

# **Redes y Comunicación de datos**

**C8280**

César Lara Avila

# Introduccion al curso C8286

UNIDAD 1: Fundamento de Redes y Computación en la Nube

UNIDAD 2: Servicios AWS

UNIDAD 3: Aplicaciones de la tecnología AWS

UNIDAD 4: Proyecto Final

# Evaluación

Examen Parcial %30

Examen Final %40

Proyecto de Curso %30

# Empezamos

# Temario

- Conceptos fundamentales de redes
- Descripción general de las redes empresariales y la interconexión de redes
- MPLS- WAN para aplicaciones de alto rendimiento
- Administración de redes
- Redes Linux

# Conceptos fundamentales de redes

Las redes informáticas permiten compartir recursos de hardware y software.

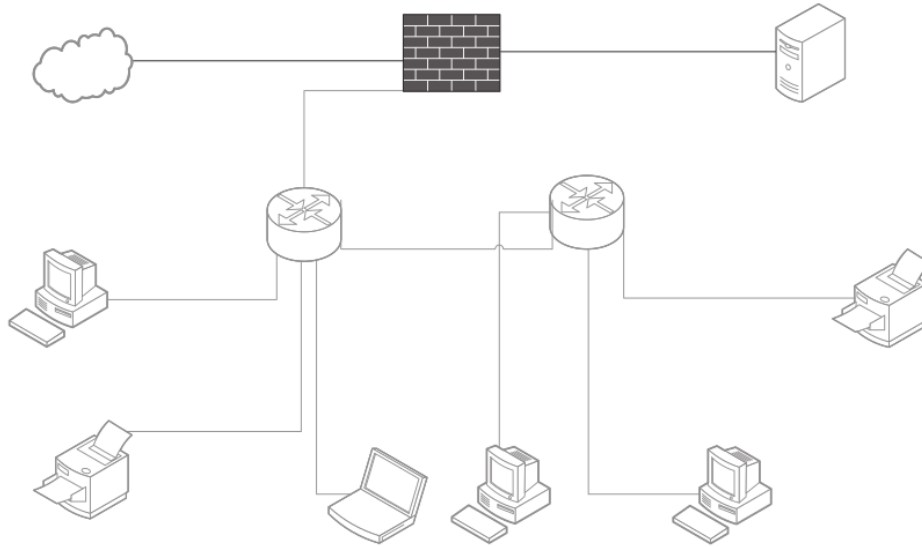
Hay dos modelos de referencia de red populares:

- Interconexión de sistemas abiertos (OSI)
- Protocolo de control de transmisión/Protocolo de Internet (TCP / IP).

Ambos proporcionan pautas generales para la construcción de redes y protocolos.

# Comunicación de redes

Una **red informática** es una colección de recursos informáticos conectados



# Dispositivos de red

Es un dispositivo que recibe un mensaje de un recurso en una red y determina cómo pasar el mensaje a lo largo de la red.

Los dispositivos de red comunes son:

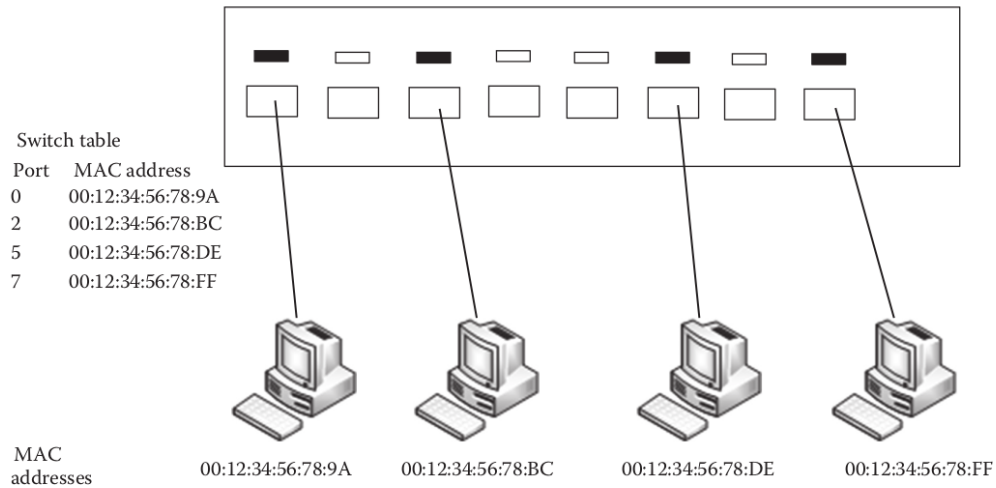
- Hub
- Switches
- Enrutadores (routers)
- Puertas de enlace (gateways).

Estos dispositivos pueden ser cableados, inalámbricos o ambos.

Un switch utiliza la dirección de destino del mensaje para determinar el dispositivo al que se debe pasar el mensaje **(MAC)** <sup>1</sup>.



Un dispositivo está conectado a un switch, el switch adquiere la dirección MAC ese dispositivo y la retiene en una tabla.



[1]media access control

# Tabla de enrutamiento

El router utiliza la dirección de red de destino del mensaje para enrutar el mensaje al siguiente paso a través de la red.

Esta dirección de red depende del tipo de protocolo de red. Asumiendo TCP/IP, la dirección de red es una dirección de Protocolo de Internet versión 4 (IPv4) o Protocolo de Internet versión 6 (IPv6).

Los routers realizan el reenvío <sup>1</sup>

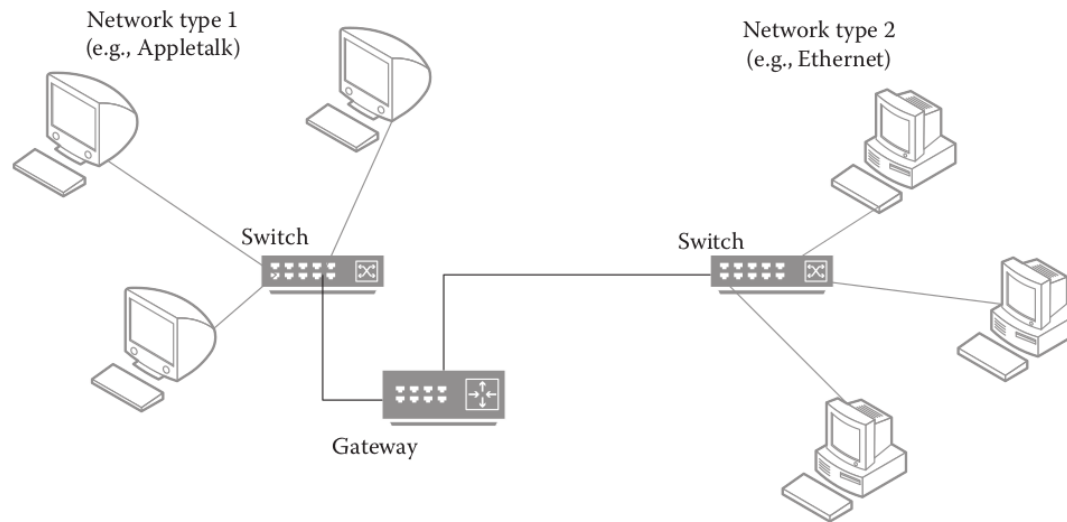
Network Destination	Netmask	Gateway	Interface	Metric
0.0.0.0	0.0.0.0	10.15.8.1	10.15.8.164	10
10.15.8.0	255.255.252.0	On-link	10.15.8.164	266
10.15.8.164	255.255.255.255	On-link	10.15.8.164	266
127.0.0.0	255.0.0.0	127.0.0.1	127.0.0.1	306
192.168.56.0	255.255.255.0	192.168.56.1	192.168.56.1	276
192.168.56.1	255.255.255.255	192.168.0.100	192.168.56.1	276
192.168.0.100	255.255.255.255	127.0.0.1	127.0.0.1	306
224.0.0.0	240.0.0.0	On-link	192.168.56.1	276
255.255.255.255	255.255.255.255	On-link	10.15.8.164	266

[1]forwarding

# Puerta de enlace

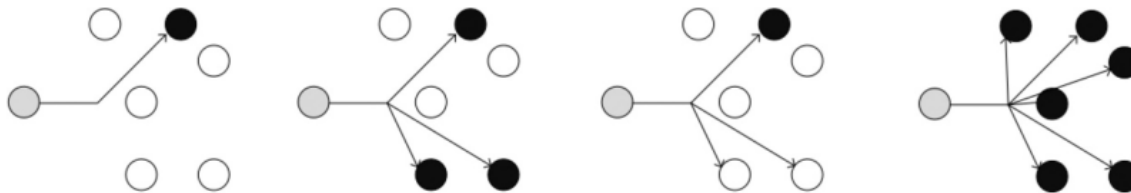
La puerta de enlace (gateway) es un router que conecta diferentes tipos de redes entre sí.

