Administración de Sistemas

Los servidores y las estaciones de trabajo en un entorno de redes

Alberto Hernández Gallardo

Universidad Europea

Índice

- Conceptos básicos
- Configuración de Red
- Domain Name Server (DNS)
- Gestión de redes y auditoría

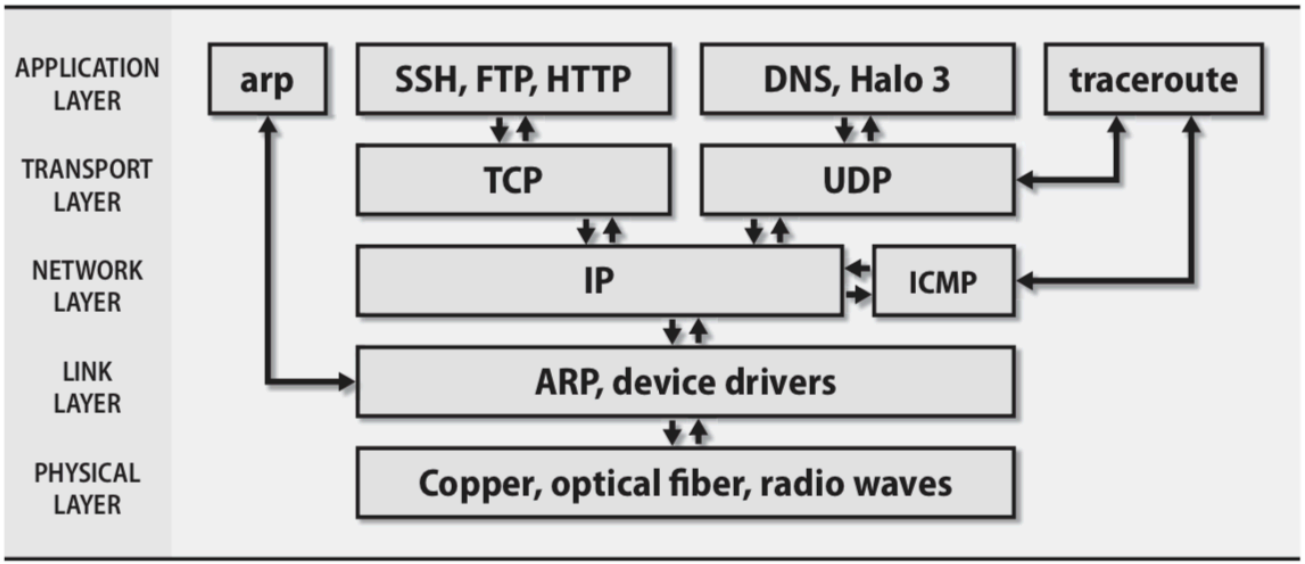
Conceptos básicos.
Protocolo TCP/IP

- TCP/IP es el sistema de redes que proviene de Internet.
- TCP/IP no depende de ningún hardware o sistema operativo en particular, por lo que los dispositivos que utilizan TCP/IP pueden intercambiar datos a pesar de sus muchas diferencias.
- TCP/IP funciona en redes de cualquier tamaño o topología, estén o no conectadas al mundo exterior.
- TCP/IP es un conjunto de protocolos de red diseñados para funcionar juntos sin problemas.

Conceptos básicos.
Protocolo TCP/IP

- IP: Protocolo de Internet, que enruta paquetes de datos de una host a otro (RFC791)
- ICMP: Protocolo de mensajes de control de Internet, que proporciona varios tipos de soporte de bajo nivel para IP, incluidos mensajes de error, asistencia de enrutamiento y ayuda de depuración (RFC792)
- ARP: Protocolo de resolución de direcciones, que convierte las direcciones IP en direcciones de hardware (RFC826
- UDP: Protocolo de datagramas de usuario, que proporciona la entrega de datos unidireccionales y no verificados (RFC768)
- TCP: Protocolo de control de transmisión, que implementa conversaciones confiables, dúplex completo, con control de flujo y con corrección de errores (RFC793)

Conceptos básicos.
Protocolo TCP/IP



Conceptos básicos.
Direcciones IP

- Excepto las direcciones de multidifusión, las direcciones de Internet consisten en una parte de red y una parte de host.
- La porción de red identifica una red lógica a la que se refiere la dirección, y la porción de host identifica un nodo en esa red.
- En IPv4, las direcciones tienen una longitud de cuatro bytes y el límite entre la red y las partes del host se establece administrativamente.
- En IPv6, las direcciones tienen una longitud de 16 bytes y la porción de red y la porción de host siempre tienen ocho bytes cada una.

