioneras y analogías	525
2.2.3	El estándar OpenFlow	527
2.2.4	El controlador SDN	530
2.2.5	Implementaciones de SDN	531
2.3	Soluciones del mercado	532
2.3.1	Soluciones libres	532
2.3.2	Soluciones propietarias	533
2.4	La SD-WAN (Software-Defined WAN)	536
2.4.1	Las nuevas expectativas de la WAN	536
2.4.2	Principios de la SD-WAN	537
2.4.3	Los actores del mercado y la evolución hacia el SASE	540
	Glosario	543
	Índice	559