Tiene la capacidad de traducir un mensaje de un protocolo a otro.



# Formas de comunicación sobre una red

- Unicast: esta forma de comunicación permite enviar un mensaje desde un dispositivo de origen a un dispositivo de destino. La comunicación puede ser unidireccional o bidireccional.
- Multicast: es cuando hay varios dispositivos de destino para los que está destinado un mensaje.
- Con anycast, hay varios destinos que comparten la misma dirección IP.
- Un broadcast es un mensaje enviado desde un dispositivo a todos los demás en su subred local



# Servidores

El uso de servidores en una red sugiere que la red está configurada usando un modelo **cliente-servidor**.

Server Type	Usage/Role	Examples
Application server	Runs application software across the network, so that applications do not need to be installed on individual computers. In older client-server networks, an application server was often used so that the clients could be diskless (without a hard disk) and thus reduce the cost of the clients.	ColdFusion, Enterprise Server, GlassFish, NetWeaver, Tomcat, WebLogic, WebSphere, Windows Server
Database server	Provides networked access to a backend database.	DB2, Informix, Microsoft SQL Server, MySQL, Oracle
DHCP server	Provides dynamic IP addresses to clients in a network.	DHCP Server, dnsmasq, ISC DHCP
Email server	Transfers email messages between local client and email servers; gives clients access to incoming email (email messages can be stored on the server, client, or both).	Apache James, IBM Lotus Domino, Microsoft Exchange Server, Novell Groupmail, Novell NetMail, OpenSMTPD, Postfix/Sendmail
File server	Shared storage utility accessible over the network; there are many subclasses of file servers such as FTP servers, database servers, application servers, and web servers.	See the more specific types of servers
FTP server	Supports File Transfer Protocol, so that clients can upload and download files to and from the server. FTP is insecure, so it is not commonly used, except for possible anonymous file transfers (permitting clients to transfer public files without logging in).	Cerberus FTP Server, FileZilla Server, ftpd, freeFTPD, Microsoft Internet Information Services, WS FTP

Gaming server	Same as an application server, except that it is dedicated to running a single game to potentially thousands or millions of users across the Internet.	Varies by game
List server	Type of mail server that manages lists, so that email messages can be sent to all on the list. This feature may be built into the mail server.	LISTSERV, Mailman, Sympa
Name server (or DNS server)	Resolves domain names (IP aliases) into IP addresses and/or serves as a cache.	BIND, Cisco Network Registrar, dnsmasq, Simple DNS Plus, PowerDNS
Print server	Connects clients to a printer to maintain a queue of print jobs, as submitted by the clients. Provides clients with feedback on status of print jobs.	CUPS, JetDirect, NetBOIS, NetWare
Proxy server	Intermediaries between web clients and web servers. The proxy server has several roles: caches web pages within an organization for more efficient recall; provides security mechanisms to prevent unwanted requests or responses; and provides some anonymity for the web clients. A reverse proxy server is used as a front end to a web server for load balancing.	CC Proxy Server, Internet Security and Acceleration Server, Squid, WinGate
SSH server	Uses the Secure Shell Protocol to accept connections from remote computers. Note that FTP does not permit encryption, but secure versions are available over SSH such as SFTP.	Apache MINA SSHD, Copssh, OpenSSH, Pragma Systems SSH Server, Tectia SSH Server

Server Type	Usage/Role	Examples
VM server	Server that creates virtual machines that themselves can be used as computers, web servers, email servers, database servers, and so on.	Microsoft Hyper-V, VMware vSphere Server
Web server	Form of file server to respond to HTTP requests and return web pages. If web pages have server-side scripts, these are executed by the web server, making it both a file server and an application server.	AOLserver, Apache, Internet Information Services, NGINX, OpenLiteSpeed, Oracle HTTP Server, Oracle WebLogic Server, TUX web server

# Medios de red

La conexión puede venir en dos formas diferentes: alámbrica e inalámbrica. Nos referimos a estas conexiones como los medios.

Las formas cableadas de conectividad de red son par trenzado (twisted-wire-pair) , cable coaxial y cable de fibra óptica.



[1] Fox, R., Information Technology: An Introduction for Today's Digital World, CRC Press, Boston, FL, 2013



Las **formas blindadas (shielded forms)** todavía se usan comúnmente para la red telefónica fija, mientras que las formas no blindadas se pueden encontrar en la LAN de estilo Ethernet.

El **cable de fibra óptica** no depende de la corriente eléctrica en absoluto, sino que es una pieza de vidrio. La información se envía a través de un cable de fibra óptica mediante la transmisión de pulsos de luz.

El cable de fibra óptica tiene numerosas ventajas sobre el cable de cobre. Estos se enumeran a continuación:

- Ancho de banda mucho mayor
- Distancia mucho mayor a la que pueden viajar las señales sin pérdida o necesidad de repetidores.
- Mucha menos susceptibilidad a las influencias externas, como el ruido de la radio o la caída de rayos.
- Hay menos riesgo de robo.

El principal inconveniente del cable de fibra óptica es que es mucho más caro que el cable de cobre.

La **fibra óptica** transmite directamente información digital (unos y ceros enviados como pulsos de luz). Por lo tanto, se requiere menos trabajo en cualquiera de los extremos de la transmisión para enviar o recibir datos de computadora.

La **comunicación inalámbrica** implica ningún tipo de cable. La información se convierte en una forma de onda y se transmite por el aire.

Requiere mecanismos de seguridad adicionales para evitar que alguien espíe fácilmente la comunicación. El **cifrado** se usa comúnmente hoy en día para reducir esta preocupación, pero solo es valioso si los usuarios saben cómo emplearlo.

# Capacidades de ancho de banda de las formas de transmisión

**Ancho de banda:** se define la cantidad de datos que se pueden transmitir a la vez.

Nos referimos al ancho de banda como el número de bits transmitidos por segundo.

## Network Media Bandwidths

Type	Minimum Bandwidth	Maximum (Theoretical) Bandwidth
Shielded twisted-wire pair	10 Mbps	100 Mbps
Unshielded twisted-wire pair	10 Mbps	1000 Mbps
Coaxial cable	10 Mbps	100 Mbps
Fiber optic cable	100 Mbps	100 Gbps
Wireless using radio frequency	9 Kbps	54 Mbps

# Tiempo de transferencia para cada uno de los medios dados

## Download Times for Various Bandwidths

Medium	Download Time
MODEM (300 bps)	7 hours, 24 minutes, 27 seconds
MODEM (1200 bps)	1 hour, 51 minutes, 7 seconds
MODEM (9600 bps)	13 minutes, 53 seconds
MODEM (14,400 bps)	9 minutes, 16 seconds
MODEM (28,800 bps)	4 minutes, 38 seconds
MODEM (56,000 bps)	2 minutes, 23 seconds
MODEM (300 mbps)	0.027 seconds
Twisted-wire and coaxial cable—minimum/maximum	0.8 second/0.08 second
Twisted-wire (unshielded)—maximum	0.008 second
Fiber optic—minimum/maximum	0.08 second/0.00008 second
3G	0.67 second
4G	0.08 second
Wireless (802.11n)	0.013 second

# Hardware de red

¿Cómo accede una computadora individual a la red?

