2024

Bloque IV. Sistemas y Comunicaciones

TÉCNICO AUXILIAR INFORMÁTICO

Índice

Bloque 4 - Tema 1: ADMINISTRACIÓN DEL SISTEMA OPERATIVO

ADMINISTRACIÓN LINUX					
Distribución	Basado en	Gestor de paquetes	Distribución	Basado en	Gestor de paquetes
Debian		APT	Red Hat (RHEL)		RPM
Ubuntu	Debian	APT	Fedora	Red Hat Linux	RPM, YUM
Linux Mint	Ubuntu	APT	CentOS	Red Hat (RHEL)	YUM
Elementary OS	Ubuntu	APT	openSUSE	SUSE Linux	YaST
Knoppix	Debian	APT	Arch Linux		Pacman
Trisquel	Debian/Ubuntu	APT	Mandriva		RPM

La estructura de directorios del sistema UNIX/Linux es:			
/	Directorio raíz	/mnt	Montaje de dispositivos externos
/bin	Comandos de usuario (ejecutables)	/media	Montaje para dispositivos de medios
/boot	Archivos de arranque	/opt	Paquetes de aplicaciones estáticas
/dev	Ficheros de dispositivos	/proc	Archivos de control de procesos
/etc	Ficheros de configuración (arranque)	/root	Directorio del superusuario root
home	Directorios de inicio de los usuarios	/sbin	Archivos ejecutables del sistema
/lib	Librerías del sistema	/tmp	Ficheros temporales
/usr	Ejecutables y documentación	/var	Archivos de log

Distribuciones Debian					
1.1	Buzz	5.0	Lenny	9.0	Stretch
2.0	Hamm	6.0	Squeeze	10.0	Buster
3.0	Woody	7.0	Wheezy	11.0	Bullseye (2021)
4.0	Etch	8.0	Jessie	12.0	Bookworm (2023)

Última actualización es la versión 12.6, publicada el 29 de junio de 2024

Versiones en mantenimiento:	**stable**	**testing**	**unstable (desarrollo)**

ARRANQUE Y PROCESO INIT	
Existen distintos gestores de arranque, LILO (LInux LOader) y GRUB (GRand Unified Bootloader)	
GRUB (de GNU)	Para arrancar el kernel lee su configuración del archivo */boot/grub/menu.lst*
GRUB 2 (versión actual)	Utiliza */boot/grub/grub.cfg* que se genera automáticamente mediante el comando *update-grub*
/etc/inittab	Indica al proceso de arranque, entre otros, a qué runlevel se entrará.
init	Sistema de inicialización tradicional que inicia y gestiona procesos y servicios durante el arranque del sistema, el cual tiene un PID(1) y PPID(0).
SysVinit	Es el primer proceso en ejecución tras la carga del kernel, se ejecuta como demonio de init y tiene **PID 1**.
SystemD	sistema de inicialización moderno y más usado. Se ejecuta como un daemon de init con PID 1.

NIVELES DE EJECUCIÓN DEL SISTEMA			
Nivel 0		para parar el sistema	/etc/rc0.d/
Nivel 1	**monousuario**	sólo root (tareas de mantenimiento)	/etc/rc1.d/
Nivel 2	**nivel multiusuario**	sin soporte de red	/etc/rc2.d/
Nivel 3		con soporte de red sin interfaz gráfica	/etc/rc3.d/
Nivel 4		Para que el usuario lo personalice	/etc/rc4.d/
Nivel 5		con soporte de red con interfaz gráfica	/etc/rc5.d/
Nivel 6		para reiniciar el sistema	/etc/rc6.d/

init	para cambiar de nivel de ejecución *init 3 #cambio al nivel 3*	***runlevel***	ver en qué nivel estamos
		who -r	ver en qué nivel estamos
halt	para el sistema	shutdown -h now	apaga
reboot	reinicia	poweroff	apaga

INFORMACIÓN DEL SISTEMA			
arch	muestra la arquitectura de la máquina. Ejemplo x86_64	lsb_release -a	toda la información del SE
uname -m		cat /proc/version	versión del kernel
uptime	la hora actual	who -b	fecha y hora del último inicio
free	información de RAM y SWAP	vmstat	estadísticas de memoria virt.

GESTORES DE PAQUETES LINUX					
APT (Advanced Packaging Tool) gestor de paquetes para **Debian**					
/etc/apt/sources.list			configuración del sistema de paquetes		
apt-cache pkgnames			para enumerar todos los paquetes disponibles		
apt-cache show <paquete>			consultar el contenido del campo Priority		
Required	*Important*	*Standard*	*Optional*	*Extra*	
apt-cache depends <paquete>			consultar las dependencias de un paquete		
depends	*recommends*	*suggests*	*conflicts*	*replaces*	*provides*
sudo apt-get update			actualizar los paquetes del sistema		
sudo apt-get upgrade			actualizar paquetes de software		
sudo apt-get install <paquete>			instalo o actualizo paquetes específicos		
sudo apt-get remove *<paquete>*			elimino paquetes sin configuración		
sudo apt-get purge *<paquete>*			elimino los paquetes por completo		

DPKG (acrónimo de Debian package manager) es el backend de APT (.deb)	
dpkg -l	listar todos los paquetes de la base de datos y su estado
dpkg -L *<paquete>*	listar los ficheros contenidos en el paquete
dpkg -r	elimino paquetes sin configuración
dpkg -P	elimino los paquetes por completo
dpkg -p	consultar el contenido del campo Priority
dpkg -s	estado de instalación del paquete

Interfaces gráfica sobre APT	
Dselect	corre sobre APT. Para entrar en ella, basta con teclear el comando dselect
aptitude	*apt-get install aptitude* para instalarla antes de usarla (no viene instalada)
Synaptic	también puede ser usado en sistemas basados en paquetes RPM

RPM (acrónimo de RPM Package Manager) gestor de paquetes para **Red Hat**	
rpm -qa	lista todos los paquetes instalados en el sistema
rpm -qi *<paquete>*	información del paquete
rpm -ivh *<paquete>*.rpm	Instala el paquete rpm
rpm -F *<paquete>*.rpm	actualiza el paquete si está instalado
rpm -e *<paquete>*.rpm	elimina el paquete rpm
rpm -checksig *<paquete>*.rpm	verifica la integridad de un paquete rpm
rpm -qa gpg-pubkey	verifica la integridad de todos los paquetes rpm

YUM (Yellow dog Updater, Modified) gestor de paquetes basado en RPM para **Fedora y CentOS (Solo root)**	
yum install *<paquete>*	instala el paquete. Con la opción -y install (sin pedir confirmación)
yum -y update *<paquete>*	actualiza el paquete a la última versión disponible
yum check-update	lista de paquetes que necesitan ser actualizados
yum upgrade	actualiza todos los paquetes instalados
yum list	lista de paquetes disponibles para instalación
yum search *<paquete>*	busca en el repositorio de paquetes instalados o para instalar
yum remove *<paquete>*	elimina el paquete

Pacman gestor de paquetes para **Arch Linux** (.tar)	
pacman -S *<paquete>*	instala el paquete
pacman -Syu	sincroniza y actualiza los paquetes del sistema
pacman -Si *<paquete>*	información detallada de un paquete
pacman -R *<paquete>*	elimina el paquete, pero no sus dependencias
pacman -Rs *<paquete>*	elimina el paquete y sus dependencias
pacman -Rsc *<paquete>*	elimina el paquete, sus dependencias y todas sus dependencias

ADMINISTRACIÓN WINDOWS		
Windows 11 Home	Windows 11 Empresas	Windows 11 IoT Enterprise
Windows 11 Pro	Windows 11 SE (Educación)	Windows 11 en modo S (seguridad)
Windows Server 2012	IPAM (IP Address Management)	Hyper-V
	ReFS (Resilient File System, sistema de archivos resiliente)	
Windows Server 2016	Contenedores	Nanoserver (nubes privadas)
Seguridad (Device Guard)	PowerShell FTP	Herramientas Sysinternals (Disk2vhd)
Windows Server 2019	Proyecto Honolulu (Azure)	Mejoras en los contenedores
Subsistema Windows para Linux	Windows Defender ATP	Storage Migration Service

Windows Server 2022	se basa en Windows Server 2019
Ediciones: Standar, Datacenter y Datacenter:Azure Edition.	

Herramientas (administrativas) de Windows en W11			
C:\Windows\System32\ o sus subcarpetas.			
Adm. de dispositivos:	devmgmt.msc	Adm. de discos:	diskmgmt.msc
Adm. de equipos:	compmgmt.msc	Adm. de impresión:	printmanagement.msc
Desfragmentación:	defrag.exe	Directiva de seguridad local:	secpol.msc
Firewall de Windows:	wf.msc	Información del sistema:	msinfo32.exe
Liberador de espacio:	cleanmgr.exe	Monitor de rendimiento:	perfmon.msc
Monitor de recursos:	resmon.exe	Programador de tareas:	taskschd.msc
Servicios:	services.msc	Servicios de componentes:	comexp.msc
Visor de eventos:	eventvwr.msc	Editor del Registro:	regedt32.exe
Management Console:	mmc.exe	Configuración del sistema:	msconfig.exe

CoMmanD (**cmd**) es el intérprete de comandos	
Tuberías:	comando1 | comando2
Redirecciones:	comando > archivo (salida a archivo)
	comando < archivo (entrada desde archivo)

Herramientas administrativas en Windows Server	
Windows Admin Center es un conjunto de herramientas de administración sin dependencia de Azure.	
Actualizaciones de características:	nuevas funciones una vez al año
Actualizaciones de calidad:	periódicamente correcciones de seguridad
Windows Update (independiente)	Windows Update para empresas
Windows Server Update Services (WSUS)	Microsoft Endpoint Configuration Manager
Windows Insider:	actualizaciones de características de manera anticipada
Windows Intune:	servicio basado en nube para la administración de dispositivos móviles (MDM)

POWERSHELL (versión actual 7)	
Es un marco de administración de configuración y automatización de tareas multiplataforma. Los comandos de PowerShell se conocen como cmdlets (Command-Let). La extensión es .ps1.	
$_	es el objeto que recibe un cmdlets como resultado de la ejecución del anterior.
Canalizaciones	Get-ChildItem **|** Out-Host -Paging
Ayuda	para ello, usamos el cmdlet **Get-Help**
Alias	admite alias para referirse a comandos con nombres alternativos ejemplo: **cls** o **clear**

NOVEDADES POWERSHELL 7	
Compress-Archive:	crea un archivo comprimido partir de archivos y directorios especificados.

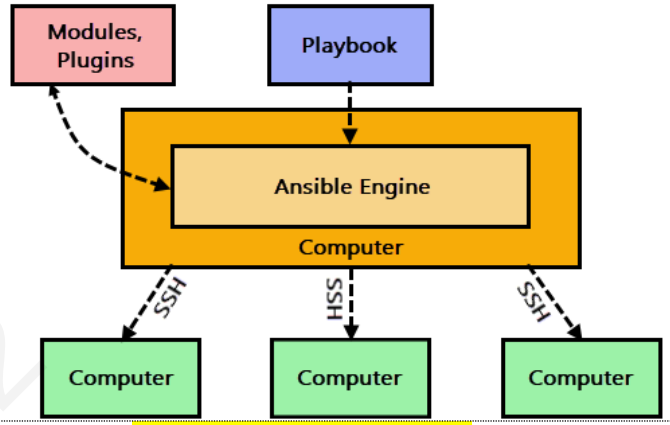
Expand-Archive:	extrae archivos de un archivo comprimido especificado.
Get-ClipBoard:	obtiene el contenido del portapapeles.
Set-ClipBoard:	establece el contenido del portapapeles.

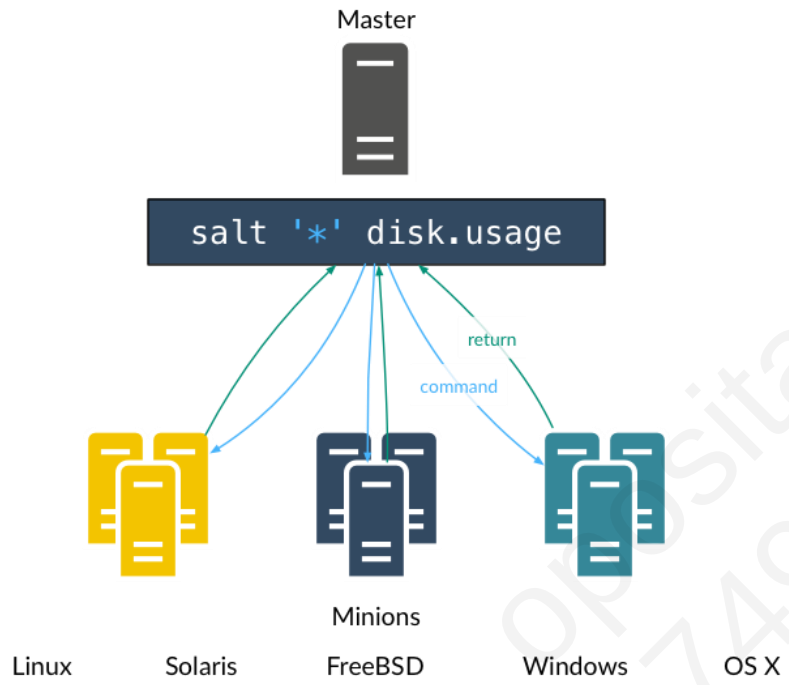
ADMINISTRACIÓN MacOS					
10.0	Cheetah	11.0	Big Sur	12.0	Monterey
13.0	Ventura	**14**.6.1	Sonoma	Consultar versiones	

Herramientas administrativas	
Información del sistema:	dividida en tres grupos: hardware, red y software.
Preferencias del sistema:	destaca FileVault que encripta automáticamente el contenido de un disco
Acceso a Llaveros:	permite ver claves, certificados y contraseñas.
Utilidad de discos:	información y manejo de discos.
Monitor de actividad:	misma funcionalidad el Administrador de tareas de Windows.
Terminal:	shell al estilo Linux. Los comandos básicos son los mismo que Linux.

Tipos de archivos de instalación de aplicaciones:		
.dmg: imagen de disco	**.pkg**: archivo de paquete	**.zip**: archivo comprimido

Gestores de paquetes:	
Fink:	de código abierto para macOS, que usa herramientas dpkg y aptget.
Homebrew (brew):	de código abierto para macOS y para Linux.

INFRAESTRUCTURA COMO CÓDIGO (IaC)	
Es la gestión de la infraestructura (redes, máquinas virtuales, balanceadores, etc) mediante un modelo descriptivo y usando herramientas de control de versiones. Es clave en la práctica DevOps y se usa en conjunto con despliegue. Los archivos de configuración normalmente tienen formato JSON o YAML.	
Herramientas más destacadas	
Chef	Creada para CPDs de Amazon y Microsoft. Está compuesto por un servidor de gestión **"Chef Server" y estaciones de trabajo "Workstation"** que interactúan con Chef server.
Ansible	Aplicación open source que gestiona la configuración, provisión y despliegue de aplicaciones en servidores on-premise o en la nube. El controlador u orquestador se encarga de comunicar a otros hosts o nodos. Cuenta con un inventario, donde se instancian todas las máquinas y a través de un **playbook**, se escribe todo el workflow. 
Puppet	Utiliza arquitectura cliente-servidor (Master-Agent).
Vagrant	Para administrar entornos de máquinas virtuales a partir de un fichero de configuración (Vagrantfile). No ejecutaa máquinas virtuales, solo especifica las características. Pueden ser construidas desde cero o desde imagen base (box). Existen máquinas ya creadas por la "comunidad" en Vagrant Cloud. Soporte nativo para VirtualBox, Hyper-V y Docker o alternativos como VMware o AWS.
Terraform	Software desarrollado por HashiCorp que provee flujos de trabajo para gestionar servicios en la nube. Utiliza un lenguaje de configuración declarativo denominado HashiCorp Configuration Language (HCL). El fichero de configuración Terraform (extensión ".tf" o ".tf.json"), en el que se conecta Mysql y se crea una base de datos denominada terraformbbdd.

HERRAMIENTAS DE GESTIÓN DE LA CONFIGURACIÓN AUTOMÁTICA	
Destinado al control y la vigilancia automatizados de los sistemas de servidores.	
SaltStack	Software de código abierto y multiplataforma de Apache permite instalar y configurar el software desde un ordenador central. Utiliza la biblioteca de intercambio de mensajes Messenger ZeroMQ los ficheros de configuración son formato YAML. Salt master (servidor), Salt minion (clientes), Salt syndic (Salt master intermedio). 

Bloque 4 - Tema 2: ADMON BD, ALMACENAMIENTO Y VIRTUALIZACION

ADMINISTRACIÓN DE BASES DE DATOS	
Incluye el diseño físico, implementación, configuración de seguridad e integridad y symonitorización	
Esquema sentencias básicas SQL según ISO/IEC 9075:2016	
DDL (definición)	CREATE, ALTER, DROP, TRUNCATE
DML (modificación)	SELECT, INSERT, UPDATE, DELETE
DCL (control)	COMMIT, ROLLBACK, SAVEPOINT, GRANT, REVOKE

TIPOS DE BASES DE DATOS			
RELACIONALES		**ORIENTADAS A OBJETOS**	
- Oracle. - MySQL. - MariaDB. - SQLite. - PostgreSQL.	- SQL Server. - Apache Derby. - MaxDB. - HSQLDB. - Aurora.	- Db4o. - Zope ObjectDB (ZODB).	- Gemstone. - ObjectDB.
NoSQL - Clave -> valor:		**NoSQL - Documentales:**	
- Cassandra. - Redis. - DynamoDB. - Memcached.	- Oracle NoSQL. - Aerospike. - Riak.	- MongoDB. - CouchDB.	- SimpleDB. - RethinkDB.
NoSQL - Grafos:		**NoSQL - Columnas o tabular:**	
- Neo4j (**7474**). - AllegroGraph. - FlockDB.	- InfinityGraph. - OrientDB (Java).	- Bigtable.	- HBase.
NoSQL - Multimodelo:		**Bases de datos en la NUBE**	
- OrientDB. - ArangoDB.	- Azure Cosmos DB.	- Google Cloud SQL. - Oracle Database Cloud. - Amazon RDS.	- Microsoft Azure SQL. - Amazon Aurora.

Puertos por defecto					
PostgreSQL	5432	Oracle	1521	DynamoDB	8000
MySQL	3306	MongoDB	27017	Redis	6379
SQL Server	1433	Cassandra	9042	Apache Derby	1527

ORACLE

SGBD relacional para empresas, aunque cuenta con una versión gratuita (Express Edition o XE).
Destaca por: Soporte de transacciones, Estabilidad, Escalabilidad y Multiplataforma.
Maneja vistas materializadas.
Base de datos: conjunto de archivos en disco, que almacenan de forma permanente los datos.
Instancia: conjunto de estructuras de datos en memoria (SGA) que administran archivos de db.

ESTRUCTURA FÍSICA	ESTRUCTURA LÓGICA
Ficheros de datos (DATAFILES). Ficheros de REDO LOG. Ficheros de control (CONTROLFILES).	TABLESPACE SYSTEM (diccionario de datos). OBJETOS (tablas, vistas, índices, etc.). Otros TABLESPACES (división lógica de la base de datos). SEGMENTOS (pertenecen a un tablespace): - De datos: almacenan las tablas. - De índices: acceso rápido a los datos. - De rollback: restauración de las transacciones. - Temporales: eliminados cuando la sentencia finaliza. - De bootstrap: definiciones del diccionario (en SYSTEM). EXTENSIONES: bloques de datos Oracle contiguos en disco.

Las ESTRUCTURAS DE MEMORIA asociadas con Oracle Database son:	
SGA (Área global del sistema):	memoria compartida caché.
PGA (Área global del programa):	memoria no compartida, existe un PGA para cada proceso. La vista **V$PGASTAT** son estadísticas a nivel de instancia.
UGA (Área global de usuario):	variables de sesión.
Áreas de código de software:	código que se ejecuta o se puede ejecutar.

PROCESOS DE ORACLE (en segundo plano):

La vista **V$PROCESS** contiene información de los procesos en memoria (datos de la sesión).

PMON (Process Monitor Process)	**DBW** (Database Writer Process)	**MMNL** (Manageability MoNitor)
PMAN (Process Manager)	**LGWR** (Log Writer Process)	**RECO** (Recoverer Process)
LREG (Listener Registration Proc.)	**CKPT** (Checkpoint Process)	**ARCn** (Archiver Processes)
SMON (System Monitor Process)	**MMON** (Manageability MONitor)	**FBDA** (FlashBack Data Archiver)

Un proceso de servidor:	realiza un trabajo basado en una solicitud del cliente.
Un proceso esclavo:	realiza tareas adicionales para un proceso en segundo plano.

FICHEROS DE CONFIGURACIÓN	
tnsnames.ora	contiene nombres de servicios de red
listener.ora	archivo de configuración para el listener de Oracle
sqlnet.ora	archivo de configuración del perfil

HERRAMIENTAS PARA DBAS	
Oracle Enterprise Manager	Tools for Database Installation and Configuration
SQL*Plus	Tools for Oracle Net Configuration and Administration
RMAN (Recovery Manager)	Tools for Data Movement and Analysis

SENTENCIAS PROPIAS DE ORACLE PARA DBAS

ANALYZE	*CALL*	*EXPLAIN PLAN*	*AUDIT*
COMMENT	*SET ROLE*	*SET TRANSACTION*	

VISTAS ADMINISTRATIVAS		
V$VERSION	V$SESSION	V$TABLESPACE
V$SESSTAT	V$SYSSTAT	V$STATNAME

ADMINISTRACIÓN DE USUARIOS			
Cuentas PRINCIPALES	SYS (superadministrador o DBA)	SYSTEM (DBA sin backups)	
Cuentas ESPECIALES	SYSDBA	SYSBACKUP (con RMAN)	SYSKM (claves de cifrado)
	SYSOPER	SYSDG (Data Guard)	SYSRAC (Clusterware)

La vista **DBA_USERS** describe todos los usuarios existentes.

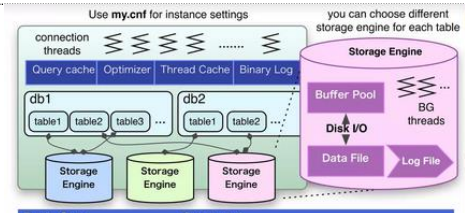
La vista **DBA_SYS_PRIVS** describe los privilegios de sistema asignados a usuarios y roles.

```
CREATE USER nombre {IDENTIFIED BY contraseña |
  EXTERNALLY | GLOBALLY AS nombreGlobal}
  [DEFAULT TABLESPACE tableSpacePorDefecto]
   [TEMPORARY TABLESPACE tableSpacetTemporal]
    [QUOTA {cantidad [K|M] | UNLIMITED} ON tablespace
     [PASSWORD EXPIRE]
      [ACCOUNT {UNLOCK|LOCK}];
       [PROFILE {perfil | DEFAULT}]
```

MySQL o MariaDB

Es un SGBD multihilo, multiusuario y software libre (GNU GPL). Actualmente usa el motor InnoDB.

