Redes de Computadoras y Cortafuegos con GNU/Linux

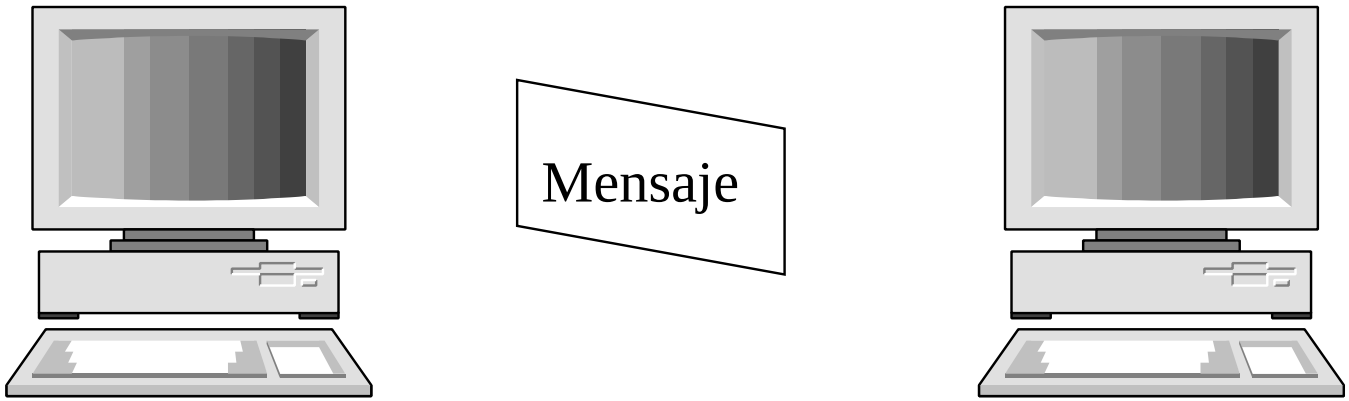
Dr. Luis Gerardo de la Fraga

Departamento de Computación
Cinvestav
Correo-e: fraga@cs.cinvestav.mx

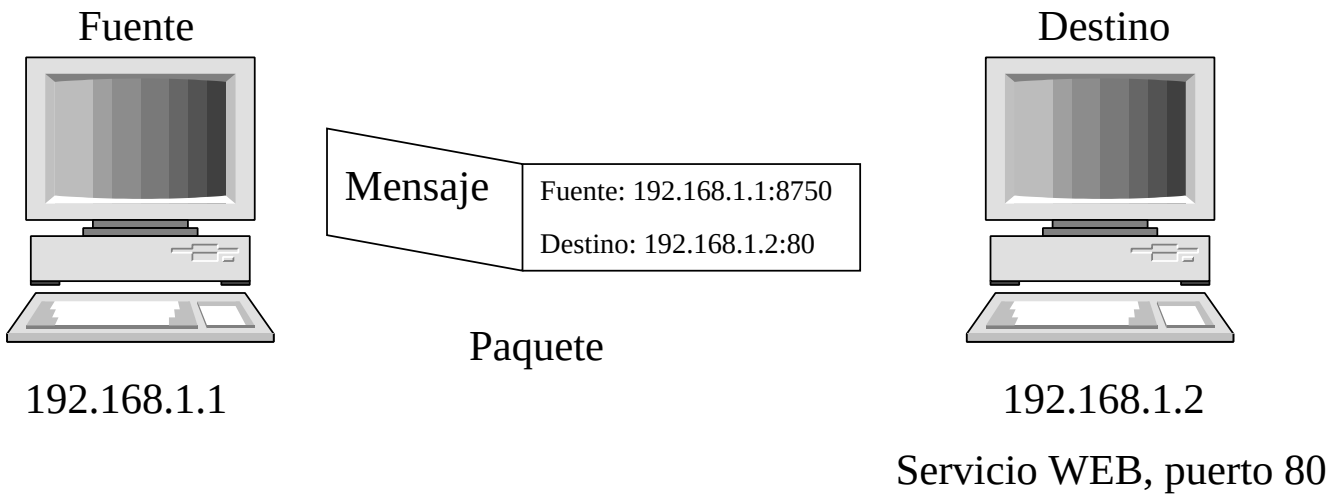
13 de noviembre de 2006

Contenido

Comunicación entre dos computadoras



Formación de paquetes



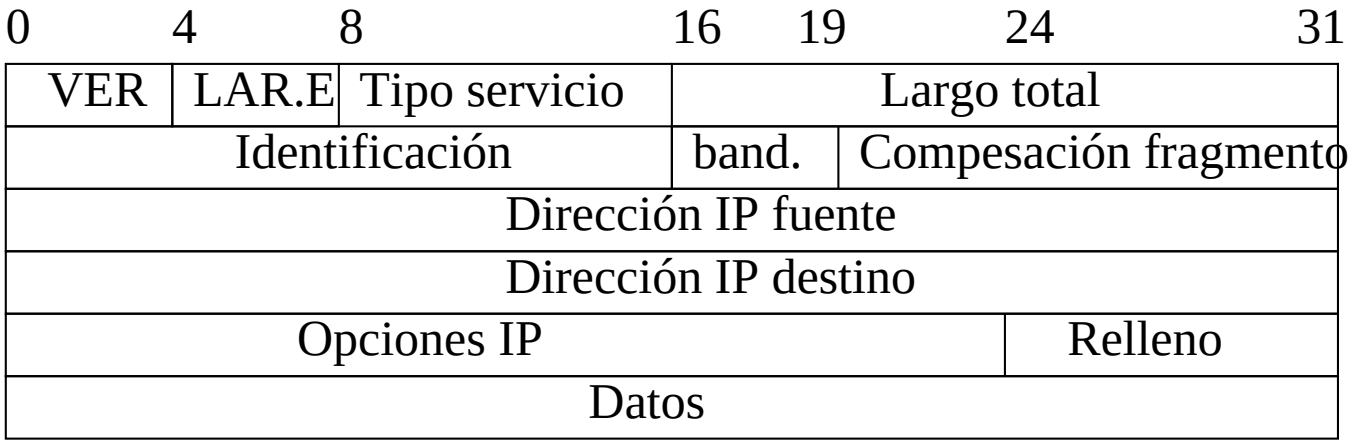
¿Por qué usamos redes de computadoras?

- Para eficientar el uso de los recursos
- Para establecer un medio de comunicación
- Como entretenimiento
- Debe de haber una justificación para el uso de redes

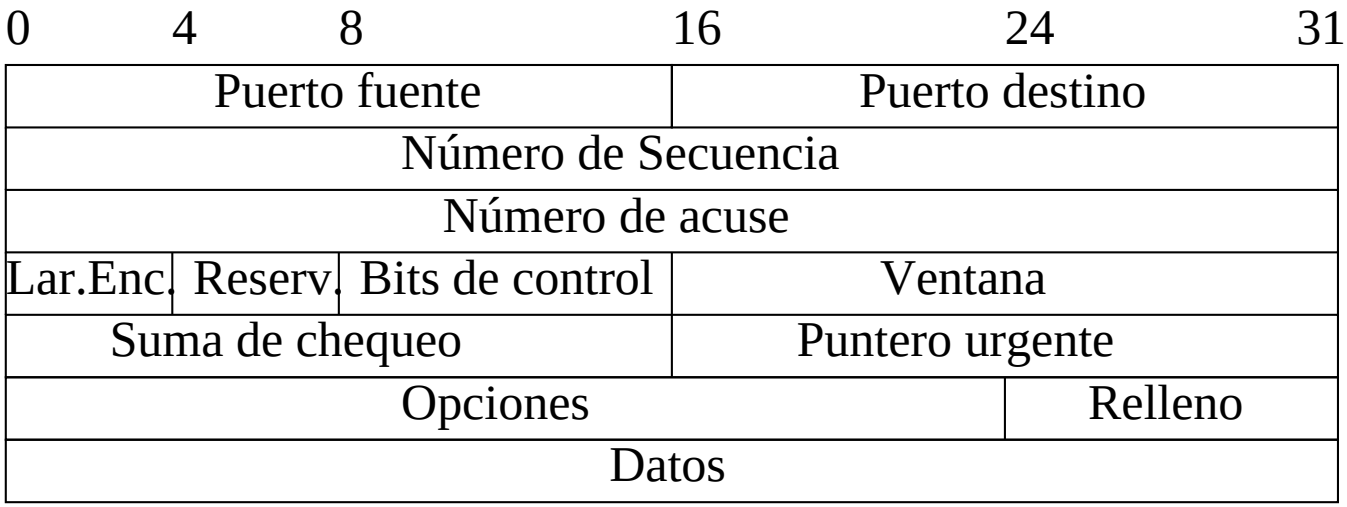
Internet

- Internet nació en 1969
- Se definió el uso del protocolo TCP/IP para el intercambio de paquetes
- El concepto es *switcheo de paquetes*, inventado por Paul Baran.

