Redes de Computadoras y Cortafuegos con GNU/Linux

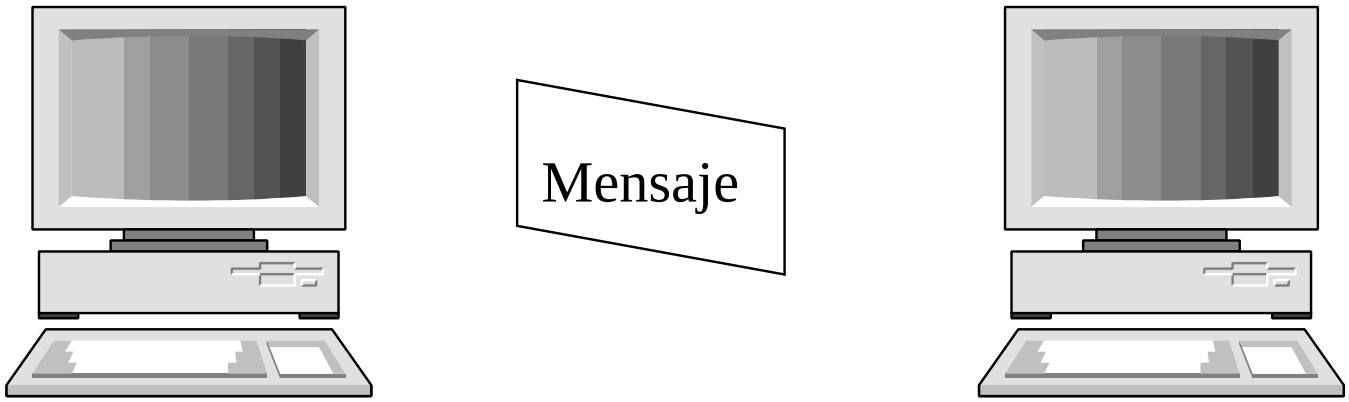
Dr. Luis Gerardo de la Fraga

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

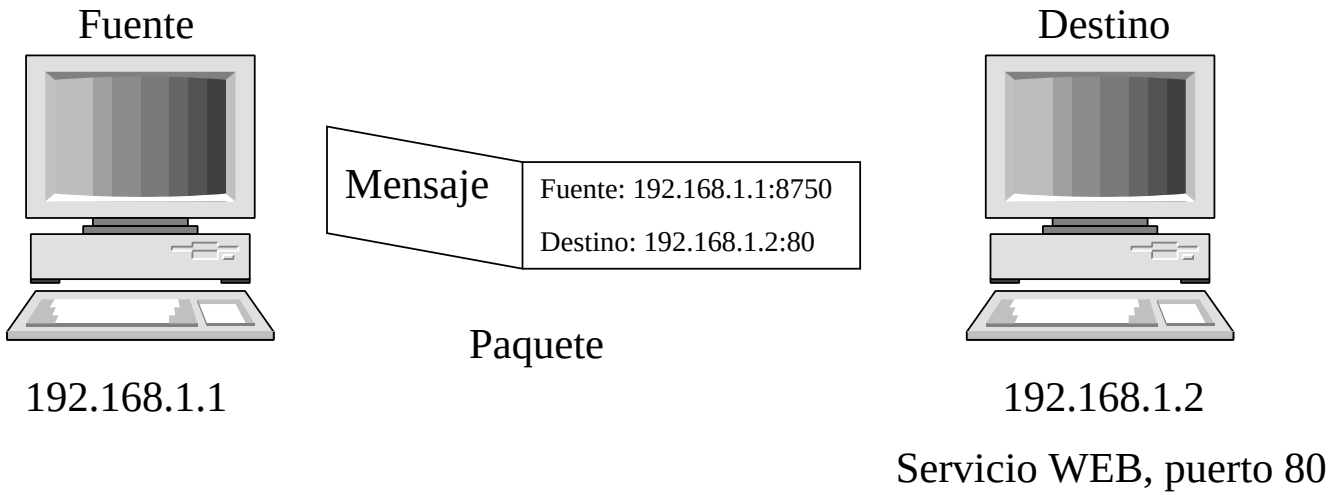
9 de mayo de 2007

Contenido

Comunicación entre dos computadoras



Formación de paquetes



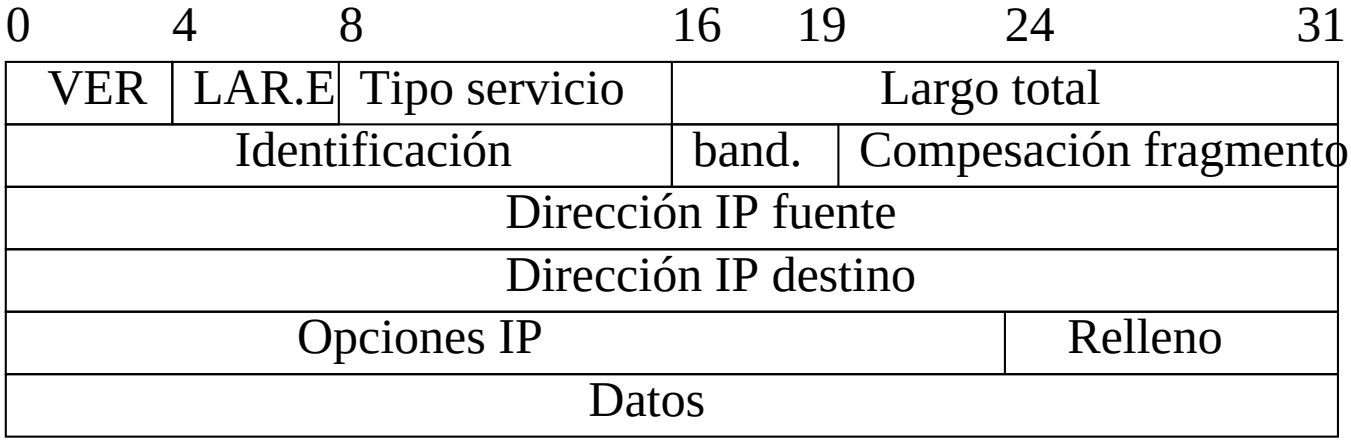
>Por qué usamos redes de computadoras?

