Seguridad y Configuración de Redes de Computadoras con GNU/Linux

Enrique Bonilla Enríquez y Luis Gerardo de la Fraga

E-mail: fraga@cs.cinvestav.mx

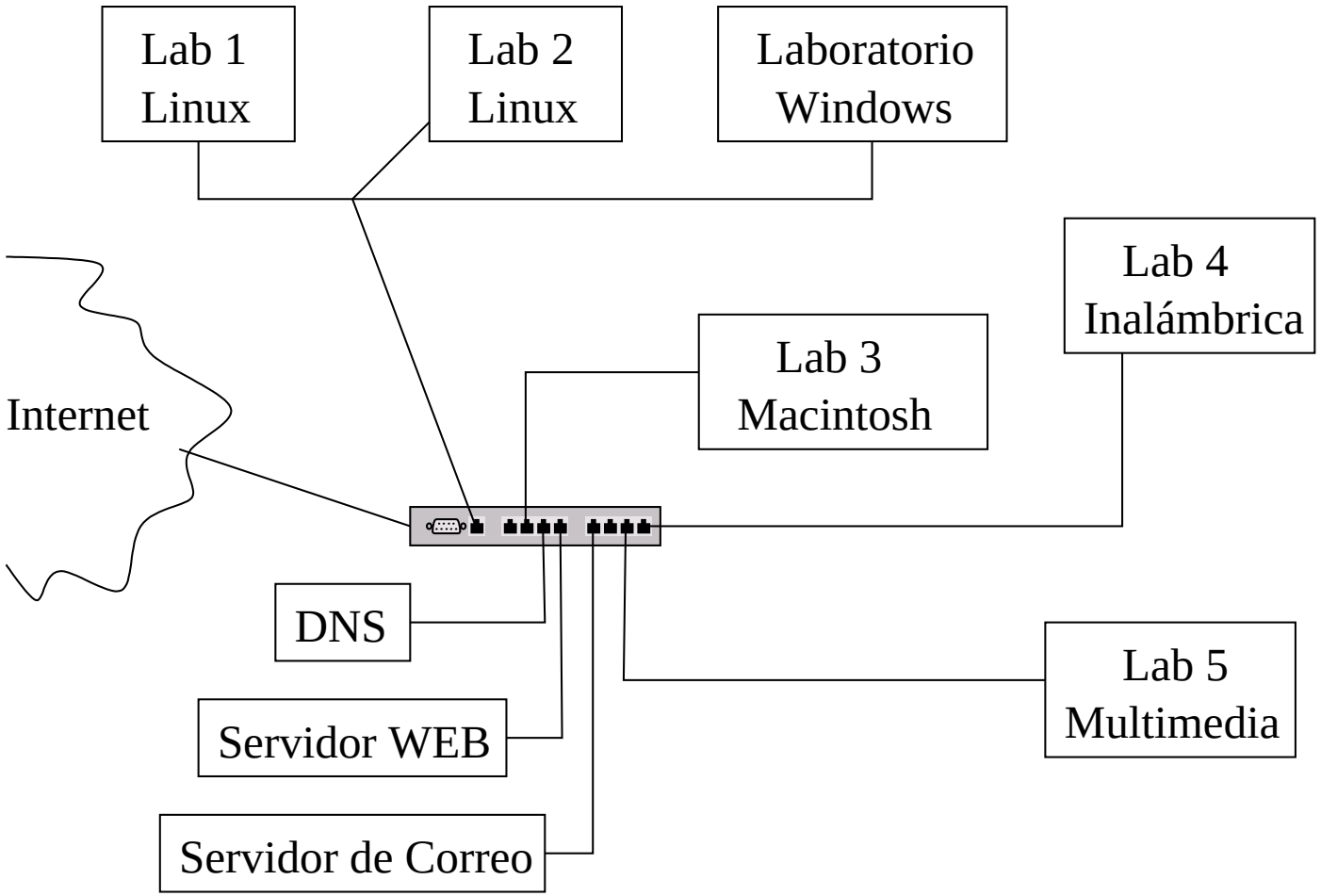
Sección de Computación

Departamento de Ingeniería Eléctrica

CINVESTAV-IPN

11 de febrero de 2004

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.