TCP/IP. El encabezado de IP



TCP/IP. El encabezado de TCP

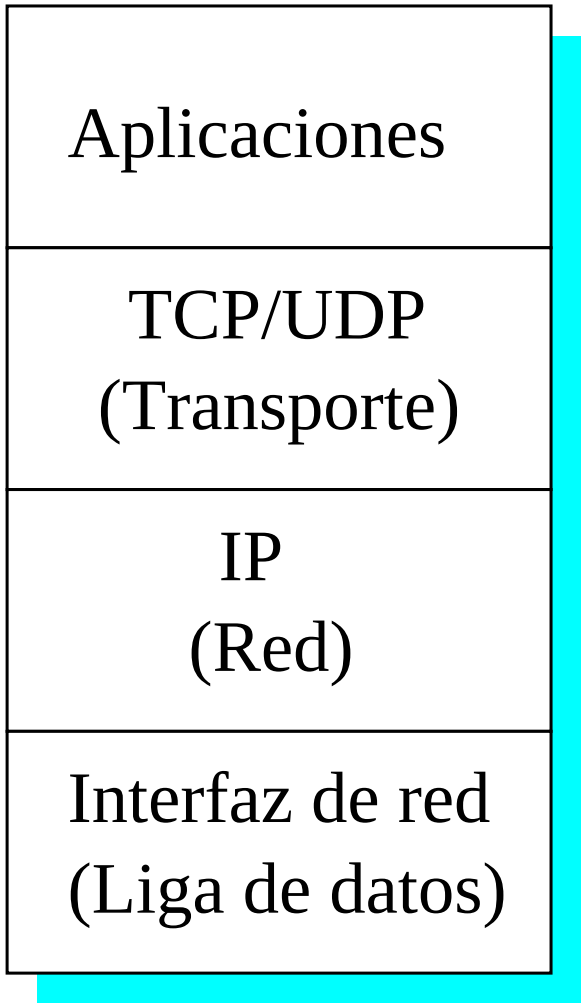


Ventajas de usar TCP/IP

TCP/IP permite plataformas-entrelazadas o administración de redes. TCP/IP también tiene las siguientes características:

- Buena recuperación de las fallas
- Habilidad de añadir redes sin interrumpir los servicios ya existentes.
- Manejo de alto porcentaje de errores
- Independencia de la plataforma
- Bajos gastos indirectos de información.

Capas TCP/IP


Aplicaciones
TCP/UDP
(Transporte)
IP
(Red)
Interfaz de red
(Liga de datos)

Fluejo de paquetes en TCP

TCP, el Protocolo de Control de Transmisión, provee una entrega fiable del flujo y el servicio de conexión a las aplicaciones

1. Huésped A —— SYN(ISN) ⟶ Huésped B
2. Huésped A ⟵ SYN(ISN+1)/ACK — Huésped B
3. Huésped A —— ACK ⟶ Huésped B

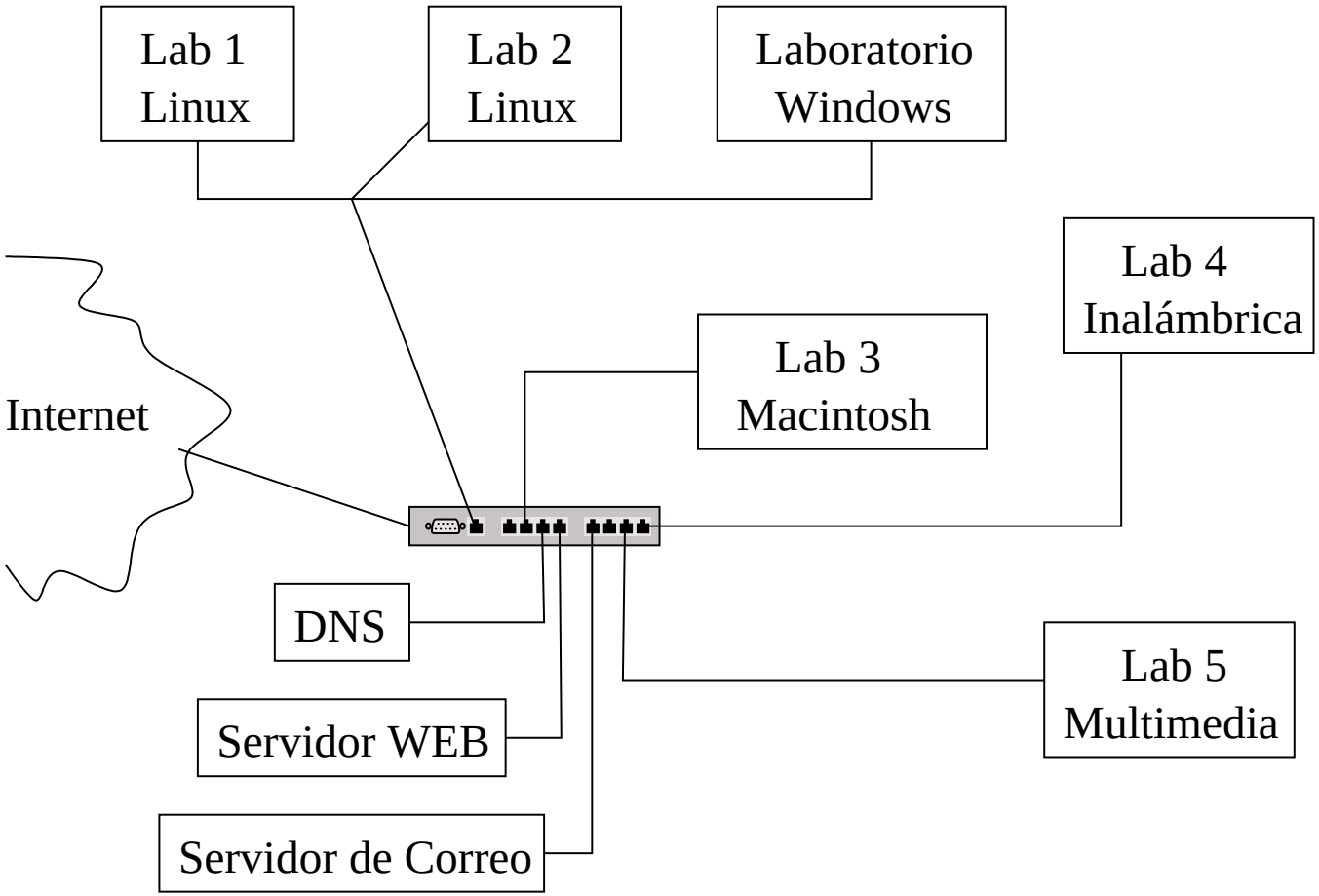
Esto no sucede con los paquetes de UDP, los cuales se consideras "no fiables" y no intentan corregir los errores ni negociar una conexión antes del envio a un huésped remoto.

Dirección IP	192.168.120.21
Máscara de red	255.255.255.0
Número de red	192.168.120.
Número de huésped	.21
Dirección de Red	192.168.120.0
Dirección de Difusión	192.168.120.255

Direcciones IP *inválidas* son las especificadas en el RFC1918 para diseñar redes privadas o intranets, y son las recomendadas para usarse cuando se experimenta con redes. Estas direcciones son 10.∗.∗.∗, 172,16.∗.∗—172,31.∗.∗ y 192,168.∗.∗.