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

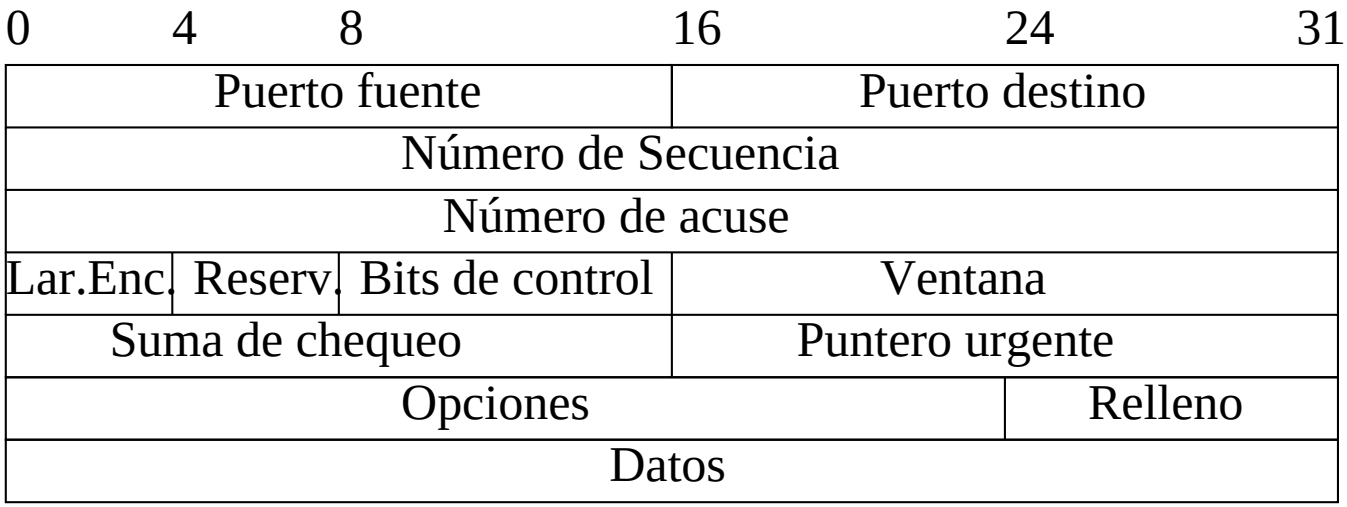
Internet

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

TCP/IP. El encabezado de IP



TCP/IP. El encabezado de TCP

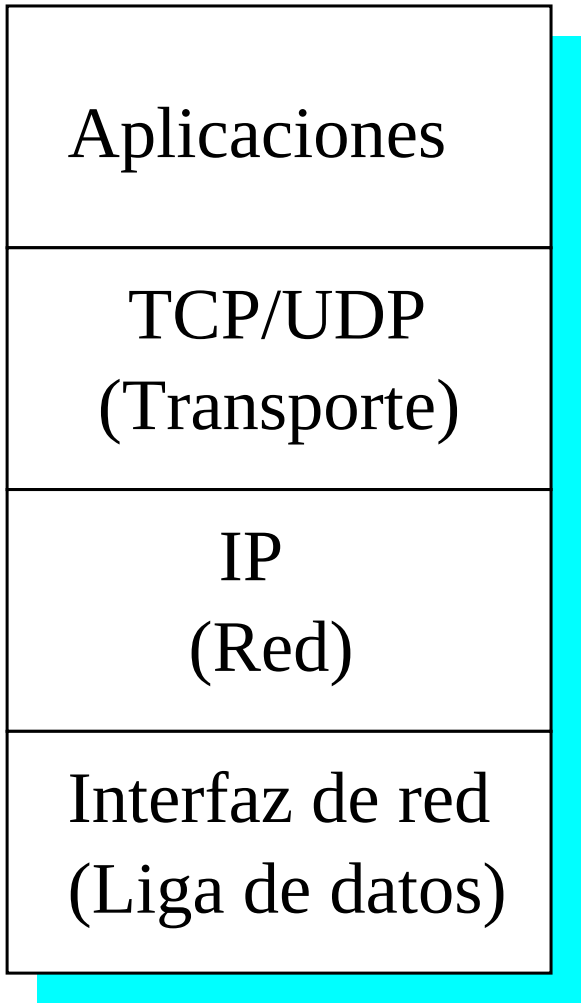


Ventajas de usar TCP/IP

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)

Origen de las inseguridades en TCP/IP

1. No se consideró la seguridad en su diseño.
2. No está bien especificado el uso de todos los campos de los encabezados. Se pueden usar esos campos para transmitir información.
