Administración de sistemas en red

Tomás P. de Miguel

Dpto. de Ingeniería de Sistemas Telemáticos

Administración de redes

- Plan de numeración
- Interconexión de redes
- Pruebas de conectividad
- Servicio de nombres
- Servicios básicos de red

Tareas de administración de red

- Dirección IP de la máquina
- Máscara de red, si se usan subredes
- Dirección de broadcast
- Router por defecto
- Dirección de la dirección interna (lookback)
- Nombre completo de la máquina
- Dirección de un servidor de nombres

Plan de numeración

- Las modernas aplicaciones distribuidas consumen mas ancho de banda.
- Lo normal es dividir la red asignada en subredes.
- Se utilizan los mismos números, distribuidos en redes con menos estaciones y así se obtienen mas redes
- En algunos casos se utilizan direcciones falsas para disponer de mas números y se traducen direcciones en el router de salida a Internet.

Arquitectura IPv4

- Clasificación de direcciones (RFC 1466, RFC 1918)

clase	rango	redes	máquinas
Clase A	1 a 126	126	16777214
Lookback	127		
Clase B	128.0 a 191.255	16384	65534
Clase C	192.0.0 a 223.255.255	2097152	254
Clase D (mdestino)	224.0.0.0 a 239.255.255.255		
Clase E (reservada)	240.0.0.0 a 247.255.255.255		

- Subnetting y CIDR (Classless InterDomain Routing)
  - por falta de direcciones
  - agrega máquinas a redes de forma arbitraria
  - se utiliza una máscara (255.255.255.0 es una red con 254 máquinas)
- Lookback (127.0.0.1)
  - utiliza los protocolos IP dentro de la misma máquina
  - no se pasa por el interfaz físico
  - se utiliza para servicios locales

Arquitectura IPv4

- Difusión por broadcast
  - En via un mensaje en un solo paquete a todas las estaciones de una red.
  - Hay varios niveles de difusión

estación	dir. destino	accede a
10.0.1.1	255.255.255.255	todas las de la red
10.0.1.1	10.0.1.255	todas las de la subred
10.0.1.1	10.255.255.255	todas las de la red 10
10.0.1.1	8.255.255.255	todas las de la red 8

- Se utiliza para mantenimiento y con algunos protocolos
  - BOOTP, DHCP o RARP
- Multidestino (Multicast)
  - Se distribuye solo a grupos de máquinas
  - IGMP ayuda a registrar en un router un host en un grupo
  - DVRMP o PIM para distribuir paquetes por Internet

Ficheros de configuración

- Nombre de la máquina
  - /etc/HOSTNAME o /etc/hostname
- Máquinas conocidas /etc/hosts
- Redes conocidas /etc/networks
  - lookback 127.0.0.0
  - localnet 138.4.5.0
  - ditnet 138.4.2.0
- Para adivinar los IP desconocidos /etc/host.conf
  - order hosts,bind
  - multi on
- Configuración del servicio de nombres /etc/resolv.conf

Configuración de interfaces de red

- Directorio /etc/sysconfig/network-scripts
  - DEBIAN /etc/network/interfaces
- Ifconfig : para configurar y supervisar
  - ifconfig interfaz direccion
  - ifconfig eth0 inet 138.4.2.10 \
    netmask 255.255.255.192 broadcast 138.4.2.63
  - comprobación: ifconfig eth0
- Subinterfaces
  - Una interfaz física y varias lógicas
  - Varias direcciones sobre la misma interfaz física
  - Por ejemplo:
    - eth0
    - eth0:1
    - eth0:2

Encaminamiento

- Política de configuración de la red
  - La red se configura con rutas estáticas
  - La red se configura dinámicamente
  - Se aplica una estrategia combinada
    - se activan rutas dinámicas durante un tiempo
    - se fija el resultado como un plan de rutas estáticas.
- Configuración de rutas
  - desde donde estamos
  - por donde hay que salir para llegar a donde queremos
    - destino pasarela
- Las rutas se configuran en el núcleo
  - /sbin/route : para examinar y configurar las rutas

Protocolos de encaminamiento

- Estático (route)
- Routing Information Protocol (RIP)
- Open Shortest Path First (OSPF)
- Interior Gateway Routing Protocol (IGRP)
- External Gateway Protocol (EGP)
- Border Gateway Protocol (BGP)
- Distance Vector Multicast Routing Protocol (DVMRP)