Esto lo hace uno de dos dispositivos, una tarjeta de interfaz de red (NIC) <sup>1</sup> o un MÓDEM <sup>2</sup>

NIC

- Es una placa de circuito electrónico que se desliza en una de las ranuras de expansión de una computadora en la placa base.
- La NIC recibe datos de la memoria como palabras o bytes y luego envía los bits secuencialmente o recibe bits secuencialmente de la red y los vuelve a compilar en bytes y palabras para enviarlos a la memoria.
- La NIC tiene su propia dirección de hardware única, comúnmente conocida como dirección MAC.

[1]Network Interface Card

[2]MOfulation DEModulation

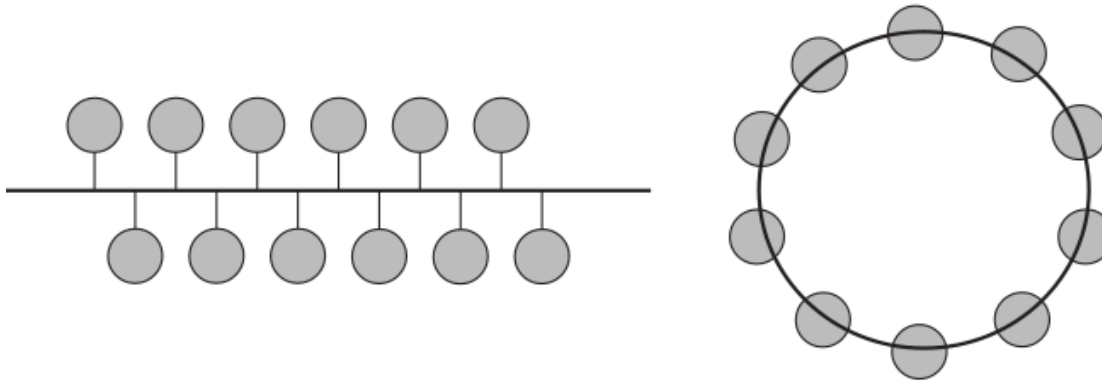
- La NIC tiene un puerto o una conexión que sobresale de la computadora. La NIC está físicamente conectada a este puerto a través de algún tipo de enchufe (plug) como el RJ-45,
- Una NIC inalámbrica es aquella que envía señales de radio a un dispositivo cercano llamado punto de acceso.
- La señal de radio que transmite la NIC más común es una señal de alta radiofrecuencia de banda estrecha. La señal de radio está limitada en distancia a no más de unos pocos miles de pies antes de que la señal se degrade hasta el punto de que haya pérdida de datos.

## MODEM

- Los términos de MODEM expresan la conversión de información digital en información analógica (modulación) y de información analógica en información digital (demodulación).
- El problema con el uso de un MODEM es la dependencia del ancho de banda relativamente bajo disponible en la red telefónica pública.

# Tipos de redes

## Topología de red

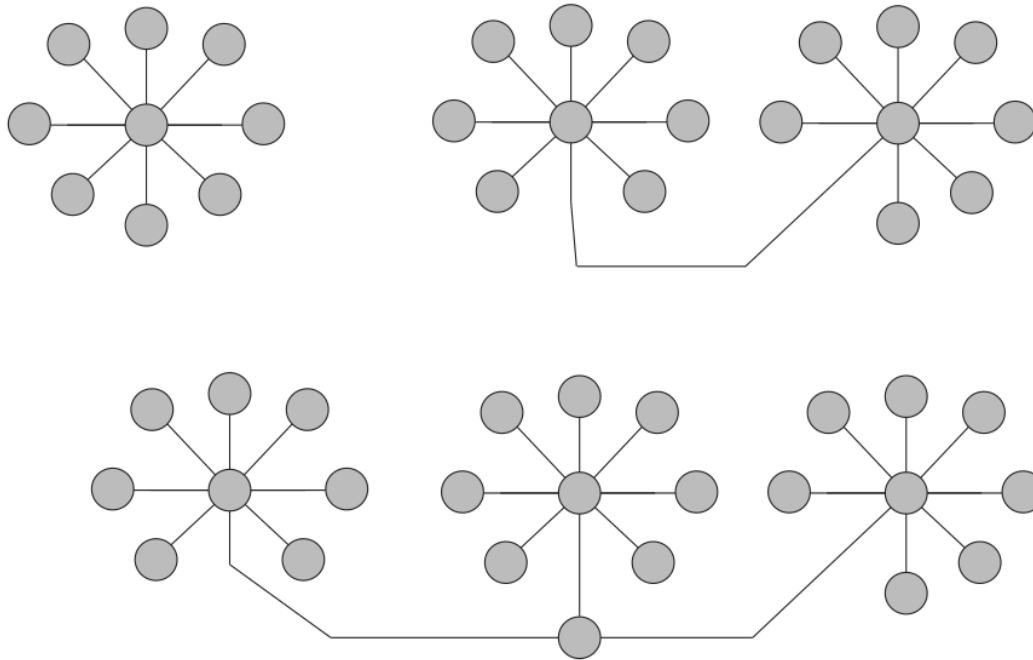


Importante

La tecnología Ethernet desarrolló una estrategia para manejar las colisiones conocida como CSMA/CD <sup>1</sup> en estos casos.

[1] Carrier-sense multiple access with collision detection.

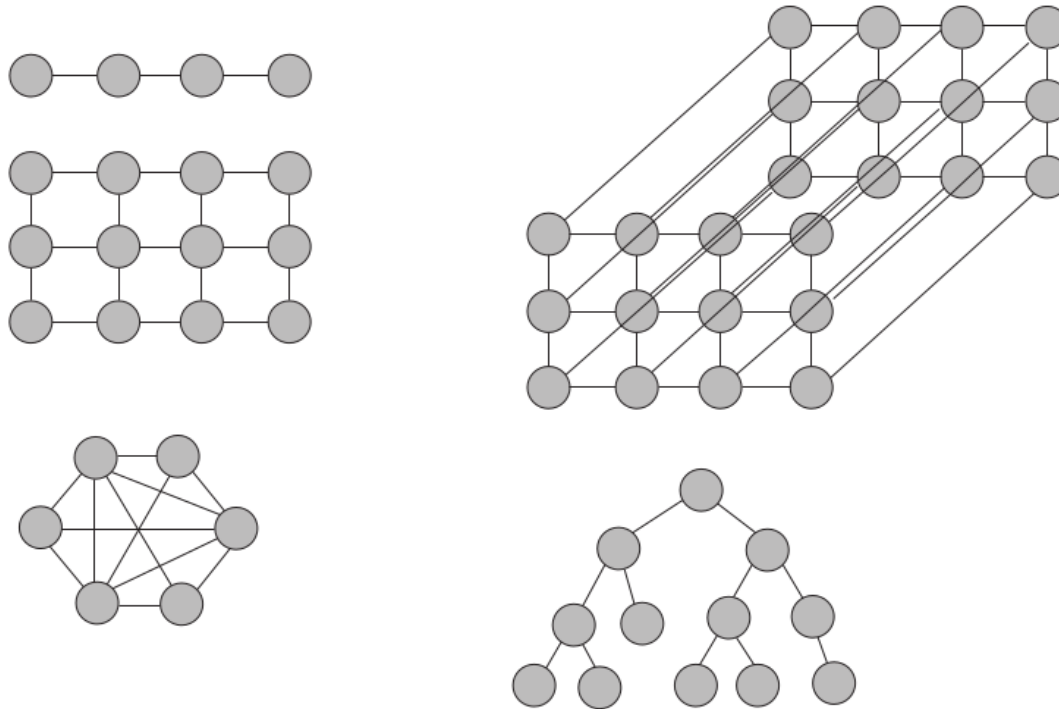
## Topología de estrella



**Figura 7: diversas formas de la topología estrella.**



## Topología de vecino más cercano



**Figura 8: diseño de los vecinos más cercanos.**

# Clasificación de redes

La idea de conectar switches/routers juntos se conoce como encadenamiento.

- LAN a menudo se refiere a una red de unas pocas docenas a unos pocos cientos de recursos en las proximidades.
- Una red pequeña es la red de área personal (PAN), que encontraremos en muchos hogares.
- Una CAN (área de campus), es una red que se extiende a lo largo de muchos edificios de una organización.
- WAN (red de área amplia).
  - Red de área metropolitana (MAN).
  - **Internet**

# Protocolos de red

Un **protocolo de comunicación**, o un protocolo de red, es un conjunto de reglas que determinan cómo se transmiten, direccionan, enrutan e interpretan los datos.