Conceptos básicos.
Direcciones IP Privadas

- IPv4 define un subconjunto de direcciones IP privadas, descritos en RFC1918.
- Estas direcciones son utilizadas por su sitio internamente, pero nunca se muestran en Internet.
- Los routers traducen entre su espacio de dirección privada y el espacio de dirección asignado por su ISP.
- RFC1918 reserva 1 red de clase A, 16 redes de clase B y 256 redes de clase C que nunca serán asignadas globalmente y pueden ser utilizadas internamente por cualquier sitio.

IP class	From	To	CIDR range
Class A	10.0.0.0	10.255.255.255	10.0.0.0/8
Class B	172.16.0.0	172.31.255.255	172.16.0.0/12
Class C	192.168.0.0	192.168.255.255	192.168.0.0/16

Conceptos básicos.
NAT

- Para permitir que los hosts que usan estas direcciones privadas tengan conexión con Internet, el router ejecuta un sistema llamado NAT (Traducción de dirección de red).
- NAT intercepta los paquetes dirigidos con estas direcciones internas y vuelve a escribir sus direcciones de origen, utilizando una dirección IP externa real y opcionalmente un número de puerto de origen diferente.
- Mantiene una tabla de las asignaciones que ha hecho entre pares de direcciones/puertos internos y externos para que la traducción se pueda realizar al revés cuando los paquetes de respuesta llegan desde Internet.
- El uso de NAT con asignación de puerto multiplexa varias conversaciones en la misma dirección IP.

Conceptos básicos.
Enrutamiento

- El enrutamiento es el proceso de dirigir un paquete a través del laberinto de redes que se interponen entre su origen y su destino.
- La información de enrutamiento se almacena en forma de reglas ("rutas"), como "Para llegar a la red A, enviar paquetes a través de la máquina C."
- También puede haber una ruta predeterminada que indique qué hacer con los paquetes con destino a una red a la que hay ninguna ruta explícita
- Podemos visualizar la tabla de enrutamiento con el siguiente comando:
    - $ netstat -r

Conceptos básicos.
ARP

- Aunque las direcciones IP son independientes del hardware, las direcciones de hardware son necesarias para transportar datos a través de la capa de enlace de una red.
- ARP descubre la dirección de hardware asociada con una dirección IP particular. Se puede usar en cualquier tipo de red que admita la transmisión, pero se describe más comúnmente en términos de Ethernet.
- Si el host A desea enviar un paquete al host B en la misma Ethernet, utiliza ARP para descubrir la dirección de hardware de B. Si B no está en la misma red que A, el host A usa el sistema de enrutamiento para determinar el enrutador del siguiente salto a lo largo de la ruta hacia B y luego usa ARP para encontrar la dirección de hardware del enrutador.

Conceptos básicos.
ARP

- El comando arp examina y manipula la caché ARP del kernel, agrega o elimina entradas, y vacía o muestra la tabla.
    - $ arp -a
- Los formatos de salida varían. El comando arp generalmente es útil solo para la depuración y para situaciones que involucran hardware especial.
- Por ejemplo, si dos hosts en una red están usando la misma dirección IP, uno tiene la entrada correcta de la tabla ARP y el otro es incorrecto.

Conceptos básicos.
DHCP

- Si conectamos un dispositivo a una red, generalmente obtiene una dirección IP para sí mismo en la red local, configura una ruta predeterminada apropiada y se conecta a un servidor DNS local. Todo esto es gracias al protocolo DHCP.
- DHCP permite obtener una variedad de parámetros administrativos y de red de un servidor central que está autorizado para distribuirlos.
- Es recomendable para entornos donde existen hosts que frecuentemente no están en uso y para las redes que deben admitir conexiones transitorias.
- Es posible configurar un servidor Linux como Servidor DHCP mediante el software dhcp3.