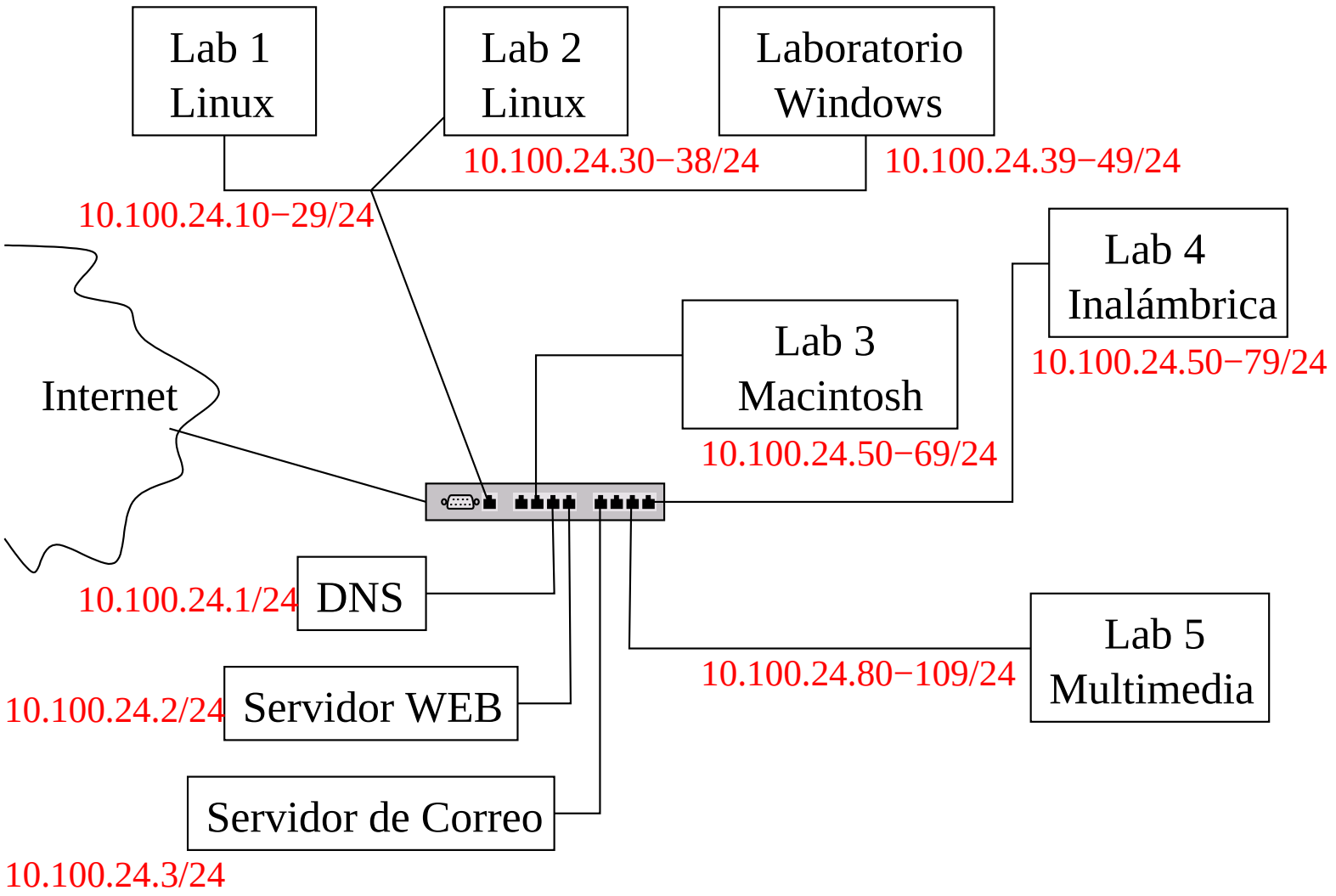
El Problema (3/3)

En este escenario existen dos preocupaciones básicas:

1. La seguridad y
2. la facilidad de mantenimiento

de toda nuestra red.

Seguridad (1/3)