MariaDB nace a partir de la adquisición de MySQL por parte de Oracle para seguir como open source.



Basic Ops	Command
Check mysqld version	shell> mysql --version mysql> SELECT VERSION;
Check set values	shell> my_print_default_mysqld
Show compile options	shell> mysqlbug
Connect to MySQL server	shell> mysql -u *user* -p *db1*
Instance Level Ops	**Command**
Start mysqld	shell> mysqld_safe & shell> sudo /etc/init.d/mysqld start shell> service mysqld start
Stop mysqld	shell> mysqladmin -uroot -p shutdown shell> sudo /etc/init.d/mysqld stop shell> service mysqld stop
Check status	shell> mysqladmin -u root -p status mysql> \s
Show system variables	mysql> SHOW GLOBAL VARIABLES;
Show status variables	mysql> SHOW GLOBAL STATUS;
List connected clients	mysql> SHOW [FULL] PROCESSLIST;
Database Ops	**Command**
List existing databases	mysql> SHOW DATABASES;
Create a database	mysql> CREATE DATABASE *db1*;
Switch database to use	mysql> USE *db1*;

Table Ops	Command
List existing tables	mysql> SHOW [FULL] TABLES;
Show table information	mysql> SHOW TABLE STATUS [LIKE '*table1*'];
Check table properties	mysql> DESC *table1*; mysql> SHOW CREATE TABLE *table1* \G
Create table	mysql> CREATE TABLE *table1* [columns...] ENGINE=*desired storage engine*
Modify table properties	mysql> ALTER TABLE table1 ...
Transaction Ops	**Command**
Switch off auto commit	mysql> SET AUTOCOMMIT=0;
Start a transaction	mysql> START TRANSACTION; mysql> BEGIN;
Execute SQL statement	mysql> SELECT ... (any SQL statement)
Commit	mysql> COMMIT;
Place a save point	mysql> SAVEPOINT *name of save point*;
Rollback	mysql> ROLLBACK;
Admin Ops	**Command**
Export to a file	mysql> SELECT ... INTO OUTFILE 'file name';
Read from a file	mysql> SET @@character_set_database=binary; mysql> LOAD DATA INFILE '*file name*' INTO TABLE '*table name*';
Backup	mysql> mysqldump [options] -B *db1,db2* > *dump.sql* --single-transactions (snapshot using MVCC) --master-data=2 (output position of binary log) --flush-logs (switch binary logs)
Restore	mysql> mysql *db1* < *dump.sql*
Defrag	mysql> OPTIMIZE TABLE *table1*;
Update Statistics Info	mysql> ANALYZE TABLE *table1*;
Switch logs	mysql> FLUSH LOGS;
Export table	mysql> FLUSH TABLES [WITH READ LOCK];

SQL Server

Es un SGBD propietario de Microsoft basado en el lenguaje Transact-SQL. Maneja vistas indexadas.

HERRAMIENTAS PARA DBAS		
AlwaysOn	Azure Data Studio	Distributed Replay
Azure Blob Storage	Configuration Manager	Extensión mssql de VS
Monitor de rendimiento	Data Migration Assistant	SQL Server Data Tools (SSDT)
SQL Server PowerShell	SQL Server Management Studio (SSMS)	

PostgreSQL

Es un SGBD multiplataforma orientado a objetos y es de código abierto (licencia BSD). Herramienta de la administración llamada pgAdmin. Se basa en cliente-servidor (cliente psql y servidor postmaster) con soporte JSON.

Connecting to PostgreSQL	
`psql`	open PostgreSQL interactive terminal
`psql -c {command}`	execute a single command and exit
`psql -d {database}`	connect to a particular database
`psql -U {role}`	connect as a particular user
`psql -l`	list all databases
Executed from your system command line	

psql commands	
`\du`	list all roles with their permissions
`\l`	list all databases with their owners
`\c`	show the current user and the database that you are connected to
`\c {database}`	connect to a particular database
`\dt`	list all tables in a connected database
`\d {table}`	list all columns and indexes for a specific table in a connected database
Executed inside `psql` interactive terminal	

Roles and databases management	
`createuser {user}`	create a new PostgreSQL role
`dropuser {user}`	drop an existing PostgreSQL role
`createdb {database}`	create a new database
`dropdb {database}`	drop an existing database
Executed from your system command line	

Database backup	
`pg_dump {database} \ > dump.sql`	dump a database to a text file
`psql {database} \ < dump.sql`	restore a database from a text file
`pg_dump -Ft \ -f dump.tar \ {database}`	dump a database to an archive file
`pg_restore -d \ {database} dump.tar`	restore a database from an archive file
`pg_dumpall > dump.sql`	dump all databases to a text file

Medios de almacenamiento masivo	
Discos	HDD y SSD (ver tema B2T2 Periféricos).
RAID	Usados como una sola unidad lógica de almacenamiento secundario.
Cabinas de discos	Proporcionan rendimiento (mediante caché), disponibilidad e integridad de los datos (mediante RAID) habituales de las redes SAN. **Front-end**: protocolo de acceso por bloques (FC, iSCSI, FCoE) o ficheros (NFS, CIFS). **Back-end**: protocolo nativo de dichos discos (FC o SAS). **Controladora:** replicación (RAID), cifrado, deduplicación, compresión, snapshots3, copias remotas...
JBOD	Just a Bunch of Disks o ***solo un montón de discos***. La capacidad es la suma de las capacidades de cada disco. No redundancia ni integridad frente a fallos.

Cintas magnéticas	El acceso a los datos es secuencial. Helicoidal o Longitudinal.
Bibliotecas de cintas	Las cintas magnéticas se ubican en librerías o bibliotecas de cintas automatizadas.

Métricas de fiabilidad	
MTBF (Mean Time Between Failures)	Tiempo medio entre fallos (de discos individuales).
MTTR (Mean Time To Recover)	Tiempo medio de recuperación.
MTTDL (Mean Time To Data Loss)	Tiempo medio hasta que un fallo provoque pérdida.
UBER (Unrecoverable Bit Error Rate)	Tasa de errores de bit irrecuperables

RAID
(Redundant Array of Independent Disks o matriz de discos independientes redundantes)

C = capacidad total. **n** = número de discos. **d** = capacidad del disco.

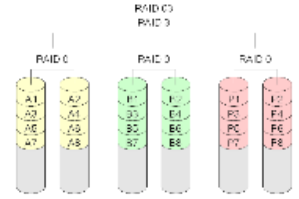
Todos los discos deben tener la misma capacidad el resto no se usa (desperdiciado).

Paridad (parity): se obtiene un resumen de los datos se calcula usando el operador lógico XOR.

Particionado (**STRIPPING**): en tiras | Duplicación (**MIRRORING**): espejado

Nivel	Mecanismo	Utilidad	Capacidad	Mínimo	Recuperar	
RAID 0	Stripping de bloque	Rendimiento (producción de video)	C = n*d	2 discos	No hay redundancia	
RAID 1	Mirroring de bloque	Redundancia (backups y minería)	C = n*d/2	2 discos	1 avería de disco sin pérdida	
RAID 2	Stripping de bit	Paridad dedicada (rendimiento e integridad)	C = (n-1)*d	3 discos	1	
RAID 3	Stripping de byte				1	
RAID 4	Stripping de bloque				1 (disco de comprobación)	
RAID 5	Stripping de bloque	1 bloque de paridad			1	
RAID 6	Stripping de bloque	2 bloques de paridad	C = (n-2)*d	4 discos	2 averías de disco sin pérdida	
RAID 5E y RAID 6E	Son variantes de RAID 5 y RAID 6 con disco de reserva.					

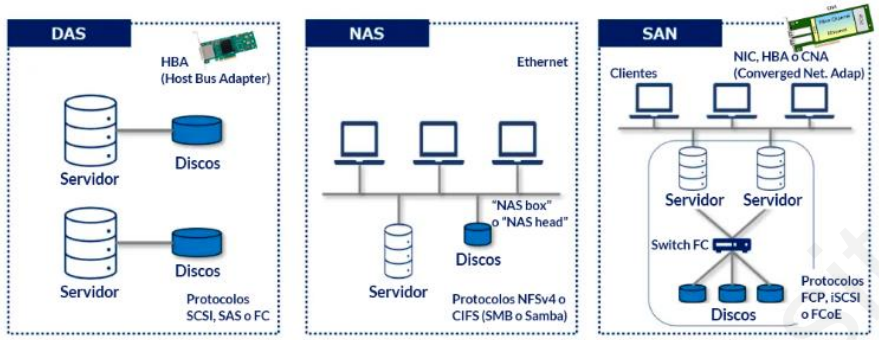
Además, existen niveles RAID anidados o compuestos **RAID A+B** o **RAID AB.**
A nivel INTERIOR y **B** el EXTERIOR.

RAID 0+1	Mirroring (RAID 1)	Misma tolerancia que RAID 5.	C = n*d/2	múltiplos de 4.	2	
RAID 1+0	Stripping (RAID 0)	Misma tolerancia que RAID 1.	C = n*d/2	4 discos		
RAID 0+3	Stripping (RAID 3)			6 discos		
RAID 0+5	Stripping (RAID 5)			6 discos		
RAID 1+5	Stripping a (RAID 5)			6 discos		
RAID 10+0	Se combinan varios conjuntos RAID 1 (espejados) en RAID 0 (particionados) entre sí			8 discos		

Conexión de los discos: RAID por software (más lento) y RAID por hardware (rápido).

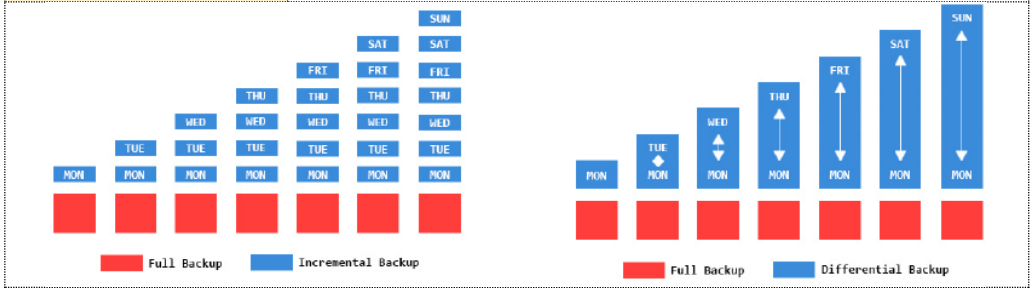
Arquitecturas de almacenamiento	
DAS (Almacenamiento de conexión directa)	Discos conectados directamente a través de un HBA (Host Bus Adapter) a los servidores (lo más simple), cabinas de disco o unidades de cinta. **Protocolos**: **SCSI, SAS** o **FC** (Fibre Channel). Opera a nivel de BLOQUES de datos.
NAS (Almacenamiento conectado a la red)	Dispositivos conectados a una red de datos (Ethernet). Interfaz llamada "NAS box" o "NAS head". **Protocolos**: **IP**, **NFS**v4 (Network File System) o **CIFS** (Common Internet File System, SMB o Samba) Opera a nivel de FICHEROS.
SAN (Red de almacenamiento)	Red independiente dedicada exclusivamente al almacenamiento. Capa de ALMACENAMIENTO: disp. de almacenamiento. Capa de INFRAESTRUCTURA: switches y cables. Capa de HOSTS: servidores mediante tarjetas NIC, HBA o CNA (Converged Network Adapter). **Protocolos**: **FCP** (Fibre Channel Protocol), **iSCSI** (Internet SCSI **TCP 860** y **3260**) o **FCoE** (Fibre Channel over Ethernet). **Topologías**: Punto a punto, Anillo o en Estrella. Opera a nivel de BLOQUES.
SDS (Almacenamiento definido por software)	SDS también es conocido como VSAN (**Virtual SAN**) es un programa informático que administra los recursos del almacenamiento y no depende del hardware de almacenamiento físico subyacente. Soluciones SDS: VMware vSAN, Red Hat Ceph Storage, IBM SAN Volume Controller (SVC), StarWind VSAN.

Nube Almacenamiento en la **nube**	Servicio que permite almacenar datos transfiriéndolos a través de Internet a un sistema de almacenamiento externo (a terceros). Soluciones: (Google Drive, AWS, Google Cloud, Mega, Azare, etc.).
LVM (Almacenamiento virtualizado)	Herramientas que se utilizan para disponer de un entorno de almacenamiento con múltiples dispositivos de forma transparente al usuario. - LVM (Logical Volume Management) para Linux. - LDM (Logical Disk Manager o Administrador de discos lógicos) de Windows. - CoreStorage para macOS. **THIN provisioning** no asigna asignar todos los recursos y requiere que se planifique el consumo de recursos. **THICK provisioning** asigna la totalidad de los recursos requeridos.



PROTOCOLOS	
NFS	Network File System: protocolo NAS en red que permite que puedan acceder a ficheros a través de la red como si el sistema de archivos fuese local. NFSv4 es la última versión.
CIFS	Common Internet File System: protocolo NAS de Microsoft que permite compartir archivos e impresoras entre nodos de una red. En sistemas Unix y macOS existe Samba.
FCP	Fibre Channel Protocol: protocolo SAN transmite comandos SCSI sobre redes Fibre Channel
FCIP	Fiber Channel over IP: protocolo SAN permite la transmisión de tramas Fibre Channel sin modificar a través de túneles IP con el objetivo de facilitar la extensión geográfico de una red SAN
iSCSI	Internet SCSI: protocolo NAS de la capa de transporte que encapsula los comandos SCSI dentro de una trama Ethernet y utiliza conexiones TCP/IP
FCoE	Fibre Channel over Ethernet: protocolo SAN encapsula tramas Fibre Channel dentro de un trama de Ethernet

POLÍTICAS DE BACKUP Y SU RECUPERACIÓN	
Una buena práctica a la hora de realizar copias de seguridad es adoptar la **estrategia 3-2-1** - Mantener **3 copias** de cualquier fichero importante: el archivo original más dos backups. - Almacenar las copias en **2 soportes distintos.** - Almacenar **1 copia** de seguridad **fuera de nuestra organización.**	
Plan de Recuperación ante Desastres (DRP) o Plan de Continuidad del Negocio	
RTO (Recovery Time Objective)	Tiempo máximo que el servicio puede permanecer interrumpido.
RPO (Recovery Point Objective)	Tiempo máximo que se pueden perder los datos (asume la pérdida de datos), es decir, cantidad de datos que puede permitirse perder.
Arquitecturas de sistemas de backups	
Backup en red PRIVADA	Las copias de seguridad se guardan en la misma red que los datos. Pueden ser NAS o redes SAN.
Backup en la NUBE	Las copias se guardan en una red externa. Cuando se guarden en una nube pública, estos deberán enviarse cifrados.
Tipos de sistemas de backup	
Herramientas de sincronización	Duplican el contenido de una serie de directorios en la misma máquina o en distintas.
Copias	Herramientas que realizan copias periódicas.
Instantáneas (Snapshots)	Copias de todo un sistema o parte de un sistema que permiten recuperarlo en un estado que se sabe que es correcto.
Continuous data protection	Herramientas que guardan automáticamente una copia de todas las modificaciones que se realizan en los datos con versionado.
Tipos de backup	
COMPLETO	Copia integral de los datos y borra el bit de modificado.
INCREMENTAL	Se copian los datos modificados desde la anterior copia incremental y elimina el bit de modificado en los archivos respaldados.
DIFERENCIAL	Se copian los datos modificados desde la última copia completa desde que se hizo ese backup completo, pero no elimina el bit de modificado.
INTERMEDIO	Similar al backup completo, pero no se borra el bit de modificado.



Un esquema común es el método abuelo-padre-hijo, que utiliza en total **12+4+7=23** cintas:
- **Backup** completo cada **mes** y se guarda durante **un año** (**abuelo**).
- **Backup** completo cada **semana** y se guarda durante **un mes** (**padre**).
- **Backup diario** (completo, incremental o diferencial) y se guarda durante **una semana** (**hijo**).

VTL (Virtual Tape Library)	Permiten presentar un dispositivo de almacenamiento como si fuera una librería de cintas para su uso con un software de backup preexistente.

Soluciones de backup	
Veeam Backup & Replication	AWS Backup
Azure Backup	Acronis Backup

VIRTUALIZACIÓN

Computación en la nube: "*rápidamente aprovisionados y puestos en producción con un esfuerzo de mantenimiento mínimo o sin interacción del proveedor*", ya que de eso se trata, precisamente, la tecnología **hiperconvergente**.

Nube pública	Recursos y capacidades de forma compartida a través de Internet o redes públicas, normalmente en un modelo de pago por uso.
Nube híbrida	Mezcla de nubes públicas y privadas que las organizaciones utilizan para aprovechar las ventajas de los servicios de pago por uso, pero manteniendo el control sobre sus servicios "Core" en sus instalaciones.
Nube privada	Todos los recursos están alojados y controlados por la organización. Su acceso es limitado y restringido a los usuarios o autorizados de la organización (autoservicio, escalabilidad, automatización, monitorización, seguridad, etc.).

La **virtualización** se entiende como la recreación de un recurso físico (hardware) o lógico (software), por medio de un hipervisor (hypervisor) creándose una capa de abstracción que permite la ejecución de más de un entorno al mismo tiempo.
Una máquina virtual (guest o invitado) es un entorno de ejecución aislado creado por el hipervisor encargado de gestionar todos los recursos del hardware.
El equipo que presta los medios físicos y sobre el que se instala el hipervisor es conocida como host o anfitrión.

Virtualización completa	El hipervisor simula un entorno completo de hardware para cada máquina virtual, de modo que la máquina virtual no tiene acceso al hardware físico del sistema anfitrión. VMware Workstation, VMware ESXi, Oracle VM VirtualBox, KVM, Microsoft Hyper-V y Windows VirtualPC.
Paravirtualización	El hipervisor ofrece solo una interfaz de programación (API) a través de la que máquina virtual acceden al hardware físico del anfitrión. Citrix XenServer, Virtuozzo y OpenVZ.

Tipos de hipervisores			
Hipervisor de TIPO 1		**Hipervisor de TIPO 2**	
Se conoce como hipervisor nativo o bare metal o unhosted. Esta forma de VMM se instala directamente en el hardware físico y no está conectada con el sistema operativo del host (entorno empresarial).		También conocido como hosted o alojado) requiere un sistema operativo existente, que a su vez se base en el hardware físico (entorno doméstico).	
Citrix XenServer	VMware ESXi y vSphere	VMware Workstation	Oracle VM VirtualBox
KVM (Kernel-based VM)	Oracle VM Server	Virtuozzo	Red Hat Virtualization
Microsoft Hyper-V	Proxmox VE	Windows VirtualPC	OpenVZ

Tipos de virtualización	
Virtualización del escritorio	El procesamiento se produce en los servidores. El almacenamiento de datos se produce en los servidores remotos, de forma que el cliente no almacena ningún dato sensible en su dispositivo. Se denominan **Thin Clients (clientes ligeros)** y tienen recursos mínimos de almacenamiento, memoria, procesamiento y sistema operativo. Otro tipo de clientes aún más ligeros son los **Zero Clients**, que no llegan a tener ni sistema operativo, y utilizan un firmware específico para poder establecer la conexión. **Tecnologías**: - **VDI (Virtual Desktop Infra.)**: con VDI persistente o no persistente. VMWare Horizon, Azure Virtual Desktop, Citrix Workspace o XEN Desktop. En una infraestructura de máquinas virtuales. - **RDS (Remote Desktop Services) de Microsoft**: se basa en sesiones de usuarios concurrentes en un mismo sistema operativo (Windows Server) mediante el protocolo RDP. - **DAAS (Desktop As A Service) o VDI cloud**: puede tener la capa de control y la capa de recursos alojadas en la organización (on-premise) o en la nube. Amazon WorkSpaces o Citrix Virtual Apps and Desktop S. - **VDI Híbrido** cuando la capa de control está en la nube y los recursos se encuentran on-premise mediante un conector para comunicarlos.

Virtualización de las aplicaciones (contenedores).	Tecnologías que permiten encapsular en un entorno aislado o sandbox (contenedor), los ejecutables de las aplicaciones, junto con los ficheros necesarios, servicios y árbol de registro, todo listo para su despliegue en red utilizando una imagen base. Permiten una gran capacidad para despliegues rápidos. Docker, Podman o Linux Containers.
Virtualización de servidores	Facilita el despliegue de entornos, posibilita la ejecución de varios sistemas operativos en una única máquina física y permite un aprovechamiento de la capacidad del hardware.
Virtualización del almacenamiento	A diferencia de los sistemas tradicionales como NAS (almacenamiento conectado a la red) o SAN (red de área de almacenamiento), el almacenamiento definido por software (SDS) permite unificar en un solo espacio o conjunto lógico, múltiples discos físicos instalados localmente en cada servidor del clúster de hiperconvergencia.
Virtualización de la red (NV - Network Virtualization)	Hace uso de dos tecnologías (NFV y SDN) para transformar redes estándar en redes virtuales. - NFV (Network Function Virtualization): flexibiliza la red, permitiendo a cada nodo convertirse en un microcentro de datos, capaz de hospedar varias apps. - SDN (Software defined Network): gestión centralizada de la red mediante un software del enrutamiento o la optimización WAN y Firewall.

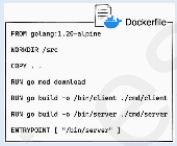
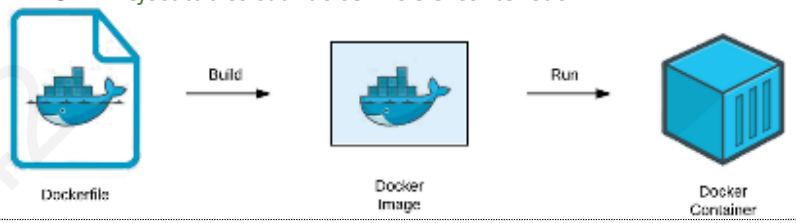
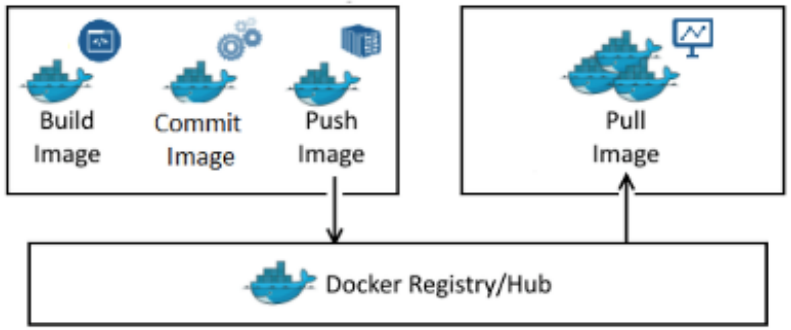
Hiperconvergencia

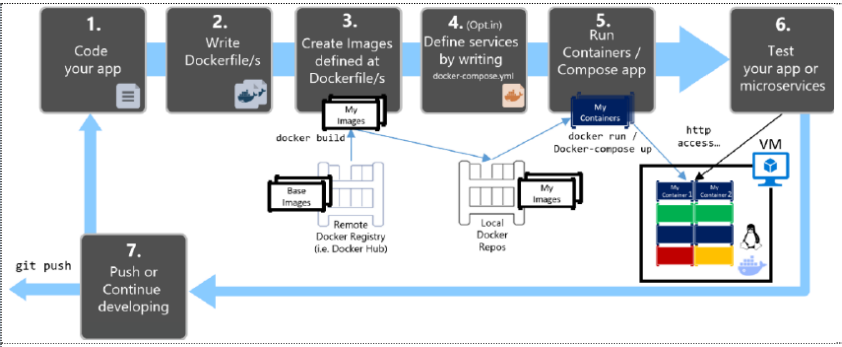
Una arquitectura hiperconvergente está compuesta como mínimo de una capa de hipervisor, una red definida por software (SDN) y un almacenamiento definido por software (SDS). Todo ello permite unificar los elementos físicos en capas lógicas, con una gestión centralizada de todo el conjunto en una única consola administrativa.
Las infraestructuras basadas en **hiperconvergencia (HCI)** están definidas por software en su totalidad, en donde se aíslan todas las operaciones relacionadas con el hardware del sistema y se unifican a nivel de hipervisor en un único bloque.