3. En IPv6 si se tienen definidos todos los campos, si se necesitán más se definen nuevos encabezados.
4. En IPv4 se implemente la seguridad en las aplicaciones. IPv6 puede usar IPSec en la capa base de interfaz de red.

Flujo 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) $\longrightarrow$ Huésped B
2. Huésped A $\leftarrow$ SYN(ISN+1)/ACK — Huésped B
3. Huésped A —— ACK $\longrightarrow$ Huésped B

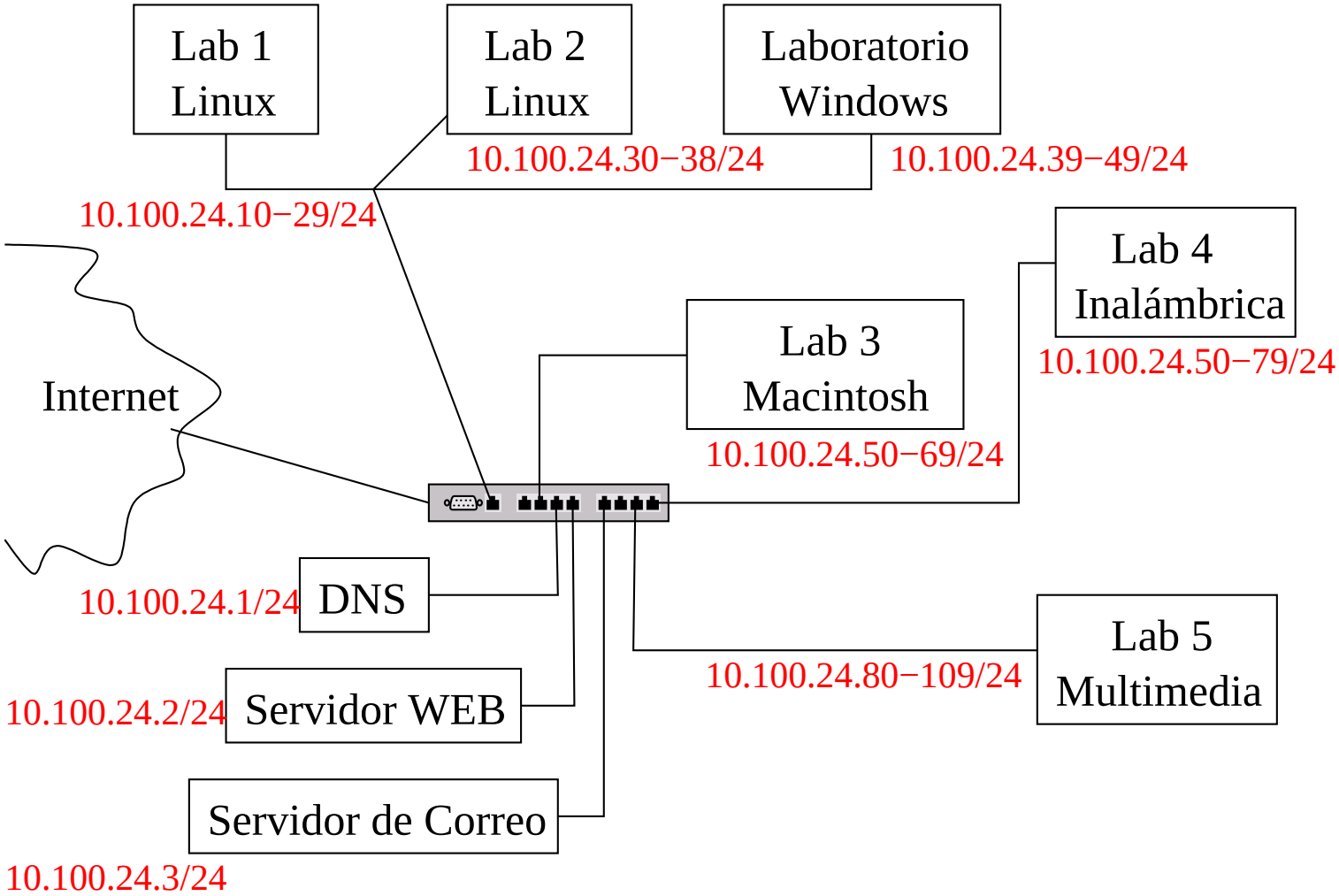
Esto no sucede con los paquetes de UDP, los cuales se consideras "no fiables" y no intentan corregir los errores ni negociar una conexión antes del envio a un huésped remoto.