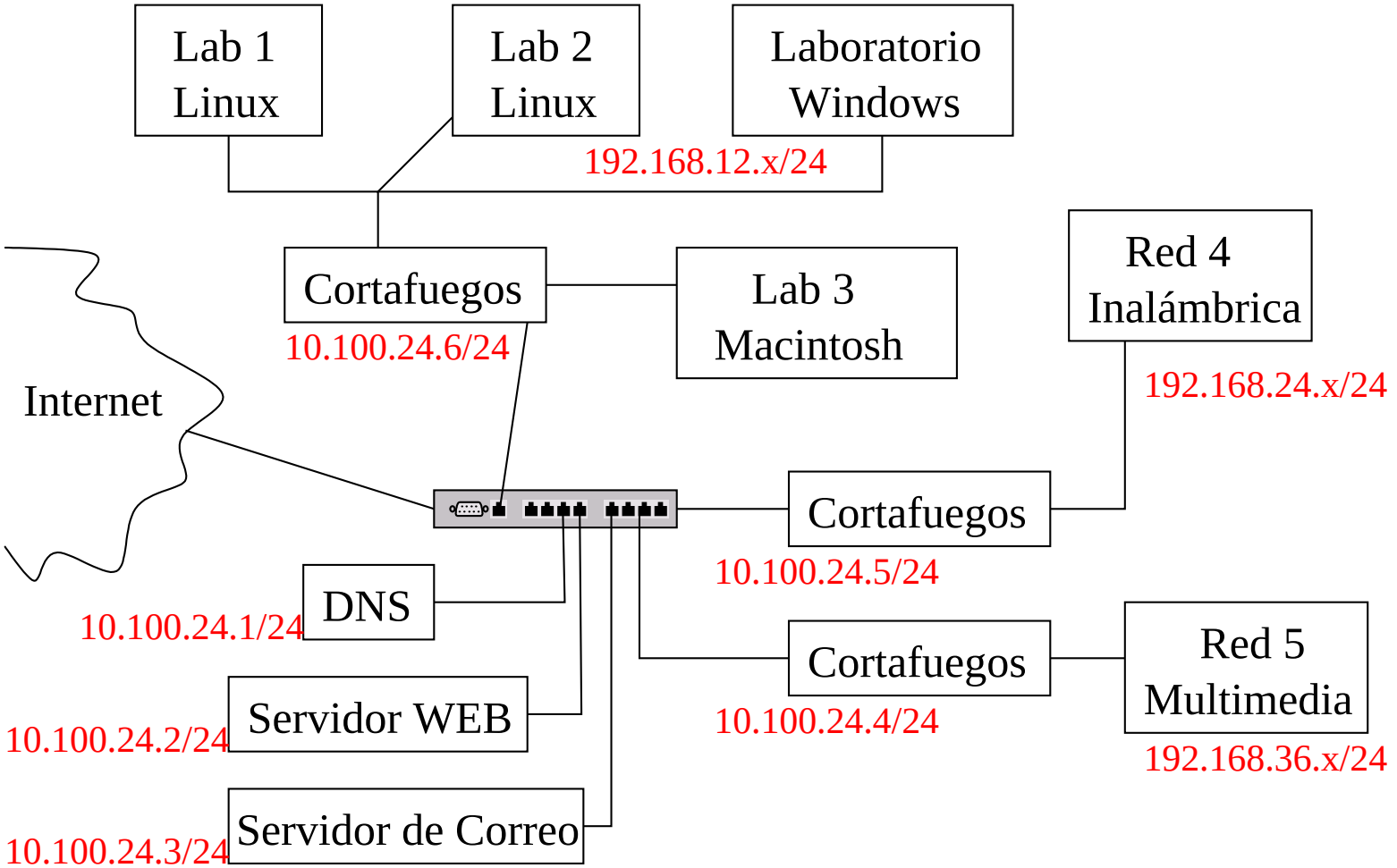


Seguridad (2/3)

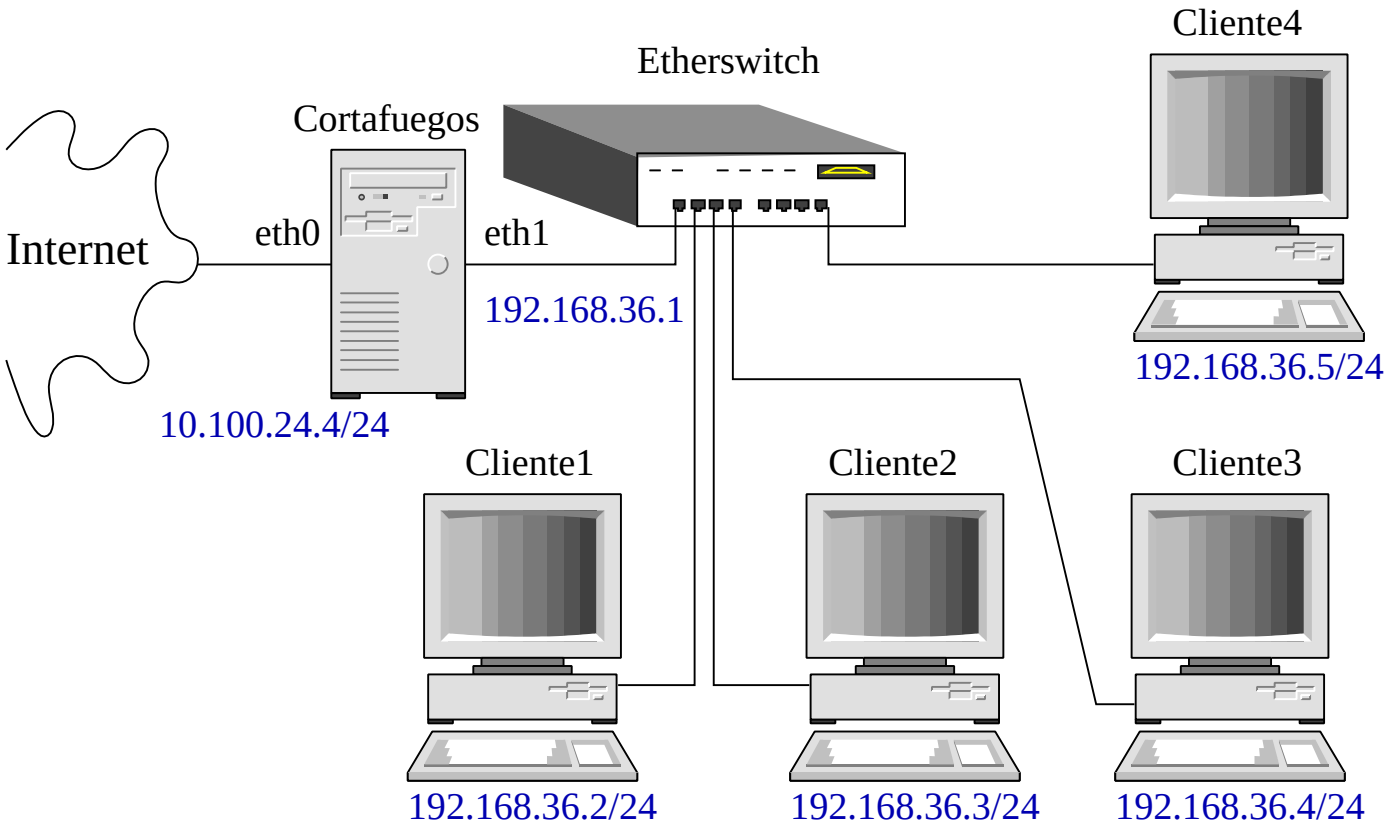
En la red anterior (IPs registrados para todas las máquinas) nos generan los siguientes problemas:

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



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. ∗ .∗.

