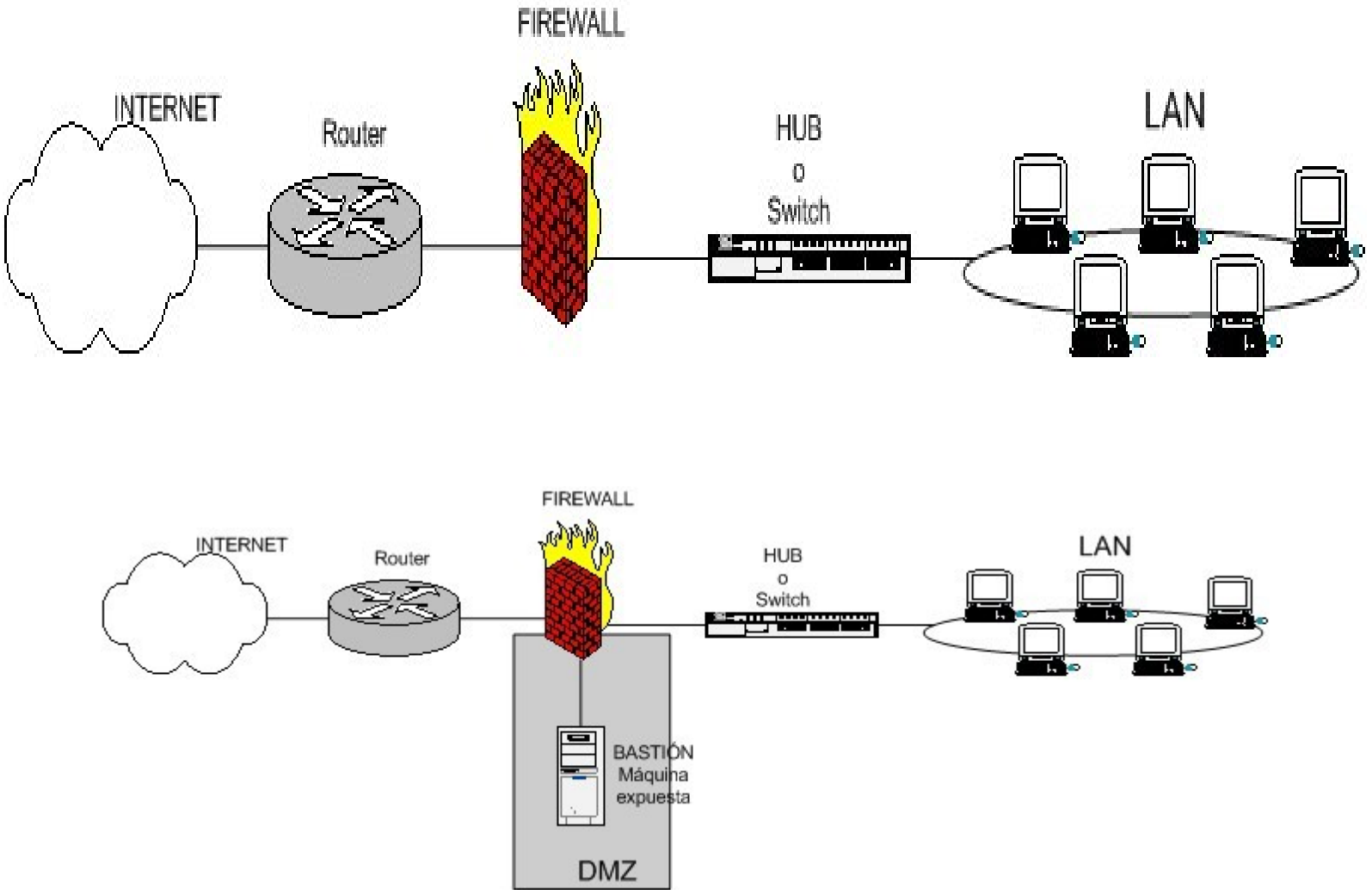
CORTAFUEGOS

Cortafuegos o firewall

- Un firewall es un **dispositivo** que filtra el tráfico entre redes, como mínimo dos.
- El firewall puede ser un **dispositivo físico** o un **software sobre un sistema operativo**.
- En general debemos verlo como una caja con DOS o mas interfaces de red en la que se establecen una **reglas de filtrado**
- Deciden si una **conexión** determinada puede establecerse o no.
- Incluso puede ir más allá y realizar **modificaciones** sobre las comunicaciones, como el NAT o DNAT.
- Decide si un paquete **pasa**, se **modifica**, se **convierte** o se **descarta**

