Università di Padova

Servizio Formazione

Incontro a tema

realizzazione di un filtering bridge (firewall trasparente)

Alberto Cammozzo

Cosa faremo

1) Ripasso elementi teoria

   routing e bridging, 3-way handshake TCP, firewall

2) HW e setup bridge + firewall

   kernel Linux 2.6, tools

   `http://foss.stat.unipd.it/mediawiki/index.php/Filtering_bridge`

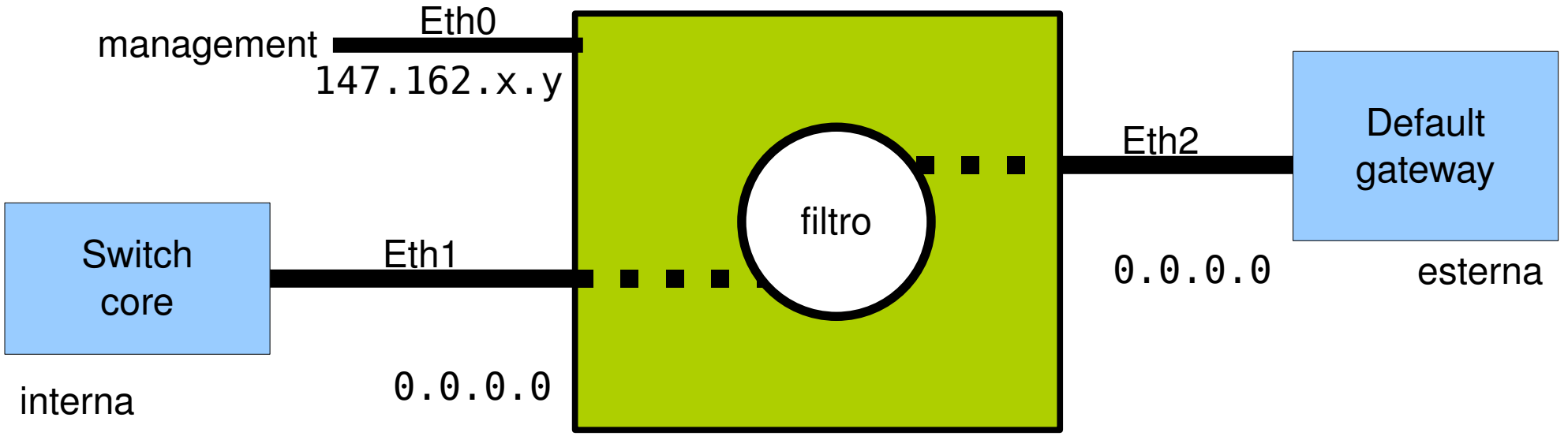
3) Rilevazione traffico

   tcpdump

4) Prove sul campo, approfondimenti