DOCKER

Un contenedor (visión dinámica) es un proceso en que está aislado, es decir, instancia ejecutable de una imagen (visión estática). Se puede ejecutar en máquinas locales, máquinas virtuales o implementarse en la nube.

El motor de Docker (**DOCKER ENGINE**): permite ejecutar un contenedor. Docker utiliza una arquitectura cliente-servidor. Se compone de:
Un servidor que es un proceso demonio **docker daemon** (comando *dockerd*).
Una **API REST** que los programas pueden usar para comunicarse con el demonio (*dockerd*) a través de sockets UNIX o una interfaz de red.
Un **cliente** de interfaz de línea de comandos (comando *docker*).

IMÁGENES DOCKER	Son plantillas (**Dockerfile**).de solo lectura con todas las instrucciones que necesita el motor de Docker para crear un contenedor. **FROM** *#establece la imagen base.* **WORKDIR** *#directorio de trabajo.* **COPY** *#copia nuevos archivos o directorios.* **ADD** *#similar a COPY copia nuevos archivos o URL de archivos.* **RUN** *#ejecutará y confirmará el comando encima de la imagen actual (varios).* **CMD** *#proporciona valores predeterminados (sólo puede haber una línea).* **LABEL** *#metadatos (clave-valor).* **ENV** *#variables de entorno (<key> =<value>).* **VOLUME** *#crea un punto de montaje con el nombre especificado.* **ENTRYPOINT** *#ejecutables cuando se inicie el contenedor.*  
DOCKER HUB	Repositorios (públicos y privados) de software basado en la nube (*hub.docker.com*).
REGISTRO DOCKER almacena imágenes de Docker	
Persistencia	**Volúmenes**: se crea un nuevo directorio dentro del directorio de almacenamiento de Docker en la máquina host (mecanismo preferido). **Montajes de enlace**: pueden enlazar cualquier archivo/directorio en el sistema de archivos del host. **Montajes tmpfs**: para datos de estado no persistentes.

CI/CD en Docker (flujo de trabajo)	
COMANDOS GENERALES	*docker -d #Start the docker daemon* *docker -help #Get help with Docker* *docker info #Display system-wide information* *docker login -u <username #Login into Docker* *docker push <username>/<image_name> #Publish image* *docker search <image_name> #Search Hub for an image* *docker pull <image_name> #Pull an image from a Docker Hub*
COMANDOS IMAGENES	*docker build -t <image_name> #Build an Image from a Dockerfile* *docker build -t <image_name> . -no-cache #Build no cache* *docker images #List local images* *docker rmi <image_name> #Delete an Image* *docker image prune #Remove all unused images*
COMANDOS CONTENEDORES	*docker run --name <container_name> <image_name> #Create* *docker run -d <image_name> #Run container in background* *docker start|stop <container_name> (or <id>) #Start* *docker rm <container_name> #Remove a stopped container* *docker exec -it <container_name> s #Open a shell inside cont.* *docker ps (optional -all) #To list currently running containers* *docker container stats #View resource usage stats*

Open Container Initiative (OCI) es un proyecto de gobernanza abierta, formada bajo los auspicios de la Fundación Linux, con el propósito de crear estándares de formatos de contenedores y runtimes.
- La especificación de tiempo de ejecución runtime-spec.
- La especificación de imagen image-spec.
- La especificación de distribución distribution-spec.

Contenedores como servicio (CaaS): son un modelo de servicios en la nube que permiten gestionar e implementar las aplicaciones usando contenedores.

Docker Hub	Azure Container Registry	Amazon Elastic Container Registry (ECR).
Harbor	Red Hat Quay	Google Cloud Container Registry
ZooKeeper		

Otras plataformas de contenedores
PODMAN
Alternativa open source a Docker, es gestionado a través de una ***CLI*** sencilla y de la biblioteca **libpod**, la cual ofrece las **API** para administrar los contenedores, aunque destaca por ser una herramienta sin daemons. Trabaja junto con herramientas como Buildah para crear y Skopeo para trasladar los contenedores.
Linux Containers (LXC)
Plataforma de contenedores open source que proporciona un conjunto de herramientas, plantillas, bibliotecas y enlaces entre lenguajes también gestionado a través de una ***CLI*** sencilla.

ORQUESTACIÓN DE CONTENEDORES	
Docker Swarm	Herramienta oficial de Docker para orquestar conjuntos de contenedores. El comando "**Docker swarm**" (**enjambre**) puede utilizarse para combinar varios Docker Engines en un SOLO MOTOR VIRTUAL. La administración y orquestación de clústeres integradas en Docker Engine se crean utilizando swarmkit.
Docker Compose	Herramienta oficial de Docker para orquestar conjuntos de contenedores. El comando "**Docker compose**" se utiliza para crear aplicaciones **MULTICONTENEDOR** conocidas como "**stacks**" o pilas. Utiliza un archivo YAML para configurar los servicios.
Kubernetes (K8s)	Plataforma portable y extensible de código abierto para administrar cargas de trabajo y servicios. Facilita la automatización y la configuración declarativa. Google donó el proyecto Kubernetes a la **C**loud **N**ative **C**omputing **F**oundation (CNCF). Los objetos básicos de Kubernetes incluyen: - Pod: son las unidades de computación más pequeñas. - Service: es un método para exponer una aplicación de red (uno o más Pods). - Volume: permite guardar los archivos que se crearon durante la vida útil. - Namespace: es el nombre que recibe un clúster virtual.
OKD (Origin)	Distribución de Kubernetes open source, considerándose la versión libre de OpenShift, la cual permite montar clústers de OpenShift en los servidores.

Servicios de orquestación en la nube	
Amazon Elastic Container Service (Amazon ECS)	Google Kubernetes Engine (GKE)
Azure Kubernetes Service (AKS)	Azure Container Apps
IBM Cloud Kubernetes Service	

FORMATO DE UN MENSAJE

Un mensaje de correo electrónico es fichero de texto plano constituido por caracteres ASCII (7 bits). Cada campo cabecera consiste en una sola línea de texto ASCII con el nombre del CAMPO (:) RFC 822

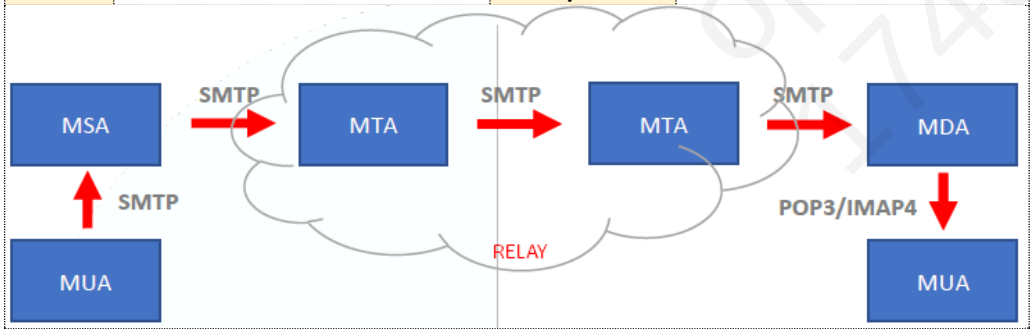
To:	**From:**	**Return-Path:**	**Message-Id:**	**References:**
Cc: (Carbon Copy)	**Sender:**	**Date:**	**Subject:**	**Content-Type:**
Bcc: (Blind CC):	**Received:**	**Reply-To:**	**In-Reply-To:**	**Delivered-To:**

Para permitir el uso de otros caracteres (acentos, alfabetos no latinos y de adjuntos binarios) dentro del cuerpo del mensaje, se creó **MIME (Multipurpose Internet Mail Extensions)**. MIME sólo afecta a los agentes de usuario, ya que para SMTP es totalmente transparente.
MIME-Version: versión (1.0) de las extensiones MIME utilizadas en el mensaje. Si no existe esta cabecera se considera que el texto es plano.

Listas de distribución:	Dirección virtual para varios destinatarios a la vez, llamados suscriptores. Soluciones de software: **Mailman** (Python) **Sympa** (GNU GPL).

COMPONENTES DE UN SISTEMA DE CORREO

MUA	**Mail User Agent** o Agente de usuario de correo: cliente de correo electrónico. Tipos: Clientes en modo texto (shell), pesados (de escritorio), ligeros (webmail) y móvil.		
MTA	**Mail Transfer Agent** o Agente de transferencia de correo: es el encargado "estafeta" del transporte de los mensajes de un nodo a otro usando el protocolo SMTP.		
MSA	**Mail Sending Agent**: primera MTA a la que el cliente entrega su correo por SMTP.		
MDA	**Mail Delivering Agent**: última MTA que recibe el correo y lo entrega al cliente destinatario.		
SMTP	Correo saliente	**POP/IMAP**	Correo entrante

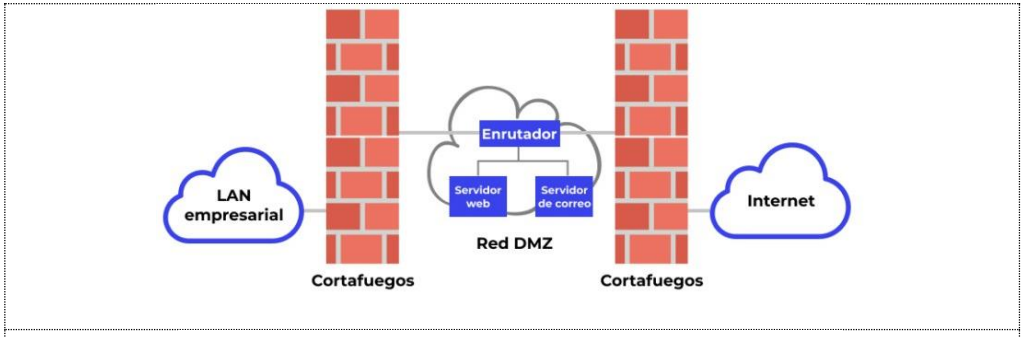


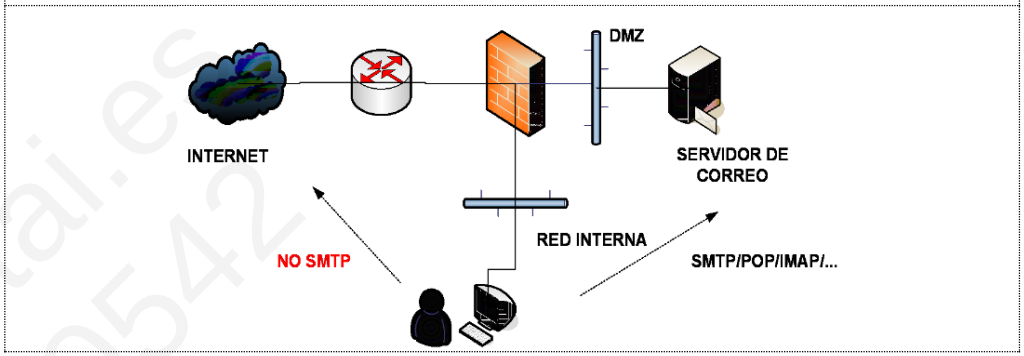
PROTOCOLOS DE CORREO ELECTRÓNICO

SMTP	**Simple Mail Transfer Protocol** o Protocolo Simple de Transferencia: protocolo estándar para envío de correos electrónicos. Para ello consultará el registro MX (DNS).					
	25/TCP	texto plano		**465**/TCP	SSL/TLS	
	587/TCP	STARTTLS		**2525**/TCP	alternativa al puerto 587	
Códigos	211	Estado (HELP)	354	Comienza el mensaje	500	Error de sintaxis
	220	Servicio preparado	421	Servicio no disponible	552	Excedido tamaño
	250	Solicitud OK	450	Buzón no disponible	554	Fallo en la transacción
ESMTP	**Extended SMTP** o SMTP Extendido: nuevas capacidades SMTP en especial las relativas a autenticación (ASMTP) de usuarios o transporte seguro de datos. Obligatorio **587/TCP**					
POP3	**Post Office Protocol versión 3**: permite descargar mensajes (correo entrante) desde el servidor y son eliminándolos del servidor.					
	110/TCP	sin cifrado		**995**/TCP	cifrada con TLS (POP3S).	
Códigos	+OK	funcionó correctamente.		+ERR	El comando falló	
IMAP4	**Internet Message Access Protocol**: permite que los buzones de correo de los usuarios se encuentren centralizados en el servidor de correo sin necesidad de descarga.					
	143/TCP	sin cifrado		**993**/TCP	cifrada con TLS (IMAPS)	
Códigos	OK	satisfactorio	NO	insatisfactorio	BAD:	error
	PREAUTH	autenticado	BYE	Conexión cerrada		
IMAP IDLE	Extensión IMAP que permite que el servidor avise al cliente cuando ha llegado un correo.					
QMTP	**Quick Mail Transfer Protocol**: protocolo de transmisión de correo electrónico diseñado para tener un mejor rendimiento que SMTP. Usa el puerto 209.					

SEGURIDAD EN CORREO ELECTRÓNICO	
STARTTLS	Permite inicializar un intercambio TLS con el servidor de correo previo al envío de las credenciales del usuario.
SPF	Sender Policy Framework: protección contra la falsificación de direcciones, permite comprobar las máquinas autorizadas a enviar correo para un dominio determinado.
DKIM	DomainKeys Identified Mail: asegura la integridad del correo electrónico enviado, incorporando una nueva cabecera al correo con una firma digital del contenido.
DMARC	Domain-based Message Authentication, Reporting & Conformance: es un registro de dominios de autenticación de correos electrónicos fue creado por PayPal junto con Google, Microsoft y Yahoo.
S/MIME	Secure/Multipurpose Internet Mail Extensions: permite el cifrado de correos electrónicos mediante criptografía asimétrica y la firma digital.
PGP	Pretty Good Privacy: programa creado por Phil Zimmermann para comunicaciones seguras que ofrece la opción de la firma digital.
GNU PG	GNU Privacy Guard: software de cifrado y firma digital de código abierto bajo licencia GPL con la misma funcionalidad que PGP. Es una implementación del estándar OpenPGP.
Antispam	Apache SpamAssassin y MailScanner.
Antivirus	ClamAV: software antivirus open source bajo licencia GPL.

ARQUITECTURA DE RED DE UN SISTEMA DE CORREO	
El servidor de correo electrónico corporativo debe estar ubicado en una zona desmilitarizada (**DMZ**). Dicha zona de red es el segmento en el que la organización ubica los sistemas que están ofreciendo servicios a Internet debe estar aislado tanto de Internet como de la red interna. Es importante que la organización evalúe denegar, en el cortafuegos corporativo, todo el tráfico SMTP excepto los de sus propios servidores SMTP.	
Dos cortafuegos	uno para aislar dicha zona de la red interna y otro para aislarla de la externa preferiblemente de tecnologías diferentes para evitar que un problema de seguridad.
Un único cortafuegos (redundado o no)	(redundado o no) para separar zonas de red (interna/DMZ/Internet) mediante el uso de tarjetería de red adicional en el sistema (se requiere al menos una tarjeta por cada zona de la red).





CLIENTES DE CORREO ELECTRÓNICO				
Modo texto	Mutt: cliente en modo texto para sistemas Unix de código abierto (GPL).			
Clientes pesados	Apple Mail	Evolution	Microsoft Outlook	Spark
	Claws Mail	Inky	Mozilla Thunderbird	Spike
	eM Client	Mailbird	SeaMonkey	Lotus Notes
Clientes ligeros (webmail)	AfterLogic	BlogMail	Ilohamail	RoundCube
	Alt-N Technologies	Horde	MailEnable	SquirrelMail
	AtMail	BlogMail	Openwebmail	Zimbra

SERVIDORES DE CORREO ELECTRÓNICO		
Trabajen de forma asíncrona de forma que el cliente envía un mensaje y no tiene que esperar respuesta. El servidor de correo permanece a la "escucha" de conexiones de otros servidores para la recepción de mensajes.		
Microsoft Exchange Server	Postfix (IBM Wietse Venema)	Qmail
Sendmail (Proofpoint)	Exim	Dovecot
Formato de almacenamiento de un buzón de correo		
MailDir	guarda correo cada electrónico en un único fichero.	
Mailbox (o mbox)	guarda todos los correos en un fichero.	

COMANDOS PARA ADMINISTRACIÓN DE REDES LINUX

ping [**-a**] [**-b**] [**-c** count] [**-i** intervalo] [**-t** TTL] **objetivo**

ping -i 5 8.8.8.8 *#Envía paquetes cada 5 segundos*

-a *Resuelve el nombre host*	***-i*** *Intervalo de tiempo. Por defecto 1 segundo*
-b *Para hacer ping a la dirección de broadcast*	***-t*** *Número de saltos. Valor para TTL (Time To Live). Máximo 255*
-c *Número de paquetes a enviar*	

traceroute objetivo

traceroute 8.8.8.8 *#Muestra la ruta de un paquete hasta el destino*

ifconfig interfaz [**dirección** [**parámetros**]]

ifconfig eth0 192.168.1.1 netmask 255.255.255.0 up *#Asigna una máscara de subred*

-a *Muestra las direcciones de todas las interfaces*	***netmask*** *Asigna una máscara de subred a interfaz*
Up / down *Marca la interfaz como disponible*	***broadcast*** *Asigna la dirección de difusión*

route [**-e**] [**-n**]

route –n *#Muestra contenido tabla en formato numérico*

-e *Muestra contenido tabla en formato hostname*	***add*** *Añade nueva ruta a la tabla*
-n *Muestra contenido tabla en formato numérico*	***del*** *Elimina ruta de la tabla*

iw [opciones] **objeto** [comando]

iw dev wlan7 info *#Muestra info de la interfaz*

dev *Interfaz de red*	***phy#*** *Índice dispositivo inalámbrico*
phy *Nombre dispositivo inalámbrico*	

netstat [opciones]

netstat –r *#Muestra la tabla de enrutamiento*

-r *Muestra la tabla de enrutamiento*	***-l*** *Muestra conexiones activas de escucha (LISTEN).*
-i *Muestra las interfaces*	***-c*** *Muestra la información con refresco periódico*
-s *Muestra estadísticas de red*	***-a*** *Muestra sockets activos. Añadiendo t (-at) solo conexiones TCP, si u (-au) solo conex. UDP*

ip [opciones] **objeto** [comando [argumentos]]

ip add show *#Muestra las direcciones IP*	ip neigh show *#Muestra la cache ARP*
-s Estadísticas	**-f** Familia de protocolo a usar (inet, inet6, link)
Objetos: link, address, route, neigh	**Comandos:** add, del, set, show, via

mtr objetivo [opciones] *#(My Trace Route)*

mtr 8.8.8.8 –r *#Combina traceroute y ping*

objetivo *Nombre host destino*	***-i*** *Intervalo entre paquetes. Defecto 1 segundo*
-c *Número máximo de ping*	***-r*** *Muestra estadísticas*

nslookup [opciones] **HOST/IP**

nslookup www.inap.es *#Obtiene IP para ese nombre de host*

dig [@servidor] [dominio] [tipo] [-x dirIP] [opciones]

dig www.correos.es a +short *#Obtiene la IP, registro A en modo "corto"*

@servidor *Servidor DNS de petición.*	***-x*** *Dirección IP por la que se busca*
dominio *Dominio sobre el que se busca*	***+short*** *Búsqueda en modo "corto"*
tipo *Tipo de registro DNS a consultar*	

ssh usuario@host [**-p** puerto] {comando|'comandos'} *#(Secure Shell)*

ssh root@92.243.54.126 uptime *#Conexión a máquina remota y ejecuta el comando uptime*

usuario *Usuario de la máquina remota*	***comando*** *Comando a ejecutar en máquina remota*
host *Host de la máquina remota*	***comandos*** *Comandos separados por ; a ejecutar en máquina remota.*
-p *Puerto de escucha del servidor. Defecto 22*	

who [**-a**] [**-b**] [**-H**] [**-m**] [**-q**] [**-r**] [**-u**]

who -b -u *#Ultimo arranque del sistema y usuarios conectados*

-a *Todas las opciones*	***-m*** *Nombre de host y usuario*
-b *Fecha y hora del último inicio del sistema (boot)*	***-r*** *Nivel de ejecución (runlevel)*
-H *Imprime encabezado para cada columna*	***-u*** *Nombre de usuarios conectados*

scp [userorigen@hostorigen:]/[dir_file] userdestino@hostdestino:/[dir_dest] *#(Secure Copy Protocol)*

scp /usuario1/dir/info root@191.162.0.2:/compartido/informes *#Copia ficheros entre dos máquinas*

userorigen *Usuario host origen*	***userdestino*** *Usuario host destino*
hostorigen *Host de la máquina origen*	***hostdestino*** *Host de la máquina destino*
dir_file *Directorio o ficheros a copiar*	***dir_dest*** *Directorio para información copiada*

sftp usuario@host

sftp root@192.168.1.1 *#Copia ficheros entre máquinas de forma interactiva*

usuario Usuario de la máquina remota	**host** Nombre o dirección IP de la máquina remota

w [usuario]

w [usuario] *#Información de usuarios conectados y sus procesos (qué están haciendo).*

arp [userorigen@hostorigen:]/[dir_file] userdestino@hostdestino:/[dir_dest]

arp -a 192.168.1.3 *#Muestra info de un host*

-a Muestra toda la caché.	**-d** Elimina una entrada.	**-s** Añade una entrada a la tabla

GESTIÓN DE USUARIOS LINUX

FICHEROS DE CONFIGURACIÓN

/etc/passwd	contiene las cuentas de usuarios.

usuario:password:uid:gid:comentario:directorio:shell-inicio

pepe:x:1002:1002:Pepe Pótamo,123,981234321,:/home/pepe:/bin/bash

usuario	Debe tener entre 1 y 32 caracteres de longitud.