La mayoría de los protocolos de red realizan sus variadas tareas través de una **serie** de traducciones, no a través de una sola traducción de un mensaje de las señales de red transportadas por la red. Esto se hace al tener capas en el protocolo.

Cuando hay varias capas, generalmente nos referimos a la serie como una pila de protocolos porque cada capa es manejada por un protocolo diferente.

Una sola capa en un protocolo es un conjunto de reglas para traducir el mensaje a una nueva forma, ya sea para prepararlo para la transmisión a través de la red o para preparar el mensaje transmitido para ser presentado al usuario.

Toda la comunicación a través de una red se divide en bits.

Necesitamos una forma de informar al hardware y al software que al examinar un mensaje pueda interpretar información como:

- ¿A quién va dirigido el mensaje (dirección de destino)?
- ¿Qué software de aplicación debería usar el mensaje?
- ¿Cuánto dura el mensaje?
- Si el mensaje está completo o es solo un paquete de muchos.
- Si hay un error en el mensaje transmitido y cómo manejar el error.
- ¿Cómo se debe establecer una conexión entre los recursos de origen y destino (si es necesario)?
- Si el mensaje incluye datos codificados y/o está encriptado.

Dichos detalles se dejan en manos del protocolo de red utilizado para empaquetar y transmitir el mensaje.

A medida que un mensaje desciende en la pila de protocolos, se agrega información al comienzo del mensaje. Este contenido agregado se conoce como **encabezado**, y cada capa de la pila de protocolos puede agregar su propio encabezado.

En algunos casos, se puede agregar información adicional al final del mensaje, en cuyo caso la información agregada se conoce como pie de página.<sup>1</sup>

Al recibir un mensaje, la pila de protocolos funciona a la inversa, eliminando encabezados (y/o pies de página) a medida que el mensaje asciende por las capas.

[1] footer

# TCP/IP

- TCP/IP se compone de dos conjuntos de protocolos separados TCP y IP
- Todas las redes y dispositivos se describen a través de una dirección de red.
  - Protocolo de Internet versión 4 (IPv4) o IPv6
- Las direcciones IPv4 son direcciones de 32 bits e IPv6 son direcciones de 128 bits.
- Los mensajes que se envían de un dispositivo a otro se envían mediante algún tipo de protocolo.
  - El dispositivo receptor utilizará ese protocolo para interpretar la secuencia de bits del mensaje. Este protocolo se indica mediante un número de puerto.
  - El puerto dicta una aplicación para utilizar, como un navegador web, para usar cuando el dispositivo recibe un mensaje codificado mediante el Protocolo de transferencia de hipertexto (HTTP).

# OSI

Es un modelo con la intención de ofrecer a los arquitectos de red una estructura a la que apuntar al desarrollar nuevos protocolos.

Las siete capas se clasifican en dos tipos de capas: las capas de host y las capas de medios.

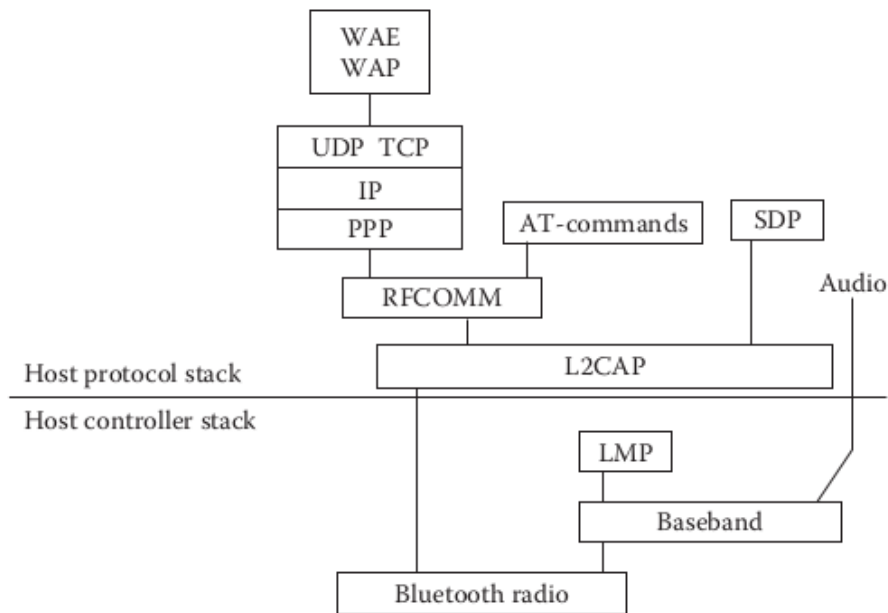
## The Seven Layers of OSI

Layer Name	Layer Type	Layer Data Unit	Role
7. Application	Host layers	Data	Application software produces/displays message
6. Presentation			Application neutral format
5. Session			Maintain communication between hosts
4. Transport		Segments	Deal with errors and packet ordering
3. Network	Media layers	Packets/datagrams	Addressing and traffic control
2. Data link		Bit/frame	Connection between two network nodes
1. Physical		Bit	Network transmission

# Bluetooth

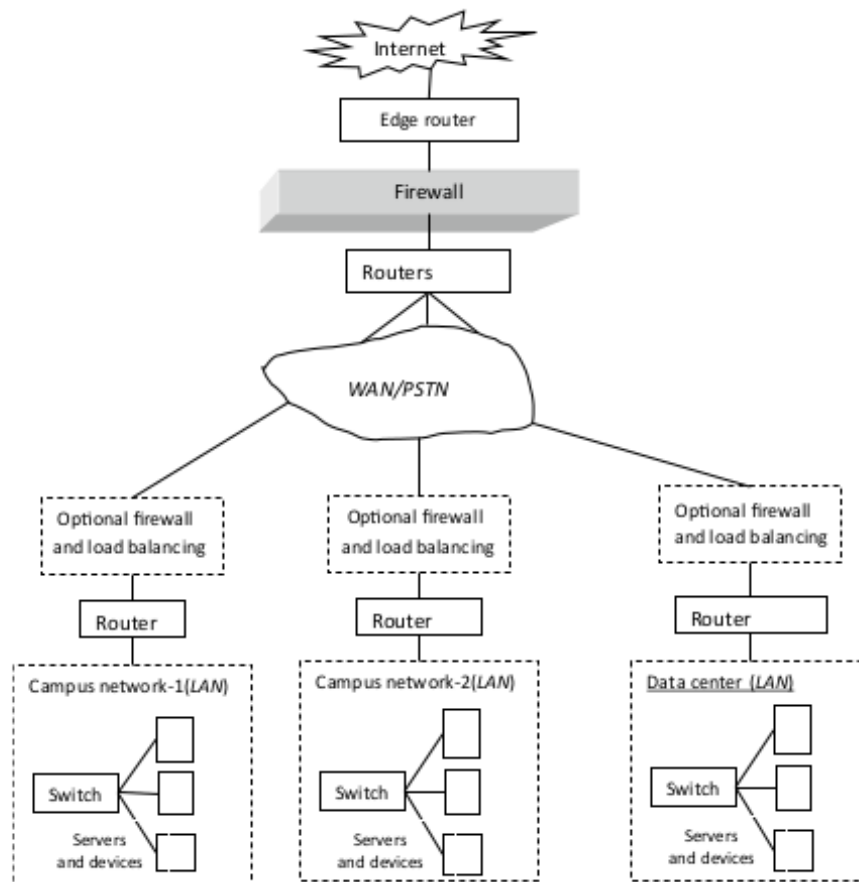
Esta tecnología inalámbrica, es una combinación de hardware y protocolo para permitir la comunicación de voz y datos entre recursos.

La pila de protocolos de Bluetooth se divide en dos partes: una pila de controlador de host que se ocupa de los problemas de temporización y la pila de protocolo de host que se ocupa de los datos.





# Descripción general de las redes empresariales y la interconexión de redes



Por lo general, una empresa tiene varias redes de campus, sucursales y centros de datos diferentes en diferentes ubicaciones que están conectados entre sí mediante LAN o WAN.