Conceptos básicos.
VPN

- VPN es una tecnología de red que permite una extensión segura de la red local sobre una red pública o no controlada.
- Permite que el host en la red envíe y reciba datos sobre redes compartidas o públicas como si fuera una red privada con toda la funcionalidad, seguridad y políticas de gestión de una red privada.
- Esto se realiza estableciendo una conexión virtual punto a punto mediante el uso de conexiones dedicadas, cifrado o la combinación de ambos métodos.

Configuración de Red

- Los pasos básicos para agregar una nueva máquina a una red local son los siguientes:
  - Asignar una dirección IP única y un nombre de host.
  - Asegurar que las interfaces de red estén configuradas correctamente en el momento del arranque.
  - Configurar una ruta predeterminada y quizás un enrutamiento más elegante.
  - Indicar un servidor de nombres DNS para permitir el acceso al resto de Internet.
- Si confía en DHCP para el aprovisionamiento básico, la mayoría de las tareas de configuración para una nueva máquina se realizan en el servidor DHCP

Configuración de Red.
Hostname

- El archivo /etc/hostname contiene el nombre del host que se configurará al inicio del sistema
- El comando hostname asigna un nombre de host a una máquina.
    - $ hostname miservidor
- El archivo /etc/hosts permite establecer un mapeo local entre IPs hostnames
- /etc/hosts es mejor reservarlo para las asignaciones que se necesitan en el momento del arranque (por ejemplo, el propio host, la puerta de enlace predeterminada y los servidores de nombres).
- Use DNS para encontrar asignaciones para el resto de la red local y el resto del mundo.

Configuración de Red.
Interfaces de Red

- El comando ifconfig habilita o deshabilita una interfaz de red, establece su dirección IP y la máscara de subred, y configura otras opciones y parámetros.
- Por lo general, se ejecuta en el momento del arranque con los parámetros de la línea de comandos tomados de los archivos de configuración, pero también puede ejecutarse manualmente para realizar cambios sobre la marcha.
- Tenga cuidado si está realizando cambios ifconfig y se registra de forma remota.
    - $ ifconfig interface [family] address option
    - $ ifconfig eth0 192.168.1.13 netmask 255.255.255.0 up

Configuración de Red.
Interfaces de Red

- La dirección IP, la máscara de red y la puerta de enlace predeterminada se configuran en /etc/network/interfaces.
- La palabra clave iface introduce cada interfaz. Que puede ir seguida de líneas con sangría que especifican parámetros adicionales.

```
auto lo eth0
iface lo inet loopback
iface eth0 inet static
        address 192.168.1.102
        netmask 255.255.255.0
        gateway 192.168.1.254
```

Configuración de Red. Enrutamiento

- El comando de route define rutas estáticas, entradas explícitas de la tabla de enrutamiento que nunca cambian, incluso si ejecuta un demonio de enrutamiento.
    - $ route add -net 192.168.45.128/25 gateway.net
- Linux también acepta un nombre de interfaz (por ejemplo, eth0) como destino de una ruta. Tiene el mismo efecto que especificar la dirección IP principal de la interfaz como la dirección de la puerta de enlace.
- Las redes de destino se especificaban tradicionalmente con direcciones IP y máscaras de red separadas

Configuración de Red.
DNS

- Para configurar una máquina como un cliente DNS, solo necesita configurar el archivo /etc/resolv.conf.
- El archivo resolv.conf enumera los dominios DNS que deben buscarse para resolver nombres que están incompletos y las direcciones IP de los servidores de nombres con los que se debe contactar. para búsquedas de nombres.
- Si el host local obtiene las direcciones de sus servidores DNS a través de DHCP, el software del cliente DHCP inserta estas direcciones en el archivo resolv.conf.

Domain Name Server

- ¿Qué contiene DNS?
  - Un espacio de nombres jerárquico para hosts y direcciones IP
  - Una base de datos distribuida de información de nombre de host y dirección
  - Un servicio para consultar esta base de datos
  - Autenticación de enrutamiento y remitente mejorada para correo electrónico
  - Un mecanismo para encontrar servicios en una red.
  - Un protocolo utilizado por los servidores de nombres para intercambiar información.