password	Un carácter x indica que la contraseña cifrada se almacena en /etc/shadow
uid	El UID 0 (cero) está reservado para root y a partir del 1000 para usuarios normales.
directorio	(Home directory) ruta absoluta del directorio, suelen tenerlo en /home.
shell	Shell que utiliza por defecto el usuario. Por defecto /bin/bash.
/etc/shadow	contiene las contraseñas cifradas de los usuarios.
usuario:password:lastchg:min:max:warn:inactive:expire:reserved	
pepe:1.QKDPc5E$SWlkjRWexrXYgc98F.:12825:0:90:5:30:13096:	
lastchg	Días desde el último cambio de contraseña desde el 01/01/1970
warn	Número días en que se avisa al usuario.
inactive	Número de días en que se deshabilitará la cuenta desde que caduque.
expire	Días en que la cuenta se deshabilitará, contados desde el 1/1/1970
/etc/group	contiene los grupos de usuarios.
grupo:password:gid:miembros	
users:x:100:pepe,elena	
password	Un carácter x indica que la contraseña cifrada se almacena en /etc/gshadow
miembros	Lista separada por comas con los nombres de usuario
/etc/gshadow	contiene las contraseñas cifradas de los grupos.
/etc/skel/	directorio que contiene el directorio home para cada nuevo usuario

COMANDOS DE GESTIÓN DE USUARIOS		
useradd [opciones] **usuario**		
useradd -c "Pepe Ramirez" pepe *#Crea un usuario usando comentarios*		
***-c** comentario*	***-g** gid*	***-f** inactive*
***-d** homedir*	***-G** group1,...*	***-s** shell*
***-e** expire*	***-p** password*	***-u** uid*
userdel [**-r**] **usuario**		
userdel -r pepe *#Elimina un usuario. [-r] elimina el directorio del usuario*		
usermod [opciones] **usuario**		
usermod -G grupoTIC pepe *#Reemplaza el grupo del usuario*		
***-a** añade*	***-l** Nuevo nombre de usuario*	***-u** Nuevo uid del usuario*
***-g** nuevo grupo primario*	***-L** Bloquea la cuenta*	***-U** Desbloquea la cuenta*
***-G** grupos separados por comas*		
passwd [opciones] **usuario**		
passwd -l pepe #Bloquea la cuenta juan		
-d Elimina la contraseña	**-n** Nº días antes cambio pass	**-x** Número de días de validez pass
-l Bloquea la cuenta	**-S** Estado de	**-w** Nº días antes de que caduque
chage [opciones] **usuario** *#(Change age)*		
chage -l pepe *#Muestra información de caducidad del usuario pepe*		
-d Fecha de última mod. pass	-E Fecha de caducidad pass	-M Validez, equivale a passwd -x
finger usuario *#Información del usuario*		

chfn [usuario] *#Cambio de información del usuario (campo comentario o GECOS)*	
chsh [-l] -s shell [usuario] *#(Change Shell)*	
-l Listado de shells disponibles	**-s** Nuevo shell.
id [usuario] *#Muestra información del uid y gid del usuario*	
pwck *#Verificación de la integridad en /etc/passwd y /etc/shadow*	
Existe una "variante" denominada **adduser** y **userdel** utilizados en distribuciones Debian.	
COMANDOS DE GESTIÓN DE GRUPOS	
groupadd [-g gid] **grupo**	**gpasswd** [-a usuario] [-A usuario1,...] **grupo**
groupdel grupo	**newgrp grupo**
groupmod [-g gid] [-n nuevonombregrupo] **grupo**	**groups usuario**

Microsoft Active Directory

COMANDOS PARA ADMINISTRACIÓN DE REDES WINDOWS			
arp	*Muestra y modifica las entradas incluidas en la tabla ARP*		
getmac	*Muestra la dirección MAC de todos los adaptadores de red*		
gpresult	*Muestra información sobre las directivas de grupo*		
gpupdate	*Actualiza la información sobre las directivas de grupo*		
ipconfig	*Información IP de cualquier adaptador*		
	***/reléase** (libera direcciones)*	***/renew** (renovarse)*	***/flushdns** (vaciar caché DNS)*
net	*Configura y muestra ajustes de red*		
	***accounts** (políticas de cuentas)*	***computer** (añade en dominio)*	***start** (inicia un servicio)*
	***statistics** (estadísticas)*	***use** (muestra conexiones)*	***share** (recursos compartidos)*
	***time** (sincroniza el reloj)*	***view** (equipos del dominio)*	
netsh	*Inicia el shell de red (Network Shell)*		
	Contextos:	*advfirewall, bridge, dhcpclient, dnscliente, http, interface, ipsec, lan, wlan*	
	Opciones:	*set, show, add, delete, exec*	
	Ejemplo:	**netsh** interface show interface *#Muestra interfaces de red*	
netstat	*Muestra estadísticas y datos sobre conexiones TCP/IP*		
nslookup	*Envía una solicitud DNS sobre una IP*		
ping	*Envía una solicitud de eco mediante ICMP*		
route	*Muestra la tabla de enrutamiento*		
tskill	*Termina un proceso en un ordenador remoto*		

GESTIÓN DE USUARIOS WINDOS (Active Directory)	
GESTIÓN DE USUARIOS (CMD)	
net user [opciones] **usuario**	
net user pepe ***** *#Cambia la contraseña del usuario pepe*	
Opciones:	*/DOMAIN, /ADD, /DELETE, /TIMES (horas permitidas), /ACTIVE:no*

net localgorup [grupo] **usuario**		
net localgroup administradores *#Muestra info del grupo administradores*		
Opciones:	*/ADD, /DELETE*	
GESTIÓN DE USUARIOS (POWERSHELL)		
Get-LocalUser [**-Name** nombreusuario] #Lista las cuentas de usuarios locales		
Get-LocalUser -Name pepe #Muestra información del usuario pepe		
New-LocalUser [opciones]		
New-LocalUser "User01" -Password $Password -FullName "Pepe Ramirez"		
-AccountExpires	*-Disabled*	*-NoPassword*
-AccountNeverExpires	*-FullName*	*-Password*
-Description	*-Name*	*-PasswordNeverExpires*
Set-LocalUser [opciones]		
Set-LocalUser -Name "Admin01" -Description "Cambio descripcion de la cuenta"		
-AccountExpires	*-FullName*	*-Password*
-AccountNeverExpires	*-Name*	*-PasswordNeverExpires*
Remove-LocalUser [-Name] nombreusuario *#Elimina una cuenta de usuario local*		
Rename-LocalUser [-Name] nombre [-NewName] nuevonombre *#Modifica el nombre del usuario*		
Disable-LocalUser [-Name] nombreusuario *#Deshabilita la cuenta del usuario*		
Enable-LocalUser [-Name] nombreusuario *#Habilita la cuenta del usuario*		
COMANDOS DE GESTIÓN DE GRUPOS		
Get-LocalGroup [**-Name** grupo]		
Get-LocalGroupMember [**-Name** grupo]		
New-LocalGroup [**-Description** descrip] [**-Name** grupo]		
Add-LocalGroupMember [**-Group** grupo] [**-Member** miembro]		
Set-LocalGroup [**-Description** descrip] [**-Name** grupo]		
Remove-LocalGroupMember [**-Group** grupo] [**-Member** miembro]		
Remove-LocalGroup [**-Name**]]		
Rename-LocalGroup [**-Name**]]		

GESTIÓN DE DISPOSITIVOS MÓVILES	
Modelos de propiedad de los dispositivos según guía CCN-STIC 496:	
BYOD	**Bring Your Own Device**: propiedad del usuario (No existe trazabilidad).
BYOA	**Bring Your Own App**: aplicaciones públicas en sus dispositivos móviles personales
CYOD	**Choose your own device**: permite a los trabajadores la elección del modelo, con control total de la empresa pudiendo permitir su uso para fines personales.
COPE	**Corp. Owned, Personally Enabled**: propiedad de la empresa con espacio personal separado.
COBO	**Corp. Owned, Business Only**: propiedad y control total de la empresa.
Gestión centralizada de los dispositivos:	
MDM	**Mobile Device Management**: gestión de dispositivos móviles.
MAM	**Mobile Application Management**: gestión de las aplicaciones móviles.
MC	**Mobile Content Management**: gestión del contenido móvil.
EMM	**Enterprise Mobility Management**: gestión de la movilidad de la empresa (seguridad y apps).
MTD	**Mobile Threat Defense**: defensa contra las amenazas móviles (seguridad corporativa).
UEM	**Unified Endpoint Management**: gestión unificada de terminales (IoT, móviles, tablets, ect.).

Actualmente se ha evolucionado de MDM a UEM con un servidor centralizado, un software-cliente en cada dispositivo, una base de datos centralizada y una comunicación (**OTA**).
Funciones: Inventario, monitorización, configuración, políticas de seguridad, comunicaciones y apps.

Soluciones Mobile Device Management (MDM):		
AirWatch (VMware).	Meraki (Cisco).	Odyssey (Symantec).
Citrix Endpoint Management.	Microsoft Intune.	Sophos Mobile Control.
Fiberlink MaaS360.	MobileIron.	Trend Micro Mobile Security.

Soluciones Unified Endpoint Management (UEM):		
Citrix Endpoint Management.	Ivanti UEM.	Sophos Mobile.
IBM Security MaaS360 with Watson.	MobileIron UEM.	VMware Workspace ONE.

Guías de Seguridad CCN-STIC

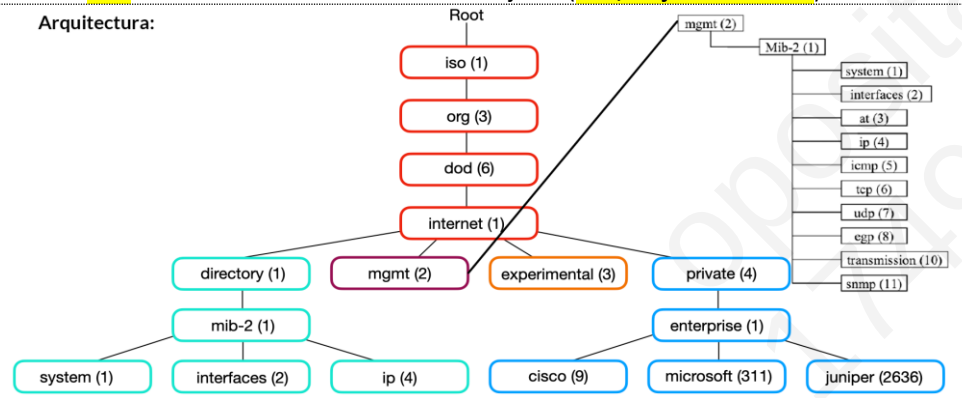
CCN-STIC 496: Sistemas de comunicaciones móviles seguras.
CNN-STIC 827: Gestión y uso de dispositivos móviles.

MONITORIZACIÓN Y CONTROL DEL TRÁFICO	
La ISO define la **gestión de red** como el conjunto de elementos de control y supervisión de los recursos que permiten que la comunicación tenga lugar sobre la red.	
NMS	**Network Management Server**: plataforma de gestión o elemento que supervisa.
NMA	**Network Management Agent**: elemento o host a gestionar o agente.
NME	**Network Management Entity**: nombre del software del agente.
Potocolo	Protocolo de comunicación (CMIP, SNMP o CMOT).
MIB	**Management Information Base**: base de datos de los recursos de los dispositivos a gestionar
Modelo de gestión de red OSI	
Conocido como modelo FCAPS (Fault, Configuration, Accounting, Performance, Security).	
CMIS	**Common Management Information Services**: el servicio para la colección de información.
CMIP	**Common Management Information Protocol**: protocolo OSI que soporta a CMIS.
MIB	**Management Information Base**: la base de datos jerárquica

Servicios de Directorio	define las funciones necesarias		
Modelo de gestión de red TCP/IP			
Potocolos	**SNMP** Simple Network Management Protocol	**CMIP** sobre TCP/IP (CMOT)	
Los dos protocolos emplean la misma base de administración de objetos MIB (Mgmt. Info. Base).			
Modelo de gestión de red TMN por la ITU-T			
Modelo de gestión de red MTNM			

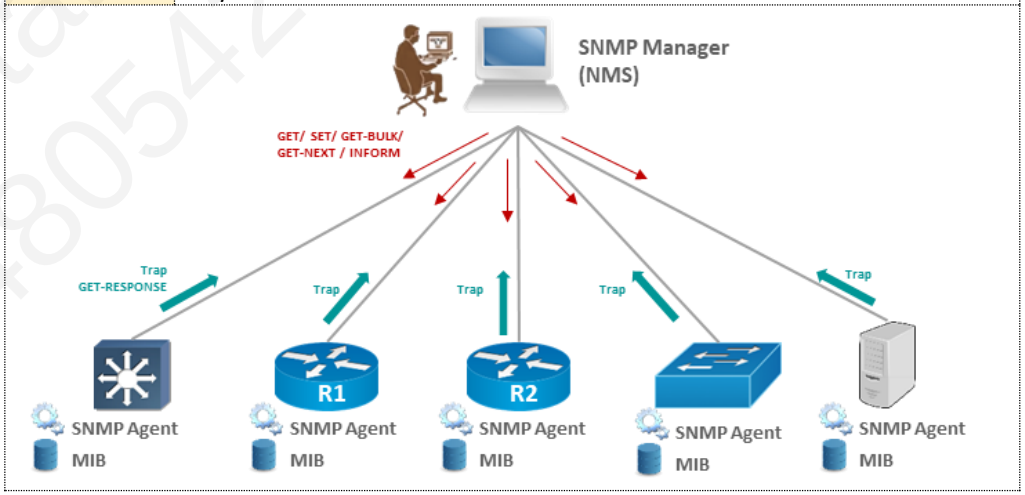
SNMP Simple Network Management Protocol			
El Protocolo Simple de Administración de Red o **SNMP (Simple Network Management Protocol)** es un protocolo de nivel de aplicación (capa 7 del modelo OSI) y enviada sobre UDP (capa de transporte). SMPM puede trabajar tanto de forma síncrona **(Polling: GET / SET)** cómo asíncrona (**TRAP**).			
Puerto UDP 161:	GESTOR -> AGENTE	Sondeo **GET / SET**	síncrona
Puerto UDP 162:	AGENTE -> GESTOR	Interrupción (TRAP)	asíncrona
La **SMI (Structure of Management Information)** define la estructura jerarquica de la MIB, es decir, la sintaxis y semántica de los objetos de la MIB. Utiliza como notación un subconjunto de ASN.1 para describir datos transmitidos. Para obtener/establecer la información de gestión se usa el método de identificadores de objetos (**OID, Objetc IDentifier**).			

Arquitectura:



MIB-II y extensiones	Dentro de la rama internet (OID 1.3.6.1)
mgmt(2):	contiene definiciones de información aprobadas
private(4):	rama en la que se pueden añadir extensiones.
experimental(3):	objetos experimentales que en un futuro podrían pasar al subárbol mgmt.

SNMPv1	RFC 1157, utiliza el protocolo UDP con las siguientes posibilidades **GET, SET y TRAP.** Se basa en el concepto de **community string** como un método de seguridad. Operaciones: GetRequest, GetNextRequest, SetRequest, GetResponse y Trap.
SNMP v2	RFCs 1441-1452, 3416-3417), puede soportar tanto gestión centralizada como distribuida. Operaciones: GetBulkRequest, InformRequest y Report (sin desarrollar).
Seguridad	**SNMPsec** (Party-based SNMPv2) — **SNMPv2*** (no se estandarizó) **SNMPv2c** (Community-based SNMPv2) — **SNMPv2u** (User-based SNMPv2)
SNMP v3	RFCs 3410-3415, elimina el concepto de **community string** y se enfoca principalmente en la seguridad (autenticación, privacidad y control de acceso). Seguridad basada en usuarios o **USM** (User Security Model). Modelo de control de acceso basado en vistas o **VACM** (View-based Access Control Model).
RMON v2	**Remote MOnitoring**, usa una sonda tradicionalmente conocidos como sniffers.
SMON	**Switched MONitoring**, parte de RMON, capaz de gestionar los dispositivos de red y VPNs.



Herramientas de monitorización y control de tráfico			
Nagios®	Solarwinds	OpenNMS	Sampled Flow (sFlow)
Pandora FMS	Zenoss	Whatsup Gold	Check_MK (Checkmk)
Otras herramientas:	Cacti	Wireshark	MRTG (Multi Router Traffic Grapher)
SATAN (System Administrator Tool for Analyzing Networks)		Nmap	Microsoft Message Analyzer

Bloque 4 - Tema 5: SEGURIDAD, CPD Y CRIPTOGRAFÍA

CONCEPTOS DE SEGURIDAD DE LOS SISTEMAS DE INFORMACIÓN

Se define SEGURIDAD como la capacidad de resistir accidentes o acciones tanto internos como externos que comprometan los datos. Es por ello que es necesario proteger las diferentes DIMENSIONES de seguridad:

(**CITAD**) **C**onfidencialidad, **I**ntegridad, **T**razabilidad, **A**utenticidad, **D**isponibilidad.

Amenazas según la Seguridad de las Tecnologías de la Información y Comunicaciones (**STIC**):

INTERRUPCIÓN (disponibilidad)	**MODIFICACIÓN** (integridad)
INTERCEPTACIÓN (confidencialidad)	**FABRICACIÓN** (original y la fabricada)

Medidas según la Guía de Seguridad de las TIC **CCN-STIC 400** Manual STIC:

TRANSEC (Transmisiones)	**NETSEC** (Redes)
COMPUSEC (Ordenadores)	**CRYPTOSEC** (Criptológica)
EMSEC (Emisiones)	

Normativas:

ISO 31000 (Gestión de riesgos).	**UNE 71504**:2008 (Metodología).
UNE-ISO/IEC Guía 73:2010 (Vocabulario).	

Conceptos:

Sistema de información: Según **MAGERIT**, es el conjunto de elementos físicos, lógicos, elementos de comunicación, datos y personal.

Sistema de Gestión de la Seguridad de la Información (SGSI): Conjunto de políticas, procedimientos y directrices junto a los recursos y actividades asociados en la búsqueda de proteger sus activos de información esenciales.

Activo: componente o funcionalidad susceptible de ser atacado deliberada o accidentalmente con consecuencias para la organización.

Vulnerabilidad: debilidad o fallo de un sistema que puede ser aprovechado con fines maliciosos.

Amenaza: Causa potencial de un incidente o circunstancia desfavorable que puede ocurrir con consecuencias negativas sobre los activos provocando indisponibilidad o funcionamiento incorrecto.

Ataque: acción deliberara o intento de destruir, exponer, alterar un sistema de información.

Impacto: efecto o consecuencia produce un incidente, desastre, problema o cambio en los SLA y cómo se ven afectados en el caso de que se materialice dicha amenaza.

Análisis de impacto: estudio de las consecuencias que tendría una parada de X tiempo.

Riego: posibilidad de que una amenaza o vulnerabilidad se convierta en un daño real. Tipos: acumulado, potencial, repercutido y residual. **RIESGO = IMPACTO X PROBABILIDAD.**

Análisis de riesgos: proceso que comprende la identificación de activos, vulnerabilidades, amenazas, probabilidad e impacto a los que se encuentran expuestos.

Gestión de riesgos: actividades coordinadas e implantación de salvaguardas para conocer, prevenir, impedir, reducir o controlar los riesgos.

Incidente: suceso que afecte a la confidencialidad, integridad o disponibilidad de los activos.

Salvaguarda: procedimientos o mecanismos tecnológicos que reducen el riesgo.

MAGERIT (requisito mínimo de seguridad del ENS)

MAGERIT versión 3 es la **Metodología** de Análisis y Gestión de Riesgos de Sist. De Información. Consta de 3 libros y es un instrumento para facilitar la implantación y aplicación del ENS.
Se alinea con la norma **ISO 31000**. **PILAR** es una herramienta que implementa MAGERIT.

Serie ISO 27000 (certificación de los SGSIs).

Conjunto de guías para implantación, mantenimiento, auditoría y certificación. **ISO/IEC 27000-27799**

ISO 27001 (requisitos)	ISO 27003 (críticos)	ISO 27006 (auditoría)	ISO 27018 (P. Datos)
ISO 27002 (objetivos)	ISO 27004 (métricas)	ISO 27017 (C. Computing)	ISO 27030 (IoT)

Evaluación de seguridad de productos - Common Criteria (CC)

Para medir el nivel de seguridad de las TIC se utiliza la norma ISO/IEC 15408, también conocida como **Common Criteria (CC)** que define los criterios de evaluación para la seguridad.
El Common Criteria establece 7 niveles de confianza (**EAL**, Evaluation Assurance Level):

EAL0: sin garantías.	**EAL4**: diseñado, probado y revisado metódicamente.
EAL1: probado funcionalmente.	**EAL5**: diseñado y probado semiformalmente.
EAL2: probado estructuralmente.	**EAL6**: diseñado, probado y verificado semiformalmente.
EAL3: probado y chequeado metódicamente.	**EAL7**: diseñado, probado y verificado formalmente.

LINCE es una metodología desarrollada por el CCN y basada en los principios de Common Criteria.

SEGURIDAD FÍSICA

Conjunto de medidas usadas para proporcionar protección física a los recursos contra amenazas intencionadas o accidentales.

Protección de las instalaciones e infraestructuras:

Control de accesos físico	Climatización	Protección frente a inundaciones
Áreas de trabajo separadas	Acondicionamiento de los locales	Registro de entradas y salidas
Energía eléctrica	Protección frente a incendios	Instalaciones alternativas (respaldo)

Protección de los equipos:

Puestos de trabajo despejados	Protección de equipos portátiles
Bloqueo de puestos de trabajo	Medios alternativos

Protección de los soportes de información:

- Las unidades de **almacenamiento** deben ser **etiquetadas**, estar **cifrada** (criptografía), **custodiadas** y establecer un mecanismo de **borrado seguro** datos **y destrucción** de los soportes.
- **Redundancia de discos**: RAID.