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

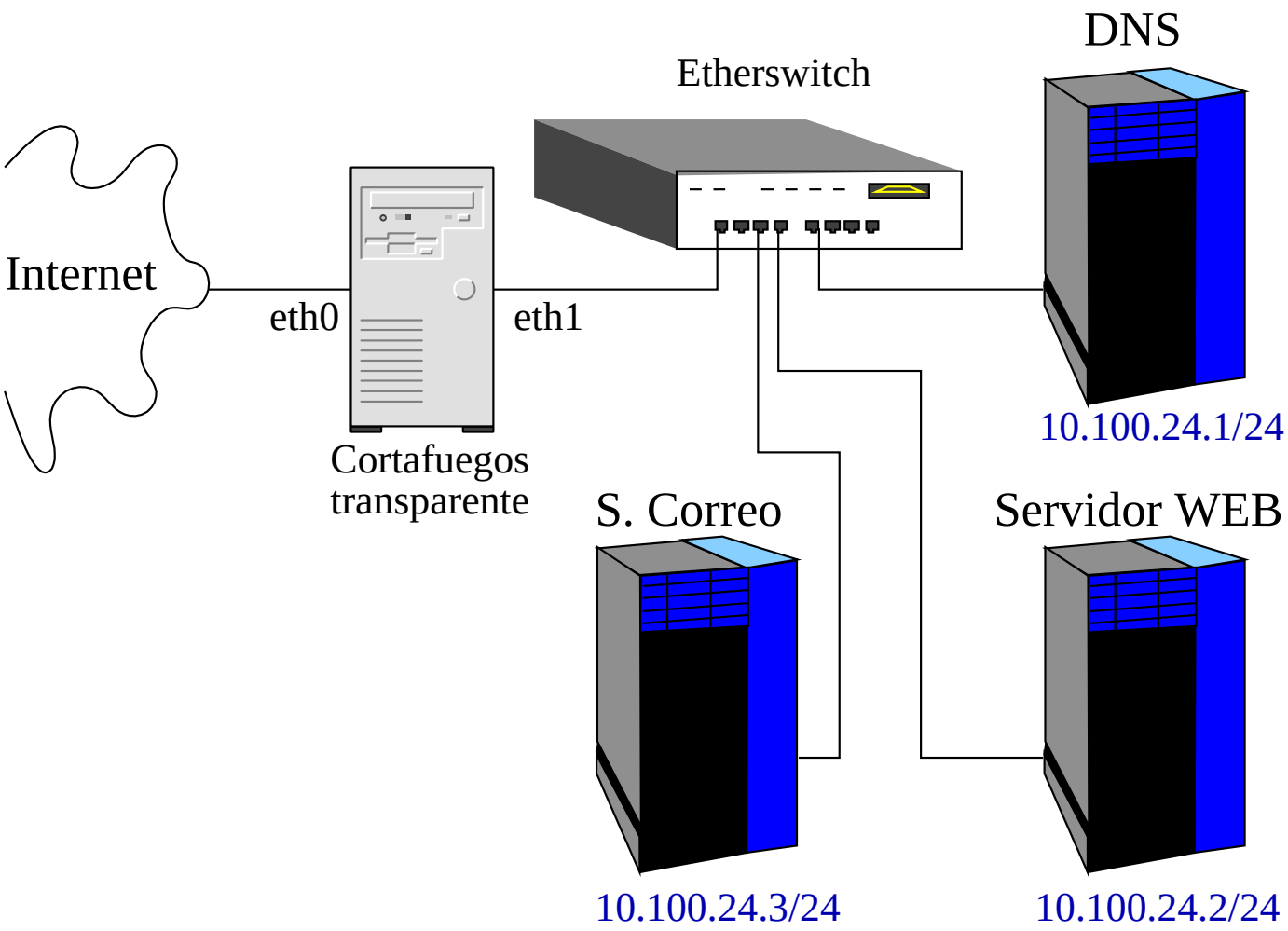
# Permitimos que regresen los paquetes asociados
# a estas conexiones
#
iptables -A FORWARD -m state --state ESTABLISHED,RELATED \
    -i $INTERFAZ_EXT -s ! $REDINTERNA -j ACCEPT