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

Seguridad (1/3)

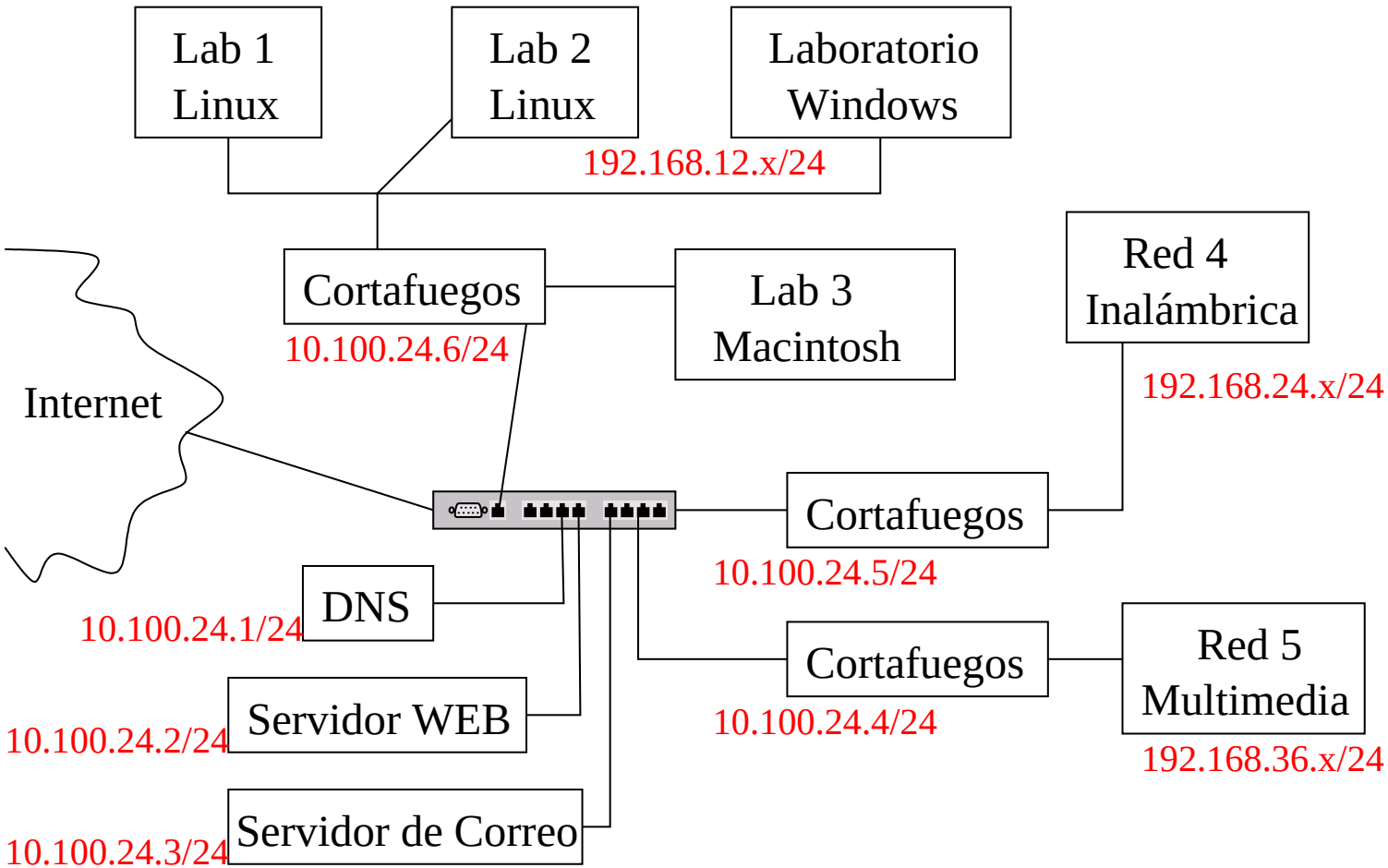


Seguridad (2/3)

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. Posibles 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)



IPTables (1/2)