Esquema típico



Políticas por defecto

- Hay dos maneras de implementar un firewall:

  1) Política por defecto ACEPTAR: en principio todo lo que entra y sale por el firewall se acepta y solo se denegará lo que se diga explícitamente.

  2) Política por defecto DENEGAR: todo esta denegado, y solo se permitirá pasar por el firewall aquellos que se permita explícitamente.

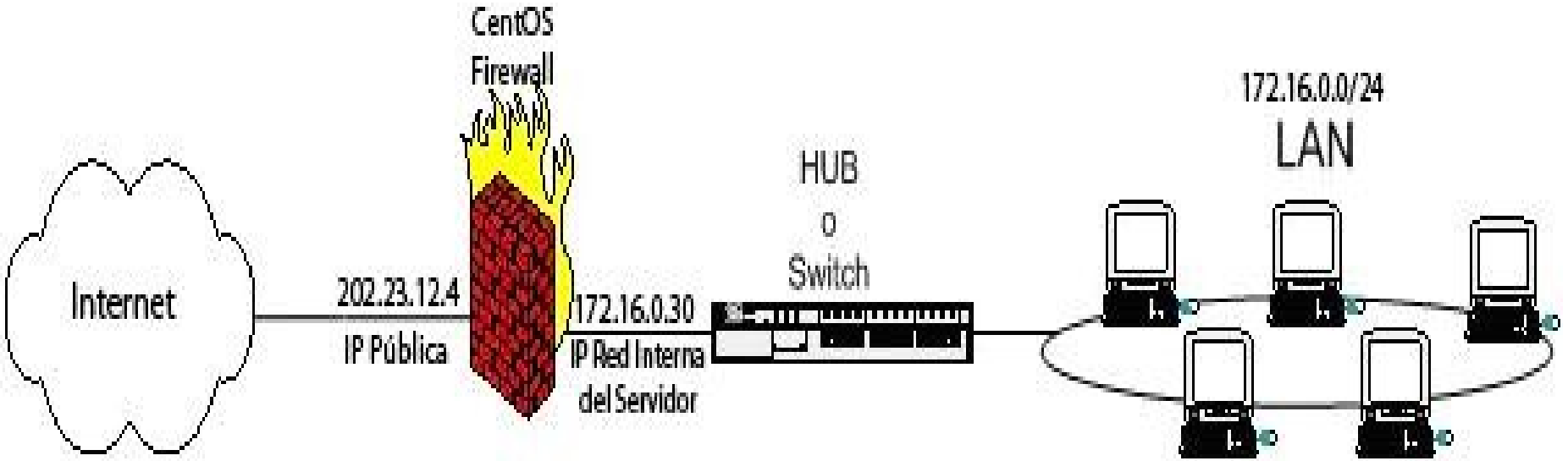
IPTABLES

- **IPtables** es un sistema de firewall **incluido en el kernel** de linux (a partir versión 2.4)
- Un firewall de iptables no es un **servicio o demonio** que iniciamos o detenemos
- iptables esta integrado con el **kernel**, es parte del sistema operativo.
- ¿Cómo se pone en marcha? Realmente lo que se hace es **aplicar reglas**. Para ello se ejecuta el **comando iptables**.
- Comandos iptables permiten **añadir, borrar, o crear reglas**.
- Por ello un firewall de iptables no es sino un simple **script** de shell en el que se van ejecutando las reglas de firewall.