- Podemos bloquear los inicios de conexión
- Podemos bloquear por direcciones IP y redes
- Podemos bloquear por servicios
- Podemos bloquear por protocolo

El Problema (1/3)



El Problema (2/3)

- En total son unas **cincuenta** computadoras fijas con unas **dos docenas** de computadoras que accesan la red inalámbrica.
- Tenemos que dar servicio acerca de 80 estudiantes de posgrado, 12 investigadores y a varios servidores generales (correo, WEB, nombres, etc.)
- Y algunos de nuestros estudiantes están trabajando en sus tesis con redes y servicios experimentales (IPv6, p.e), monitoreo de redes y redes inalámbricas.

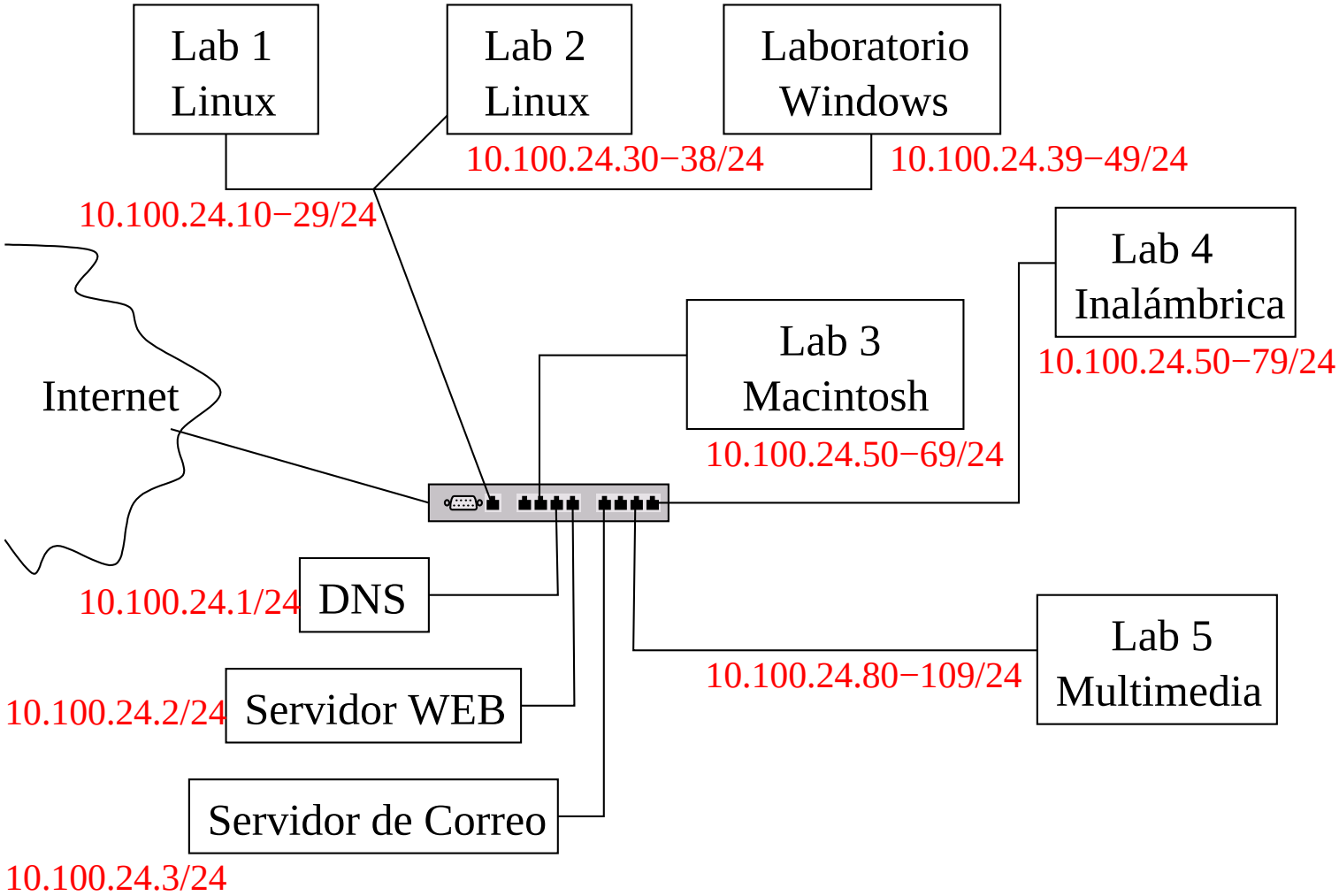
El Problema (3/3)

En este escenario existen dos preocupaciones básicas:

1. La seguridad y
2. la facilidad de mantenimiento

de toda nuestra red.

Seguridad (1/3)

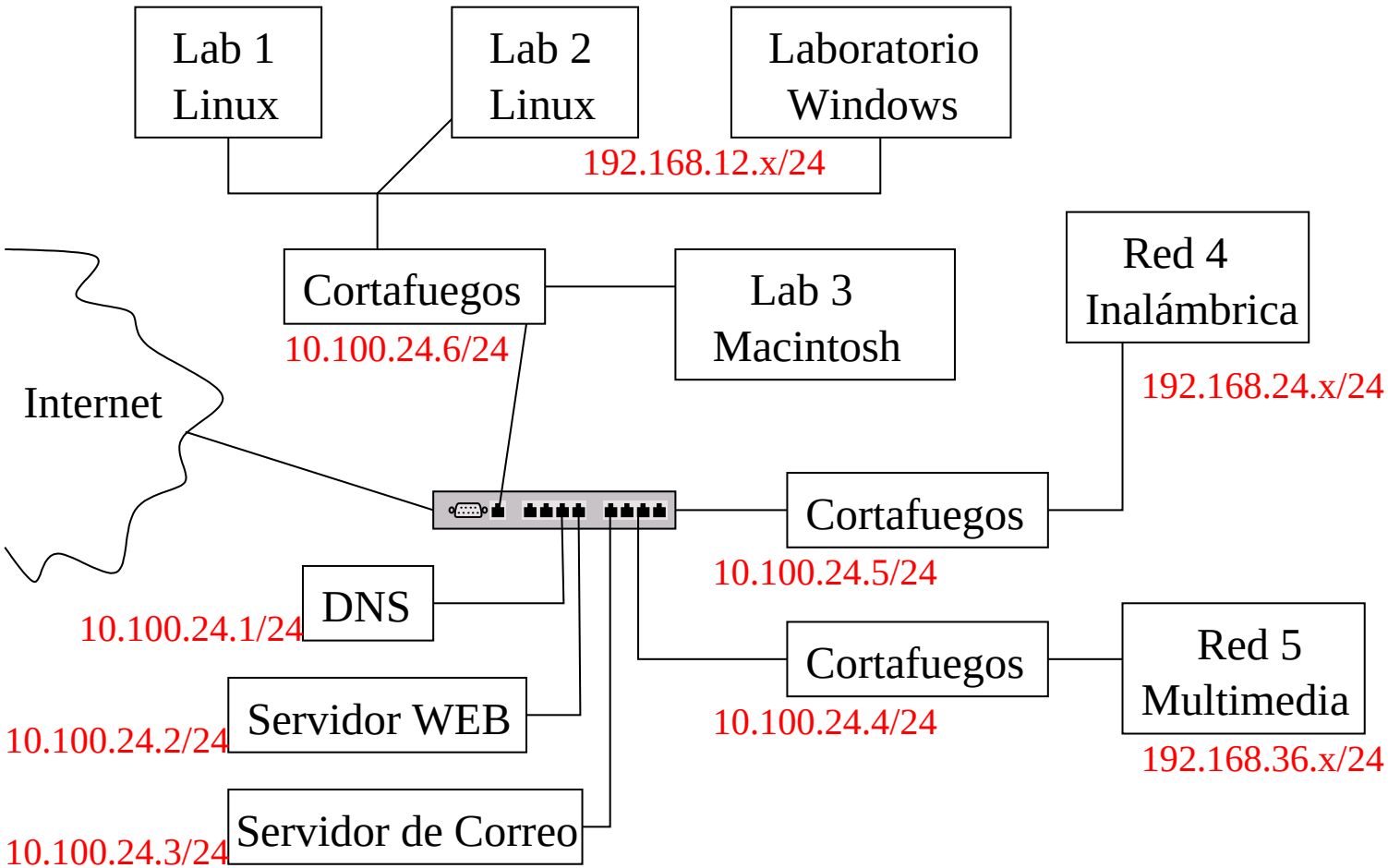


Seguridad (2/3)