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

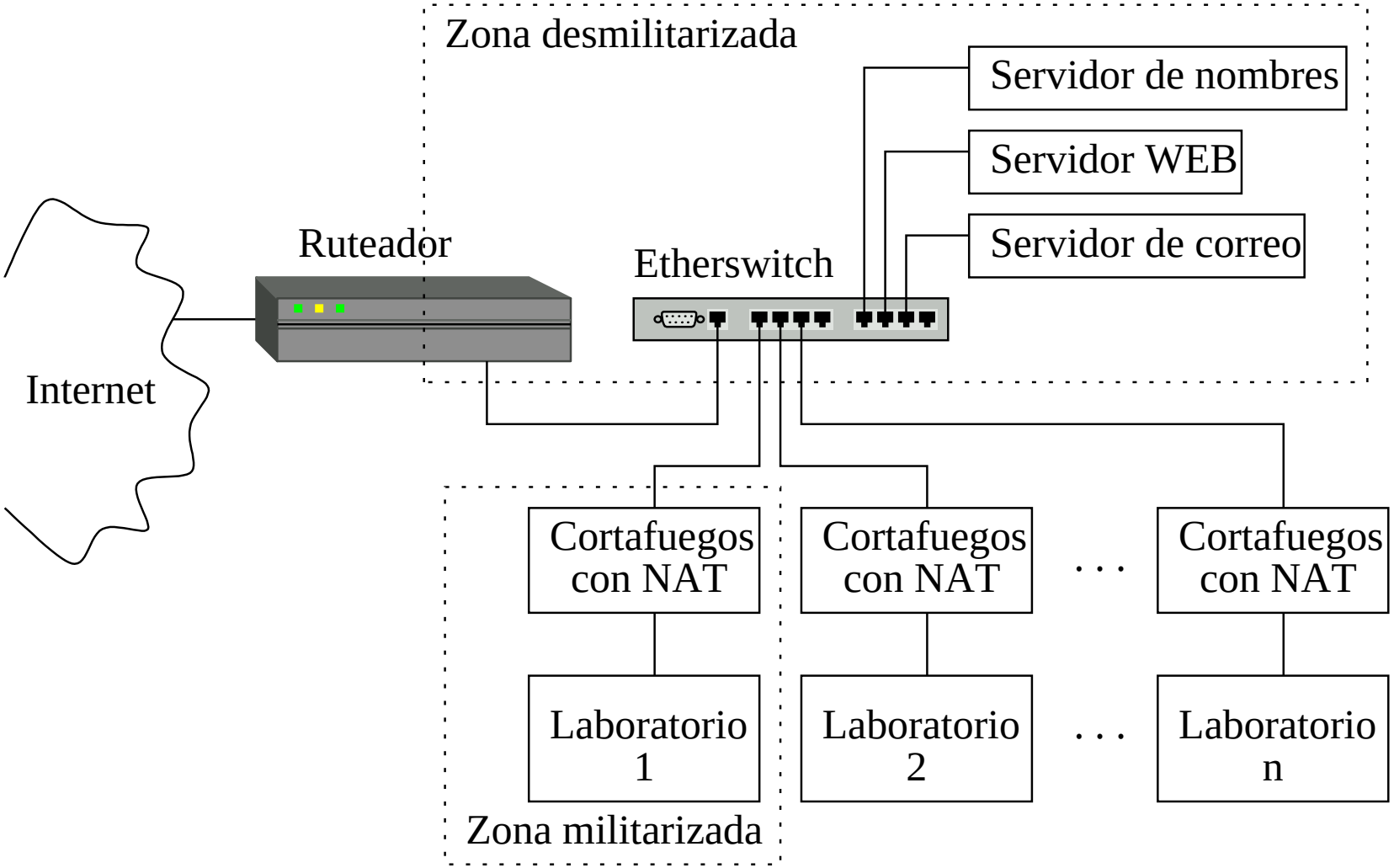
Instalación del script

1. ```
   # ./puerta
   # /sbin/iptables-save > iptables
   # cp iptables /etc/sysconfig
   ```
2. Se pueden configurar el script como parte de los servicos de arranque (en `/etc/rc[0-6].d` con `chkconfig`).
   ```