SEGURIDAD LÓGICA		
Uso de software y los sistemas, la protección de los datos, procesos y programas, así como la del acceso ordenado y autorizado de los usuarios a la información.		
Control de acceso:		
Identificación	Permisos y ACLs	Mecanismos de autenticación
Acceso usuario/password	Segregación de funciones	Intentos de acceso: limitados
Explotación:		
Protección frente a código dañino: antivirus.	Registro de las actividades de los usuarios.	
Protección de las comunicaciones:		
Perímetro seguro (firewalls)	Autenticidad y de la integridad	Medios alternativos
Protec. de la confidencialidad	Segregación de redes (DMZ)	Monitorización
Protección de las aplicaciones informáticas:		
Desarrollo (seguridad integral)	Aceptación y puesta en servicio (análisis de vulnerabilidades)	
Protección de los servicios:		
Protección del correo electrónico	Protección de servicios y aplicaciones web	
Protección frente a la denegación de servicio (frente a ataques DoS y DDoS)		

AMENAZAS		
Causa potencial de un incidente que puede causar daños a un sistema de información.		
SOFTWARE MALICIOSO (MALWARE):		
Virus	Rogueware (falsa desinfección)	**Troyanos**:
Gusano (copias)	Criptojacking (criptomonedas)	- Puerta trasera (backdoor)
Bomba lógica	Adware (múltiples ventanas)	- Keylogger (teclado,)
Código móvil malicioso	Rootkit (ocultar intrusión)	- Stealer (información privada)
Botnet(red zombi)	Spyware y Joke	- Ransonware (secuestra datos)
ATAQUES A CONTRASEÑAS:		
Fuerza bruta	Ataques por diccionario	
ATAQUES POR INGENIERÍA SOCIAL		
Spam	Baiting o Gancho (cebo)	Phishing (email)
Shoulder surfing (mirar por encima del hombro)	Dumpster diving (buscar en la basura del usuario)	Vishing (llamadas)
		Smishing (sms)
ATAQUES A LAS CONEXIONES		
Ataques a cookies	Pharming (web falsa)	Secuestro de sesión
Ataque piggyback	Ping mortal	Man in the middle
Ataque smurf	Portscan	**Ataques DoS:**
Clickjacking	Redes trampa	- TCP SYN attack
Inyección SQL	Sniffing	- SYN Flood (inundando)
IP, ARP, MAC, Web, Mail y DNS Spoofing (suplantar)	Secuestro de DNS (domain hijacking)	- ICMP Flood
Envenenamiento de DNS (DNS cache poisoning)	Envenenamiento del motor de búsqueda (search engine poisoning)	
OTROS ATAQUES		
Amenazas avanzadas persistentes (APT) ciberespionaje	Exploit (vulnerabilidad)	

SOLUCIONES DE C IBERSEGURIDAD						
Soluciones desarrolladas por el CCN para garantizar la seguridad de los sistemas.						
ADA	Plataforma de análisis avanzado de malware.					
- MARTA	Análisis **dinámico**		- MARÍA	Análisis **estático**		
AMPARO	Implantación de seguridad y conformidad del ENS.					
ANA	**A**utomatización y **N**ormalización de **A**uditorías.					
ANGELES	Portal de formación y talento en ciberseguridad.					
ATENEA	Plataforma de desafíos de seguridad (ATENEA Escuela).					
CARLA	Protección y trazabilidad del dato.					
CARMEN	Defensa de ataques avanzados/APT.					
CCNDroid	Seguridad para Android (Wiper y Crypter).					
CLARA	Auditoría de Cumplimiento ENS/STIC en Sistemas Windows.					
CLAUDIA	Herramienta de detección de amenazas complejas en puesto de usuario.					
microCLAUDIA	Centro de vacunación.					
ELENA	Simulador de técnicas de cibervigilancia.					
EMMA	Visibilidad y control sobre la red.					
GLORIA	**G**estor de **L**ogs, basado en SIEM (Sec. Information and Event Mgnt).					
INES	**IN**forme de **E**stado de **S**eguridad en el ENS.					
IRIS	Estado de la ciberseguridad del sector público.					
LORETO	Almacenamiento en la nube.					
LUCIA	Sistemas de Gestión Federada de Tickets.					
MARIA	Plataforma Multiantivirus en tiempo real.					
MARTA	Análisis avanzados de ficheros.					
MONICA	Gestión de eventos e información de seguridad.					
OLVIDO	Borrado seguro de datos.					
metaOLVIDO	Gestión de metadatos.					
PILAR	Análisis y Gestión de Riesgos (**MAGERIT**).					
- PILAR Basic	PYMES.	- microPILAR	rápidos.	- RMAT	Extensiones.	
REYES	Intercambio de Información de Ciberamenazas.					
ROCIO	Inspección de Operación. Auditoría de configuraciones de dispositivos de red.					
VANESA	Grabaciones y emisiones de **V**ídeo en streaming.					

INFRAESTRUCTURA FÍSICA DE UN CPD

CPD (Centro de Proceso de Datos) o Data Center donde se concentra el equipamiento de servicios TIC.

Zonas de un CPD

Centro de operaciones (técnicos de soporte).	Sala principal o Sala TI (armarios rack).
Sala de entrada (almacenes y carga).	Otras zonas (áreas de distribución).

Elementos de CPDs

ORGANIZACIÓN FÍSICA

Racks	Patch panel	Suelos técnicos elevados	Falsos techos
1U = 1.75" / 44.45 mm	*Categoría 6A y OM4*	*estándar 60x60cm*	

ALIMENTACIÓN ELÉCTRICA

SAI (Sist. Alimentación Ininterrumpida)	Grupo electrógeno (exterior)	PDU (Power Distribution Unit)	Cuadros eléctricos (A y B)

CLIMATIZACIÓN

HVAC (Heating, Ventilation, and Air Conditioning)	**CRAC** (Computer Room Air Conditioners)

Free cooling (utilizar las bajas temperaturas del aire exterior)

CONFIGURACIONES

Pasillo Frío – Pasillo Caliente	Pasillo Cerrado (PODs modulares)

INFRAESTRUCTURA DE PROCESAMIENTO

SERVIDORES

Clusters de balanceo de carga	Clusters de alta disponibilidad	Clusters de alto rendimiento
Servidores Blade	Servidores en rack	Independientes (stand alone)

CERTIFICACIÓN DE CPDs

En 2005 se publicó la Norma ANSI TIA 942 basado en recomendaciones del Uptime Institute se establecen 4 niveles (tiers) según los distintos grados de disponibilidad para cada uno de los cuatro subsitemas (Telecomunicaciones, Arquitectura, Sistema eléctrico y Sistema mecánico).

	Tier I	Tier II	Tier III	Tier IV
Tipo	BÁSICO	REDUNDANTE	CONCURRENTE	TOLERANTE A FALLOS
Redundancia	N	N+1	N+1	2(N+1)
Nº de líneas	1	1	2 (1 activa)	2 activas
Disponibilidad	**99,67**1%	**99,74**1%	**99,98**2%	**99,99**5%
% de parada	0,329%	0,251%	0,018%	0,005%
T. parada al año	28,82 horas	22,68 horas	1,57 horas	26,28 minutos

La tasa de disponibilidad máxima del datacenter es 99,995% del tiempo.

TÉCNICAS CRIPTOGRÁFICAS

La criptografía debe garantizar la confidencialidad, la integridad y la autenticidad (no repudio.)

Criptografía	diseña procedimientos para cifrar (ocultar o enmascarar información).
Criptoanálisis	atacar los procedimientos de cifrado para extraer la información.
Lema de Kerckhoffs	La seguridad de cifrado debe residir, exclusivamente, en el secreto de la clave y no en el desconocimiento del algoritmo.

Métodos criptográficos de clave SIMÉTRICA (cifrado)

La clave de cifrado coincide con la clave de descifrado (Kc=Kd). Son muy rápidos.
Requieren **n(n-1)/2** claves diferentes para establecer comunicaciones seguras de cada usuario.

Algoritmo	Tipo	Observaciones	Algoritmo	Tipo	Observaciones
RC4	Flujo	WEP, WPA y SSL	AES o Rijndael	Bloque	128, 192 o 256 bits
A5/1 y A5/2		GSM	Camelia		128, 192 o 256 bits
E0		Bluetooth	DES		56 bits
Rabbit		128 bits	Triple DES		56, 112 o 168 bits
SNOW3G		128 bits	IDEA		128 bits
Salsa		256 bits	Blowfish		32 y 448 bits
Grain		80 bits	Twofish		128, 192 o 256 bits
Trivium		80 bits	RC2, RC5 y RC6		8 - 256 bits
			Skipjack		80 bits
El cifrado se aplica sobre cada bit del texto plano.			GOST		256 bits
			Modos de cifrado (ECB, CBC, CFB, OFB y CTR)		

Métodos criptográficos de clave ASIMÉTRICA (firma digital)

La clave de cifrado es diferente a la de descifrado (Kc != Kd). Usa clave PÚBLICA y clave PRIVADA.
Son muy lentos y requieren sólo **2n** claves (n claves públicas y n claves privadas).
Aunque pueden usarse para **Cifrado** (confidencialidad) **y** para **Firma digital** (integridad, autenticidad y no repudio), para el cifrado se recomienda el uso de clave simétrica por ser más rápido.

Algoritmo	Tipo	Observaciones	Algoritmo	Tipo	Observaciones
RSA	Factorización	Cifrar y firmar	ElGamal	Log. discreto	Cifrar y firmar
Diffie-Hellman	Logaritmo discreto	Sólo firmar	ECDH	Curvas elípticas	256, 384 y 512 bits
DSA		Sólo firmar	ECDSA		

PKCS es un conjunto de estándares publicados por RSA Security. De la PKCS #1 a la PKCS #15
PKCS #11: Estándar de interfaz de dispositivo criptográfico.
PKCS #13: Estándar de criptografía de curva elíptica.
PKCS #14: Generación de números pseudoaleatorios..

Método o esquema híbrido

Se utiliza la criptografía de clave asimétrica para las claves y el cifrado simétrico para los datos. Usa una clave pública para cifrar la clave de sesión y cifra simétricamente los datos.

Función Resumen o Hashing

Con el fin de ahorrar tiempo de computación, lo que se suele hacer es firmar un resumen (de longitud fija) del documento mediante una función Hash. Compresión, difusión y resistencia.
Aplicaciones de las funciones hash: MDC, MAC, firma digital y marca de tiempo TSA.

Algoritmo	Observaciones	Algoritmo	Observaciones
DSA	128 bits	Whirpool	512 bits
MD5	128 bits	Tiger	192 bits
SHA-1	160 bits	RIPEMD-160	160 bits
SHA-2	Hasta 512 bits	RIPEMD-256	256 bits
SHA-3	Hasta 512 bits	RIPEMD-320	320 bits

Formatos de firma digital

CAdES (CMS Avanzado)	Formato de salida binario, adecuado para fichero grandes.
Firmas implícitas/attached (inc. documento el original) y explícitas/detached (no incluye el doc.).	
XAdES (XML Avanzado)	Formato de salida XML, no es adecuado para fichero grandes. Firmas despegadas, envolventes o envueltas.
Firmas despegadas (no incluye el doc.) , envolventes o envueltas.	
PAdES (PDF Avanzado)	Cuando el documento original es un pdf. El contenido y firma se incluyen bajo el mismo fichero.
OOXML (Office Open XML)	formato de firma que utiliza Microsoft Office.
ODF (Open Document Format)	formato de firma que utiliza Open Office.
La aplicación cliente **AutoFirma** permite configurar el formato a utilizar.	

Firmas simples (un solo firmante)	Co-firma o en paralelo (múltiples)	Contra-firma o cascada (refrendo)
HMAC	Técnica de autenticación de mensajes que incluye una clave secreta, detectando la manipulación del contenido al tiempo que se chequea una clave de autenticación.	

PROTOCOLOS SEGUROS

SSH (Secure Shell)	Nombre de protocolo y del programa que lo implementa Puerto por defecto **TCP 22**. Hace el uso de contraseñas ordinarias, autenticación de clave pública basada en DSA, RSA y certificados X.509, Kerberos, etc. Clientes: PuTTY, KiTTY, Bitvise SSH Client y OpenSSH. Servidor: Bitvise SSH Server (solo Windows) y OpenSSH (Windows/Linux).
SFTP (SSH File Transfer Protocol)	Hace uso de SSH (autenticación y cifrado de datos) para crear un único canal. Puerto por defecto **TCP 22**. Clientes: Filezilla, CrossFTP, SmartFTP, Core FTP, Bitvise SSH, CyberDuck, WinSCP, Commander One, Viper FTP, etc.
FTPS (FTP sobre SSL/TLS)	Extensión de FTP que utiliza la capa SSL/TLS por debajo de FTP para establecer los canales de comunicación seguros (2 canales). FTPS explícito (FTPES): puerto **TCP 21** (control) y puerto **aleatorio** (datos). FTPS implícito: puerto **TCP 990** (control) y puerto **TCP 898** (datos). Clientes: Filezilla, CrossFTP, Core FTP, WinSCP, Commander One, Viper FTP, etc.
SCP (Secure Copy Protocol)	Transfiere de forma segura ficheros entre dos equipos. Basado en RCP. Puerto por defecto **TCP 22**. Clientes: WinSCP (Windows) y del shell (Linux y macOS).

SISTEMAS DE GESTIÓN DE INCIDENCIAS

Una incidencia es toda interrupción o reducción de la calidad no planificada del servicio.
Un **Centro de Atención a Usuarios** (**CAU**) o como "**Help Desk**".
El estándar de gestión de usuarios y CAU es **ITIL** (**Information Technolgy Infrastructure Library**).

Zendesk.	Jira Service Desk.	Freshservice.	Deskero.
osTicket (open source).	OTRS.	ServiceTonic.	cDesk.
GLPI (open source).	Zoho Desk.	SysAid.	cDesk.
MantisBT (open source).	Freshdesk.	Solarwinds Service Desk.	Redmine.

CONTROL REMOTO DE PUESTOS DE TRABAJO

Permite al usuario controlar de forma remota un equipo de la organización.

Protocolos de comunicación:

RDP (Remote Desktop Protocol):	desarrollado por Microsoft (**puerto 3389**).
Escritorio Remoto de Windows	Apple Remote Desktop
FreeRDP (Apache)	Microsoft Remote Desktop (para macOS.)
VNC (Virtual Network Computing):	se basa en el concepto de framebuffer o RFB (Remote Frame Buffer). Por defecto **puerto 5900, 5800 o 5500**.

TeamViewer (**5938**)	TigerVNC	AnyDesk	Dameware Mini Remote Control
Real VNC	TurboVNC	Splashtop	
TightVNC	UltraVNC	Supremo	

Bloque 4 - Tema 6: COMUNICACIONES Y REDES MOVILES

COMUNICACIONES	
Analógicas	
Señal representable mediante una función matemática continua en la que varía su amplitud y período. Amplitud (AM), Fase (PM), Frecuencia (FM). **Amplitud**: voltaje, potencia de la señal. **Periodo**: tiempo, en segundos, que necesita una señal para completar un ciclo. **Frecuencia**: número de periodos por segundo. Se mide en hercios (Hz). Para transmitir una señal analógica por un medio digital usamos modulación de código de pulso/modulación por impulso codificado (PCM - Pulse Code Modulation) que tiene 3 fases: muestre, cuantificación y codificación.	
Digitales	
La señal no puede cambiar continuamente ni puede tomar cualquier valor, sino que se compone de un conjunto determinado de valores discretos. Codificación unipolar, polar, bipolar, multinivel y por bloques.	
Principales conceptos de una señal:	
Capacidad del canal:	teorema de muestreo de Shannon-Hartley: C = B x log2(1 + S/N). El ancho de banda está sometido a la presencia de la interferencia del ruido.
Longitud de onda:	distancia entre dos puntos equifásicos consecutivos de la misma.
Frecuencia:	número de oscilaciones de una señal por segundo. Se mide en hercios (Hz).
Deterioro en la transmisión	
Interferencia:	superposición de señales que forman otra diferente.
Diafonía o crosstalk:	tipo especial de interferencia, un circuito que se acopla en otro próximo. Diafonía NEXT (Near-end crosstalk) dentro del mismo cable.
Power-Sum NEXT:	varios pares trenzados molestan a un par dentro del mismo cable.
Diafonía Alien:	interferencia ocasionada por la cercanía de otros cables de red.
Ruido:	señal externa que se suma a la transmitida corrompiéndola.
Desfase:	consecuencia de las diferentes velocidades de propagación de una señal.
Atenuación:	pérdida de potencia de la señal transmitida.
Técnicas de conmutación	
Redes de Conmutación de Circuitos: RTB / RDSI	
Se establece un camino físico entre el origen y el destino. Se reservan recursos. durante el tiempo que dure la transmisión de datos. Este camino es exclusivo para los dos extremos de la comunicación, no se comparte con otros usuarios (ancho de banda fijo).	
Analógicas (RTB):	Comunicaciones a través de líneas telefónicas analógicas.
Digitales (RDSI):	Funcionan mediante conmutación de circuitos. Canal B de 64 Kbps para datos. Protocolos HDLC y PPP. Canal D de 16/64 Kbps para señalización. Protocolo LAPD.
Redes de Conmutación de Paquetes	
Los mensajes se fragmentan en paquetes y cada uno de ellosse envía de forma independiente desde el origen al destino. La pérdida de un paquete provocará que se descarte el mensaje completo. Multiplexación, aprovechamiento total de los recursos, permite varias comunicaciones de forma simultánea, aprovechando recursos libres.	
Datagramas:	No orientado a conexión. No hay garantía de entrega. Los paquetes podrían llegar desordenados. Ej: IP.
Circuitos Virtuales: Tipos:	Orientado a conexión. Existe un establecimiento de ruta. Podrán ser permanentes (clientes importantes) o conmutados. Ej: ATM, Frame Relay / MPLS / X.25
ATM	ATM se creó para proporcionar a las aplicaciones que tuviéramos por encima distintos tipos de servicios. ATM tipifica el tráfico. En ATM, para poder comunicarte, debes establecer antes el circuito. Los PVC (Permanent Virtual Circuit) siempre están abiertos. Los SVC (Switched Virtual Circuit) deben abrirse en cada sesión. UNI: interfaz entre el cliente final y la red del proveedor. NNI: interfaz entre los nodos del proveedor. ATM intenta evitar el routing dinámico, de modo que la información vaya siempre por el mismo camino establecido, lo que le da mayor velocidad. Hay routing, pero al principio, al establecer el camino. El tamaño de una celda ATM es de 53 octetos = 48 + 5. 48 octetos para el payload y 5 para la cabecera.
FRAME RELAY	Tamaño de paquete de datos variable. Cabecera de 6 octetos, 48 bits en total. Campo Address de 16 bits. Cuando se contrata, el operador te da un CIR y un DLCI: • CIR: Ancho de banda garantizado. • DLCI: Data Link Connection Identifier. Identificador de cliente. LAPF es el protocolo de enlace en el plano de usuario, para el intercambio de datos. LAPD es el protocolo en el plano de control, para intercambiar información de red.
MPLS	**Multi-Protocol Label Switching**. Diseñado para unir el transporte entre redes basadas en circuitos y basadas en paquetes. Las redes MPLS ofrecen transporte de datos de una forma muy privada. El tráfico se etiqueta cuando entra en la red, para que no se enrute. Tráfico IP etiquetado. Una vez generadas las etiquetas para establecer el camino, a los routers ya les da igual que lleven direcciones IP, ya que no harán routing al estar el camino fijado. MPLS se sitúa en el nivel 2.5. Por un lado, permite encapsular en él tráfico IPv4 e IPv6. Por otro lado, se integra muy bien con tecnologías de nivel de enlace (ATM, FR, HDLC, etc). Convergencia multiprotocolo entre nivel 2 y 3. Nexo de unión entre nivel 2 y 3.
Redes de difusión	

Es aquella en la que el medio es compartido por las estaciones que forman la red. Todos los equipos reciben todos los paquetes, aunque solo procesan los dirigidos a ellos. Ej: LAN BUS, Wireless, etc.

Redes de punto a punto

Son aquellas que responden a un tipo de arquitectura de red en las que cada canal de datos se usa para comunicar únicamente dos computadoras. LAN Estrella.

MULTIPLEXACION

Técnica para mezclar y enviar múltiples flujos de datos a través de un medio. Técnica para aprovechar un canal. Requiere de dos elementos:
multiplexor (MUX) para multiplexar los flujos y demultiplexor (DEMUX) que toma la información del medio y la distribuye a sus destinos.
Varios tipos de multiplexación: en frecuencia, por longitud de onda (WDM), en tiempo, por división en código.

MEDIOS DE TRANSMISION

Un medio de transmisión es el material o soporte que compone el canal por el cual enviamos datos de un lugar a otro. Según la necesidad o no de utilizar un soporte físico hablamos de medios guiados (señales eléctricas u ópticas) o no guiados (radioeléctricas).

MEDIOS GUIADOS: CABLES

Los medios guiados conducen (guían) las ondas a través de un camino físico.

Coaxial	Desplazados por los cables de par trenzado. Velocidades bajas. Dos opciones : Thick y Thin.
Par trenzado	formado por uno o más pares de hilos de cobre, aislado cada uno y trenzados entre sí para reducir el efecto de la diafonía. Voz mínimo 2 pares. Datos habitualmente 4 pares (8 hilos). Conector RJ-45 hasta categoría 6. GG-45 para categoría 7.
UTP	los pares no cuentan con ningún tipo de cobertura. Categoría 1 y 2.
STP	blindaje individual en cada par, mejorando la protección frente a la diafonía.
FTP	se usa un apantallado exterior para el conjunto de cables de aluminio y plástico.
SFTP	se usa un apantallado exterior y blindado con una malla metálica contectada a tierra.
SSTP	tienen blindaje individual de aluminio en cada par y a su vez está apantallado y blindado ext.

Categorías según Norma TIA/EIA 568 e ISO/IEC 11801

Categoría	Velocidad	MHz	Clase	Conector	Distancia
5	100 Mbps	100 MHz		RJ45	100 m
5e	1 GBps		D		
6	1 GBps	250 MHz	E		
6A	10 GBps	500 MHz	E		
8.1	25 GBps	2000 MHz	8.1		30 m
8.2	40 GBps		8.2	GG45/TERA	

Fibra óptica	**Monomodo**: Necesita un láser. Clasificación ISO: OS1 y OS2. Se propaga una única longitud de onda de luz en el núcleo de fibra. No hay solapamientos. Mayores anchos de banda. Mayor velocidad. **Multimodo**: necesita un led. Clasificación ISO: OM1, OM2, OM3 y OM4 (10 Gbps). Núcleo de mayor diámetro que permite el paso de múltiples modos de luz. Mayor facilidad de conexionado. Menor coste de equipamiento. Menor ancho de banda. Menor velocidad. El rebote hace que sea más lento.

Nombre	Tipo	Distancia	Velocidad
OS1	Monomodo	10km	10 Gbps
OS2		200km	10 Gbps
OM1	Multimodo	300m	100 Mbps
OM2		500m	10 Gbps
OM3		1500 m a 1 Gbps o 300 m a 10 Gbps	
OM4		550m	10 Gbps

Transceptor: es un adaptador de medios.
GBIC es el transceptor antiguo para el conector SC. SFP es el nuevo que usa LC.

Last Mile: distribución a los usuarios finales.

FTTx (Fiber-To-The-x)	FTTH (Home)	FTTB (Building)	FTTO (Office)

En FTTH se usan redes de fibra óptica especiales llamadas pasivas (PON), porque no hay elementos como routers hasta casa.

GPON: es el ONT (terminal de fibra), los cuales se conectan al OLT. Los splitters se consideran elementos pasivos. Se usa multiplexación WDM para mezclar varios canales de varios usuarios.

No guiados	Transmitidas sin ningún medio físico, sino que se transmiten por el aire. Radiofrecuencia (regulado por ley), Microondas (directa), Infrarrojos (IrDA).