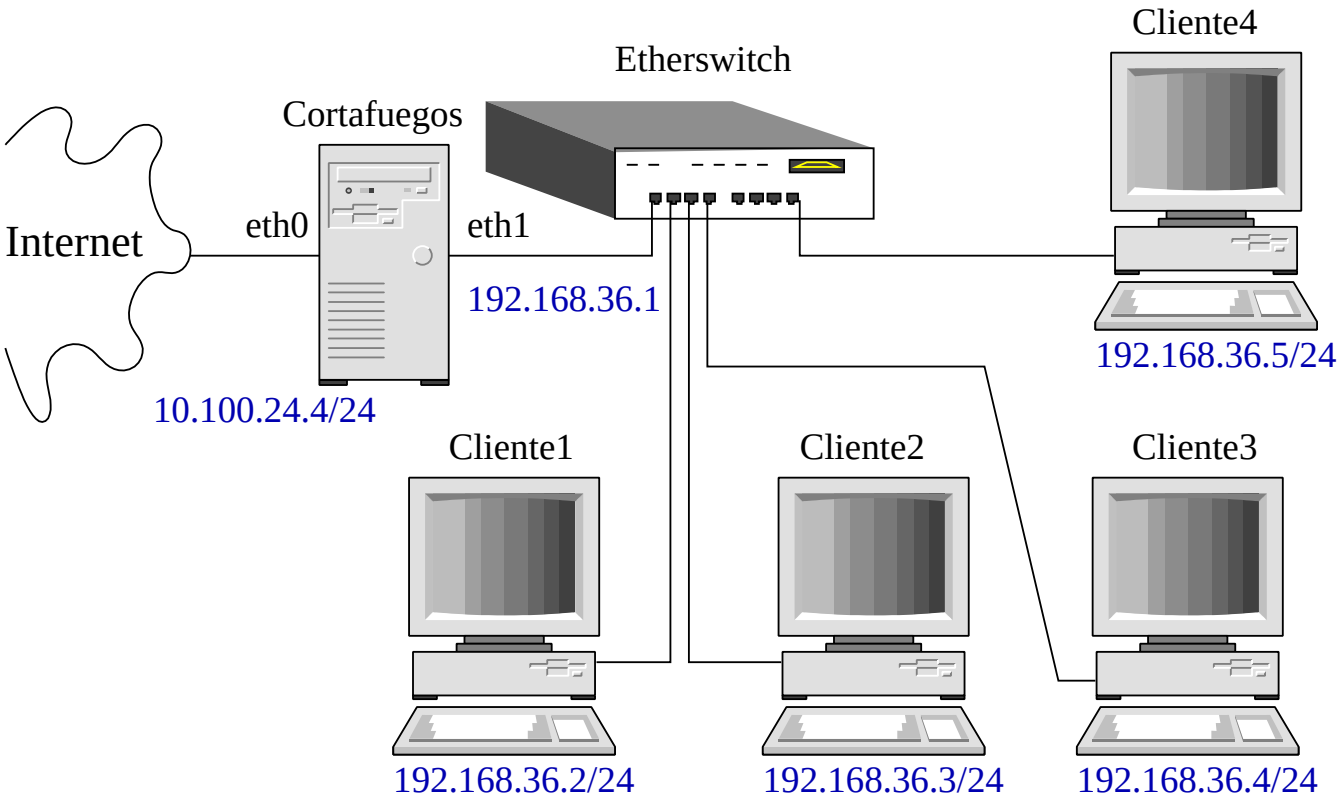
En la red anterior (IPs registrados para todas las máquinas) nos generan los siguientes problemas:

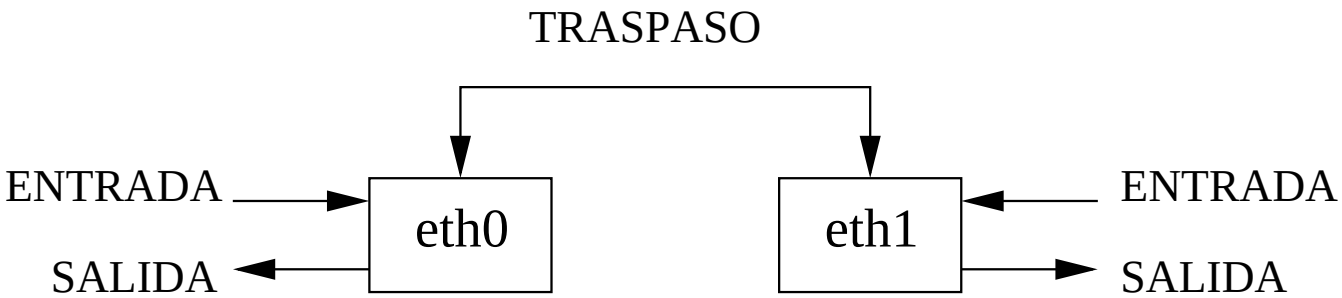
1. Los estudiantes en su trabajo de tesis se les asigna una computadora propia. Ellos instalaban servidores propios, como chat o música, que consumían todo el ancho de banda de la red.
2. Fallos de los estudiantes al empezar a trabajar en redes TCP/IP (afectan a toda la red).
3. Los ataques provenientes de Internet nos pone en una actitud defensiva.
4. Virus

Seguridad (3/3)



Red Militarizada




TRASPASO
ENTRADA
SALIDA
eth0
eth1
ENTRADA
SALIDA

Script para realizar una puerta con IPtables

```
#!/bin/sh

PATH=/sbin

INTERFAZ_EXT=eth0
IPADDR=10.100.24.4
REDLOCAL=10.100.24.0/24
#
#
INTERFAZ_INT=eth1
REDINTERNA=192.168.36.0/24
#
# Limpiamos las reglas actuales
#
iptables -F
iptables -F -t nat

# Quitamos cadenas definidas por usuarios
iptables -X

#---------------------------------------
# Establecer la política por defecto
#      Permitir entrada
#      Denegar el transpaso
#      Permitir salida
#---------------------------------------
iptables -P INPUT   ACCEPT
iptables -P FORWARD DROP
iptables -P OUTPUT  ACCEPT
```

```
##############################################
# Permitimos la salida a la red interna
#
iptables -A FORWARD -m state --state NEW,ESTABLISHED \
    -i $INTERFAZ_INT -s $REDINTERNA -j ACCEPT

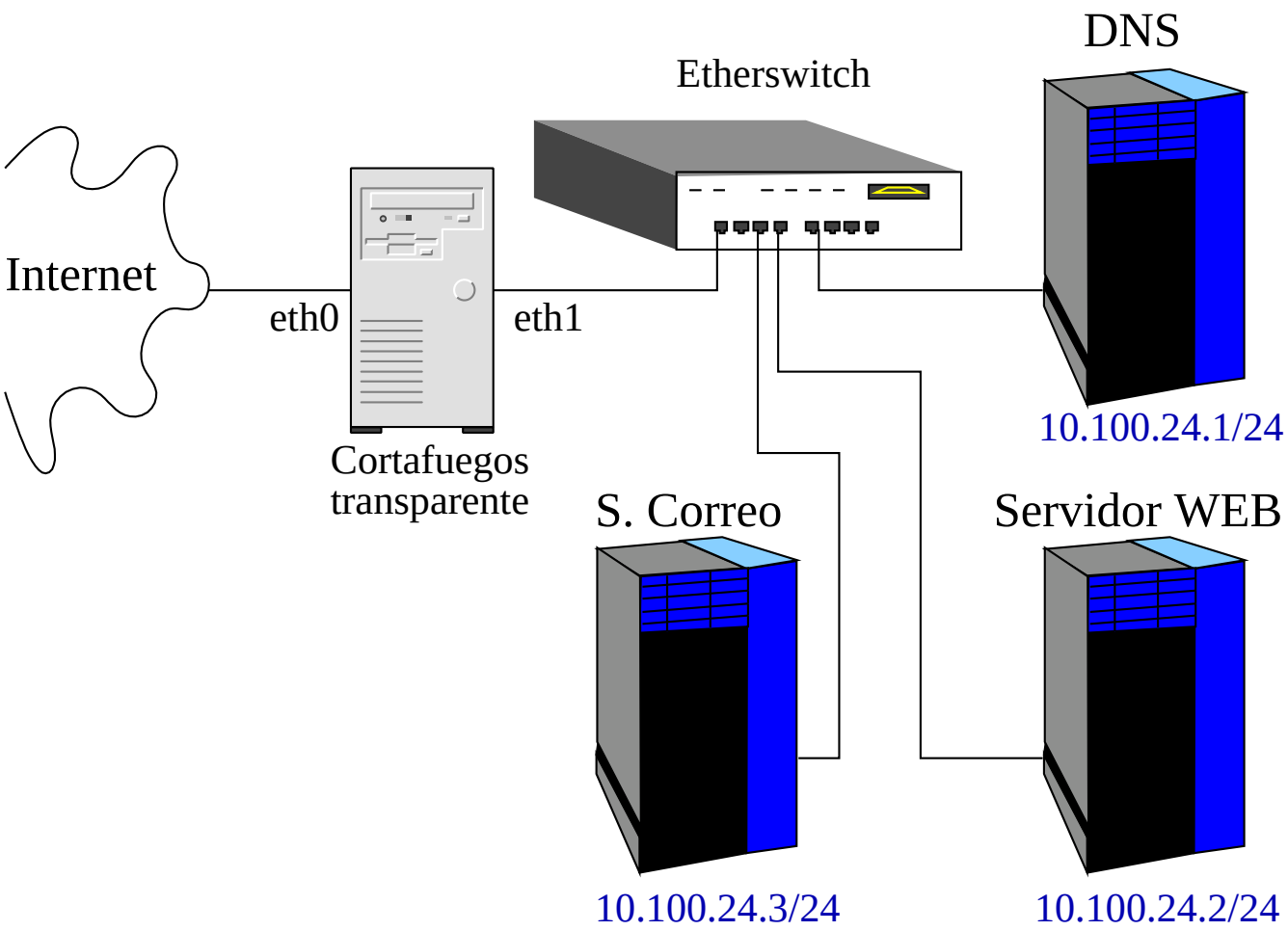
# Permitimos que regresen los paquetes asociados
# a estas conexiones
#
iptables -A FORWARD -m state --state ESTABLISHED,RELATED \
    -i $INTERFAZ_EXT -s ! $REDINTERNA -j ACCEPT

# Todo el tráfico interno es enmascarado externamente
#
iptables -A POSTROUTING -t nat -o $INTERFAZ_EXT -j MASQUERADE
```