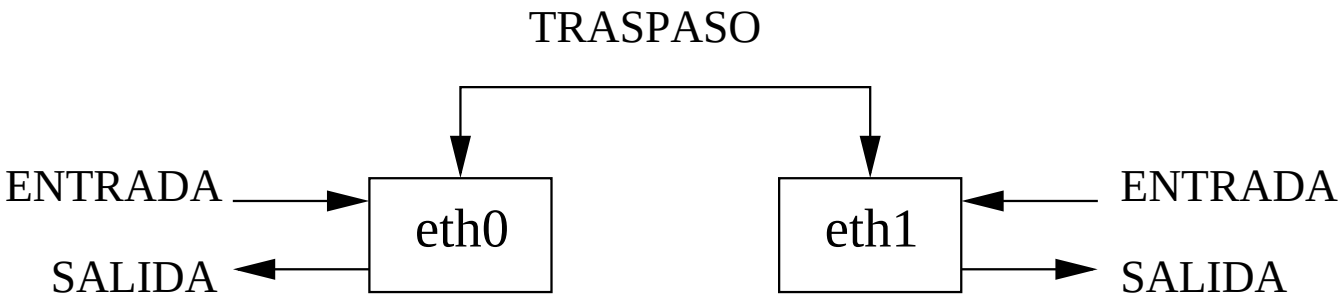
Tres cosas puede significar IPTables:

1. El software general se llama *Netfilter*, el cual provee los ganchos dentro de la pila de IP en los cuales se pueden cargar módulos que realzan operaciones sobre los paquetes.
2. IPTables viene en dos partes: los módulos en el espacio del núcleo (que son distribuidos con el mismo núcleo). El módulo principal es `ip_table` y existen módulos específicos para NAT, log, seguimiento de conexiones, etc.
3. La segunda parte son programas en el espacio del usuario que son distribuidos de forma separada. Estos comandos pueden adicionar, remover o editar reglas en los módulos. *iptables* se refiere a este comando.

IPTables (2/2

La manera en que se manejan (o filtran) los paquetes es insertando reglas dentro de los módulos que realizar una función determinada. Una lista de reglas es una *cadena*.

Cadenas por defecto en una interfaz de Red



Sintaxis de iptables (1/5)

- Se crea una cadena con:
  `iptables -N <nombre-de-la-cadena>`
- Se borra una cadena con:
  `iptables -X <nombre-de-la-cadena>`
- Se vacía toda una cadena:
  `iptables -F <nombre-de-la-cadena>`
- Lista las reglas de una cadena:
  `iptables -nL <nombre-de-la-cadena>`
- Especifica la meta de una cadena:
  `iptables -A <nombre-de-la-cadena> -j <nombre-de-la-cade`

Sintaxis de iptables (2/5)

- Se adiciona una regla a una cadena:
  `iptables -A <cadena> <especificacion_de_la_regla>`
- Se inserta una regla a una cadena:
  `iptables -I <cadena> [numero_de_regla] especificacion_d`
- Se borra una regla de una cadena:
  `iptables -D <cadena> [numero_de_regla]`
  `iptables -D <cadena> <especificacion_de_la_regla>`
- `-p` especifica el protocolo IP usado, puede ser TCP, ICMP, UDP o alguno de los protocolos menos usado.
- `--dport` especifica el puerto destino del paquete
- `--sport` especifica el puerto fuente del paquete. Se usa menos ya que las conexiones se originen de un puerto fuente aleatorio (arriba del 1024).

Sintaxis de iptables (3/5)

Comportamiento de la regla:

- `DROP` atrapa el paquete sin tomar el esfuerzo de continuar lo que sigue.
- `DENY` atrapa el paquete y regresa un paquete ICMP a la fuente del paquete para decirle que la conexión está denegada.
- `ACCEPT` deja pasar el paquete

Sintaxis de iptables (4/5)