MODOS DE COMUNICACIÓN

TIPOS DE TRANSMISIONES

Paralelo:	Bits organizados en grupos de longitud fija. Emisor y receptor conectados al mismo número de líneas de datos (cable de mismo número de hilos).
Serie:	Bits enviados de uno en uno de forma encolada. Dos modos posibles asíncrona y síncrona.

SINCRONIZACIÓN DE LA TRANSMISION

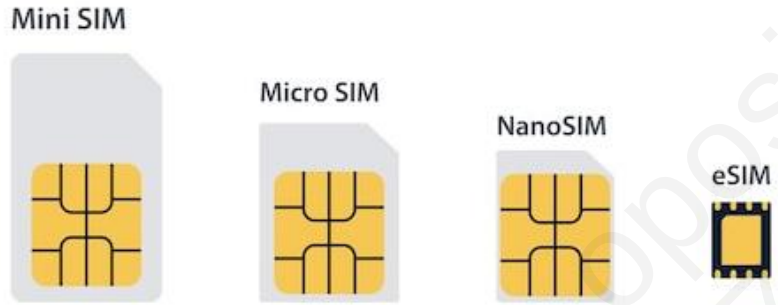
Síncrono	Transferencia de bloques de datos con una temporización continua y coherente.
Asíncrono	No requiere una sincronización activa entre el receptor y el emisor.

SENTIDO DE LA TRANSMISION	
Simplex	Comunicación entre extremo y extremo en un solo canal (unidireccional).
Semi-duplex	(Half Duplex): es una comunicación en ambos sentidos pero no simultáneamente.
Duplex	(Full-duplex): los datos se transmitan en ambas direcciones al mismo tiempo.

MULTIPLEXACION

Técnica para mezclar y enviar múltiples flujos de datos a través de un medio. Técnica para aprovechar un canal. Requiere de dos elementos:
multiplexor (MUX) para multiplexar los flujos y demultiplexor (DEMUX) que toma la información del medio y la distribuye a sus destinos.
Varios tipos de multiplexación: en frecuencia, por longitud de onda (WDM), en tiempo, por división en código.

REDES MOVILES				
	2G (GPRS)	**3G (UMTS)**	**4G (LTE)**	**5G**
Año	1993	2001	2009	2018
Velocidad	64 Kbps	43 Mbps	1 Gbps	20 Gbps
Tecnología	GSM	WCDMA	LTE, WiMAX	MIMO
Sistema de acceso	TDMA, CDMA	CDMA	CDMA	OFDMA

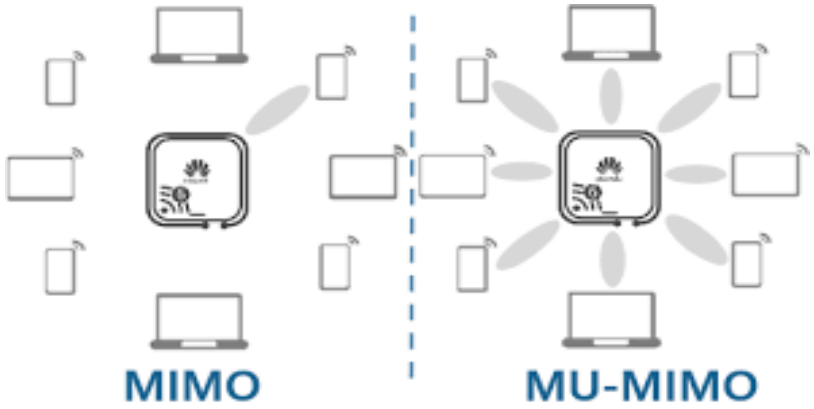


SISTEMAS DE ACCESO MULTIPLE	
FDMA:	División en frecuencia. Necesitan banda de guarda.
OFDMA:	División en frecuencia ortogonal. Dos señales ortogonales se pueden solapar.
TDMA:	División en el tiempo. No necesitan banda de guarda. Mayor rendimiento.
CDMA:	División de código. Todos emiten al mismo tiempo y en todo el rango de frecuencias.

A cada señal se le asigna un código aleatorio único, ortogonal, llamado **CHIP**. El código se mezcla con la señal de datos para hacerla única. El destinatario puede distinguirlas y separarlas.

COMUNICACIONES INALAMBRICAS						
Estándar	Alias	Modulación	Flujos	Banda	Mbps	Comentarios
802.11a	WIFI 1	64 QAM	-	5 GHz	54 Mbps	
802.11b	WIFI 2	64 QAM	-	2.4 GHz	11 Mbps	
802.11g	WIFI 3	64 QAM	-	2.4 GHz	54 Mbps	
802.11n	WIFI 4	64 QAM	-	2.4 y 5 GHz	150 Mbps	SU-MIMO
802.11ac	WIFI 5	256 QAM	4	5 GHz	3.5 Gbps	MU-MIMO
802.11ax	WIFI 6	1024 QAM	8	2.4 y 5 GHz	9.6 Gbps	OFDMA.
802.11be	WIFI 7	4096 QAM	16	2.4, 5 y 6 GHz	46 Gbps	
802.16m	WiMax	puede tener una cobertura hasta de 70 km.				
802.15.1	Bluetooth	Hasta 50 Mbps. Versión 5.1: mesh / malla. Banda de los 2.4 GHz.				
802.15.4	ZigBee	Bajo consumo, baja velocidad, bajo tráfico. Topología en malla. Domótica.				
SU-MIMO	Single User Multiple Input Multiple Output.					
MU-MIMO	Multiple User Multiple Input Multiple Output.					

SEGURIDAD	
SSID:	el router va mandando el nombre de la red en la trama Beacon Frame.
WEP:	clave de 64/128 bits. Algoritmo símetrico de cifrado RC4. Usa vector de inicialización (IV).
WPA:	protocolo TKIP que cambia las claves y los (IV) dinámicamente.
WPA2:	utiliza AES como algoritmo de cifrado. 802.11i.
WPA3:	WiFi Easy Connect. WPA3-Personal: clave de 128 bits. WPA3-Enterprise: 192 bits.



MODELO OSI (ISO/IEC 7498-1 o ITU-T X.200)

El modelo **OSI** (**Open Systems Interconnection**) es un modelo conceptual que representa la pila de protocolos de red que encapsulan todos los tipos de comunicación de red en los componentes de software (90%) y hardware (10%). Sus siete capas se centran más en las distintas funciones que se realizan para que las comunicaciones de red funcionen que en la tecnología en sí.

Cada capa impone un formato de datos de intercambio **PDU** (**Protocol Data Unit**) La finalidad era la seguridad. Desventaja: tiene una sobrecarga (overhead) enorme. Cada capa se ocupa de una serie de funcionalidades.

Nemotécnica: **A**lgunas **P**ersonas **S**ostienen que **T**odas las **R**edes son **EF**icaces. **FERTSPA**

Modelo TCP/IP				Modelo OSI		
4	Datos	**APLICACIÓN**	*HTTP, FTP, IRC, SSH, DNS, SMTP, RIP*	**APLICACIÓN**	Datos	**7**
			HTML, Sockets	**PRESENTACIÓN**		**6**
			RPC, NetBIOS, SMB	**SESIÓN**		**5**
3	Segmentos	**TRANSPORTE**	*TCP, UDP, SSL, TLS (Puertos)*	**TRANSPORTE**	Mensajes	**4**
2	Datagramas IP	**INTERNET**	*IP, ARP, ICMP, IPsec*	**RED**	Paquetes	**3**
1	Tramas	**ACCESO A LA RED**	*LLC, HDLC, PP, MAC: Ethernet, WiFi, ATM, Tokeng Ring, Frame Relay, MPLS, EIGRP*	**ENLACE**	Tramas	**2**
	bits		*Cableado, conectores, hardware*	**FÍSICA**	bits	**1**

Nivel MAC	Subcapa de control de acceso al medio incluye los protocolos de redes locales, como Ethernet (802.3) y Wi-Fi (802.11). Controla acceso de los dispositivos físicos al medio y los permisos para transmitir datos.
Nivel LLC	Subcapa de control de enlace lógico que abarca los protocolos utilizados en redes de área extensa como SLDC, HDLC, LAPB, LAPF, PPP y SLIP, que permiten interconectar dos estaciones de un enlace. Encapsula los protocolos de red, controla los errores y sincroniza las tramas.

MAC y **LLC** son subcapas del modelo IEEE, no de OSI. Su equivalencia es nivel 2.

Un PC tiene 7 niveles, pero el router solo los niveles 1, 2 y 3. El PC se comunica con el router a nivel 2.

MODELO TCP/IP

El modelo TCP/IP es un modelo de red que se basa en la estructura de la pila de protocolos de red. Cada una de las cuatro capas del modelo TCP/IP es visible dentro de un paquete de red TCP/IP.

Direccionamiento IP versión 4 (IPv4)

Internet Protocol v4, es un protocolo de interconexión de redes basados en Internet, y que fue la primera versión implementada en 1983 para la producción de ARPANET.
Definida en el **RFC 791**, IPv4 usa direcciones de 32 bits, limitadas a 2^{32}= 4.294.967.296 direcciones.

Clases de direcciones (Classful)

CLASE	FORMATO	Nº REDES	Nº HOSTS	RANGO	MÁSCARA
A	r.h.h.h	128	16.777.214	0.0.0.0 - 127.0.0.0	255.0.0.0
B	r.r.h.h	16.384	65.534	128.0.0.0 - 191.255.0.0	255.255.0.0
C	r.r.r.h	2.097.152	254	192.0.0.0 - 223.255.255.0	255.255.255.0
D	grupo	-	--	224.0.0.0 - 239.255.255.255	multidifusión
E	no válidas	-		240.0.0.0 - 255.255.255.255	reservadas

Las únicas direcciones asignables a hosts son las de las clases A, B y C. La primera dirección de cualquier red es la dirección de red y la última, su dirección de difusión.

La RFC 3927 define el **bloque de dirección especial 169.254.0.0/16** para el direccionamiento de enlace-local. Estas direcciones solo son válidas en enlaces, no son enrutables.

La red de clase A **127.0.0.0** (red sin clase 127.0.0.0/8) está reservada para **loopback**. Los paquetes IP cuyas direcciones de origen pertenecen a esta red nunca deben aparecer fuera de un host.

Redes privadas (intranets)

CLASE	RANGO
A	10.0.0.0
B	172.16.0.0 - 172.31.0.0
D	192.168.0.0 - 192.168.255.0

Una dirección IP que pertenezca a una de estas redes se dice que es una dirección **IP privada**.

Subnetting

Consiste en segmentar el espacio de host en subredes y hosts. Internet es un modelo de redes. Reducimos bits de la parte host para hacer subredes.

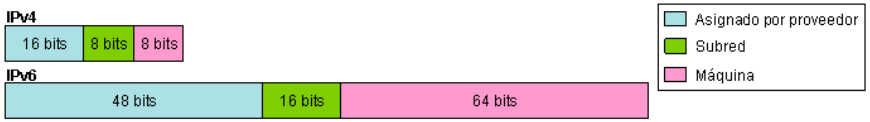
Un ejemplo de las posibles divisiones de una red de clase C podría ser el siguiente:

CIDR	MÁSCARA	BINARIO	SUBREDES	IPs	EJEMPLO
/24	255.255.255.0	00000000	1	256	.0
/25	255.255.255.128	10000000	2	128	.0, .128
/26	255.255.255.192	11000000	4	64	.0, .64, .128, .192
/27	255.255.255.224	11100000	8	32	.0, .32, .64, .96, .128, ...
/28	255.255.255.240	11110000	16	16	.0, .16, .32, .48, .64, ...
/29	255.255.255.248	11111000	32	8	.0, .8, .16, .24, .32, .40, ...
/30	255.255.255.252	11111100	64	4	.0, .4, .8, .12, .16, .20, ...

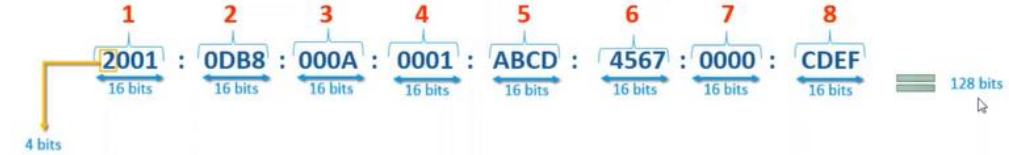
FLSM:	Máscara de red fija. No admite subredes de distinto tamaño.
VLSM:	Máscara de red variable. Aprovecha mejor el espacio de direcciones (subnetting).

Direccionamiento IP versión 6 (IPv6)

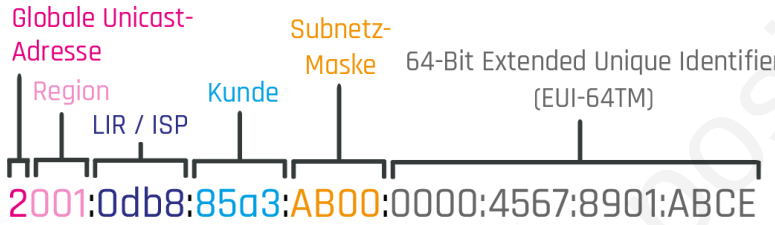
IPv6 tiene un mayor espacio de direcciones de 128 bits, a diferencia de las IPv4 que son de 32 bits. 2^{128}= 340 sextillones de direcciones.



Notación



Formado por 8 segmentos (hextetos) con valor de 16 bits (4bits * 4).
Cada segmento está comprendido de 0000 a FFFF.
Se eliminan 0 por la izquierda. Cambiar grupos seguidos de **:0** por**::** solo se puede hacer una vez.
Lo habitual es comprimir el mayor grupo de ceros. Ejemplo: **FE80::200**



Tipos de direcciones (no existe broadcast)

Dirección de **loopback** en IPv4 127.0.0.1 /8 y en IPv6 **::1/128**
Unicast: identifica unívocamente una interfaz de un nodo IPv6.
Multicast: grupo de interfaces **FF00::/8**, todos los nodos **FF02::1**, todos los routers **FF02::2**
Anycast: asigna a múltiples interfaces (típicamente en múltiples nodos). Varios equipos la misma IP y el router decide a quién le entrega la información. Se usa para sistemas de alta disponibilidad.

Transición IPv4 a IPv6

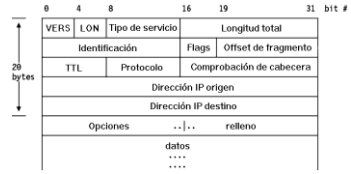
Dual Stack:	a la dirección **:ffff:192.168.0.1** se la llama mapped-address y es la forma de convertir una IPv4 en una IPv6 "interna".
Método 6to4:	técnica basada en tunneling que permite enviar paquetes IPv6 sobre redes IPv4. Concatenando el prefijo 2002: a la dirección IPv4. **2002::/48**

PROTOCOLOS TCP/IP

Protocolos de la capa de red

Protocolo IP: principal protocolo de la capa de red en el modelo TCP/IP que define la unidad básica (PDU) de transferencia de datos entre el origen y el destino.
Ofrece un servicio no orientado a conexión basado en la técnica de transmisión de bloques de datos conocidos como paquetes o datagramas. No implementa control de errores ni control de flujo.
Si el tamaño de los datagramas supera el permitido estos podrán ser fragmentados (MTU).

Datagrama:



Protocolo ICMPv4: Internet Control Message Protocol (**ping**), se encarga de informar de incidencias en la red, pero no toma decisión alguna. Esto será responsabilidad de las capas superiores.
Se encapsula directamente sobre IP, por lo que es enrutable. Cabecera de 4 bytes.

0 Echo Reply	4 Disminución traf.	8 Echo	13 Timestamp
3 Dest. inaccesible	5 Redirect	11 T. Exceeded	17/18 Sol/Res máscara

Protocolo ARP: Address Resolution Protocol, obtiene la dirección MAC de una IP. Usa broadcast (MAC FF FF FF FF FF FF). Logical address -> Physical address.
Protocolo RARP: Reverse Address Resolution Protocol, convierte direcciones de hardware exclusivas en direcciones de Internet en el adaptador de red de área local (LAN) de Ethernet.
Protocolo IGMPv3: permite que varios dispositivos compartan una dirección IP para que todos puedan recibir los mismos datos. Los dispositivos en red usar IGMP para unirse y salir de grupos de multidifusión, y cada grupo de multidifusión comparte una dirección IP.

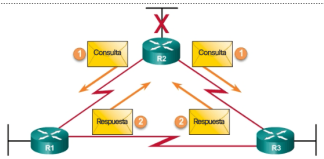
Protocolos de enrutamiento

Internos al sistema autónomo IGP (Interior Gateway Protocol):

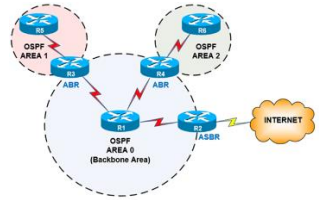
De Vector de Distancia RIPv2: Routing Information Protocol se implementa sobre otro protocolo, **UDP** (User Datagram Protocol) que lo convierte en un protocolo de la capa de aplicación. Manda por multicast la tabla de routing a todos los routers adyacentes mediante multicast a la direccion 224.0.0.9. RIPv1 usaba broadcast. Los routers domésticos usan RIP. Permite un número máximo de 15 saltos y uso de una sola métrica. Algoritmo **Bellman-Ford**

De Vector de Distancia IGRP: Interior Gateway Routing Protocol es propietario de Cisco permite un número máximo de 255 saltos y combinar varias métricas.

De Vector de Distancia EIGRP: Enhanced Interior Gateway Routing Protocol a diferencia de RIP, OSPF e IGRP, se implementa directamente en la capa de red (es decir, sobre IP). Soporta balanceo de carga y autentificación MD5.



De Estado de Enlaces OSPFv3: Open Shortest Path First, protocolo del primer camino más corto disponible se basa en el estado del enlace. Los nodos no intercambian distancias con sus vecinos, sino el estado de los enlaces a cada uno de ellos. Determina rutas alternativas. Permite el balanceo de carga mediante la distribución del tráfico entre ellas.
Algoritmo **Dijkstra**
Se puede descomponer en áreas (una de ellasllamada Backbone) y usa las siguientes direccionesmulticast 224.0.0.5 y 224.0.0.6.



Campo Tipo 8 bits:	2 = DB Descr (descripción)	4 = LS Update (resp. de estado)
1 = hello (comprobación)	3 = LS Request (sol. de estado)	5 = LS ASC (confirmación)

Protocolos que soportan VLSM: OSPF, RIPv2,IS-IS y EIGRP.

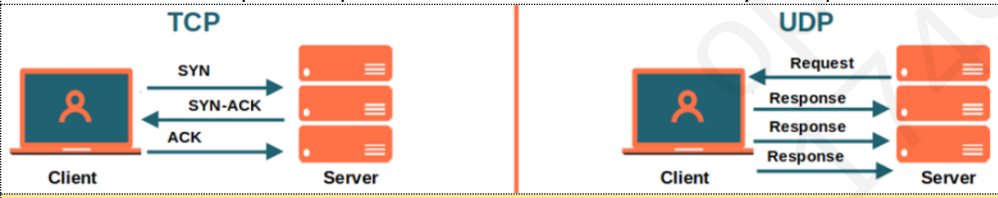
Externos al sistema autónomo EGP (Exterior Gateway Protocol):

BGP-4: Border Gateway Protocol**,** utilizado para comunicar distintos sistemas autónomos entre ISPs. El número AS lo asigna IANA..Los mensajes se encapsulan sobre segmentos TCP capa de aplicación.

Protocolos de la capa de transporte

Protocolo UDP: no garantiza el transporte de la información, esto lo garantiza el nivel de aplicación. Cabecera de 8 bytes.
Más rápido que TCP al tener menos overhead. Los equipos ya no fallan tanto.
La unidad de datos de UDP también se llama Datagrama como en IP.

Protocolo TCP: Es necesario establecer una conexión previa entre las dos máquinas (full-duplex) antes de poder transmitir ningún dato. A través de esta conexión los datos llegarán secuencialmente siempre a la aplicación destino de forma ordenada y sin duplicados.

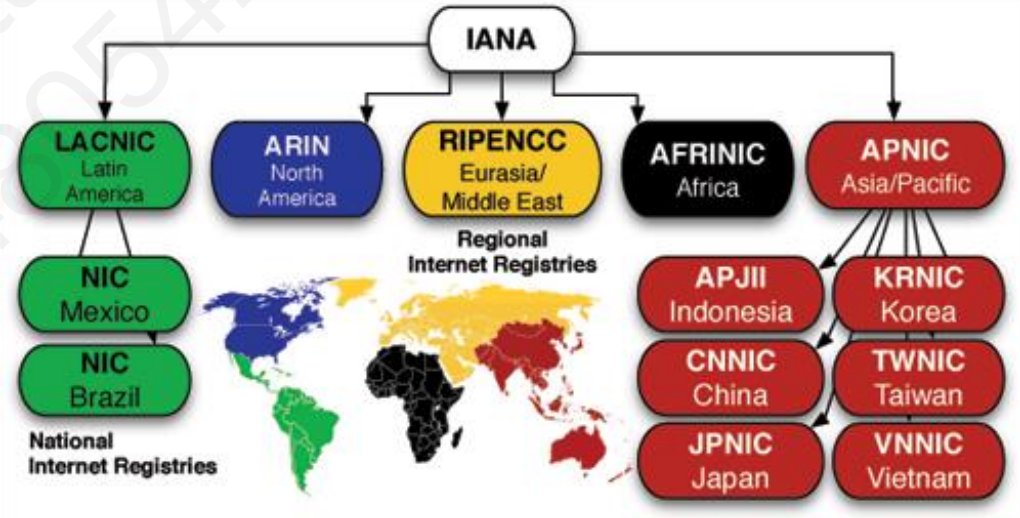


Protocolos de la capa de aplicación

La capa superior de cualquier modelo de red es la de aplicación. En esta capa se proporcionan distintos servicios de comunicación de datos a los usuarios. Estos servicios constituyen las aplicaciones de Internet más importantes y utilizadas, desde el correo electrónico o la navegación web hasta las aplicaciones multimedia. **HTTP, HTTPS, FTP, POP, SMTP, Telnet, SSH.**

GLOSARIO

SAP:	Service Access Point. Funciones lenguaje C.
IDU:	Interfaz Data Unit.
SDU:	Service Data Unit: paquete que se intercambia en vertical. ↕
ICI:	Interface Control Information. Solo usado en el SAP. No cabecera.
PDU:	Protocol Data Unit. Formato de datos de cada capa (segmento, paquete, etc). ↔
RFC:	Publicaciones que describen el funcionamiento de Internet, redes, protocolos, procedimientos, etc.
ICANN:	Corporación de Internet para la Asignación de Nombres y Números.
IANA:	La Internet Assigned Numbers Authority asignará a los RIR espacio de direcciones IPv4 suficiente para soportar sus necesidades de registro durante un período de al menos 18 meses.
RIR:	Registro Regional de Internet, se encargan de asignar direcciones IP y números de sistemas autónomos (AS) para su encaminamiento BGP.
CIDR:	Las direcciones se agrupan en Bloques Classless Inter-Domain Routing en los ISP según necesiten los RIR.