Domain Name Server

- Si nos encontramos con una organización pequeña, puede ejecutar servidores en sus propios hosts o pedir a su ISP que le proporcione un servicio de DNS en su nombre.
- Un sitio de tamaño medio con varias subredes debe ejecutar múltiples servidores DNS para reducir la latencia de las consultas y mejorar la confiabilidad.
- Un sitio de envergadura grande puede dividir su dominio DNS en subdominios y ejecutar varios servidores para cada subdominio.
- Las asignaciones de DNS hacia adelante asocian un nombre de host con una dirección IP.
- Los mapeos inversos van desde la dirección IP al nombre de host. Las asignaciones directas e inversas de un dominio deben administrarse en el mismo lugar siempre que sea posible.

Domain Name Server.
Registros

- Cada servidor mantiene una o más partes de la base de datos distribuida que conforma el sistema DNS mundial.
- Su parte de la base de datos consta de archivos de texto que contienen registros para cada uno de sus hosts; estos son conocidos como "registros de recursos".
- Cada registro es una sola línea que consta de un nombre (generalmente un nombre de host), un tipo de registro y algunos valores de datos. El campo de nombre se puede omitir si su valor es el mismo que el de la línea anterior.

google.com.	300	IN	A	209.85.171.100
google.com.	345600	IN	NS	ns1.google.com.
ns1.google.com.	345600	IN	A	216.239.32.10

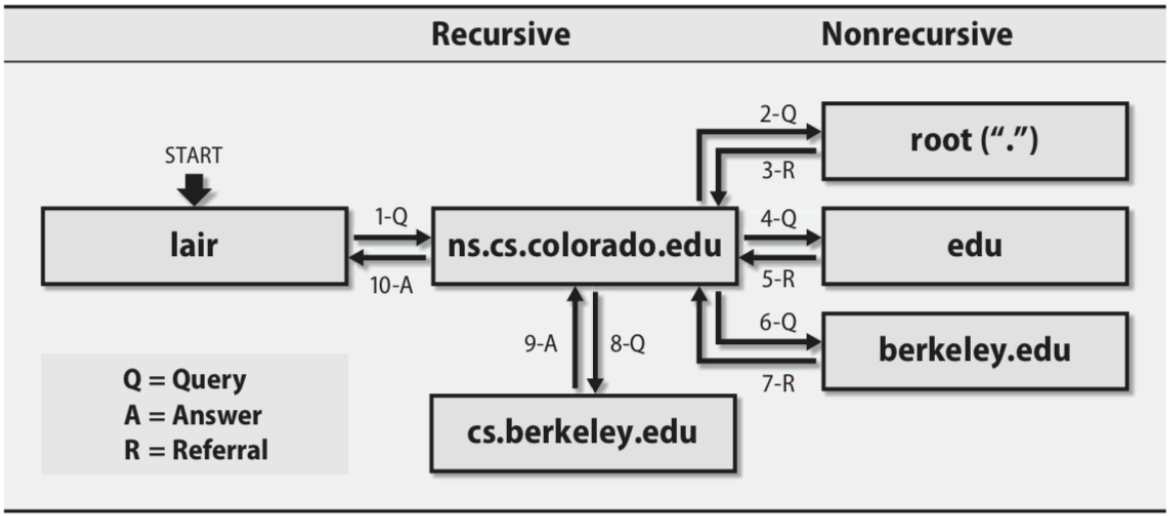
Domain Name Server. Registros

	Type	Name	Function
Zone	SOA	Start Of Authority	Defines a DNS zone
	NS	Name Server	Identifies servers, delegates subdomains
Basic	A	IPv4 Address	Name-to-address translation
	AAAA	IPv6 Address	Name-to-IPv6-address translation
	PTR	Pointer	Address-to-name translation
	MX	Mail Exchanger	Controls email routing
Security and DNSSEC	DS	Delegation Signer	Hash of signed child zone's key-signing key
	DNSKEY	Public Key	Public key for a DNS name
	NSEC	Next Secure	Used with DNSSEC for negative answers
	NSEC3[a]	Next Secure v3	Used with DNSSEC for negative answers
	RRSIG	Signature	Signed, authenticated resource record set
	DLV	Lookaside	Nonroot trust anchor for DNSSEC
	SSHFP	SSH Fingerprint	SSH host key, allows verification via DNS
	SPF	Sender Policy	Identifies mail servers, inhibits forging
	DKIM	Domain Keys	Verify email sender and message integrity
Optional	CNAME	Canonical Name	Nicknames or aliases for a host
	SRV	Services	Gives locations of well-known services
	TXT	Text	Comments or untyped information[b]