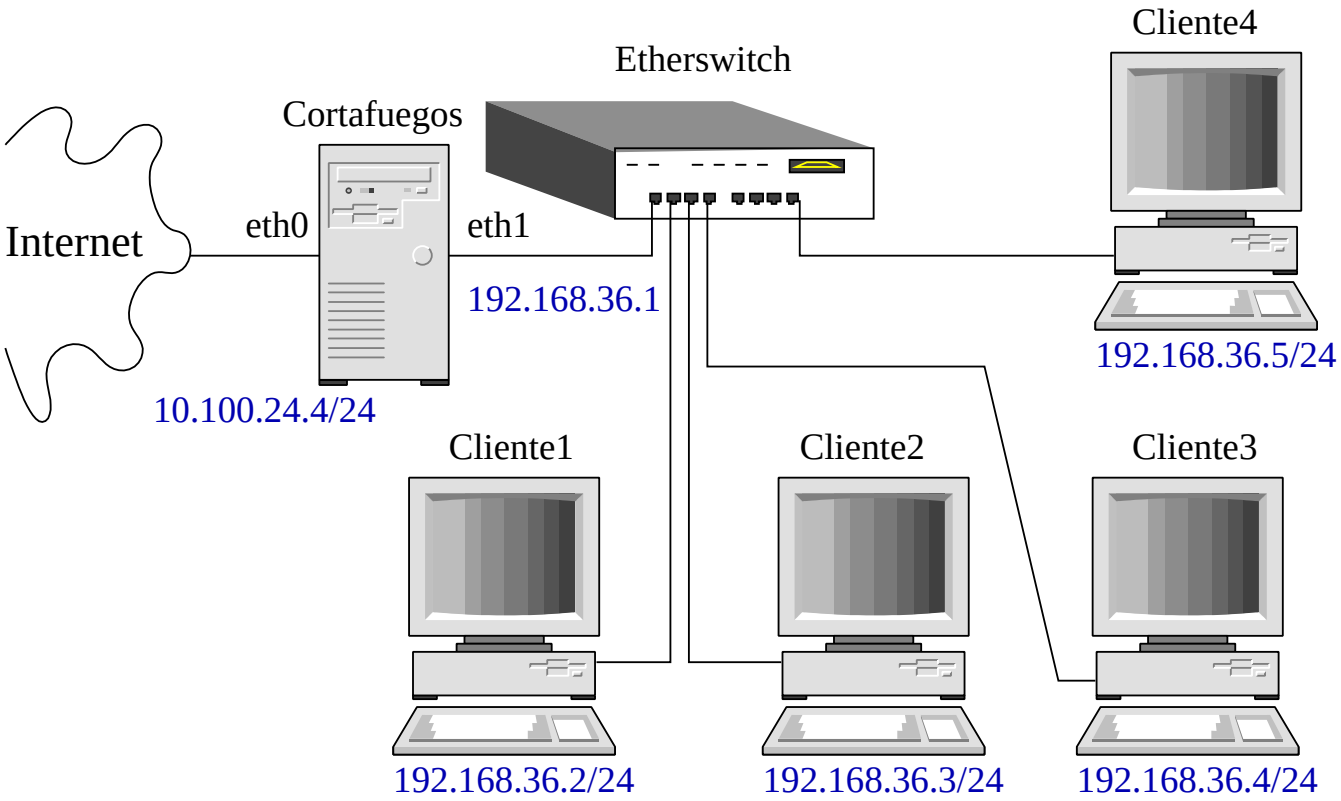
Direcciones IP fuente y destino:

- `-s <direccion_ip>`
- `-d <direccion_ip>`
- Dirección de un huésped: `192.168.20.2/32`
- Dirección de una red: `192.168.20.0/24`
- Cualquier IP: `0.0.0.0/0`

Sintaxis de iptables (5/5)

- Interfaz de entrada: `-i <nombre>`
- Interfaz de salida: `-o <nombre>`
- `-i` solo puede usarse con `INPUT`