Bloque 4 - Tema 8: HTTP, HTTPS, y SSL/TLS

INTERNET

Conjunto descentralizado de redes de comunicaciones interconectadas que utilizan una familia común de protocolos TCP e IP (TCP/IP). Sus orígenes se remontan a 1969, cuando se estableció la primera conexión de computadoras, conocida como ARPANET.
El servicio que más éxito ha tenido en internet ha sido la World Wide Web (WWW o la Web).

Estructura (jerarquía)

Acuerdos de peering: (acuerdos de pares, de iguales) contratos establecidos entre dos operadores, que se encuentran en el mismo nivel o tier, en principio sin contraprestación económica.
Peering público (capa 2) o peering privado (punto a punto).

Acuerdos de tránsito: permitir a un operador utilizar las infraestructuras del otro para transmitir tráfico con contraprestación económica.

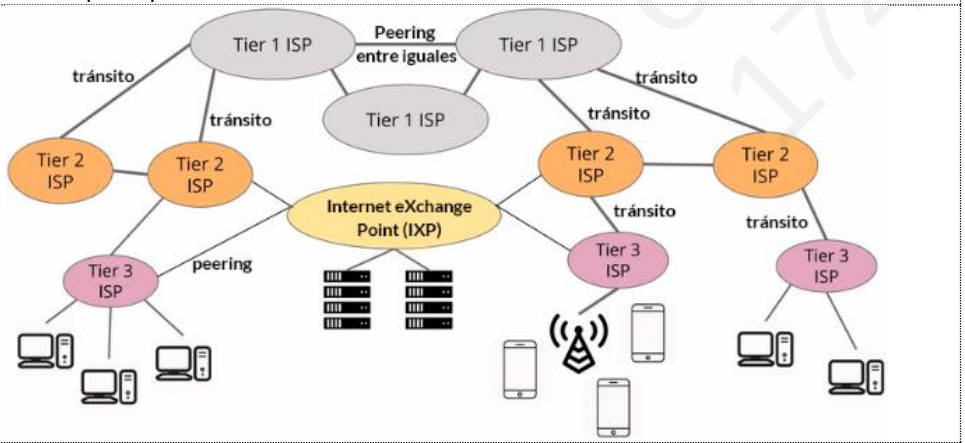
Nivel 1 (Tier-1): compuesto por grandes operadores que cuentan con enormes infraestructuras. Capaces de hacer llegar tráfico a cualquier parte únicamente con acuerdos de peering (AT&T, Deustche Telekom, Level 3 Communications, Telefónica, etc.).

Nivel 2 (Tier-2): operadores que han llegado a acuerdos de tránsito con otros para alcanzar algunas
Ubicaciones.

Internet eXchange Point (IXP): infraestructuras de conmutación que permiten el intercambio de tráfico de Internet (gracias al uso del protocolo BGP) entre los distintos proveedores. Pueden dar servicio a Tier-2 y Tier-3. Son como cooperativas. ESPANIX, CATNIX, DE-CIX.

Nivel 3 (Tier-3): compuesto por operadores que compran derechos de tránsito a otros operadores (Internet Service Provider o ISP).

Nivel 4 (Tier-4): compuesto por las redes corporativas empresariales que ofertan sus servicios a través de la parte pública de sus redes.



SISTEMA DE NOMBRES DE DOMINIO (DNS)

DNS (Domain Name System) sistema de resolución de nombres, utiliza una base de datos distribuida y jerárquica que almacena información asociada a nombres de dominio en redes como Internet. El nombre formado por toda la cadena se conoce como Fully Qualified Domain Name (**FQDN**).

Resolvers	Son servidores caché, o programas cliente, los cuales se encargan de generar las consultas necesarias y obtener la información para ofrecerla al usuario.
Root servers	La raíz de la jerarquía del DNS parte del ".", el cuál es gestionado por los denominados Root Servers. Son 13 servidores: ***a.root-servers.net - m.root-servers.net*** VeriSignn, ISI, U.Maryland, NASA, US Defence (NIC), US Army, RIPE, ICANN, etc.

Dominios regionales (.es, .pt, .fr, it, .ru, etc.) **Dominios genéricos** (tres o más letras.)

Dominio de primer nivel especial .arpa (para propósitos de infraestructura técnica)

Dominio TLD ".es"	Está administrado por ES-NIC (www.nic.es), que es un departamento de la Entidad Pública Empresarial Red.es
Dominios 2º nivel	un máximo de 63 y un mínimo de 3 caracteres.
Dominios 3er nivel	un máximo de 63 y un mínimo de 2 caracteres.
Preguntas inversas *d.c.b.a.in-addr.arpa*	permite conocer un dominio dada una dirección IP. Para evitar una búsqueda exhaustiva existe un dominio de consulta especial llamado **in-addr.arpa**

Servidores autoritativos: cuando un nombre de domino se registra a través de un servicio registrador, se solicitará la asignación de un servidor primario y sería deseable un servidor secundario para proporcionar redundancia en caso de inoperatividad de alguno de los servidores.

Servidores caché: almacenan información de consultas (queries) DNS por un determinado tiempo denominado TTL (Time To Live) de cada registro DNS.

Registros DNS: Resource Records (RR)

NAME = nombre del dominio	**CLASS** = clase del registro	**RDLENGTH** = longitude RDATA
TYPE = tipo de registro	**TTL** = Tiempo cacheado (seg)	**RDATA** = descripción

TIPO (VALOR CAMPO TYPE)

A = Address (IPv4)	**MX** = Mail Exchange	**LOC** = LOCalización
AAAA = Address (IPv6)	**PTR** = Pointer	**SRV** = SeRVicios
CNAME = Canonical Name	**SOA** = Start of authority	**HINFO** = Host INFOrmation
NS = Name Server	**TXT** = Información textual	**ANY** = Todos

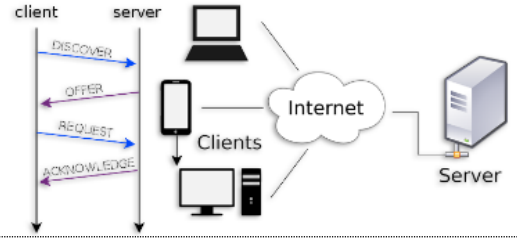
SPF = Sender Policy Framework (Ayuda a combatir el Spam).

Protocolo DNS

Generalmente, en la actividad DNS se usan datagramas UDP, otros como la transferencia de zona se usan directamente TCP. **Puertos 53/UDP, 53/TCP**

Herramienta Nslookup	Permite hacer consultas a un determinado servidor DNS.

C:\Users\Pepe>nslookup
> server 8.8.8.8
DNS request timed out.
timeout was 2 seconds.
Servidor predeterminado: [8.8.8.8]
Address: 8.8.8.8



EL SERVICIO WEB	
URI	Identificadores de recursos uniformes: Puede ser un localizador (URL) y/o un nombre (URN).
- URL	Localizador de recurso uniforme: Identifica los recursos según su método de acceso.
- URN	Nombre de recurso uniforme: identifica los recursos según su nombre o algún otro atributo suyo. Si movemos un archivo de un servidor a otro, el URN permanecerá constante, aunque su URL haya cambiado, son relacionados mediante un servicio de directorio. Sintaxis: *esquema://usuario:contraseña@host:puerto/camino-del-objeto*
Índices o directorios:	listado de sitios web organizados de forma jerárquica mediante un árbol.
Motores de búsqueda:	su información se obtiene automáticamente recorriéndose la web (robots).
Metabuscadores:	se busca simultáneamente en distintos buscadores.

La web 2.0. Herramientas de trabajo colaborativo

La 2.0 tiene como principal protagonista al usuario humano que escribe artículos en su blog o colabora en una wiki.

Blogs	CMS	Wikis	Fotográficos	Vídeos	Calendarios	Presentaciones
Buscadores	RSS	Social	Aplicaciones y servicios (mashups, mezclas).			

La web 3.0: la web semántica

La diferencia fundamental es el tipo de participante y las herramientas que se utilizan. La web semántica, está orientada hacia los procesadores de información que entiendan de lógica descriptiva en diversos lenguajes como SPARQL, POWDER u OWL (Ontology Web Language).

INTERNET DE LAS COSAS - IoT

Interconexión de objetos a través de Internet, dotados de electrónica, sensores y conectividad a la red, que les permiten recoger e intercambiar datos, así como ser controlados remotamente.

Hardware SoC (System on a Chip): integran gran parte o todos los módulos que componen un sistema electrónico en un solo chip.

Comunicaciones: RFID, NFC, Bluetooth (desde v4.0 BLE), HaLow (variante de Wi-Fi), Li-Fi, PLC, ZigBee…

Procolos: CoAP, REST y MQTT.

Sistemas operativos: RiotOS, VxWorks, ARM mbed OS, Android Wear, Apple watchOS, Apple tvOS, Nucleus RTOS, Integrity y Windows 10 for IoT.

Plataformas de gestión: IBM Watson IoT Platform, Amazon Web Services IoT Platform, Microsoft Azure IoT Hub, Google Cloud IoT, etc.

SERVICIO DE TRANSFERENCIA DE FICHEROS (FTP)	
El servicio **FTP** (File Transfer Protocol) se ofrece en la capa de aplicación utilizando los puertos **TCP 20** (para transferencia o pasiva) y **TCP 21** (para la conexión y la ejecución de comandos).	
Modo activo: (predeterminado)	El servidor utilizará el **puerto 20** para la transferencia de datos, mientras que transmitirá los comandos utilizando el **puerto 21**. El cliente en cambio utilizará un **puerto aleatorio superior al 1023** (comando **PORT**) para la transferencia de comandos, y el **siguiente puerto** para la transferencia de datos.
Modo pasivo:	El servidor usa el **puerto 21** como puerto de comandos y un **rango de puertos superior a 1023** para datos. Del lado del cliente seguimos manteniendo el puerto **superior a 1023** para control (comando **PASV**), y **desde el puerto siguiente al puerto de control** para datos.
Antes de cada nueva transferencia tanto en el modo Activo como en el Pasivo, el cliente debe enviar otra vez un **comando** de control (**PORT** o **PASV**, según el modo).	
Trivial FTP:	ocolo de transferencia de archivos trivial (**tftp**) ofrece funciones similares a ftp pero los usuarios no pueden ver el contenido de un directorio ni cambiar directorios (deben conocer el nombre completo del archivo). Puerto **69 UDP.**
FTPS:	FTP implícito sobre TLS (obsoleto). Antes de intercambiar información con el servidor FTP, se realiza la negociación TLS.
FTPES:	FTP explícito sobre TLS. El cliente una vez conectado, solicita explícitamente la negociación TLS. Soporta TLS 1.2 y TLS 1.3.
SFTP:	Secure File Transfer Protocol: transferencia de archivos mediante SSH.
SCP:	Secure Copy Protocol: transferencia de archivos mediante SSH.

SERVICIOS DE ACCESO REMOTO (Telnet y SSH)	
TELNET	SSH (Secure SHell)
Puerto 23	Puerto 22
telnet 192.168.1.6 **23**	ssh usuario@192.168.1.6**:22**

SERVICIOS MULTIMEDIA

El desarrollo de servicios en tiempo real necesita una especial consideración, debido al carácter no fiable y no orientado a conexión del protocolo IP. Se han propuesto distintos protocolos que posibiliten la interactividad de los servicios desarrollados sobre IP:

RTP/RTCP	RSVP	RTSP	SDP	SIP	SAP

Voz sobre IP (VoIP)

La voz se fragmenta en paquetes de datos que deben viajar a través de una red de redes IP.
Para evitar pérdidas se deberán implementar mecanismos de **QoS** **Calidad de Servicio**.
Los dos protocolos principales de VoIP son **H.323** y **SIP**, ambos de la capa de aplicación que utilizan el llamado protocolo de **transporte de tiempo real** **RTP**, el cual funciona sobre **UDP**.

PROTOCOLO HTTP

El protocolo de transferencia de hipertexto (HTTP) es el responsable de enviar "documentos HTML" desde un servidor web hasta el cliente.

HEAD	solicitud de lectura de cabecera	DELETE	borra el recurso especificado
GET	solicitud de lectura de página web	TRACE	para comprobación y diagnóstico
PUT	solicitud de un envío o escritura	OPTIONS	devuelve los métodos HTTP que soporta
POST	envía datos para que sean procesados	CONNECT	para saber si el proxy nos da acceso

Versiones de HTTP

0.9	Obsoleta. Soportaba solo un comando, GET.
HTTP/1.0	En esta versión se indica en las comunicaciones la primera versión de HTTP en las comunicaciones.
HTTP/1.1	Las conexiones persistentes están activadas por defecto y funcionan bien con los proxies.
HTTP/1.2	no tenía método PUSH y se suplió con extensiones definidas en la RFC 2774.
HTTP/2.0	Derivó de SPDY, un protocolo de Google. Usa una única conexión TCP para realizar múltiples solicitudes. Compresión de headers por defecto y lleva TLS implementado.
HTTP 3.0	Funciona sobre protocolo QUIC de Google, que va sobre UDP. Utiliza TLS v.1.3 y mejora el soporte para usuarios de smartphones.

Protocolo HTTPS

HTTPS es un protocolo de seguridad específico para HTTP que asegura los datos transmitidos.
Utiliza el puerto **TCP 443** en lugar del 80.
Seguridad mediante los protocolos **SSL** (Secure Socket Layer) y **TLS** (Transport Layer Security).

SSL/TLS: (TLS 1.2 y 1.3)	Se usa para cifrar un canal HTTP (HTTPS) o FTP (FTPS) o para email (SMTP, IMAP, POP3) o LDAP (LDAPS), etc. La criptografía sirve para asegurar la Confidencialidad, Integridad y Autenticidad (Triada CIA). Son las dimensiones/aspectos de la seguridad que se pueden asegurar respecto a un activo de tipo información.
Handshake:	Este flujo es para autentificar al servidor. Mutual Autentication es cuando el servidor te pide elegir tu propio certificado.
TLS v.1.2	Algoritmos hash: SHA256, SHA384.
TLS v.1.3	Algoritmos hash: SHA256, SHA384, AEAD (cifrado autenticado con datos asociados).

Códigos de estado HTTP

Informational							
1XX	respuestas informativas						
Success							
200	OK	**201**	Creado	**203**	Info no autoritat	**204**	Sin contenido
205	Recargar conten	**206**	Contenido parcial	**207**	Estado múltiple		
Redirection							
300	Múltiples opcion	**301**	Movido perman	**302**	Movido temp.	**303**	Vea otra
304	No modificado	**305**	Utilice un proxy				
Client Error							
400	Solicitud incorrec	**401**	No autorizado	**402**	Pago requerido	**403**	Prohibido
404	No encontrado	**405**	Método no permitido				
Server Error							
500	Error interno	**501**	No implementado	**502**	Pasarela incorrect	**503**	Serv. no dispo.
504	Tiempo agotado.	**505**	Versión de HTTP no soportada				

SERVICIOS DE DIRECTORIO (LDAP)

El protocolo LDAP (Lightweight Directory Access Protocol) utiliza el protocolo TCP 389 para solicitar información a un DSA (Directory System Agent) y, a diferencia con otros protocolos de la pila TCP/IP, no envía los comandos y respuestas en ASCII sino siguiendo la notación ASN.1.

Generalmente, el acceso se realizará para solicitar una consulta, con lo que se usará otro mensaje definido en LDAP denominado SearchRequest, respondido con un SearchResponse. El protocolo también admite opciones de actualización del directorio, para añadir, modificar o eliminar objetos. Actualmente, prácticamente todos los servicios de directorio basados en X.500 (la gran mayoría) emplean LDAP como protocolo de acceso a la información.

IKEv2 / IPSec

SEGURIDAD Y PROTECCIÓN EN REDES DE COMUNICACIONES	
En la disciplina de seguridad de las TIC (STIC) puede encontrarse la siguiente **clasificación**:	
TRANSEC	Aseguran los canales de transmisión (seguridad de las transmisiones).
NETSEC	Protegen los elementos de red (seguridad de las redes).
CRYPTOSEC	Protegen la información con criptografía (seguridad criptológica).
Seguridad de la información	
Control de accesos: sistema más aislado, privilegios mínimos, mecanismos de defensa perimetral, mecanismos de control, monitorización y rastreo.	
Protección de la información en tránsito: mediante técnicas criptográficas.	
Seguridad en las comunicaciones	
La norma IEEE 802.1x definida en el RFC 3748 y se basa en el protocolo **EAP** (**Extensible Authentication Protocol**) para el control de acceso a redes (tanto LAN como WLAN) basado en puertos. Usa certificados digitales. Solicitante, autenticador y servidor de autenticación (RADIUS o DIAMETER).	
El estándar **WPA3**: configuración **Wi-Fi Easy Connect** (**WEC**), cifrado **Wifi Enhanced Open** (**WEO**), autenticación 128 bits **entre iguales** (**SAE**) que reemplaza a la clave precompartida (PSK). Modo **WPA3 Enterprise** con 192 bits de longitud de clave.	
El protoco **IPSec** actúa en la capa de red para proteger y autenticar paquetes IP entre dispositivos IPSec participantes (Peers).	
Familia de protocolos IPSec:	
SA (**Asociación de seguridad**): es un grupo lógico de parámetros de seguridad que define la conexión entre dos extremos, es decir, contiene los detalles de la conexión.	
IKEv2 (**Internet Key Exchange**): Internet Key Exchange. Protocolos para el intercambio de claves (DH – Diffie-Hellman), intercambio de opciones criptográficas entre pares, autenticación entre pares.	
AH (**Encabezado de autenticación**): Authentication Header. establece una conexión segura entre dos dispositivos. Agrega un encabezado que contiene datos de autenticación del remitente y protege el contenido. Los 2 routers deben tener la misma clave.	
ESP (**Datos de seguridad encapsulados**): Encapsulating Security Payload. Asegura Confidencialidad, Integridad y Autenticación de origen. Realiza el cifrado de todo el paquete IP o solo de la carga útil. Cifra el payload con AES. Aunque podría configurarse para usarse sin cifrado, solo para autentificar.	
IPv6 incluye de forma nativa IPSec. No garantizan la confidencialidad. Incluye mecanismo de autenticación mutua y negociación de claves criptográficas.	
Seguridad en las transacciones	
Se basan en la utilización de protocolos criptográficos, generalmente TLS. dicionalmente, SSL puede utilizarse para crear una red privada virtual (VPN) y ofrecer túneles para comunicaciones seguras. Un ejemplo lo constituye el software de código libre OpenVPN.	
Correo electrónico seguro	
PGP (**Pretty Good Privacy**, privacidad bastante buena): herramienta de encriptación de correo electrónico que utiliza el algoritmo RSA (cifrado de clave pública)	
S/MIME (**Secure MIME**): sistema de cifrado, firma y certificación de mensajes, está soportado por RSA y utiliza los estándares PCKS números 7 y 10. Emplea un mecanismo de triple envoltorio en el que el mensaje es primero firmado, después encriptado y finalmente firmado nuevamente sin que ambas firmas procedan necesariamente de la misma persona o entidad.	
PEM (**Privacy Enhanced Mail**, correo con privacidad mejorada): poco utilizado puesto que no está preparado para correos MIME.	
LA UTILIZACIÓN DE LA INTELIGENCIA ARTIFICIAL EN LA SEGURIDAD	
La **inteligencia artificial** es la capacidad de una máquina de imitar el comportamiento humano simulando la realización de tareas.	
El aprendizaje de las máquinas (**Machine Learning**) es la capacidad de una máquina para aprender sin haber sido programada explícitamente para ello.	
En este momento predomina la aproximación **supervisada** (requiere la intervención humana), sobre todo para casos de detección automática (supervisión de Logs).	

SEGURIDAD PERIMETRAL			
Tipos de cortafuegos			
Filtrado de paquetes (Package Filtering)	Trabaja a nivel de red (3) y transporte (4). Su función es tomar decisiones de procesamiento con base en direcciones IP, protocolos o puertos.		
Puerta de enlace a nivel de circuito (Circuit-Level Gateway)	Trabaja a nivel de sesión (5), o como una "capa de compensación" entre la capa de aplicación y la capa de transporte de la pila TCP/IP. Controla que el TCP Handshake se haga correctamente.		
Firewall de inspección con estado (Stateful Inspection)	Se considera una solución más segura que el de filtrado de paquetes, debido a que procesa la información de la capa de aplicación (7). Los puertos pueden cerrarse y abrirse de forma dinámica para terminar una transacción. Tienen información histórica almacenada para toma de deciciones.		
Application Level Gateway (proxy)	Trabaja a nivel de aplicación (7), filtrando el acceso según las definiciones de la aplicación. Se sitúan en un punto intermedio de la comunicación.		
Firewall de próxima generación (NGFW)	Filtrado de paquetes básico o una toma de decisiones basada en proxy dentro de las capas 3 y 4 así como en la capa 7.		
- Sistemas de Prevención de Intrusos (IPS):	Funcionan en modo activo, monitorizando el tráfico de red y/o las actividades de un sistema, en busca de actividad maliciosa.		
NIPS: network	**WIPS**: wireless	**HIPS**: host	**NBA**: comp. anómalos

- Web Application Firewall (**WAF**):	Filtra o bloquea el tráfico HTTP hacia y desde una aplicación web. Protege a las aplicaciones web contra ataques como los de inyección SQL, XSS y falsificación de petición de sitios cruzados (CSRF). Pueden ser: (transparent bridge, transparent reverse proxy o reverse proxy).
- Gestión Unificada de Amenazas (**UTM**):	Proporciona una plataforma centralizada para la gestión de la seguridad, consolidando, controlando y supervisando múltiples medidas de seguridad (contenido, antivirus, IPS, etc.).

Cortafuegos software

Software de sistema (Microsoft Windows)

Activar: *netsh advfirewall set currentprofile state on*

Abrir TCP_80: *netsh advfirewall firewall add rule name="Open 80" dir=in action=allow protocol=TCP localport=80*

Router/Proxy/Gateway - con funcionalidad de cortafuegos.

Equipos de red que incorporan funcionalidades propias de cortafuegos.