Domain Name Server. Delegación

- Todos los servidores de nombres leen las identidades de los servidores raíz de un archivo de configuración local o los tienen integrados en el código. Los servidores raíz conocen los servidores de nombres para los dominios de nivel superior (com, net, edu, etc).

DNS query process for vangogh.cs.berkeley.edu



Domain Name Server.
Caché y eficiencia

- El almacenamiento en caché aumenta la eficiencia de las búsquedas
- Una respuesta se guarda durante un período de tiempo denominado "tiempo de vida" (TTL), que es especificado por el propietario del registro de datos en cuestión.
- La mayoría de las consultas son para hosts locales y pueden resolverse rápidamente.
- En condiciones normales, los registros de recursos deben usar un TTL que se encuentre entre 1 hora y 1 día.
- Si existe carga balanceada a través de subredes lógicas, es necesario un TTL más corto, de 10 segundos a 1 minuto.

Domain Name Server.
Caché y eficiencia

- Los servidores DNS también implementan caché negativo. Es decir, recuerdan cuándo falla una consulta y no la repiten hasta que el valor TTL del almacenamiento en caché negativo haya caducado.
- El almacenamiento en caché negativo guarda respuestas de los siguientes tipos:
  - Ningún host o dominio coincide con el nombre consultado.
  - El tipo de datos solicitados no existe para este host.
  - El servidor a preguntar no responde.
  - El servidor es inalcanzable debido a problemas de red.

Domain Name Server.
Multiples respuestas

- Un servidor de nombres puede recibir múltiples registros en respuesta a una consulta. Por ejemplo, la respuesta a una consulta para los servidores de nombres del dominio raíz enumera los 13 servidores.
- La mayoría de los servidores de nombres devuelven las respuestas en orden aleatorio como una forma primitiva de equilibrio de carga.
- Puede aprovechar este efecto de equilibrio para sus propios servidores asignando un solo nombre de host a varias direcciones IP diferentes.

Gestión de redes y auditoría

- La gestión de redes incluye las siguientes tareas:
  - Detección de fallos para redes, pasarelas y servidores críticos.
  - Esquemas para notificar a un administrador de problemas
  - Monitorización general de la red, para equilibrar la carga y la expansión del plan.
  - Documentación y visualización de la red.
  - Administración de dispositivos de red desde un sitio central.

Gestión de redes y auditoría.
Principios de actuación

- Hacer un cambio a la vez. Pruebe cada cambio para asegurarse de que haya tenido el efecto deseado. Deshazte de cualquier cambio que tenga un efecto no deseado.
- Documente la situación tal como era antes de involucrarse, y documente cada cambio que realice en el camino.
- Los problemas pueden ser transitorios, revise los logs.
- Comience en un extremo de un sistema o red y trabaje a través de los componentes críticos del sistema hasta que llegue al problema.
- Utilice las capas de la red para resolver el problema. Comience arriba o abajo y trabaje a través de la pila de protocolos.

Gestión de redes y auditoría.
Ping

- Se utiliza el comando ping para verificar el estado de los hosts individuales y para probar segmentos de la red.
- Las tablas de enrutamiento, las redes físicas y las puertas de enlace están involucradas en el procesamiento de un ping.
- Si el ping no funciona, tampoco funcionará nada más sofisticado.
  - Esta regla no se aplica a las redes que bloquean las solicitudes de echo de ICMP con un firewall. Asegúrese de que un firewall no interfiera con su depuración antes de concluir que el host de destino está ignorando un ping.
- Un ping exitoso sólo informa sobre el estado del servidor de destino.
    - $ ping hostname