- `-o` solo puede usarse con `OUTPUT`
- Pero `FORWARD` puede usar ambos.

Red Militarizada



Script para realizar una RM 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

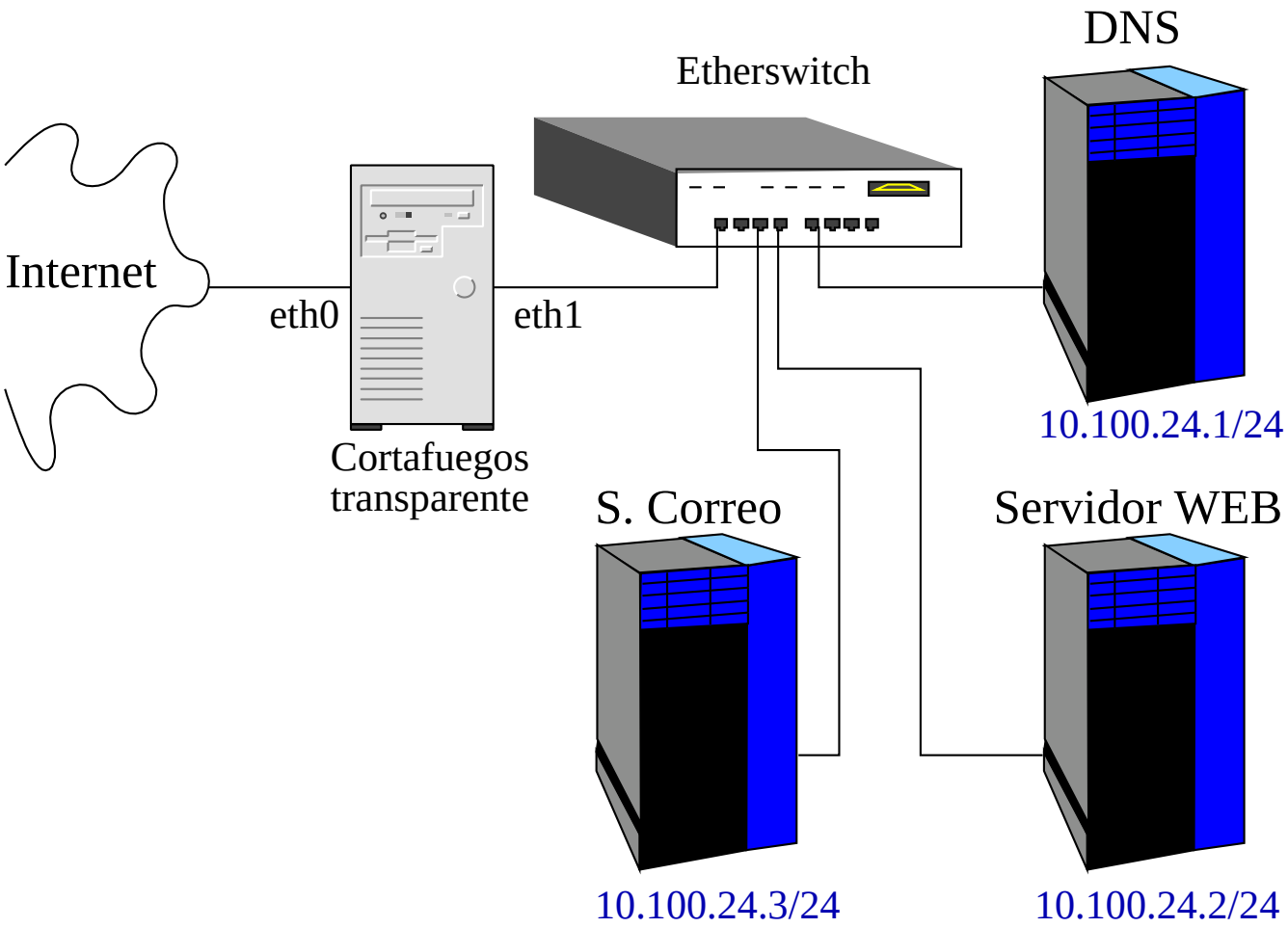
# Permitimos que regresen los paquetes asociados
# a estas conexiones
#
iptables -A FORWARD -m state --state ESTABLISHED,RELATED \
    -i $INTERFAZ_EXT -s ! $REDINTERNA -j ACCEPT