Filtering bridge

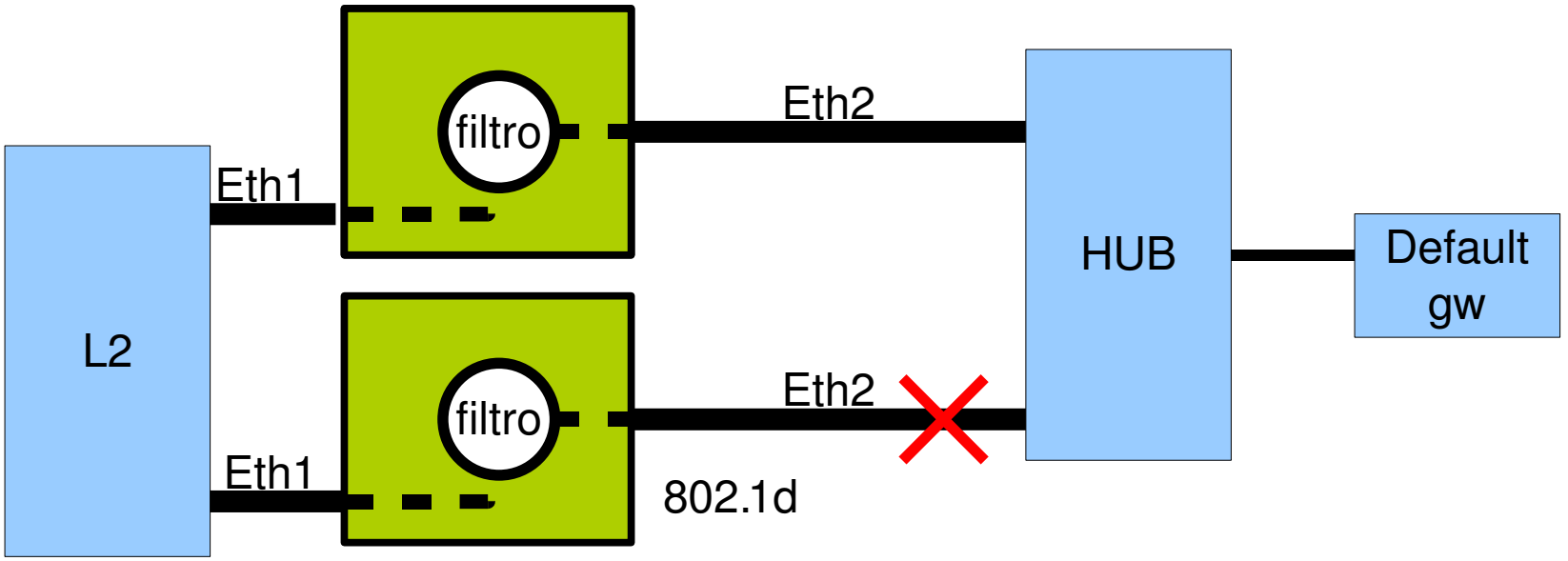
- 1 pc con 3 interfacce
  - Interna (senza ip)
  - Esterna (senza ip)
  - Management (con ip)



Perche' un filtering bridge?

Nessun intervento sulla rete

- Trasparente (stesso default gateway) anche in presenza di vlan
- Ruleset semplice (interfaccia In/Out + indirizzi)
- Fault tolerance con spanning tree (802.1d)



Bridging vs Routing

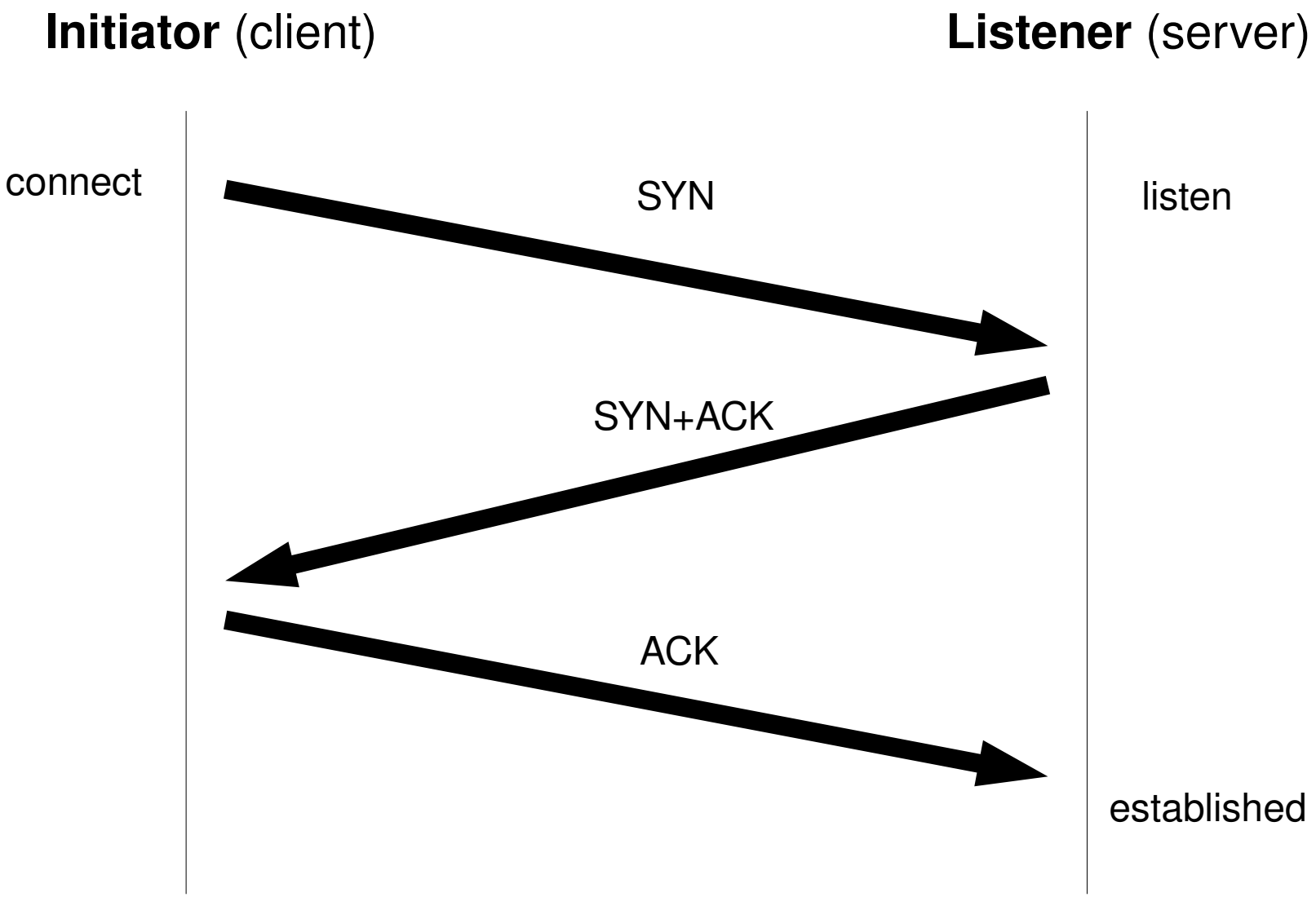
Bridge (switch L2)