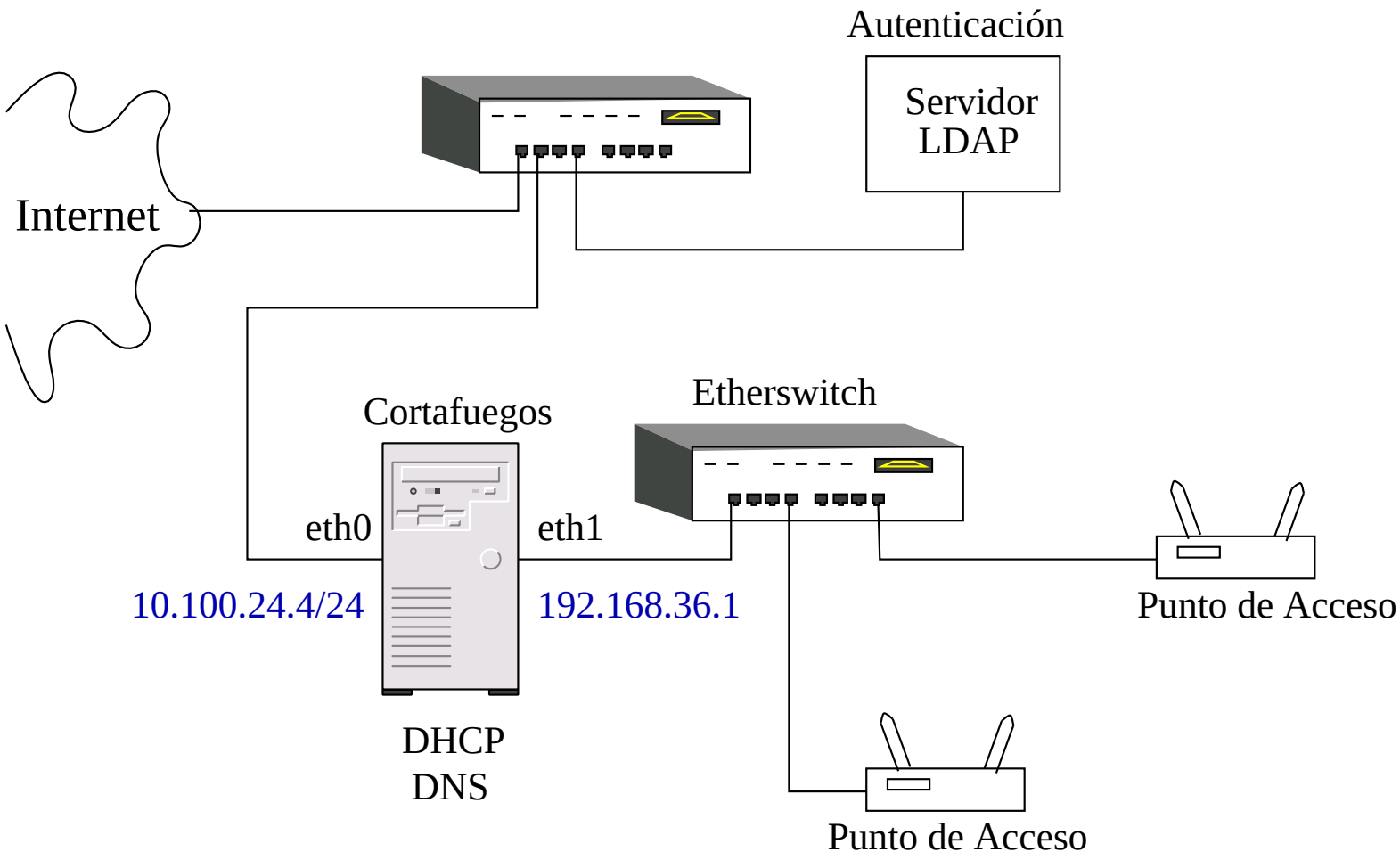
Red Desmilitarizada



Solución de Seguridad



Servidor NOCAT para la red inalámbrica

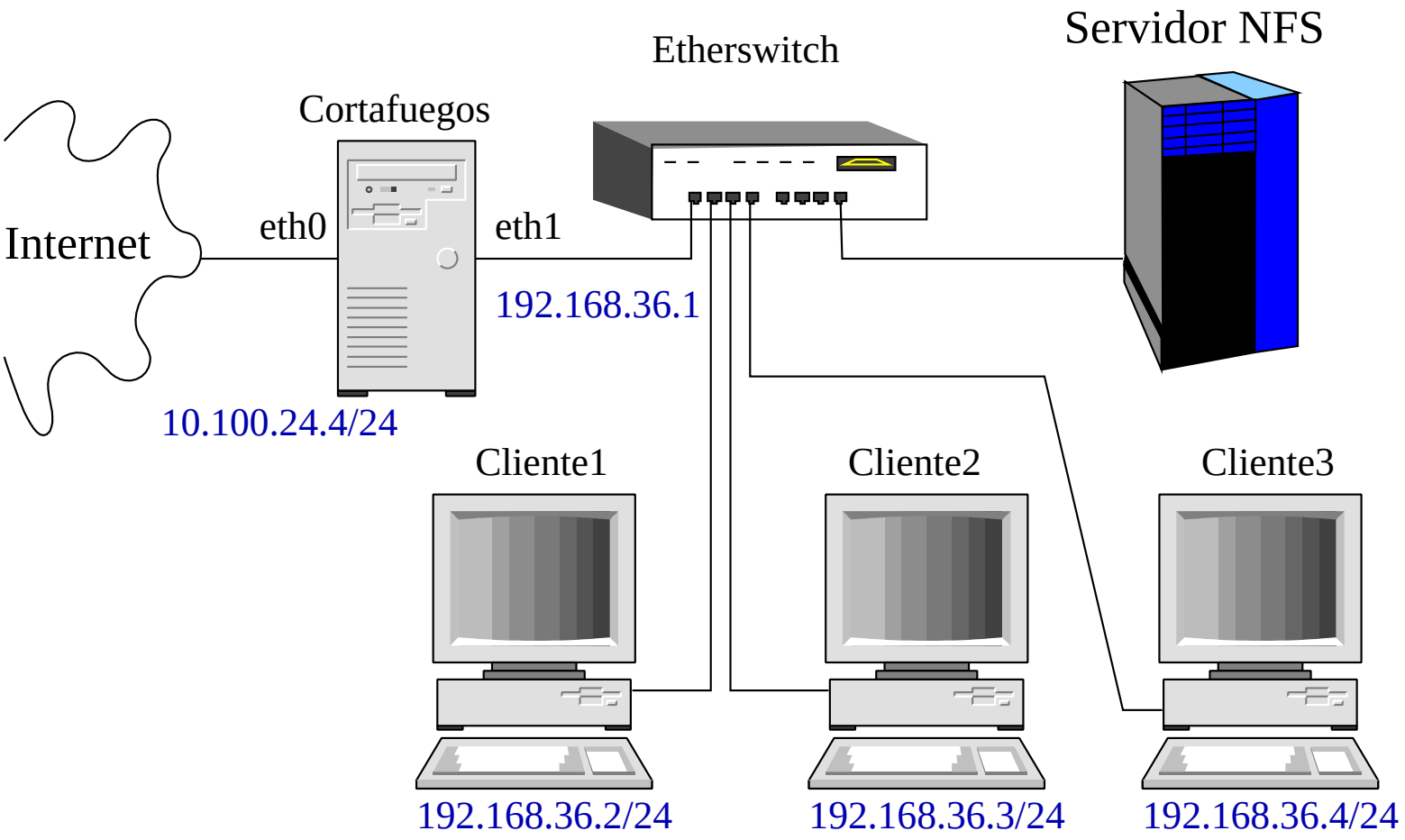