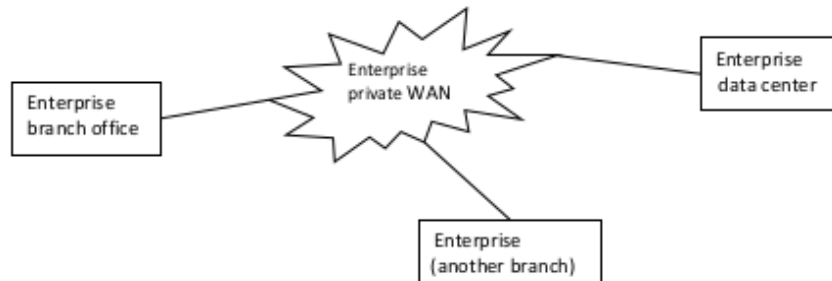
Además de las sucursales y las redes de campus, las empresas también tienen **centros de datos**.

En general, el objetivo principal de las redes empresariales es proporcionar una red troncal integrada para la comunicación entre grupos de trabajo individuales, LAN, centros de datos y usuarios.

Se utilizan varias técnicas de interconexión de redes empresariales, como WAN privada, IPVPN y WAN MPLS, para interconectar diferentes LAN y WAN.

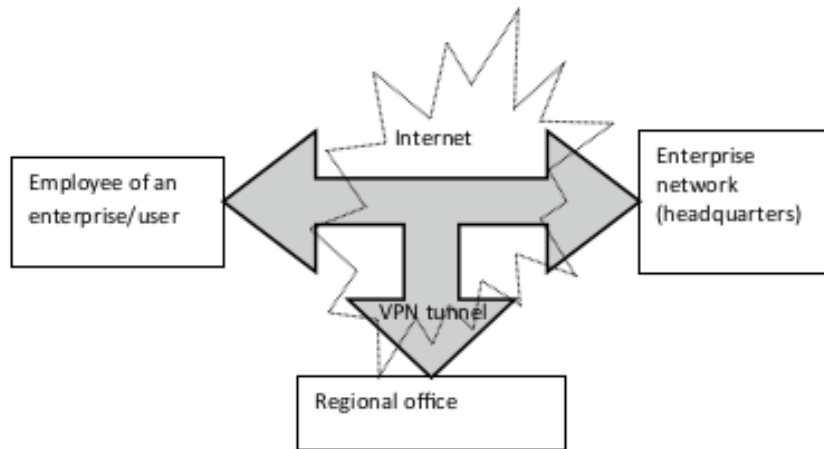
## Red privada empresarial WAN

Las redes WAN privadas empresariales interconectan las sucursales, los centros de datos y la oficina central de una empresa que están separados por más de 1 km.



## Red privada virtual de protocolo de Internet

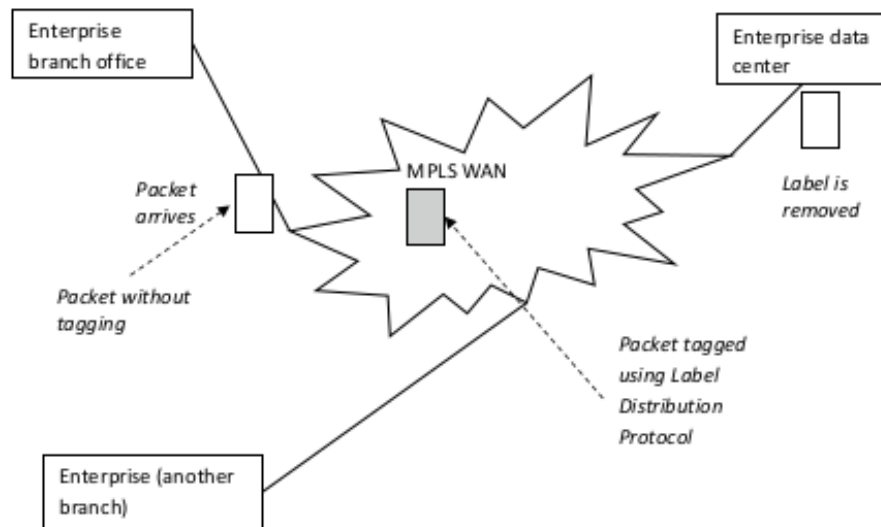
Las empresas pueden ampliar sus redes privadas mediante conexiones cifradas a través de Internet. Un empleado de una empresa que trabaja fuera de la empresa (por ejemplo, en casa) puede conectarse de forma segura a la red empresarial a través de túneles VPN.



# MPLS- WAN para aplicaciones de alto rendimiento

MPLS WAN permite usar una sola red para aplicaciones de datos, voz, video y negocios. Se utiliza para conectar centros de datos, sedes corporativas y sucursales de acuerdo con las necesidades de diversas aplicaciones de las empresas.

La red MPLS WAN es una red segura y garantizada que ofrece un servicio MPLS dedicado.



# Administración de redes

La administración de la red es la forma de hacer que una red cumpla con las expectativas que tengas de ella.

Un marco para clasificar todos los aspectos de una red a administrar conocida es FCAPS<sup>1</sup> que representa las siguientes áreas:

- Administración de fallos
- Administración de configuración
- Administración de contabilidad
- Administración del rendimiento
- Administración de seguridad

<sup>1</sup> <https://en.wikipedia.org/wiki/FCAPS>

Administrar un sistema de red significa interactuar con el sistema de alguna manera. Por lo general, involucra lo siguiente:

- Acceder a la CLI a través de SSH (¡no use Telnet!) o directamente a través de un puerto de consola para configuración, monitoreo y solución de problemas
- Monitorear (y en ocasiones cambiar) el sistema a través de agentes de Protocolo simple de administración de red (SNMP) y Bases de información de administración (MIB)
- Recopilación de registros del sistema a través de syslog
- Recopilación de estadísticas de flujo de tráfico con NetFlow o IP Flow Information Export (IPFIX)
- Enviar información y extraer información de dispositivos de red a través de interfaces de programación de aplicaciones (API), ya sea que las API sean RESTful (como RESTCONF) o no (como NETCONF o gRPC).

# Automatización

La automatización, de manera muy simple, significa usar software para realizar una tarea que de otro modo haría manualmente.

## Ventajas

La automatización ofrece las siguientes ventajas:

- Implementación rápida de cambios en la red
- Asistencia de realizar tareas rutinarias repetitivas
- Cambios de sistema consistentes, confiables, probados y que cumplen con los estándares
- Reducción de errores humanos y configuraciones incorrectas de la red
- Mejor integración con políticas de control de cambios
- Mejor documentación de red y análisis de cambios.



# Orquestación

La orquestación es la coordinación de muchas tareas automatizadas, en una secuencia específica, a través de sistemas dispares para lograr un solo objetivo (flujo de trabajo).

Hay una gran cantidad de herramientas de orquestación disponibles en el mercado que incluyen las siguientes:

- Cloud Cisco Network Services Orchestrator (NSO) <sup>1</sup> , que, como su nombre lo indica, se centra en los servicios de red.
- RedHat Ansible <sup>2</sup> , que generalmente se usa como una herramienta de automatización simple, pero también puede realizar cierta automatización del flujo de trabajo
- Kubernetes <sup>3</sup> , una plataforma especializada para orquestar cargas de trabajo y servicios en contenedores.

[1] <https://www.cisco.com/c/en/us/products/cloud-systems-management/network-services-orchestrator/index.html>

[2] <https://www.redhat.com/en/technologies/management/ansible>

[3] <https://kubernetes.io/>.