Shorewall

- **Shorewall:** herramienta de alto nivel para la configuración de muros cortafuego
- Se configura en **ficheros de texto** simples y shorewall creará las reglas de cortafuegos correspondientes a través de **iptables**
- Shorewall permite utilizar un sistema como:
  - Muro cortafuegos dedicado
  - Puerta de enlace, dispositivo de encaminamiento
  - Control de Ancho de Banda
- Una vez dominado su funcionamiento permite tener un firewall muy potente y seguro para servidores en producción

Esquema de funcionamiento



NAT

- **NAT** (acrónimo de **N**etwork **A**ddress **T**ranslation o Traducción de Dirección de Red),
- También conocido como **enmascaramiento** de IP
- Técnica mediante la cual las direcciones de origen y/o destino de paquetes IP son **reescritas** mientras pasan a través de un dispositivo de encaminamiento (router) o muro cortafuegos.
- El **NAT** es un sistema que se utiliza para asignar una red completa (o varias redes) a **una sola dirección IP**.

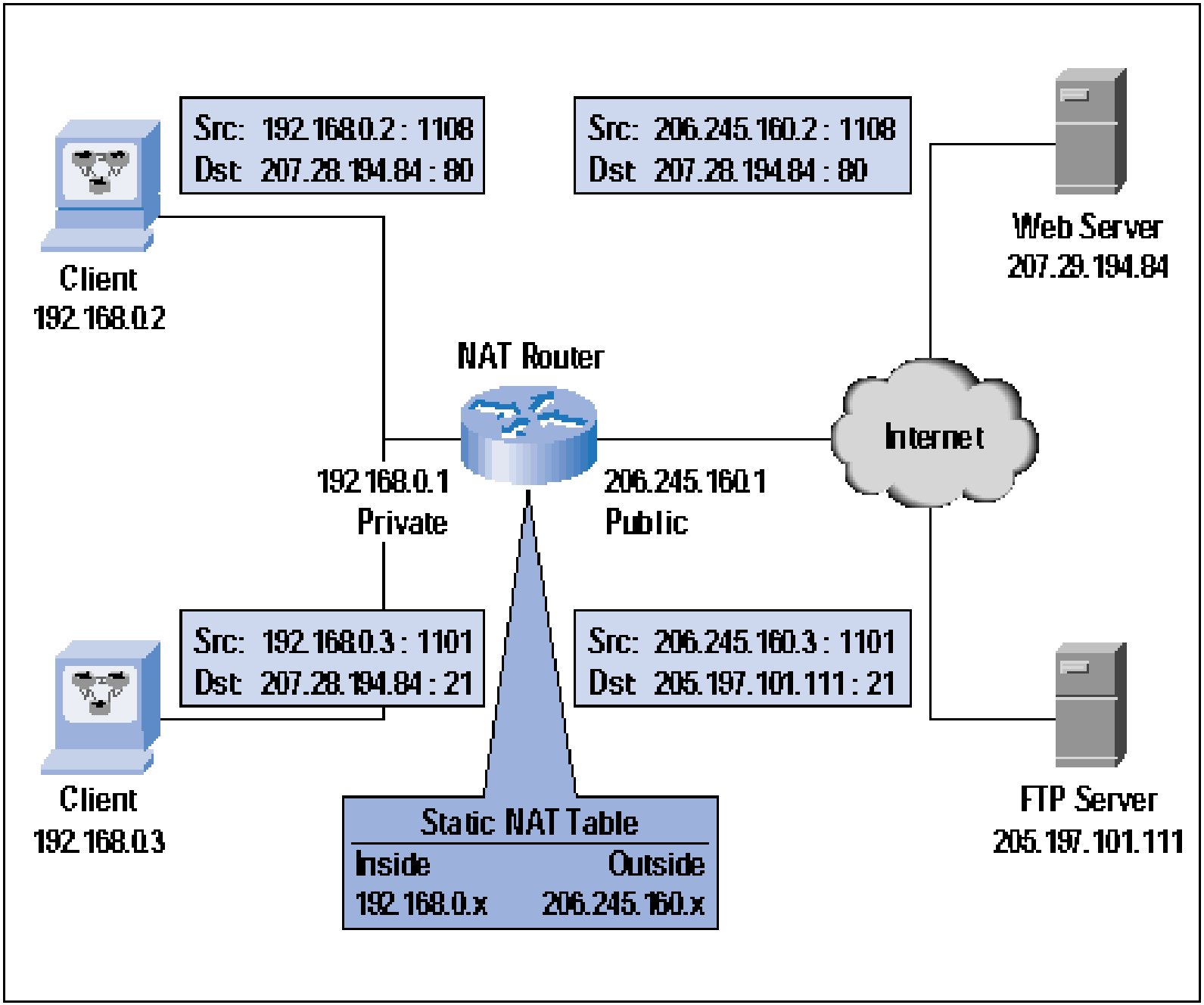
Funcionamiento NAT

- Cliente en la red interna contacta con máquina en Internet, envía paquetes IP a esa máquina.
- Estos paquetes contienen toda la información de direccionamiento necesaria para que puedan ser llevados a su destino.
- Dirección IP de origen (por ejemplo, 192.168.1.35)
- Puerto TCP o UDP de origen (por ejemplo, 2132)
- Paquetes pasan a través de la pasarela de NAT, son modificados para que parezca que se han originado y provienen de la misma pasarela de NAT.
- Asegurarnos está activado /etc/shorewall/shorewall.conf
  IP_FORWARDING=On

Funcionamiento NAT

- Pasarela NAT registra los cambios que realiza en su tabla de estado, para así poder:
  - **Invertir** los cambios en los paquetes devueltos, y
  - Asegurarse de que paquetes devueltos pasen a través cortafuegos y no sean bloqueados. Por ejemplo, podrían ocurrir los siguientes cambios:
    - IP de origen: sustituida con la dirección externa (por ejemplo, 24.5.0.5)
    - Puerto de origen: sustituido por puerto aleatorio no en uso de la pasarela,(por ejemplo, 2945)
- Proceso transparente para red interne y para servidor externo:
  - Para máquina interna, el sistema NAT es simplemente una pasarela a Internet.
  - Para el anfitrión de Internet, los paquetes parecen venir directamente del sistema NAT; ni siquiera se da cuenta de que existe la estación interna.