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

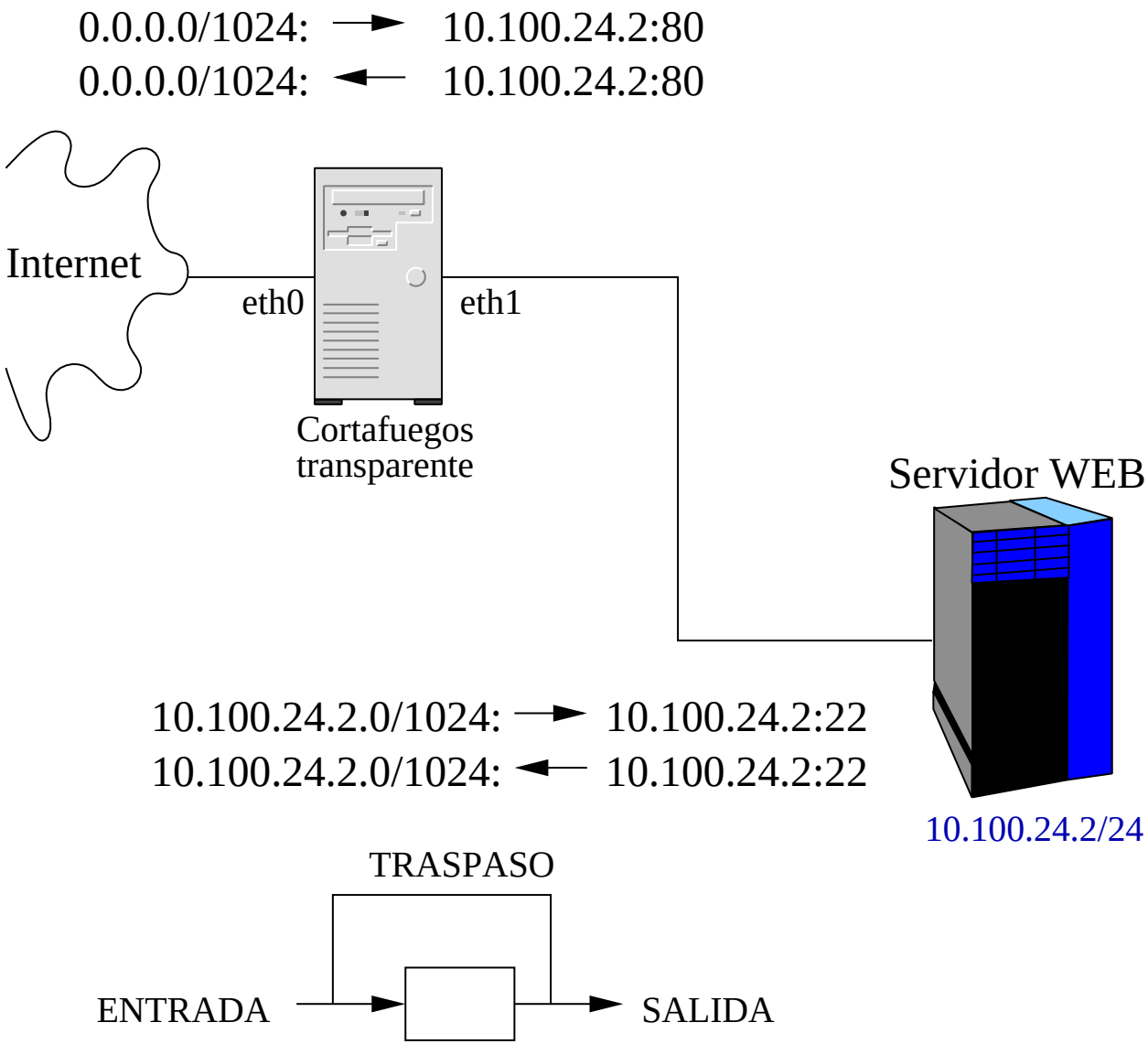
Instalación del script

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

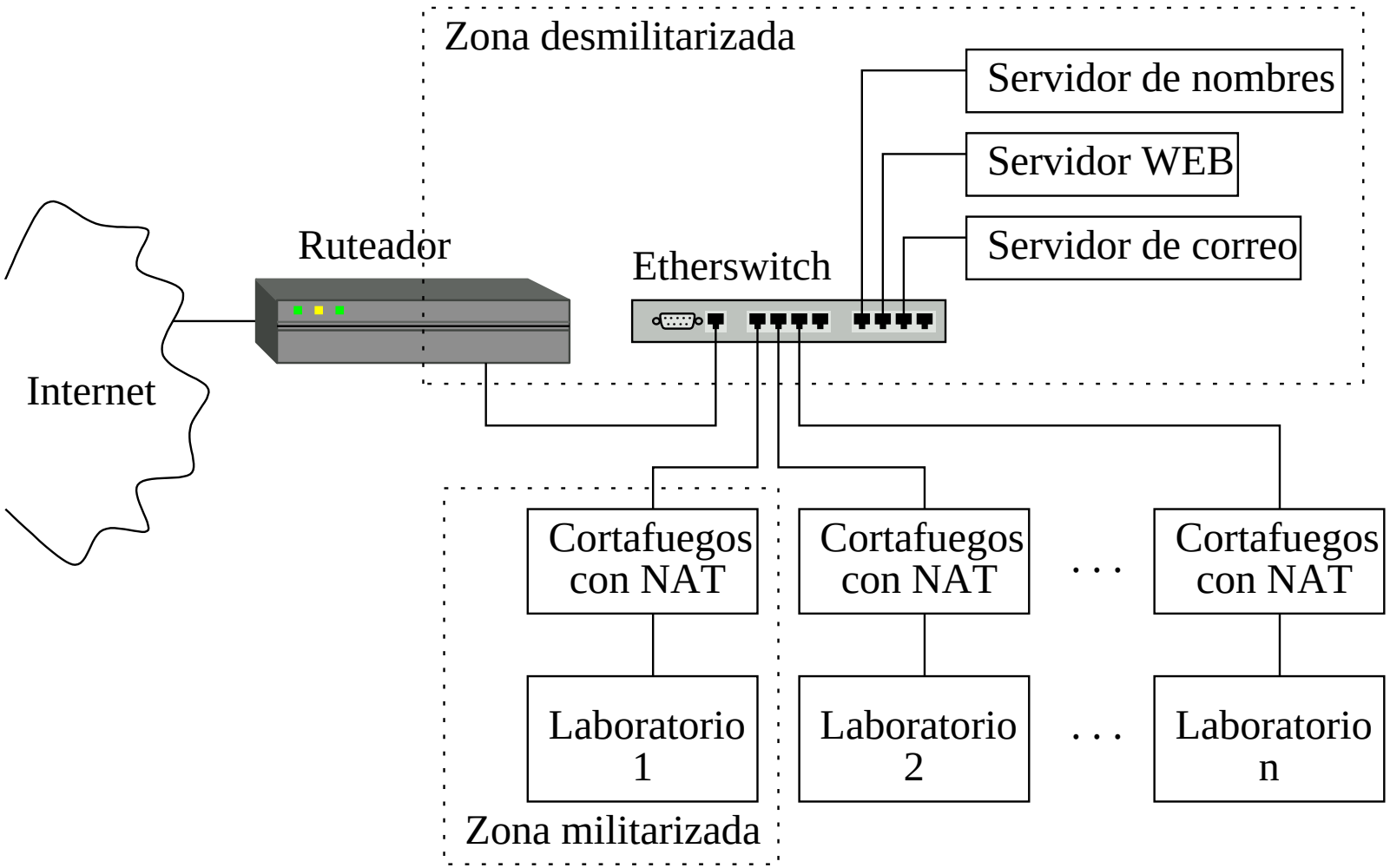
Red Desmilitarizada



Reglas en los cortafuegos



Solución de Seguridad



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

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