- Livello 2 ISO/OSI
- Indirizzo MAC (00:19:BB:D4:9A:2B)
- Bridging: inoltro pacchetti nello stesso segmento LAN
- Address resolution protocol (ARP)
- Spanning tree (802.1D)

Router (switch L3)

- Livello 3 ISO/OSI
- Indirizzo IP (147.162.35.208)
- Routing: inoltro pacchetti tra aree broadcast diverse
- Default gateway
- Vari protocolli di routing

3-way handshake TCP



Firewall (in *teoria*)

I. **Packet filtering**
   - **Criteri**: conosce src/dst addr, src/dst port, src/dst interface, protocol, ...
   - **Pro**: veloce **Contro**: spoofing, IP stack attack, active ftp, user?

II. **Circuit level**
   - **Criteri**: conosce stato della connessione
   - **Pro**: established, new, invalid. NAT. **Contro**: exploiting di applicazioni

III. **Application gateway**
   - **Criteri**: proxy, non router. Conosce il contenuto della transazione (http, telnet, ...)
   - **Pro:** user! **Contro**: application-specific

Bridging su linux: documentazione

- http://ebtables.sourceforge.net/br_fw_ia/br_fw_ia.html
- https://www.linux-magazine.com/issue/50/Bridgewall_Firewalling.pdf
- http://ebtables.sourceforge.net/documentation.html
- http://www.linux-foundation.org/en/Net:Bridge
- http://bwachter.lart.info/linux/bridges.html
- http://tldp.org/HOWTO/Ethernet-Bridge-netfilter-HOWTO.html
- http://ebtables.sourceforge.net/brnf-faq.html
- Manuale:
  - man brctl
  - man ip
  - man iptables
  - man ebtables

Kernel e tools

- Linux 2.6 (include il codice *br-nf*)
- iptables (filtering livello IP) con modulo `physdev`
- ebtables (per eventuale filtering livello ethernet)
- iproute tools (il comando ip)
- bridge-utils (comando brctl)
- tcpdump (per l'analisi)