M. Kershaw, Linux-Powered Wireless Hot Spots, *Linux Journal* , 133, Sep 2003.

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).

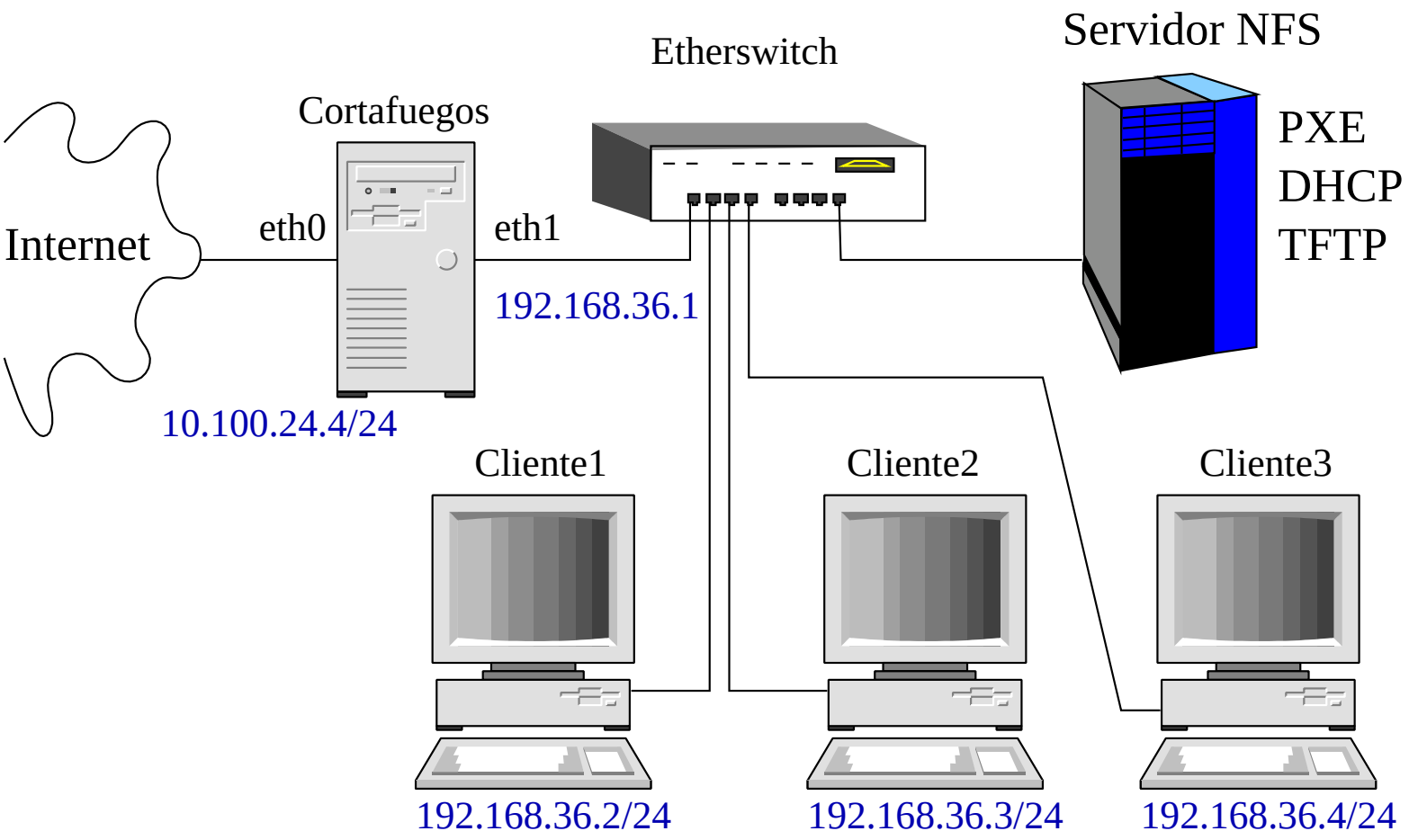
1a. Solución: Compartición del espacio en disco