# Programabilidad

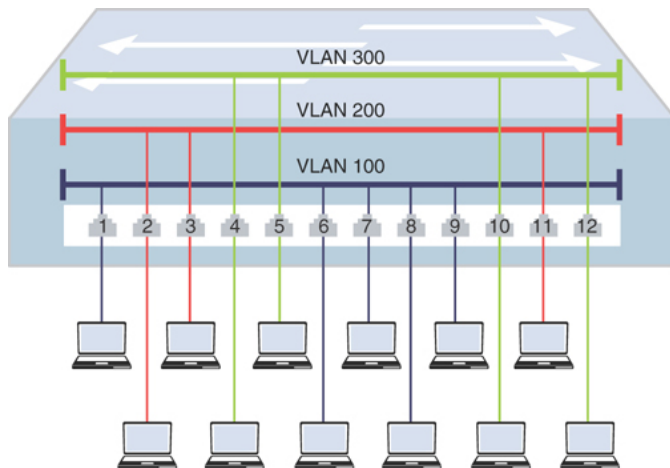
La programabilidad, utilizada en este contexto, es la capacidad de monitorear dispositivos, recuperar datos y configurar dispositivos a través de una interfaz programable, que es una interfaz de software para su dispositivo a través de la cual otro software puede hablar con su dispositivo.

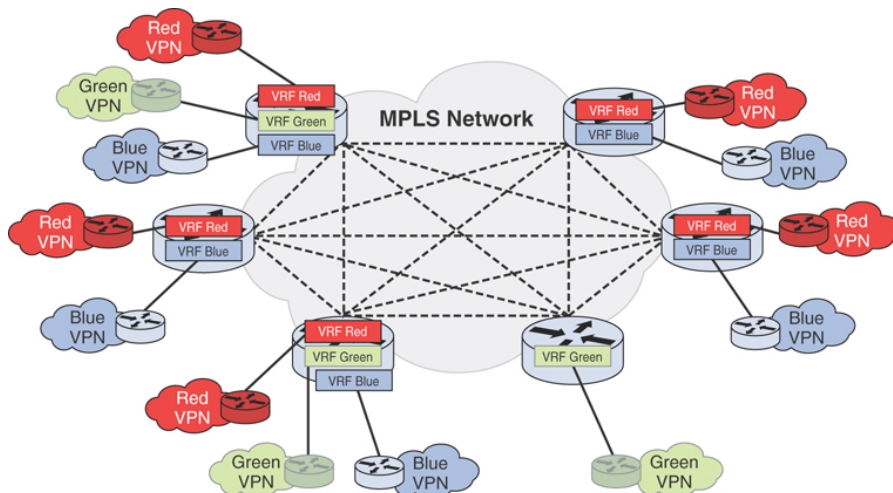
Esta interfaz se conoce formalmente como **Interfaz de programación de aplicaciones (API)**.

# Virtualización y abstracción

La virtualización es la creación de un servicio que se comporta como un servicio físico pero no lo es.

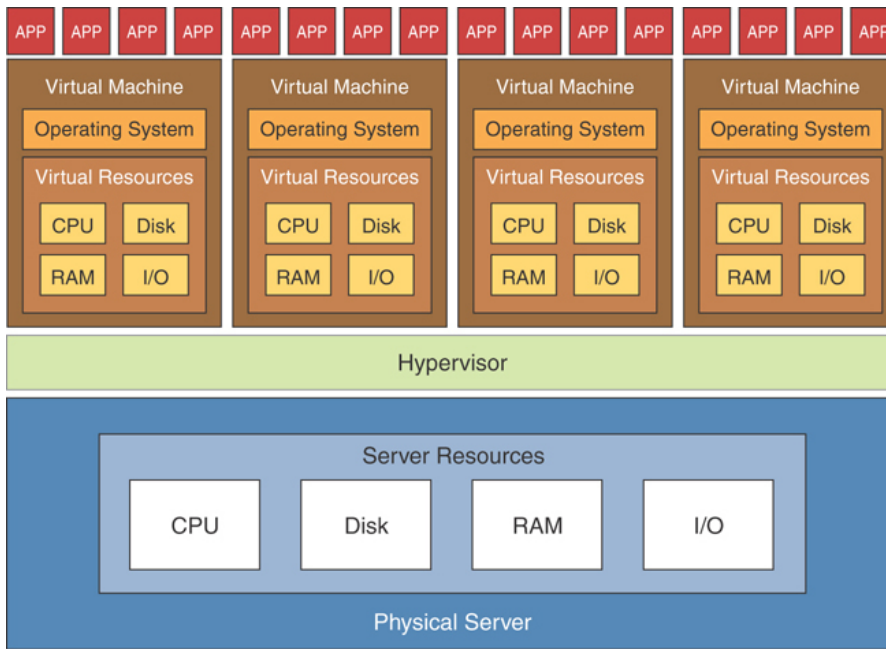
Es un servicio solo por software o definido por software construido sobre uno o más dispositivos de hardware.





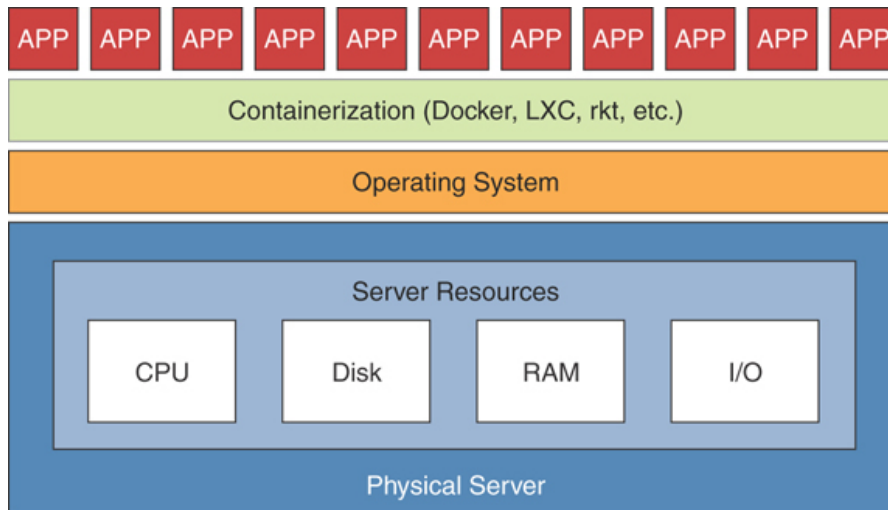
La abstracción va de la mano con la virtualización porque construimos servicios virtualizados sobre abstracciones.

Las máquinas virtuales<sup>1</sup>, por ejemplo, se basan en una abstracción del servidor físico subyacente.



<sup>1</sup> <https://www.serverwatch.com/virtualization/server-virtualization/>

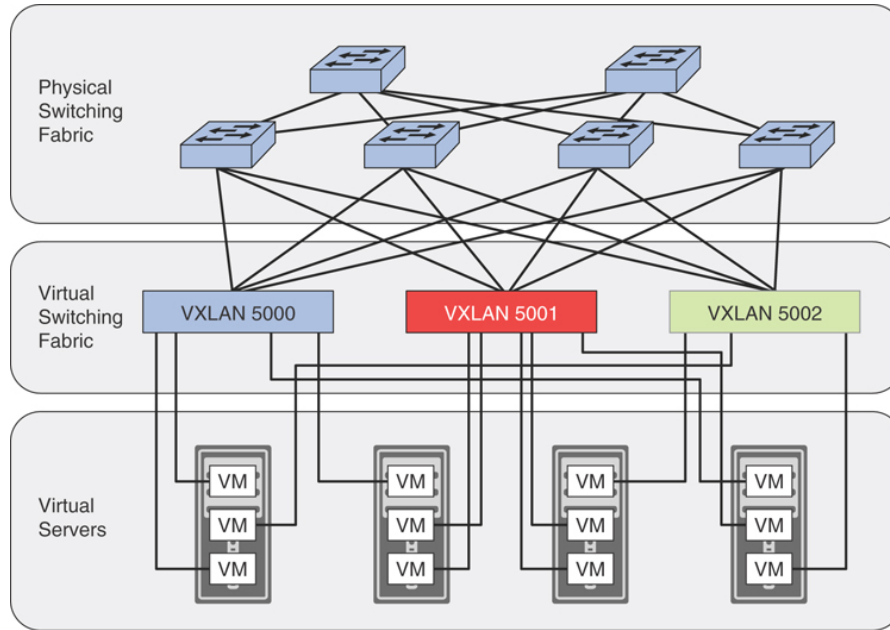
Otro ejemplo, que se apega a los servidores, es una plataforma de contenedores como Docker <sup>1</sup>.