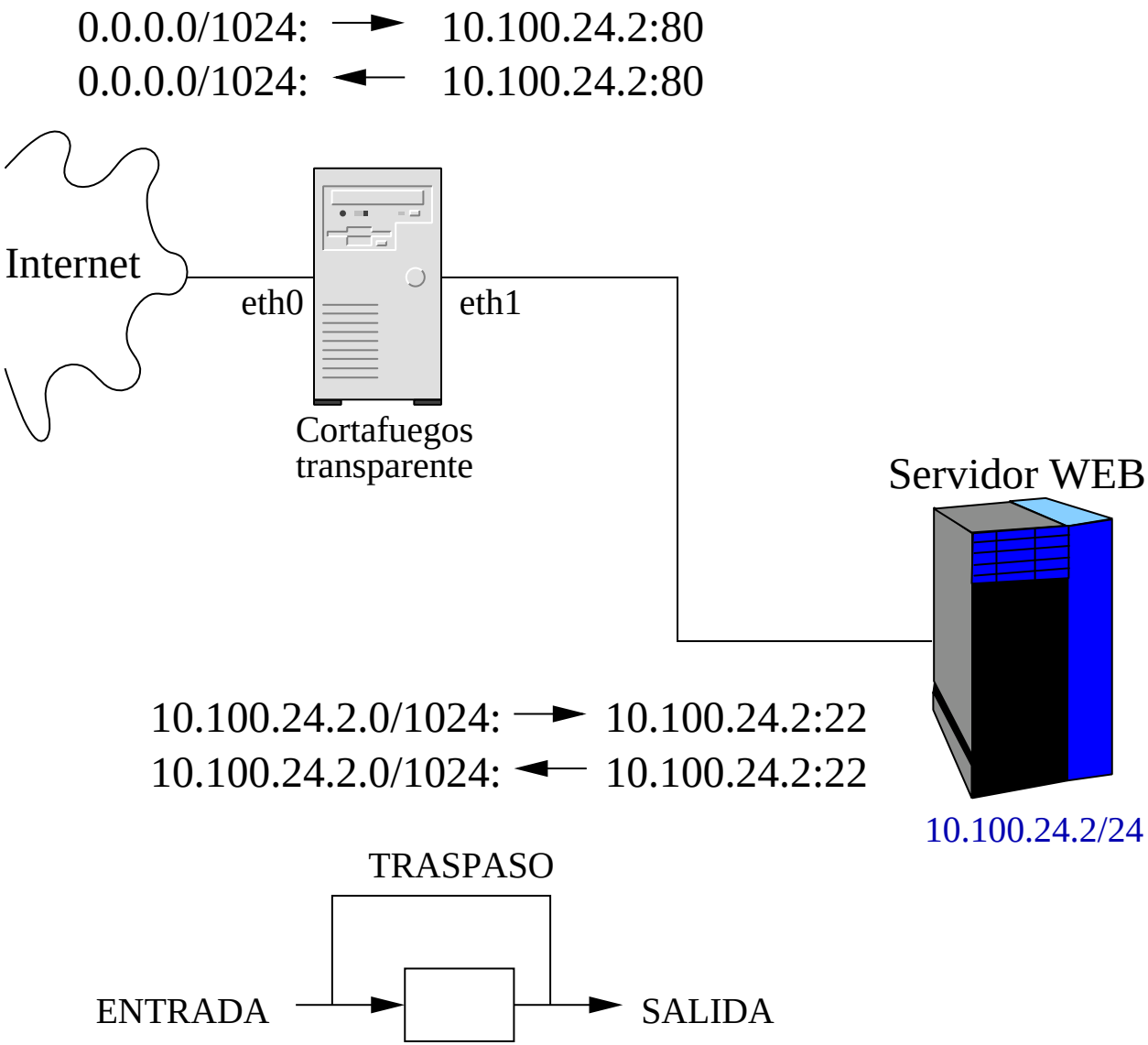
Instalación del script

1. ```
   # ./puerta
   # /sbin/iptables-save > iptables
   # cp iptables /etc/sysconfig
   ```
   normalsize
2. Se pueden configurar el script como parte de los servicos de arranque
   ```