Cortafuegos UTM o Gestión unificada de amenazas

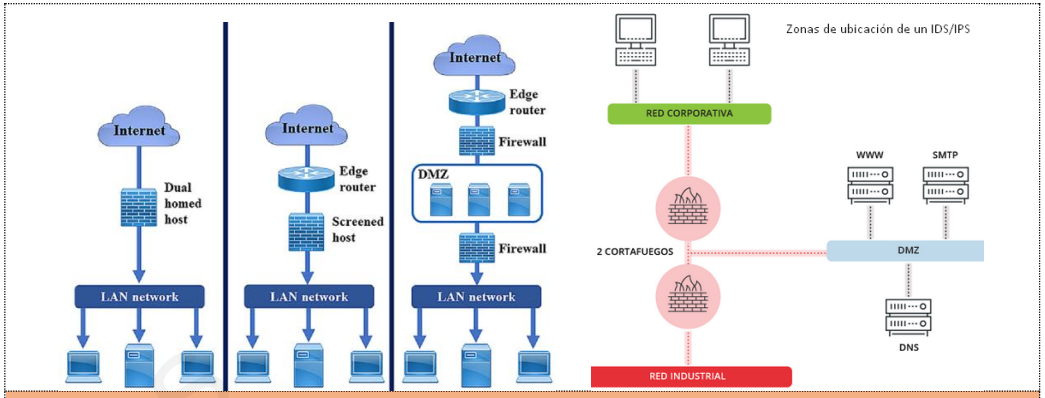
Servidores que integran distintas soluciones de seguridad con un único interfaz de gestión.

Cortafuegos en formato appliance

Plataformas hardware más software diseñadas con una funcionalidad específica (email, malware, navegación, etc.) pero que no disponen necesariamente de gestión unificada

Arquitecturas

Screening Router (router)	Es la modalidad más sencilla (choke). Filtrado de paquetes. Separa red externa de la interna con un único equipo, el router. El router está expuesto.
Dual-Homed Host (host bastión)	El anfitrión de dos bases (máquina Unix) que tiene 2 tarjetas de red, una para la red interna y otra para la externa. Intercambio a nivel de aplicación (capa 7). No hay routing, solo "reparto". Establece de dónde a dónde va a permitir que se dialogue.
Screened Host (router + host bastión)	Solo se permiten conexiones hacia un determinado host. Todo pasa por el Bastion Host. Máquina accesible desde el exterior que debemos securizar/fortificar (hardening). Hace de proxy frente a otros hosts. El router sigue estando expuesto. Filtrado de paquetes.
Screened Subnet (**DMZ**):	Este FW solo permitirá acceso a elementos que tengamos en la DMZ: web, DNS autoritativo, MTA, proxy inverso, servidor de VPN, etc. El tráfico de la DMZ a la red interna está prohibido. El router externo generalmente hace PAT (Port Address Translation).



Sistemas de protección contra intrusos (IDS)

Funcionan en modo pasivo, obteniendo copias del tráfico de red e informando de las amenazas.

Tipos de IDS

NIDS (Network-based IDS): vigila la red. Captura tráfico de la red.
Productos: SNORT, Suricata.

HIDS (Host-based IDS): vigila cambios en host como abusos de privilegios.
Productos: OSSEC, SAGAN, TRIPWIRE

IDS Híbridos: La combinación permite explotar las ventajas de ambas arquitecturas.
Productos: Prolude

Productos: SNORT, Suricata, OSSEC, Sagan, Bro, Fail2Ban, AJDE, Samhain. Existen soluciones IDS/IPS como proyecto Suricata está soportado por la Open Information Security Foundation (OISF).

SIEM (Gestión de Eventos e Información de Seguridad)

Funcionan en modo pasivo. Analizan la información de muchos sitios, recogiendo logs.
El administrador establece qué mensajes son relevantes.
Se centraliza e interpreta la información para aplicar IA y ML. La información de los logs debe normalizarse y correlacionarse.
Productos: ELK, Qradar, Metron, OSSIM (nmap (análisis puertos), snort (IPs), nagios (monitorización de red), nikto (análisis vulnerabilidades)), Gloria/Mónica (CCN).

Honeypots

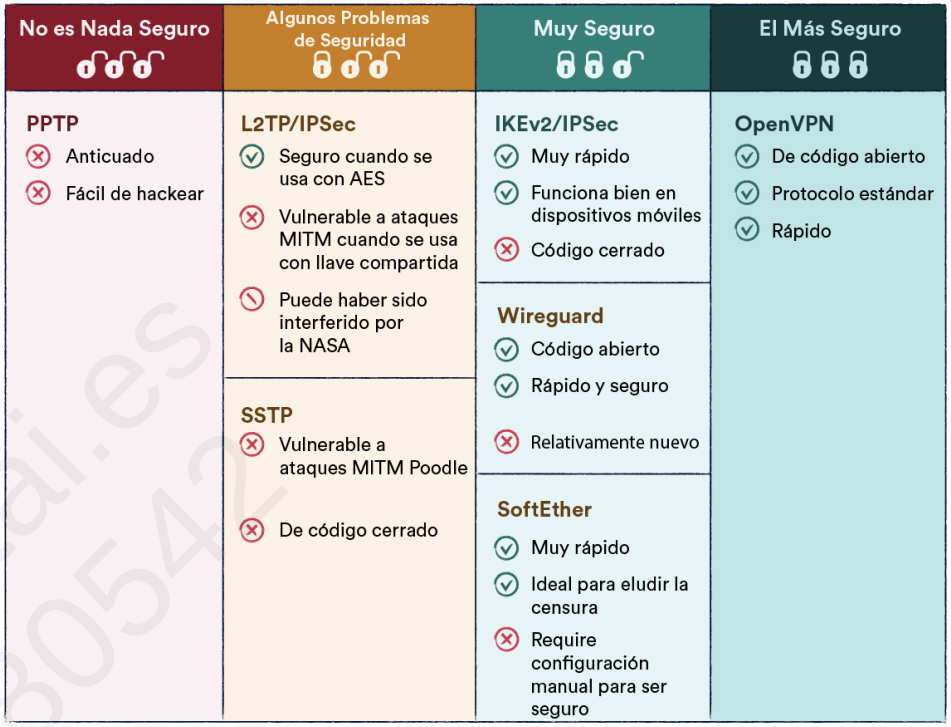
Sistemas de engaño o sistemas diseñados para ser atacados y configurados con vulnerabilidades para atraer a los atacantes y estudiarlos. Separado de la red real.

Catálogos de vulnerabilidades

CVE (Common Vulnerabilities and Exposures): vulnerabilidades asociadas a un producto concreto. Vulnerabilidades de día 0: según se publican las usan los atacantes hasta que los fabricantes las solucionan.

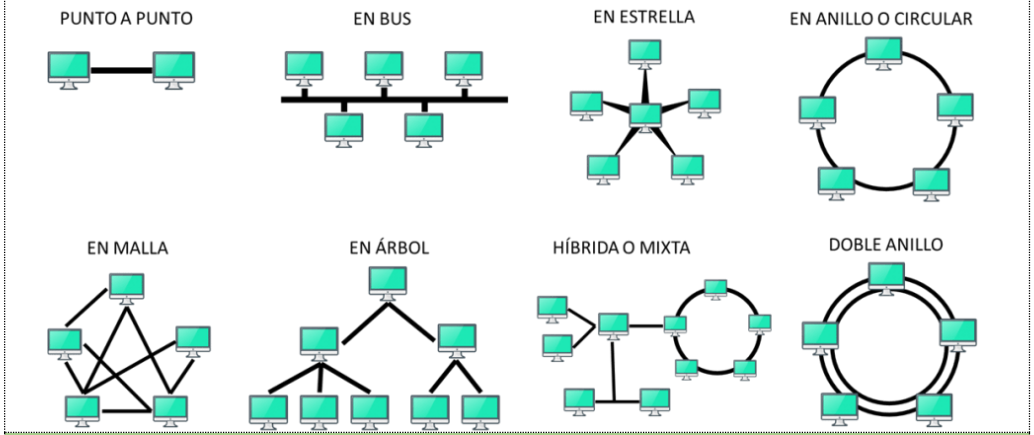
CWE (Common Weakness Ennumeration): vulnerabilidad no asociada a ningún producto. Es como lo que hace la Fundación OWASP (Open Web Application Security Project).

ACCESO REMOTO SEGURO A REDES. REDES PRIVADAS VIRTUALES (VPN)	
Extensión de una red LAN a través de una red pública. Reduce los costes al no necesitar líneas dedicadas. Ofrece mecanismos de **confidencialidad, integridad y autenticación** (***CIA***). Guía CCN 836.	
VPN de acceso remoto	
PPTP	Encripta y autentica. Para encriptar usa la extensión MPPE. Nivel 2. Usa GRE.
Layer Two Forwarding **(L2F)**	Encripta y autentica. No encripta por sí solo. Nivel 2
L2TP / IPSec	Encriptación y autenticación. Encripta con IPSec. Nivel 2. Sobre UDP.
SSL/TLS	Nivel de transporte. Producto: OpenVPN.
SSH	Nivel de aplicación.
SSTP	Protocolo de túnel de sockets seguro o SSTP es un protocolo VPN desarrollado por Microsoft que usa SSL.
WireGuard	Aplicación y protocolo. Trabaja a nivel de red.
VPN de sitio a sitio	
Familia IPSec	Los protocolos IPSec envían paquetes de datos de forma segura. AH, ESP y IKE.
Generic Routing Encapsulation **(GRE)**	GRE: Protocolo para encapsular datos. IP **protocol 47**. No seguro. Usado con otros para dar seguridad. El payload de GRE es el paquete IPde tráfico privado. GREP va sobre paquete IP con IPs públicas porque atraviesa internet. Podría llevar IPv4 dentro e IPv6 fuera o al revés.
VPN de equipo a equipo	
No se tiene acceso a las redes a las que pertenezcan los equipos, sólo al equipo.	
Servidores de autenticación	
Son sistemas AAA: Autenticación (user/pass), Autorización (para acceder o no al recurso), Contabilización (Accounting: facturación por uso). Ejemplos: Radius, Kerberos, TACACS+, Diameter.	

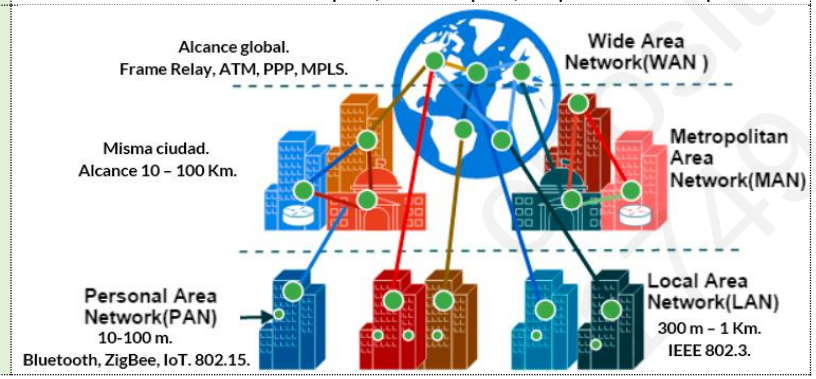


Bloque 4 – Tema 10: REDES LAN

REDES LOCALES



TIPOS DE REDES

Redes de difusión	Redes broadcast. Canal compartido entre todos los terminales. Hub / Concentrador.
Redes punto a punto	Entre pares. El destino es unívoco y no es necesario poner dirección de destino. Modalidades: Simplex, Half-Duplex, Duplex o Full-Duplex.
En función de la distancia	

TIPOLOGÍA

ANSI, a través del IEEE define los estándares 802 para la estandarización de nivel físico (subcapa MAC) y enlace en redes PAN, LAN y MAN.

Noma	Tecnología	Otros datos
802.1q	VLAN.	
802.1x	Control de acceso a redes en base a puertos	
802.2	Control del enlace lógico. LLC	
802.3	**Ethernet** (10 Mbps)	Categoría 5 UTP
802.3u	**Fast Ethernet (**100 Mbps**)**	Par trenzado, Cat.5
802.3z	**Ethernet Gigabit** (1000BASE-X)	Fibra óptica (SM y MM).
802.3ab	1000BASE-T / 1 Gbps	Par trenzado, Cat.5 o superior.
802.3ae	10GBASE-SR, 10GBASE-LR / 10 Gbps	Fibra óptica (MM).
802.3af	Power-over-Ethernet / PoE 15,4W	
802.3an	**Ethernet 10 Gigabit** (10 GBASE-T)	Categoría 6 UTP
802.3at	PoE+ 25,5W	
802.3ba	**Ethernet 40 y 100 Gigabit**	Fibra óptica optimizada para (MM y SM)
802.3bt	PoE++ 60W	
802.4	Token Bus.	Topología física en bus y lógica en anillo.
802.5	Token Ring	Física en estrella y lógica en anillo.
802.11	Inalámbrica (Wi-Fi) (Wireless Fidelity)	
802.15.1	Bluetooth	
802.15.4	ZigBee (Low Rate WPAN)	
802.16	Wimax (MAN inalámbrica)	

ETHERNET – IEEE 802.3

Ethernet fue el origen y luego se estandarizó como 802.3.
Velocidades de 10 Mbps a 400 Gbps (802.3db).
Trama Ethernet de la 802.3 tiene el campo longitud. No se puede definir qué protocolo lleva la trama.
Trama Ethernet II (DIX Ethernet) usa el campo ethertype (es lo que se usa) en vez del campo longitud.
La trama Ethernet más pequeña es de 64 bytes y se llama Runt Frame.
Jumbroframe: payload es de 9000 bytes en lugar de 1500 bytes.
Topología física en bus o estrella (con un switch). Topología lógica en bus.
Codificación Manchester: para no perder sincronismo al mandar muchos 0 o 1.
Par trenzado 100m, Coax-thin 200m, Coax-thick 500m, Fibra multimodo 2,5Km.

Especificaciones:	**10BASE-T**			
	10: velocidad	BASE: transmisión	T: par de cobre	F: Fibra óptica

MÉTODOS DE ACCESO AL MEDIO

Reglas que definen cómo un equipo ofrece o toma datos en la red. Conocidas como MAC (Medium Access Control).

Acceso controlado

Reserva	Las estaciones reservan el canal antes de enviar datos. Eficiente si hay pocos terminales.
Daisy chain	Necesita un canal extra que recorra en anillo las estaciones, siendo un bus el canal que utilizan para enviar los datos.

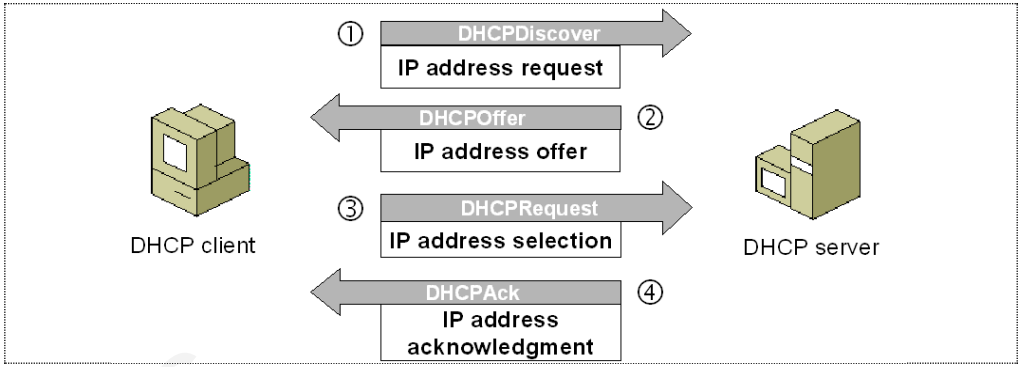
Polling (Sondeo)	Requiere un control centralizado. La estación central sondea al resto para ver quién quiere enviar y le asigna un tiempo de envío.
Token	se pasa un token por las estaciones. Cuando la estación tiene el token puede transmitir. Pasa el token a la siguiente.
- Token Bus	Topología física en bus y lógica en anillo. Cada estación tiene un tiempo para transmitir.
- Token Ring	Física en estrella y lógica en anillo. Estación central MAU (Multistation Access Unit). Admite multicast. Admite prioridad.
Acceso aleatorio	
Aloha	la estación que quiere transmitir lo hace y escucha si hay colisión. Si hay colisión, espera un tiempo aleatorio para volver a transmitir.
Aloha ranurado	las estaciones transmiten sin escuchar. El tiempo se divide en ranuras. Se transmite al comienzo de la ranura.
CSMA	Carrier Sense Multiple Acces. Las estaciones conocen el estado del canal. Si está libre, transmiten. Si no, esperan.
- CSMA/CD	Collision Detection. Usado en Ethernet 802.3 cuando era half-duplex. Escucha antes de transmitir. Si durante la transmisión detecta una colisión, interrumpe la transmisión y espera.
- CSMA/CA	Collision Avoid. Usado en Wi-Fi.
Canalización	
FDMA	División por frecuencia. Cada señal de entrada se modula con frecuencia portadora distinta (canal). Separación por banda de guarda.
TDMA	División por tiempo. Cada estación tiene un slot de tiempo para emitir. Transmisión síncrona (tiempo fijo) o estadística (tráfico).
CDMA	División por código. Cada estación tiene un código ortogonal. Todos pueden emitir al mismo tiempo y en la misma frecuencia. Elreceptor separa y decodifica cada señal.

DISPOSITIVOS DE INTERCONEXIÓN
Dominio de colisión
Conjunto de nodos que comparten el mismo medio de transmisión y compiten por el acceso. Puede haber colisiones. En un hub se producen colisiones. Cuanto más grande es el dominio de colisión (mayor número de equipos) peor es el rendimiento de la red. Para mejorar el rendimiento lo que se hace es segmentar la red. En caso de quedar un solo equipo en cada dominio de colisión hablamos de microsegmentación.
Dominio de difusión: direcciones de broadcast FF:FF:FF:FF:FF:FF.
Conjunto de estaciones de una misma LAN que pueden recibir mensajes de broadcast de otra estación de la red. Tormentas de broadcast: Se produce en redes mal diseñadas o en las que existan caminos redundantes no previstos (bucles). Un mensaje broadcast puede quedarse en la red indefinidamente, degradándola o colapsándola.

Repetidores	Trabajan a nivel 1 (físico). Regeneran y amplifican la señal cuando hay atenuación. Reenvían todos los datos, extendiendo el dominio de colisión (malo).
Concentradores / Hubs	Trabajan a nivel 1 (No tienen lógica). Conexión de equipos adyacentes mediante bus común. La señal entra por un puerto y se reparte a todos los demás por lo que se divide la velocidad entre todos los puertos. Se comparte el dominio de colisión y difusión.
Puentes / Bridges	Trabajan a nivel 1 y 2. Separan dominios de colisión (1 por cada interfaz) pero no de difusión. Separan redes a nivel de enlace. Permiten interconectar redes locales que usan distintos medios físicos. Aprenden las MAC de los equipos de la red y los almacenan en una tabla. Permite realizar filtrado y reenvío de tramas (software). Maneja grupos, de modo que solo pasa información al otro lado cuando hace falta.
Conmutadores / Switches	Trabajan a nivel 2, son la evolución de los bridges transparentes. Separan dominios de colisión pero no de difusión. A diferencia de los Hubs el ancho de banda no se reparte entre los distintos puertos. Encaminamiento gracias a tablas MAC.
Encaminadores / Routers	Soportan hasta nivel 3. Separan dominios de colisión y de difusión. El tráfico de difusión se queda en cada subred.
Pasarelas / Gateways	Operan en los niveles más altos de OSI (4 - 7). Interconectan redes con protocolos de alto nivel diferentes y aseguran que los datos de una red son compatibles con los de la otra red. Ventajas: Permiten la interconexión de protocolos. Desventajas: Muy caros. La conversión de protocolos supone una alta carga en el Gateway pudiendo producirse cuellos de botella si la red no está optimizada.
Cortafuegos / Firewalls	Restringe el intercambio de tráfico entre redes. También se pueden usar para segmentar una red de área local en subredes. Las restricciones de tráfico se establecen mediante reglas en el firewall. En función de a qué nivel operen las reglas, podemos encontrar diferentes tecnologías de cortafuegos: de filtrado de paquetes (nivel 3); a nivel de circuito, conteniendo una lista de las conexiones validas (nivel 4); a nivel de aplicación, restringiendo el tráfico de ciertas aplicaciones.

Proxies	Equipo que actúa de intermediario para el acceso a servicios. Los proxies pueden incluir las siguientes funciones: •Centralización y control de tráfico entre clientes y servidores. •NAT de salida, asignando la misma IP de salida a todos los usuarios de la red local. •Cacheado de contenidos, permitiendo agilizar el acceso a páginas a las que se ha accedido recientemente.
DMZ	Zona en la que se suelen ubicar los servidores que van a ser accesibles desde el exterior de la organización. Una DMZ es una subred aislada del exterior y de la LAN por los cortafuegos. En la DMZ están los servidores web, DNS, servidor de correo, etc.

PROTOCOLO DHCP		
Sirve para asignar una IP a un equipo. Va sobre UDP. DORA. Métodos de asignación de direcciones IP. **DORA** = **D**ISCOVER, **O**FFER, **R**EQUEST, **A**CK.		
Manual o estática	asigna una dirección IP a una máquina determinada (Ej: en base a la MAC).	
Automática	asigna una dirección IP de un Pool a una máquina cliente la primera vez que hace la solicitud al servidor DHCP y hasta que el cliente la libera (si no es permanente).	
Dinámica:	el único método que permite la reutilización dinámica de las direcciones IP de un Pool (tiene un tiempo de "préstamo").	
DHCPDISCOVER	Cliente pregunta qué DHCPs hay.	
	Puerto Origen 68.	Puerto Destino 67.
	Destino: MAC FF:FF:FF:FF:FF:FF.	Destino: IP 255.255.255.255.
DHCPOFFER	Servidores DHCP reservan una IP y la ofrecen, indicando el tiempo de lease.	
	Puerto Origen 67.	Puerto Destino 68.
	Destino: MAC Cliente.	Destino: IP propuesta.
DHCPREQUEST	Cliente pide a un servidor DHCP esa IP. Usa broadcast para avisar al resto de servidores DHCP de la IPelegida y para que puedan liberar las IPs ofrecidas.	
	Puerto Origen 68.	Puerto Destino 67.
	Destino: MAC: FF:FF:FF:FF:FF:FF.	Destino: IP 255.255.255.255.
DHCPACK	Servidor confirma. ACK.	
	Puerto Origen 67.	Puerto Destino 68.
	Destino: MAC Cliente.	Destino: IP Cliente.
Puertos UDP para DHCP	Cliente: 68	Servidor: 67



VLAN - 802.1q
Permiten crear grupos de usuarios servidos por uno o varios switches, separando dominios de difusión por switch.
El switch por defecto crea la VLAN 1 con todos los equipos. En un switch defines las VLANs y asignas los hosts. Mediante el protocolo VTP (VLAN Trunk Protocol) se propaga la definición de VLANs al resto de switches. También GVRP (Generic VLAN Registration Protocol) y MVRP (Multiple VLAN Registration Protocol).
Para configurar VLANs en el nivel 2 tendremos puertos etiquetados o Trunk o troncales. También tendremos puertos no etiquetados o Access o de acceso. Terminología Cisco (Trunk / Access).
802.1q es una modificación de la trama Ethernet, metiendo una cabecera (4 bytes), tagging o encapsulación, donde se informa el id de la VLAN (12 bits: 4096 redes). Quien pone la etiqueta es el switch.
El tráfico etiquetado va por los puertos trunk, para las conexiones entre puertos troncales. Los hosts no saben a qué VLAN pertenecen, por lo que el tráfico será no etiquetado y va por puertos de tipo access.