Ajuste de rutas

- Encaminamiento estático
  - más sencillo, para pocos movimientos, sin alternativas
  - route add -net 138.4.2.64 \
    netmask 255.255.255.192 \
    gw 138.4.2.5
  - Ruta por defecto : route add default gw 138.4.2.1
- Encaminamiento dinámico
  - para varias interfaces
  - ICMP redirect
  - difusión de rutas con RIP (routed)
- Supervisión de la red
  - traceroute 192.138.3.4
  - netstat -a
  - tcpdump port route
  - http://samspade.org/classic/

/sbin/route

- Argumentos
  - add para añadir rutas
  - del para eliminar rutas
- Información
  - Destination: red destino
  - Gateway : pasarela
  - Netmask : máscara
  - Flags : U=arriba,H=sistema,G=pasarela,D=dinámica
  - Metric : coste de aplicar esa ruta (no actua en el kernel)
  - Ref : rutas que dependen de esta
  - Use : numero de veces que se ha usado esta ruta
  - Iface : interface asociada a la ruta

úmeros IP y nombres

- Para recordar más facilmente las direcciones de las máquinas se emplean nombres.
- Los nombres se componen de:
  - nombre de máquina
  - nombre de dominio
  - 138.4.2.10 sanson.dit.upm.es
- Los nombres son independientes de los números de red, las direcciones de máquina o las rutas de acceso.
- Las aplicaciones necesitan localizar
  - los nombres asociados a un número de máquina
  - los números de máquina asociados a un nombre

Tabla de máquinas

- Fichero /etc/hosts
- Puede incluir máquinas en una o varias redes
- La tabla de máquinas incluye:

127.0.0.1	localhost	localhost.localdomain
138.4.2.9	itaca fax news nis	itaca.dit.upm.es
138.4.2.9	mail	mail.dit.upm.es
138.4.2.10	sanson dns	sanson.dit.upm.es
138.4.2.13	yeti dns2	yeti.dit.upm.es
138.4.2.13	mail2	mail2.dit.upm.es
138.4.2.60	loro www ftp proxy hora	loro.dit.upm.es
138.4.3.171	lince	lince.dit.upm.es
138.4.23.170	cajon	cajon.dit.upm.es