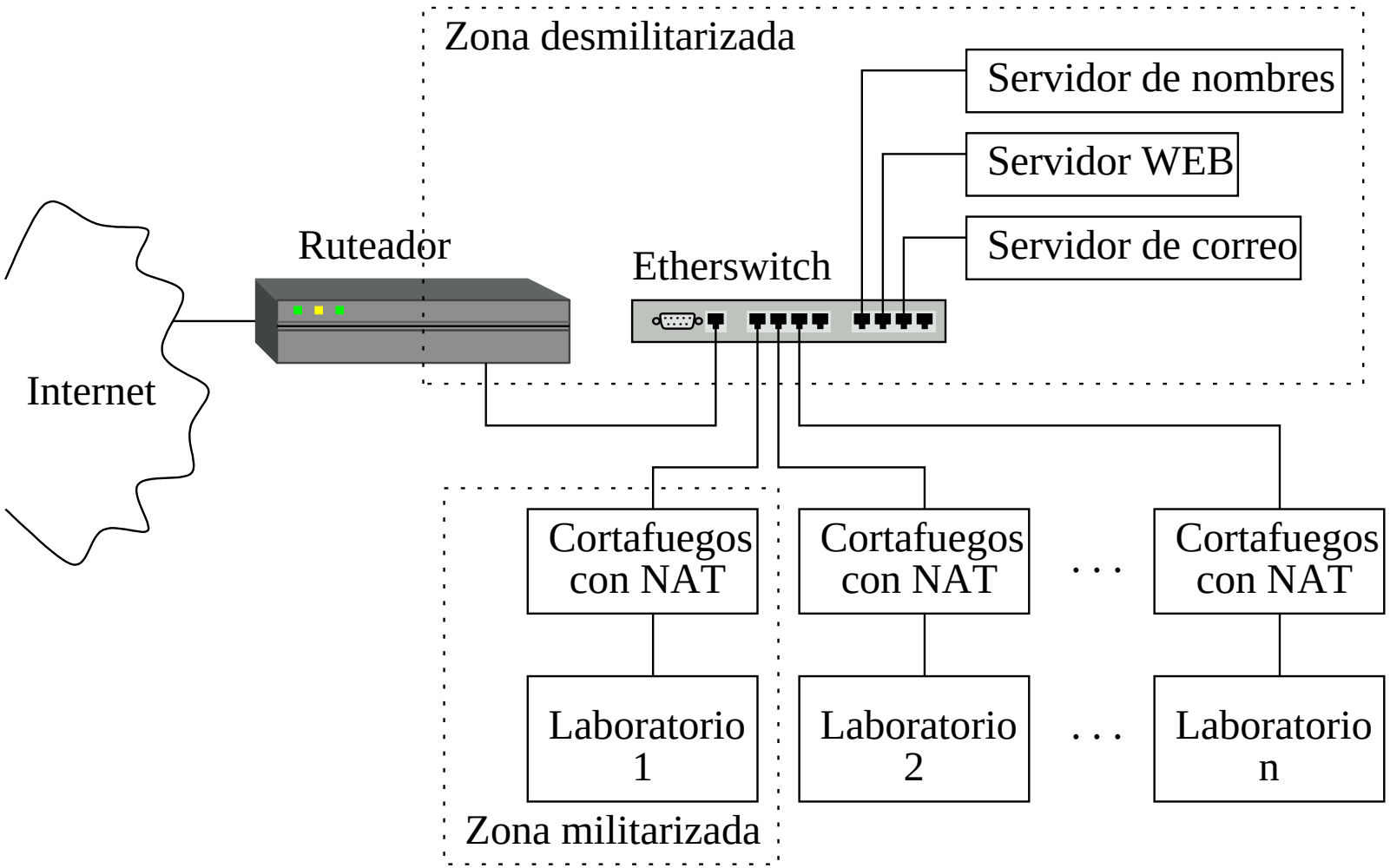
Red Desmilitarizada



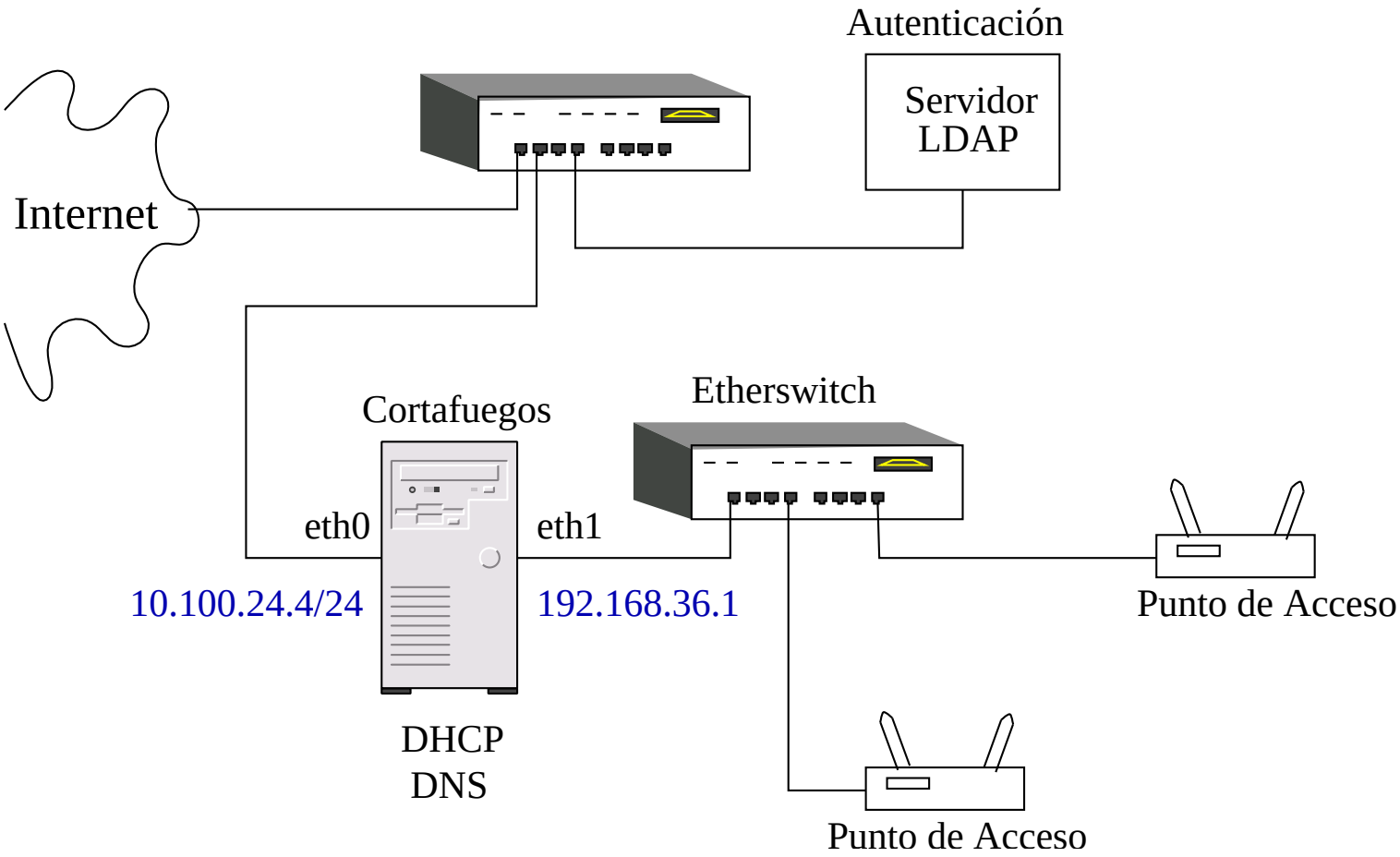
Reglas en los cortafuegos



Solución de Seguridad



Servidor NOCAT para la red inalámbrica

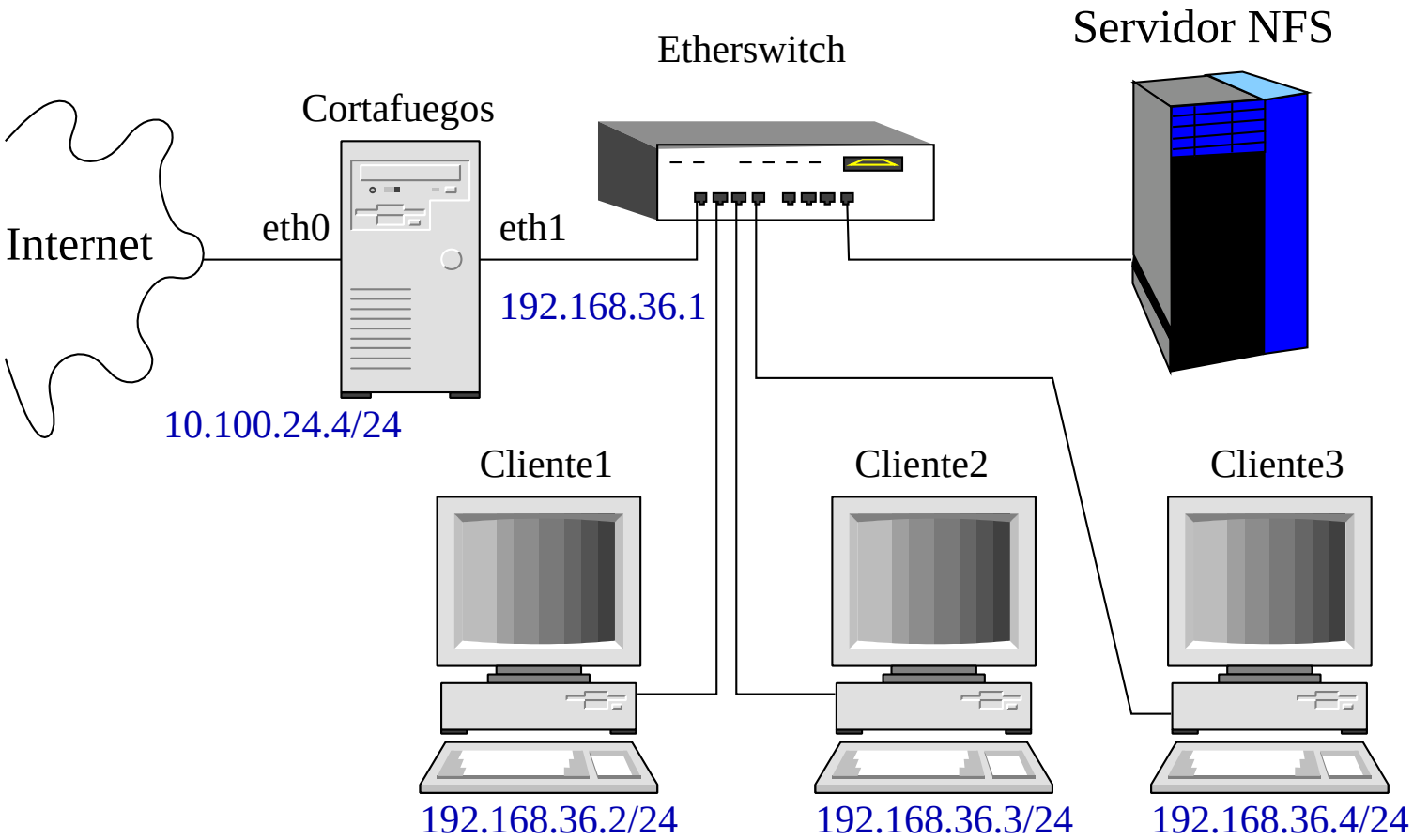


M. Kershaw, Linux-Powered Wireless Hot Spots, *Linux Journal* , 133, Sep 2003.