<sup>1</sup> <https://www.docker.com/>

La abstracción de la red es la misma idea pero con más elementos.

Al agregar una **capa de abstracción**, o abstraer la red, se concentra únicamente en la red virtualizada.



Uso de NAPALM (Network Automation and Programmability Abstraction Layer with Multivendor Support) <sup>1</sup>.

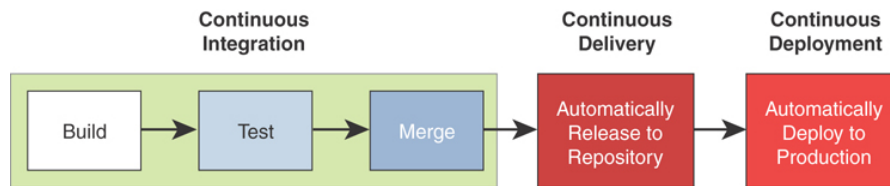
<sup>1</sup> <https://github.com/napalm-automation/napalm/tree/master>



La abstracción de la red da lugar a la red como código (NaC) o la infraestructura más amplia como código, que abarca la red, el almacenamiento y la computación.

NaC<sup>1</sup> es el código que une la abstracción, la virtualización, la programación y la automatización de la red para crear una interfaz inteligente para su red.

NaC también lleva las redes al ámbito de DevOps y permite la aplicación de prácticas de software comprobadas como CI/CD.



<sup>1</sup> <https://victorops.com/blog/network-as-code-ansible-and-automation-for-an-agile-infrastructure>.

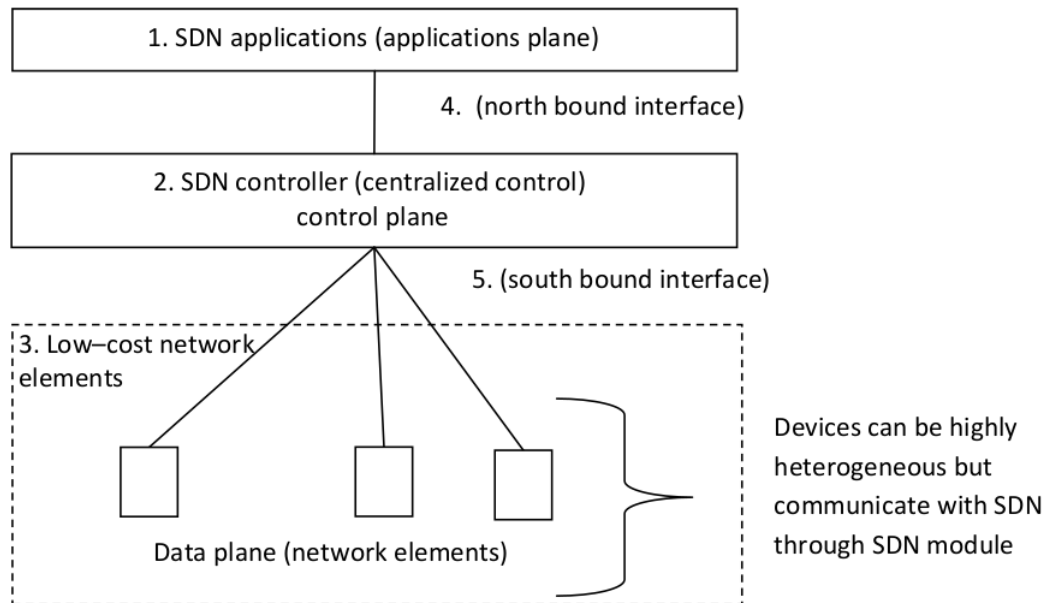
En estos días, las herramientas de automatización interactúan con los dispositivos de red a través de API, que son en sí mismas abstracciones del dispositivo físico subyacente.

La diferencia es que las API residen en los dispositivos individuales y son específicas de su propio dispositivo.

El software de automatización generalmente se comunica con las API a través del eXtensible Markup Language (XML) o JavaScript Object Notation (JSON), o XML Schema Definition (XSD), y JSON Schema Definition (JSD).

# Redes definidas por software (SDN,

SDN es un marco conceptual en el que las redes se tratan como abstracciones y se controlan mediante programación, con un toque directo mínimo de los componentes individuales de la red.



# Un concepto más formal

David Ward en el libro SDN: Software Defined Networks de Ken Gray y Tom Nadeau:

SDN permite funcionalmente que los operadores accedan a la red de manera programática, lo que permite la administración automatizada y técnicas de orquestación, aplicación de la política de configuración en múltiples enrutadores, switches y servidores y el desacoplamiento de la aplicación que realiza estas operaciones del sistema operativo del dispositivo de red.

# Redes basadas en intención

Intent-Based Networking (IBN) es el siguiente paso evolutivo más allá de SDN.

Dependiendo de la implementación, el sistema IBN envía las configuraciones desarrolladas a un controlador para su implementación en la infraestructura

Una vez que tu intención está configurada un sistema IBN usa telemetría de circuito cerrado y tablas de estado para monitorear la red y asegurarse de que no se desvíe de tu intención expresada (garantía de la intención).

# Necesidad de una configuración de red programable/automática

SOA proporciona interacciones de aplicación a aplicación con la ayuda de un bus de servicio empresarial (ESB).

La arquitectura de microservicios reciente (MSA) proporciona la arquitectura para desarrollar aplicaciones en forma de **microservicios**. Los microservicios son autónomos y auto-desplegables. Esto hace que la implementación sea mucho más sencilla.

Las empresas se enfocan en el modelo de proceso de desarrollo de software reciente, es decir, Agile. Lo hacen porque el modelo Agile acepta las demandas cambiantes y dinámicas de los clientes y enfatiza la integración continua y la entrega continua del desarrollo de software.

Si la configuración de la red se hace programable, las necesidades de las empresas pueden satisfacerse fácil y rápidamente. La entrega continua y el modelo ágil se pueden introducir sin problemas.

# Redes en Linux

Hay tres métodos populares para administrar redes Linux:

- Uso de la utilidad ip de la línea de comandos
- Usando el servicio NetworkManager
- Usando archivos de configuración de red.

# La utilidad ip

**ip** es una utilidad de línea de comandos que forma parte del grupo de utilidades `iproute2`.

Se invoca mediante el comando `ip [options] {objet} {action}`.

```
ip link show
```

Para limitar la salida a una interfaz específica, puedes agregar `dev {intf}` al final del comando, como también se muestra en el ejemplo.

```
ip link show dev lo
```



## Objetos que se utilizan comúnmente con el comando ip.

Object	Description
<b>address</b>	IPv4 or IPv6 protocol address
<b>link</b>	Network interface
<b>route</b>	Routing table entry
<b>maddress</b>	Multicast address

Las acciones que se pueden utilizar con el comando **ip** se limitan a tres opciones enumeradas:

Action	Description
<b>add</b>	Adds the object
<b>delete</b>	Deletes the object
<b>show (or list)</b>	Displays information about the object

- El comando `ip addr` enumera todas las interfaces del sistema, cada una su información de dirección IP
- El comando `ip maddr` muestra la información de multidifusión para todas y cada una de las interfaces
- El comando `ip neigh` muestra la tabla ARP.
- Puedes activar o desactivar una interfaz en Linux utilizando el comando `ip link set {intf} {up|down}`. La acción de establecer solo es aplicable al objeto de enlace.

## Ejemplo

```
ip link show dev lo
```

Agrega una dirección IP a una interfaz usando el comando `ip addr add {IP_address} dev {intf}`.

El comando `ip addr show dev lo` se utiliza para inspeccionar la dirección IP de la interfaz antes y después del cambio.

```
ip addr show dev lo
ip addr add 10.1.0.10/24 dev lo
ip addr show dev lo
ip addr del 10.1.0.1/24 dev lo
ip addr show dev lo
```

En modo sin control, una interfaz acepta todos y cada uno de los paquetes entrantes. Puede habilitar este modo usando el comando `ip link set {intf} promisc on`.