Gestión de redes y auditoría.
Traceroute

- Muestra la secuencia de saltosa través de las cuales viaja un paquete IP para llegar a su destino.

```
$ traceroute nubark
traceroute to nubark (192.168.2.10), 30 hops max, 38 byte packets
 1  lab-gw (172.16.8.254)  0.840 ms  0.693 ms  0.671 ms
 2  dmz-gw (192.168.1.254)  4.642 ms  4.582 ms  4.674 ms
 3  nubark (192.168.2.10)  7.959 ms  5.949 ms  5.908 ms
```

- Funciona estableciendo el campo TTL de un paquete saliente en un número exacto. Cuando los paquetes llegan a una puerta de enlace, su TTL disminuye. Cuando el TTL llega a 0, se envía un mensaje de "tiempo excedido" de ICMP al servidor de origen.
- Algunos firewalls bloquean los mensajes de "tiempo excedido" de ICMP
- En los últimos años han aparecido nuevas herramientas que permiten eludir los firewall ICMP-blocking.

Gestión de redes y auditoría.
Netstat

- Inspeccionar la configuración de las interfaces: muestra la configuración y el estado de las interfaces de red del host junto con los contadores de tráfico asociados. La salida es generalmente tabular pero los detalles varían según el sistema:
    - $ netstat –i

Name	Mtu	Net/Dest	Address	Ipkts	Ierrs	Opkts	Oerrs	Collis	Queue
lo0	8232	loopback	localhost	319589661	0	319589661	0	0	0
e1000g1	1500	host-if1	host-if1	369842112	0	348557584	0	0	0
e1000g2	1500	host-if2	host-if2	93141891	0	121107161	0	0	0

Gestión de redes y auditoría.
Netstat

- Supervisar el estado de las conexiones de red: los servicios inactivos que están esperando conexiones normalmente están ocultos, pero puede verlos con:
  - $ netstat –a

Proto	Recv-Q	Send-Q	Local Address	ForeignAddress	State
tcp	0	0	*:ldap	*:*	LISTEN
tcp	0	0	*:mysql	*:*	LISTEN
tcp	0	0	*:imaps	*:*	LISTEN
tcp	0	0	bull:ssh	dhcp-32hw:4208	ESTABLISHED
tcp	0	0	bull:imaps	nubark:54195	ESTABLISHED
tcp	0	0	bull:http	dhcp-30hw:2563	ESTABLISHED

Gestión de redes y auditoría.
Netstat

- Identificar los servicios de red que están escuchando: para visualizar sólo los procesos que están escuchando en algún puerto se debe utilizar el siguiente comando:
    - $ netstat -lp

tcp	0	0	0.0.0.0:22	0.0.0.0:*	LISTEN	23858/sshd
tcp	0	0	0.0.0.0:25	0.0.0.0:*	LISTEN	10342/sendmail
udp	0	0	0.0.0.0:53	0.0.0.0:*		30016/named
udp	0	0	0.0.0.0:962	0.0.0.0:*		38221/mudd

Gestión de redes y auditoría.
Netstat

- Examinar la tabla de enrutamiento:
  - $ netstat -r

Destination	Gateway	Genmask	Flags	MSS	Window	irtt	Iface
192.168.1.0	0.0.0.0	255.255.255.0	U	0	0	0	eth0
10.2.5.0	0.0.0.0	255.255.255.0	U	0	0	0	eth1
127.0.0.0	0.0.0.0	255.0.0.0	U	0	0	0	lo
0.0.0.0	192.168.1.254	0.0.0.0	UG	0	0	40	eth0

Gestión de redes y auditoría.
Netstat

- Visualización de estadísticas operativas para varios protocolos de red: la salida tiene secciones separadas para IP, ICMP, TCP y UDP.
  - $ netstat -s

```
Tcp:
    4442780 active connections openings
    1023086 passive connection openings
    50399 failed connection attempts
    0 connection resets received
    44 connections established
    666674854 segments received
    585111784 segments send out
    107368 segments retransmited
    86 bad segments received.
    3047240 resets sent
Udp:
    4395827 packets received
    31586 packets to unknown port received.
    0 packet receive errors
    4289260 packets sent
```