Facilidad en el Mantenimiento

- La administración de muchas máquinas cliente se vuelve fatigosa
- Se desea que un usuario pueda conectarse desde cualquier máquina (que "vea" siempre sus mismos archivos).

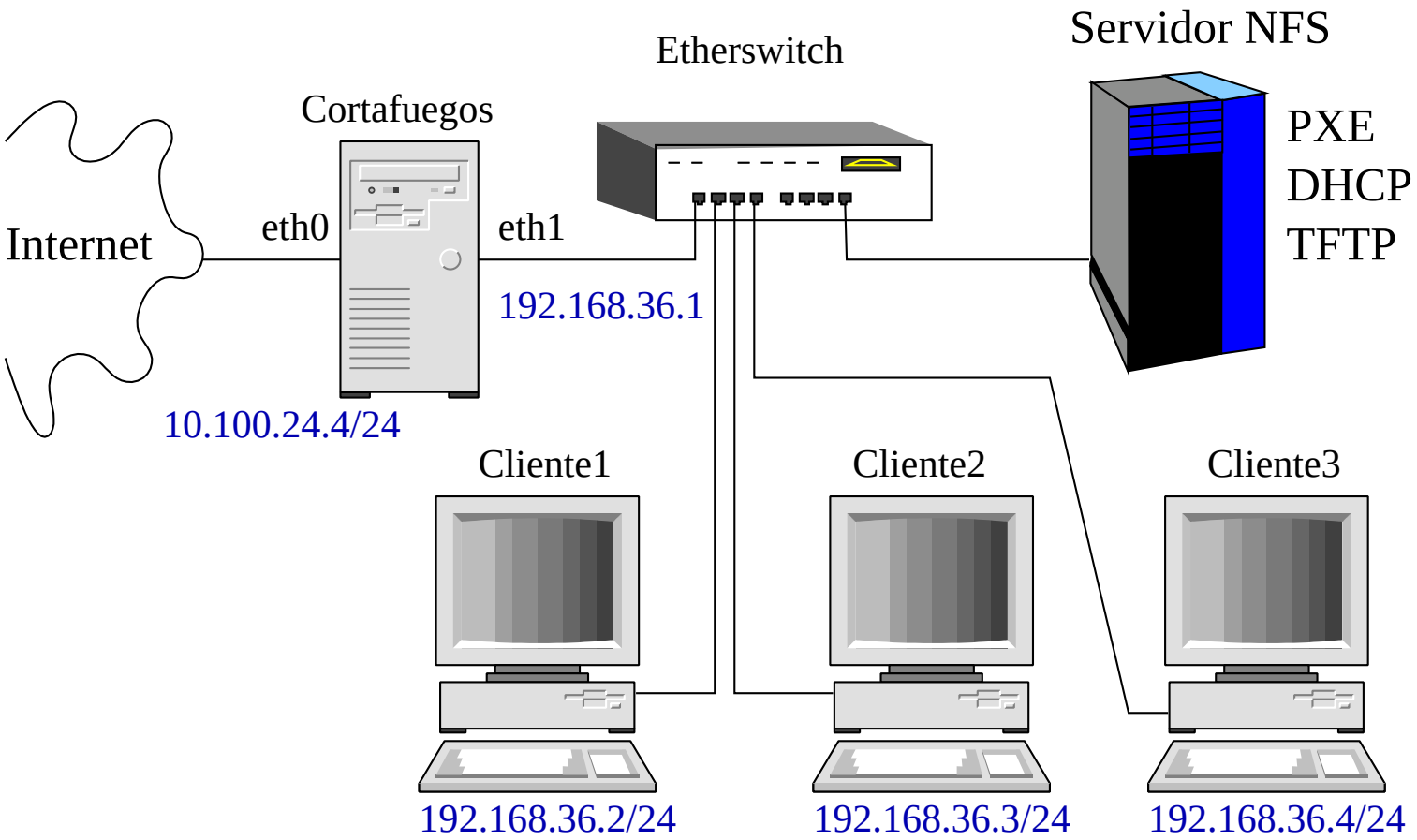
1a. Solución: Compartición del espacio en disco