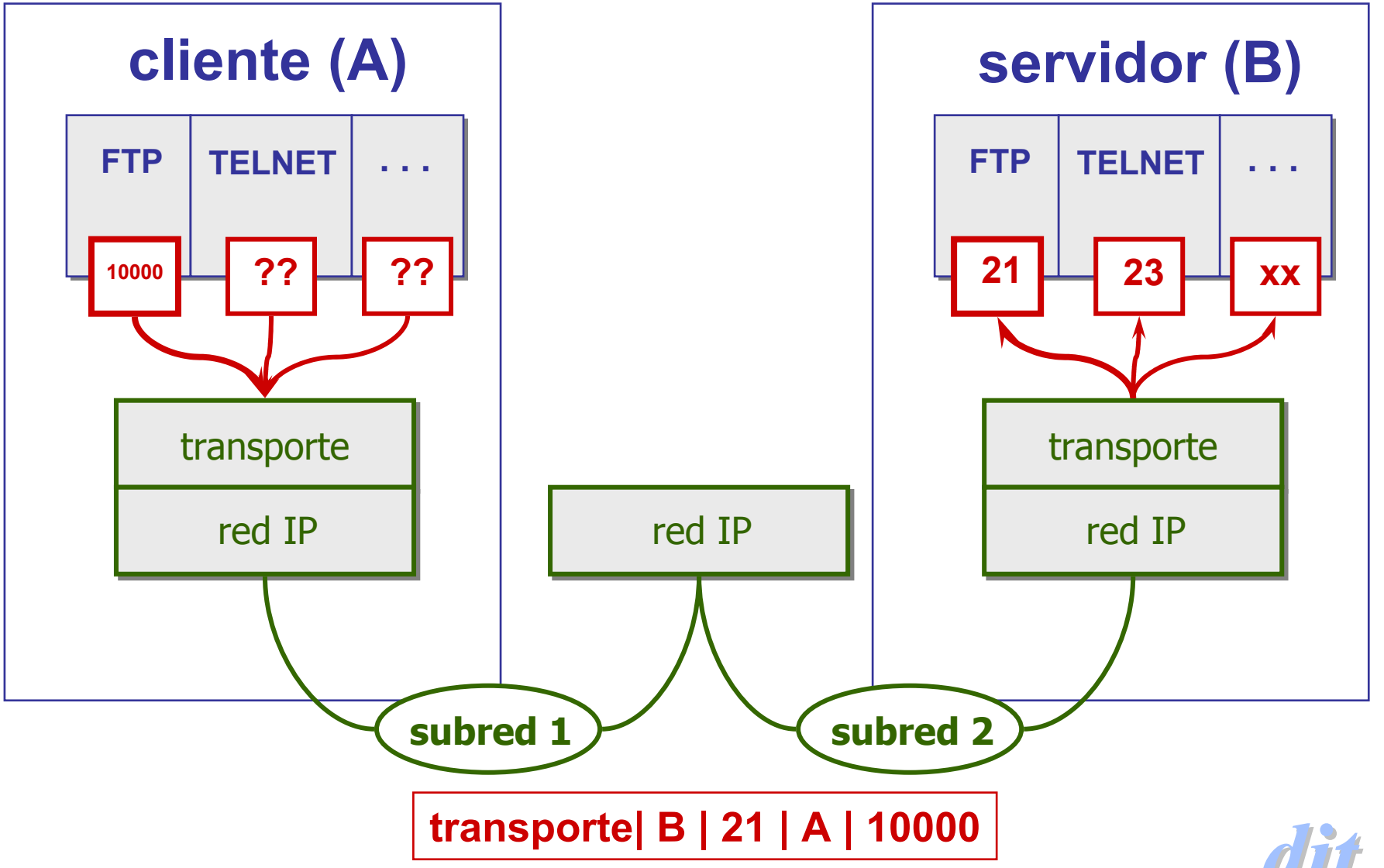
Servicios básicos de la red

- Servicio de nombres
  - DNS (Domain Name Server)
  - NIS (Network Information Service)
- Configuración a través de la red
  - BOOTP (BOOT Protocol)
  - DHCP (Dynamic Host Configuration Protocol)
- Identificación de usuarios en red
  - PAM (pluggable authentication module)
    - es el procedimiento mas flexible en UNIX
  - SMB
    - cuando la conexión es con equipos Windows
  - LDAP (Lightweight Directory Access Protocol)
    - mas flexible que DNS o NIS
    - no está integrado en libc

Modelo de aplicaciones distribuidas

- Modelo cliente - servidor
- Tipos de servicios
  - Diseño centrado en la comunicación (telnet)
    1. Definir el protocolo.
    2. Diseñar el formato de los mensajes.
    3. Diseñar cliente y servidor.
  - Diseño centrado en la aplicación (nfs)
    1. Diseñar la aplicación como un programa convencional.
    2. Dividir el programa en piezas.
    3. Añadir un protocolo para hacer que cada pieza pueda ejecutar en una máquina diferente.
- Un servidor para varios servicios inet
  - un solo demonio varios puertos

Identificación de servicios con puertos



transporte| B | 21 | A | 10000

Servicios de acceso remoto

- Conexión remota: telnet y rlogin
- Ejecución remota: rsh
- Copia remota: rcp
- Obligan a identificar al usuario
  - el mismo en las dos máquinas
  - información de identificación en la conexión
  - se puede aceptar siempre a un usuario o una máquina
    - $HOME/.rhosts
    - /etc/hosts.equiv
- El servicio solo se puede configurar en un puerto privilegiado (<1024)
- Para evitar problemas de seguridad utilizar ssh

Control de acceso

- Se trata de que solo ciertos usuarios o ciertas máquinas tengan acceso a los servicios locales
- El control se consigue a través de un demonio que se llama tcpd
  - Cuando alguien demanda un servicio pasa por TCPD:
    - primero evalua los permisos y
    - después ejecuta el servicio
- Configuración de permisos
  - /etc/hosts.allow y /etc/hosts.deny
    - servicio:usuario
  - Ejemplos
    - ALLOW= in.ftpd : 192.168.1 (solo a los de la red)
    - DENY= ALL : ALL (nada permitido desde ningún sitio)
    - allow tiene prioridad sobre deny

TCPwrapper

- Esta compuesto por
  - un demonio (TCPD) y
  - una biblioteca (libwrap0)
- Algunos servicios usan directamente la biblioteca
  - sendmail
  - mountd
  - portmap
- Ejemplos de host.allow

```
ALL : LOCAL
in.tftpd : 128.5.1
in.tftpd : 128.5.1.0 / 255.255.255.192
```