Funcionamiento NAT



DNAT

- **DNAT** son las siglas de **D**estination **N**etwork **A**ddress **T**ranslation o Traducción de dirección de red de destino
- DNAT permite redirigir puertos hacia máquinas que se encuentran en una red interna o Red Privada.

Ficheros de configuración de Shorewall

- Ficheros de configuración en el directorio

  `/etc/shorewall`

- Por defecto desactivado. Se activa en `/etc/default/shorewall`
- Plantillas con ficheros de configuración en

  `/usr/share/doc/shorewall-common/examples/`**`two-interfaces`**
- Los copiamos a /etc/shorewall y partimos de ellos
- los ficheros que vamos a configurar a continuación son: **zones, interfaces, policy, rules, routestopped**

Fichero `zones`

- Define las zonas que se administraran desde el firewall. La zona **fw** está predefinida, asociada al propio cortafuegos.
- **net** Normalmente asociado a la zona de Internet
- **loc** Asociado a la red local
- Las reglas para definir el tráfico a permitir o denegar se hacen en base a zonas

```
###############################
#ZONE    TYPE      OPTIONS
#
fw      firewall
net     ipv4
loc     ipv4
```

Fichero interfaces

- Permite asignar zonas a interfaces de red
- Permite, además, establecer opciones de filtrado para dichas zonas

```
###############################################################################
#ZONE   INTERFACE       BROADCAST       OPTIONS
net     eth0            detect          dhcp,tcpflags,routefilter,nosmurfs,logmartians
loc     eth1            detect          tcpflags,nosmurfs
#LAST LINE -- ADD YOUR ENTRIES BEFORE THIS ONE -- DO NOT REMOVE
```

Fichero policy

- Permite establecer las politicas por defecto de una zona a otra
- Las reglas se establecen en función de zonas

```
# If you want to force clients to access the Internet via a proxy server
# on your firewall, change the loc to net policy to REJECT info.
loc             net             ACCEPT
loc             $FW             REJECT          info
loc             all             REJECT          info

net             $FW             DROP            info
net             loc             DROP            info
net             all             DROP            info

# THE FOLLOWING POLICY MUST BE LAST
all             all             REJECT          info
```