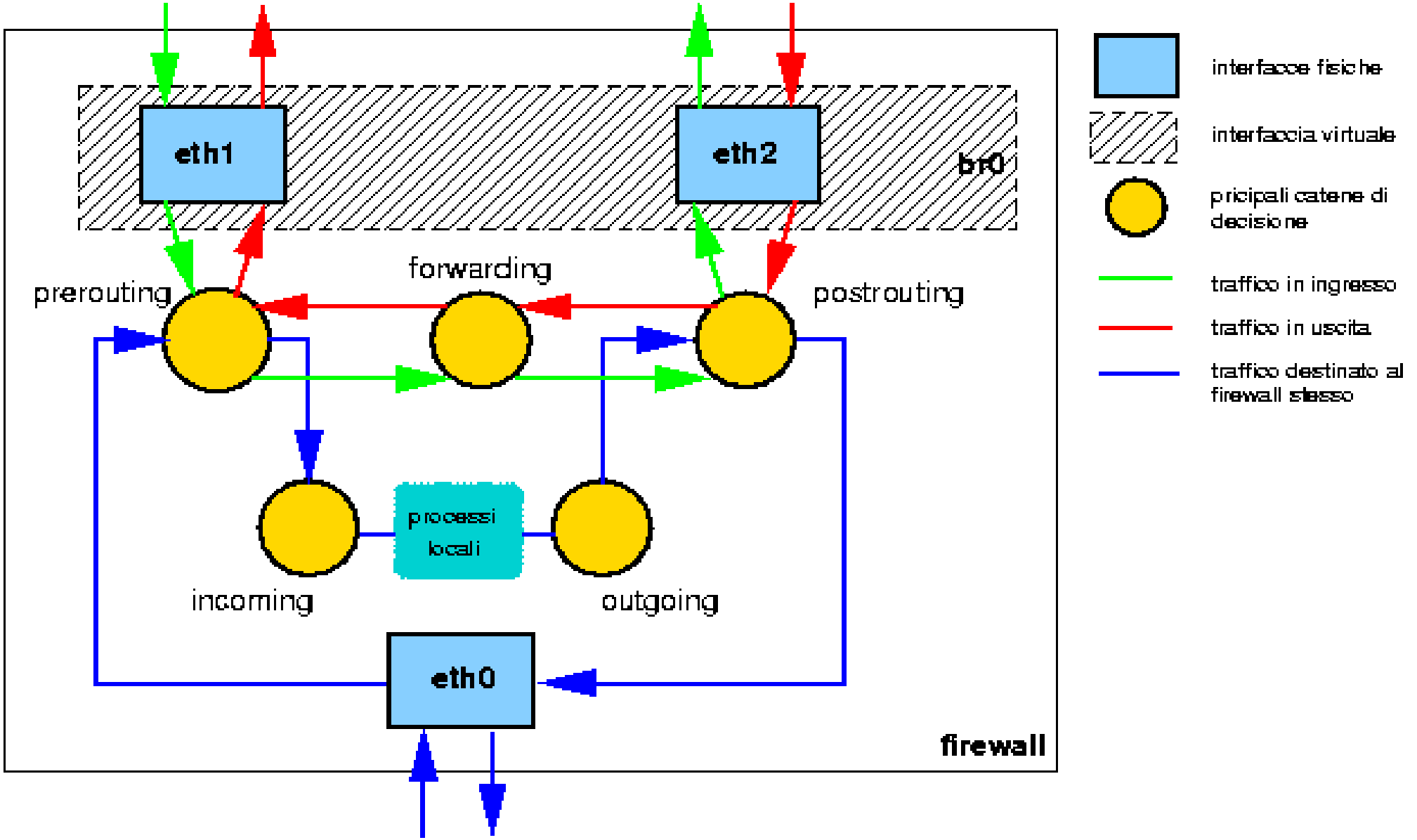
X debian:

```
apt-get install iptables ebtables iproute bridge-utils tcpdump
```