- Ejemplos de host.deny

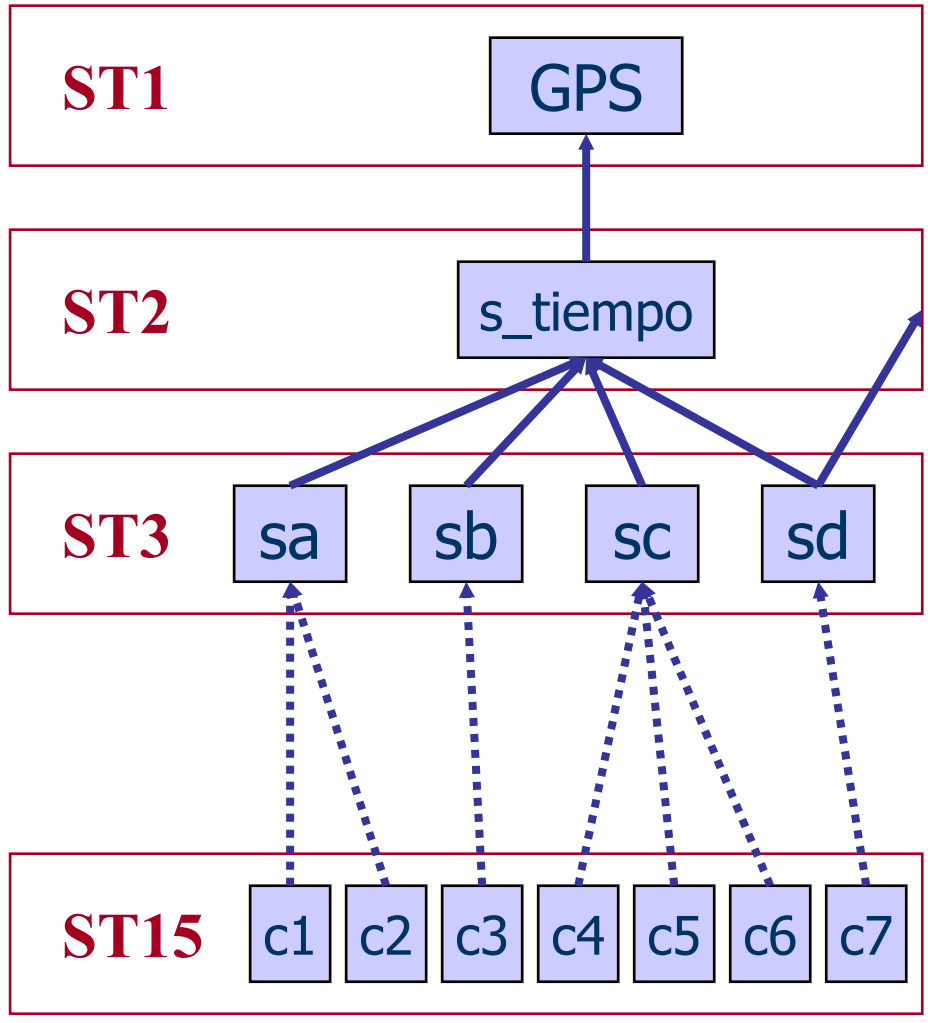
```
ALL : PARANOID
in.tftpd : ALL : \
(/usr/bin/finger -l@%h | /usr/sbin/sendmail -s %d -%h root)&
```

Sincronización de tiempo

- Necesaria para el buen funcionamiento de muchos servicios
  - correo electrónico
  - sistemas de ficheros distribuidos
- NTP: Network Time Protocol (RFC1305)
  - Protocolo para sincronizar el tiempo entre dos máquinas
  - Sincroniza con errores de decenas de milisegundos
  - Utiliza un GPS o la sincronización con varios servidores remotos
  - Servidores públicos http://www.eecis.udel.edu/~ntp

Arquitectura del servicio

- Los servidores se configuran en stratums
- El primero es un maestro de tiempo
  - relojes atómicos
  - GPS
- Los clientes se conectan a servidores secundarios que pueden coordinarse entre sí
- Los clientes pueden recibir la hora por multicast difundida desde un servidor de zona.
- Utilizar los servidores más próximos a uno mismo.



Configuración

- /etc/ntp.conf
- Configuración de un servidor

```
server  ntps1-0.cs.tu-berlin.de
server  ntp0.fau.de
server  chronos.cru.fr
server  195.220.94.163

driftfile /etc/ntp/drift

#multicastclient                # listen on default 224.0.1.1
#broadcastdelay      0.008
authenticate no

peer rackety.udel.edu prefer # preferred server
```

Utilidades

- Servidor de hora (xntpd)
- Programas de monitorización
  - ntpq
  - xntpdc
- Para configurar la hora en un cliente
  - ntpdate
- Para descubrir fuentes de sincronización
  - ntptrace