Fichero rules

```
###############################################################################
#ACTION         SOURCE          DEST            PROTO   DEST    SOURCE          O
#                                                       PORT    PORT(S)         D
#
#       Accept DNS connections from the firewall to the network
#
DNS/ACCEPT      $FW             net
#
#       Accept SSH connections from the local network for administration
#
SSH/ACCEPT      loc             $FW
#
#       Allow Ping from the local network
#
Ping/ACCEPT     loc             $FW

#
# Drop Ping from the "bad" net zone.. and prevent your log from being flooded..
#

Ping/DROP       net             $FW

ACCEPT          $FW             loc             icmp
ACCEPT          $FW             net             icmp
#
```

Ejemplos reglas(I)

- Accept SMTP requests from the LOC to the internet

```
#ACTION SOURCE  DEST PROTO     DEST    SOURCE  ORIGINAL
#                                PORT    PORT(S)  DEST
 ACCEPT  loc           net     tcp          smtp
```

- Forward all ssh and http connection requests from the internet to local system 192.168.1.3

```
#ACTION SOURCE  DEST          PROTO   DEST    SOURCE  ORIGINAL
#                                      PORT    PORT(S) DEST
DNAT    net     loc:192.168.1.3 tcp     ssh,http
```

- Forward all http connection requests from the internet to local system 192.168.1.3 with a limit of 3 per second and a maximum burst of 10

```
#ACTION SOURCE DEST          PROTO  DEST    SOURCE  ORIGINAL RATE
#                            PORT   PORT(S) DEST             LIMIT
DNAT      net      loc:192.168.1.3 tcp      http      -         -        3/sec:10
```

Ejemplos de reglas(II)

- Redirect all locally-originating www connection requests to port 3128 on the firewall (Squid running on the firewall system) except when the destination address is 192.168.2.2

```
#ACTION  SOURCE DEST     PROTO   DEST   SOURCE  ORIGINAL
#                                PORT   PORT(S) DEST
REDIRECT loc        3128     tcp     www    -       !192.168.2.2
```

- All http requests from the internet to address 130.252.100.69 are to be forwarded to 192.168.1.3

```
#ACTION  SOURCE DEST          PROTO   DEST   SOURCE  ORIGINAL
#                                     PORT   PORT(S) DEST
DNAT     net        loc:192.168.1.3 tcp     80     -       130.252.100.69
```

- You want to accept SSH connections to your firewall only from internet IP addresses 130.252.100.69 and 130.252.100.70

```
#ACTION  SOURCE DEST          PROTO   DEST   SOURCE  ORIGINAL
#                                     PORT   PORT(S)  DEST
ACCEPT   net:130.252.100.69,130.252.100.70 $FW \
                                      tcp    22
```

Ejemplos de reglas (III)

- You wish to accept connections from the internet to your firewall on port 2222 and you want to forward them to local system 192.168.1.3, port 22

```
#ACTION  SOURCE DEST              PROTO   DEST    SOURCE  ORIGINAL
#                                         PORT    PORT(S)  DEST
DNAT     net     loc:192.168.1.3:22  tcp   2222
```

- You want to redirect connection requests to port 80 randomly to the port range 81-90.

```
#ACTION  SOURCE DEST              PROTO DEST    SOURCE  ORIGINAL
#                                         PORT    PORT(S) DEST
REDIRECT net    $FW::81-90:random tcp     www
```

Fichero routestopped

- Establece el comportamiento del cortafuegos cuando este está detenido
- INTERFACE - interface
  - Iinterfaz a mediante la quelos equipos se comunican con cortafuegos.
- HOST(S) (Optional) - [-|address[,address]...]
  - Lista separada por comas de direcciones IP/subred
  - Si se deja en blanco o se incluye un “-” se supones 0.0.0.0/0

```
##############################################################
#INTERFACE      HOST(S)                    OPTIONS
eth1           -
#LAST LINE -- ADD YOUR ENTRIES BEFORE THIS ONE -- DO NOT REMOVE
```