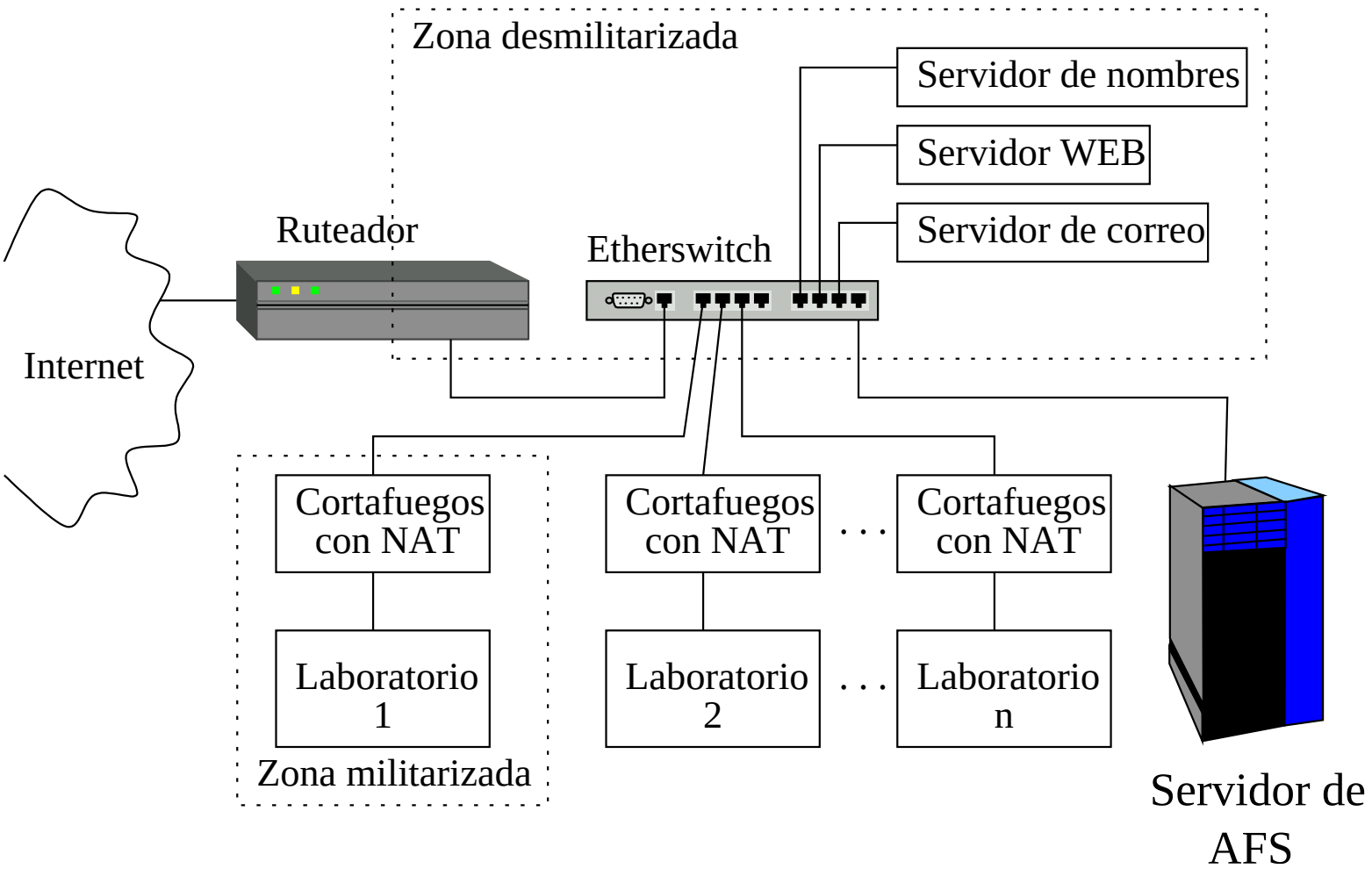
Problemas con la compartición de disco

- 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:



¿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.

Conclusiones (1/3)

Se han expuesto las soluciones implantadas en la Sección de Computación del Cinvestav-IPN para:

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. Optimizar el uso de recursos. Aquí hemos implantado el arranque en red de las máquinas cliente y la centralización del uso de disco duro. Esto nos ha permitido eficientar el uso de los discos duros (no se tienen muchos discos grandes, uno en cada máquina cliente) y facilitarnos la administración de nuestra red (se mantienen un servidor por cada laboratorio).

Conclusiones (2/3)

- 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.

Conclusiones (3/3)

Se ha planteado que AFS puede dar la solución para mostrar una misma *casa* a todos los usuarios de forma transparente. En el siguiente congreso pretendemos presentar los resultados de la implación de AFS en nuestra red.

El contenido de esta charla
puede obtenerse en

http://delta.cs.cinvestav.mx/~fraga/Programas

La página WEB de la Sección de Computación:

http://www.cs.cinvestav.mx