En la tabla de enrutamiento, la lista de rutas en el sistema se puede mostrar us el comando `ip route`.

```
ip addr
ip route
sudo ip addr add 10.2.0.30/24 dev lo
ip addr show dev lo
ip route
```

# Funcionalidad de la tabla de enrutamiento en Linux



```
#Server 1
ip addr add 10.1.0.10/24 dev lo
ip addr add 10.2.0.10/24 dev l1
ip addr show enp0s7 | grep "inet "
ip addr show enp0s8 | grep "inet "

#Server2
ip addr add 10.1.0.20/24 dev l3
ip addr show enp0s3 | grep "inet "

#Server3
ip addr add 10.2.0.30/24 dev l3
ip addr show dev enp0s3 | grep "inet "
```

Un ping al servidor conectado directamente se realiza correctamente en los tres servidores. Sin embargo, cuando el server2 intenta hacer ping al server3, el ping falla.

## Posible respuesta?

```
! server2
# ip route add 10.2.0.0/24 via 10.1.0.10
# ip route
ping -c 1 10.2.0.10
```

```
! server3
# ip route add 10.1.0.0/24 via 10.2.0.10
# ip route
# ping -c 1 10.1.0.10
# ping -c 1 10.1.0.20
```

La sintaxis general para agregar una ruta a la tabla de enrutamiento es `ip route add {destination} {/ mask} via {nexthop}`.

## ! server2

```
# ip route add 10.2.0.0/24 via 10.1.0.10
# ip route
# ping -c 1 10.2.0.10
# ping -c 1 10.2.0.30
```

## ! server3

```
# ip route add 10.1.0.0/24 via 10.2.0.10
# ip route
# ping -c 1 10.1.0.10
# ping -c 1 10.1.0.20
```

## Como se habilita el reenvío en el kernel de server1?.

```
# echo 1 > /proc/sys/net/ipv4/ip_forward
# cat /proc/sys/net/ipv4/ip_forward

! El ping de server2 a server3 es exitoso
# ping -c 1 10.2.0.30

! El ping de server3 a server2 es exitoso
# ping -c 1 10.1.0.20
```

### Algunas funciones de ip

- Elimina una entrada de la tabla de enrutamiento `ip route delete {destination} {/ mask} via {nexthop}`.
- Que las rutas apunten a las interfaces de salida `ip route add {destination} {/ mask} dev {intf}`.
- Puedes agregar una ruta predeterminada usando la sintaxis `ip route add default via {next_hop} dev {intf}`.



# El servicio NetworkManager

NetworkManager es el servicio de administración de red que puede verificar un estado y puede iniciarlo, detenerlo, habilitarlo o deshabilitarlo como puede hacerlo con cualquier otro servicio en Linux mediante el comando `systemctl`.

- Interfaces gráficas de usuario (GUI)
  - Network Control Center
  - Connection Editor
- NetworkManager command-line interface (nmcli)
- NetworkManager text user interface (nmtui)
- API

NetworkManager se ocupa de objetos llamados **conexiones**.

```
# nmcli con show
```

Para activar|desactivar una conexión inactiva nmcli con up|down {connection\_name}.

Detalles de una conexión específica y enumerar su configuración y sus valores, usar nmcli con show {connection\_name}.

```
# nmcli con show "redpucp"
```

Para enumerar los dispositivos en el sistema usa el comando nmcli dev status para todos los dispositivos

- Para un dispositivo específico nmcli dev show {device\_name}.

```
# nmcli dev status
```

```
# nmcli dev show lo
```

## ¿ Qué crees que hacen estos comandos ?

```
# nmcli con show
# nmcli con del "Wired connection 1"
# nmcli con del "Wired connection 2"

# nmcli con show
# nmcli con add con-name NetDev_1 type ethernet ifname enp0s8 ip4
10.1.0.10/24 gw4 10.1.0.254

# nmcli con show
# nmcli con show --active
# nmcli dev status
# nmcli dev show lo
# ping 10.1.0.20 -c 3
```

Después de que se crea una conexión, podemos modificar su configuración usando el comando nmcli con `mod {connection_name} {setting} {value}`.

## ¿ Qué crees que hacen estos comandos ?

```
# nmcli con show NetDev_1 | grep ipv4.addr
# nmcli dev show lo | grep IP4.ADD
# nmcli con mod NetDev_1 ip4 10.1.0.100/24
```

```
# nmcli con show NetDev_1 | grep ipv4.addr
# nmcli dev show lo | grep IP4.ADD
```

```
# nmcli con up NetDev_1
# nmcli dev show lo | grep IP4.ADD
# nmcli con mod NetDev_1 ipv4.address
# nmcli con up NetDev_1
```

```
# nmcli con show NetDev_1 | grep ipv4.addr
# nmcli dev show lo | grep IP4.ADD
```

# Scripts de red y archivos de configuración

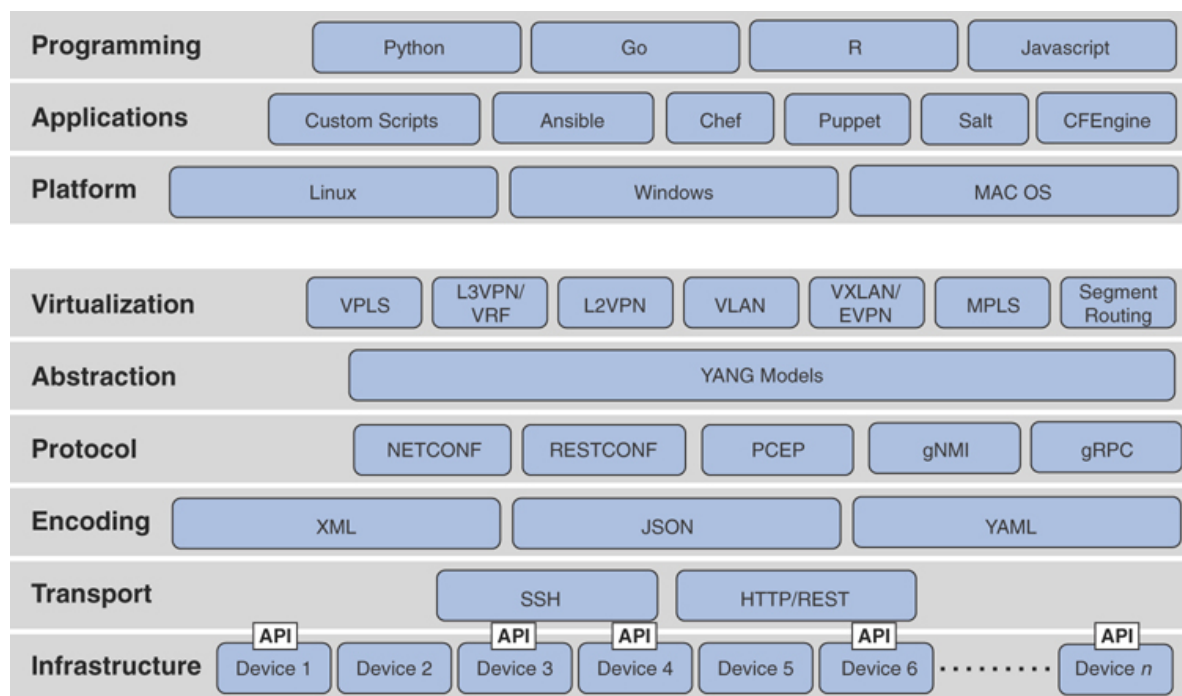
Modifica los archivos de configuración y los scripts de red directamente.

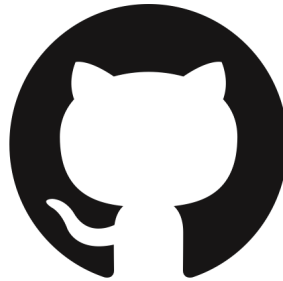
En las distribuciones de Linux algunos de los archivos de configuración para las interfaces de red se encuentran en el directorio `/etc/sysconfig/network-scripts`.

El primer script que se ejecuta al arrancar el sistema es `/etc/init.d/network`.

# Caja de herramientas de automatización y programación de redes

La figura siguiente ofrece una perspectiva sobre cómo se pueden clasificar las herramientas a utilizar en clase.





## **Actividades y código del curso**

# ¿Preguntas?