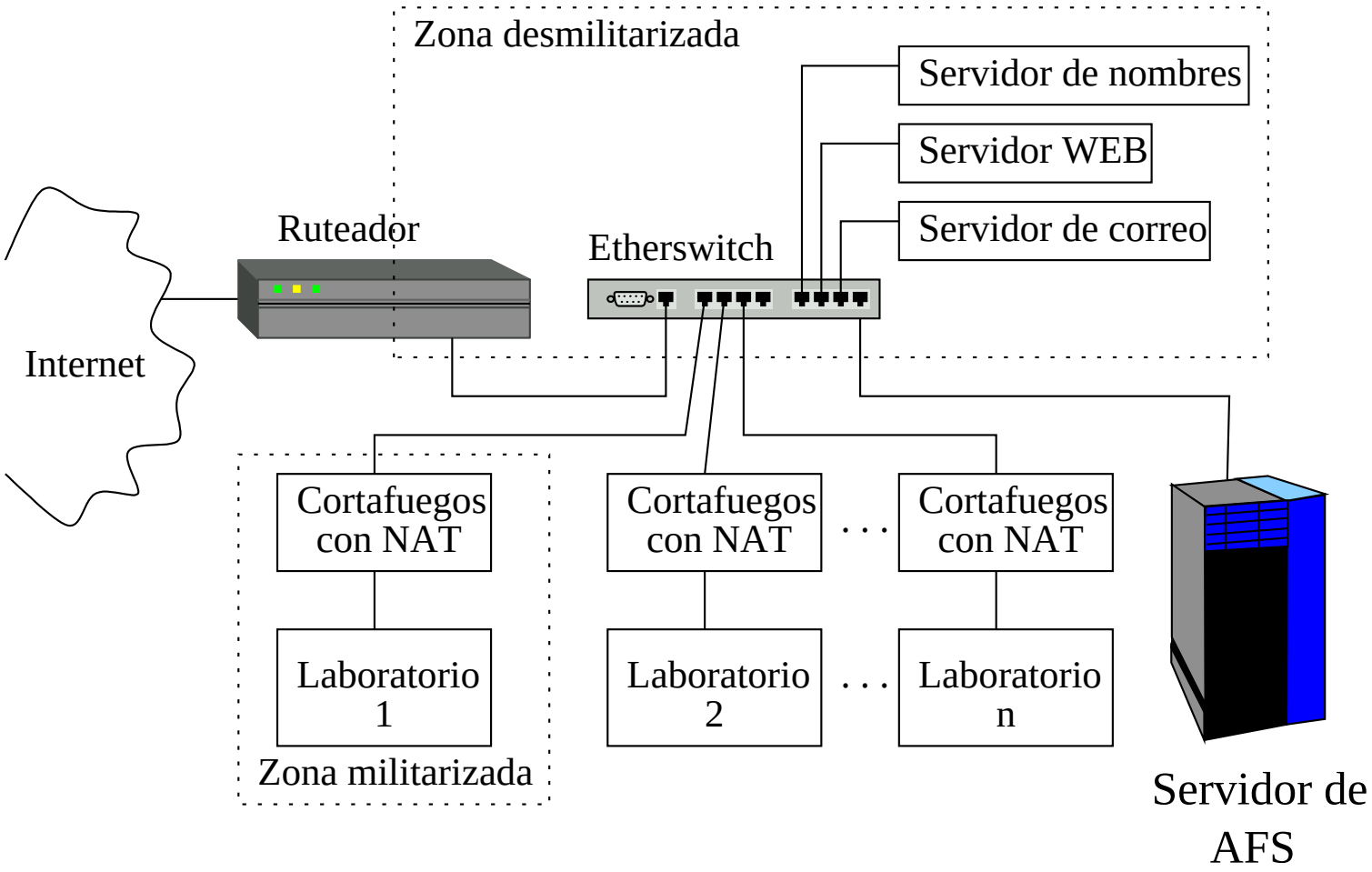
Problemas con la compartición de disco

- Solución OK con discos duros pequeños (< 4 GB).
- Con discos más grandes se desperdicia espacio en ellos.
- Aún se debe instalar paquetes nuevos en todas las máquinas cliente.

2a. Solución: Arranque en red



Solución que se quiere:



¿Cuántas conexiones soporta un cortafuegos?

Opciones:

- Medir los recursos que consume una conexión
- Configurar una red para producir un ataque por denegación de servicio
- Usar una computadora con pocos recursos

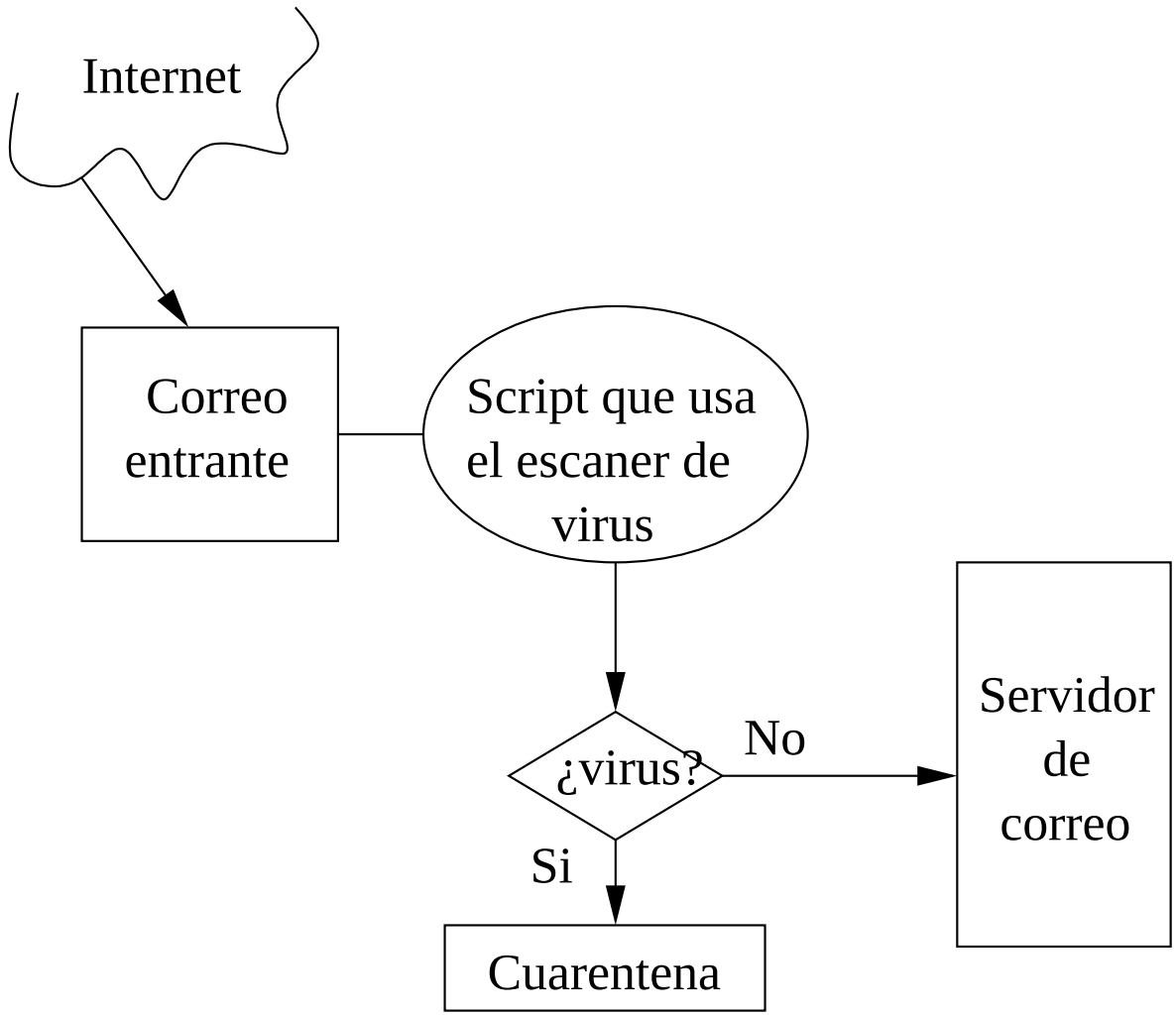
¿Por qué AFS?

- Uso de cache a nivel cliente, el cual evita accesos frecuentes al servidor.
- Seguridad de envío de password, al usarse kerberos para encriptar el pasword que viaja en la red.
- Independencia en ruta, al evitarse que cada máquina cliente necesite saber la localización del servidor.
- Escalabilidad, al permitir transparentemente agregar clientes y servidores sin tener que detener el servicio.
- Servicio para LAN y WAN, donde la relación número de clientes por servidor puede llegar a ser de 200 clientes a 1.

El CERT/CC publica que un sitio ideal en seguridad debe contar con:

1. Estar al día en parches
2. Usar cortafuegos
3. Debe monitorearse la red
4. Deben deshabilitarse los servicios y características que no son necesarios
5. Tener un software de antivirus instalado, configurado y actualizado
6. Una política para la realización de respaldos
7. Un equipo entrenado y con capacidad de respuesta a incidentes

Esquema de un sistema para detección de virus en el correo electrónico



Conclusiones (1/2)

1. Hemos visto una introducción a las redes TCP/IP y porqué son inseguras.
2. Se han expuesto las soluciones implantadas en la red del Departamento de Computación del Cinvestav
   - 2.1 Contar con una red segura. Hemos usando cortafuegos para dividir la red en zonas desmilitarizadas, donde se encuentran nuestros servidores generales, y zonas militarizadas para los laboratorios de estudiantes y laboratorios experimentales.
   - 2.2 Optimizar el uso de recursos. Se ha implantado el arranque en red y la centralización del uso de disco duro.

Conclusiones (2/2)

- Para los cortafuegos hemos usado computadoras personales simples, que pueden ser máquinas viejas de baja velocidad, con el sistema operativo GNU/Linux. Nosotros hemos usado la distribución de RedHat.
- Actualmente usamos el arranque remoto vía PXE en la máquinas cliente con tarjetas madre nuevas y se arranca en CDROM usando Etherboot para las máquinas sin PXE interconstruido. Se usa NFS para centralizar el uso de disco duro. AFS se usará en el futuro.

El contenido de esta charla
puede obtenerse en
http://delta.cs.cinvestav.mx/~fraga/

La página WEB del Departamento de Computación:

http://www.cs.cinvestav.mx