Il Bridge

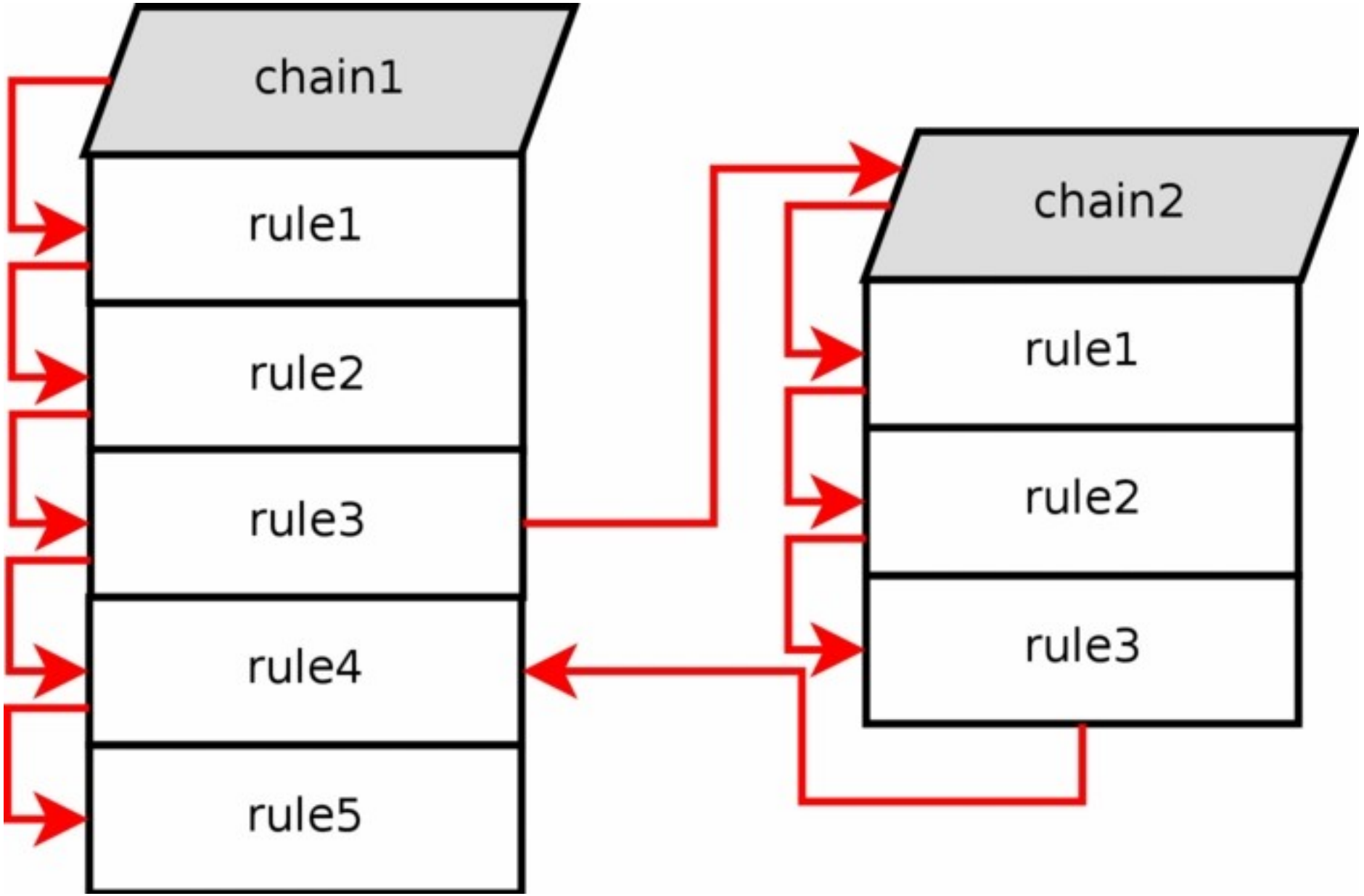
```
#alias per comodita'
ip link set dev eth1 name int
ip link set dev eth2 name ext
#costruzione del bridge
brctl addbr br0
brctl addif br0 int
brctl addif br0 ext
#nessun IP assegnato
ifconfig int 0 0.0.0.0
ifconfig ext 0 0.0.0.0
```

Struttura


eth1
eth2
br0
prerouting
forwarding
postrouting
processi locali
incoming
outgoing
eth0
firewall
interfacce fisiche
interfaccia virtuale
pricipali catene di decisione
traffico in ingresso
traffico in uscita
traffico destinato al firewall stesso

IPTABLES: chains

- Chain INPUT e OUTPUT
  - Riguardano i pacchetti destinati alle interfacce presenti sul PC (in ingresso ed uscita)
- Chain FORWARDING
  - Riguarda i pacchetti in transito
- Altre chain:
  - PREROUTING, POSTROUTING
- Chain definite dall'utente



Source: http://iptables-tutorial.frozentux.net/iptables-tutorial.html#TRAVERSINGOFTABLES

IPTABLES: tables

- Tabella filter (default)
  - INPUT, OUTPUT, FORWARD
- Tabella nat
  - PREROUTING, OUTPUT, POSTROUTING
- Tabella mangle
  - Manipolazione dei pacchetti
- Tabella raw

Tcpdump e analisi

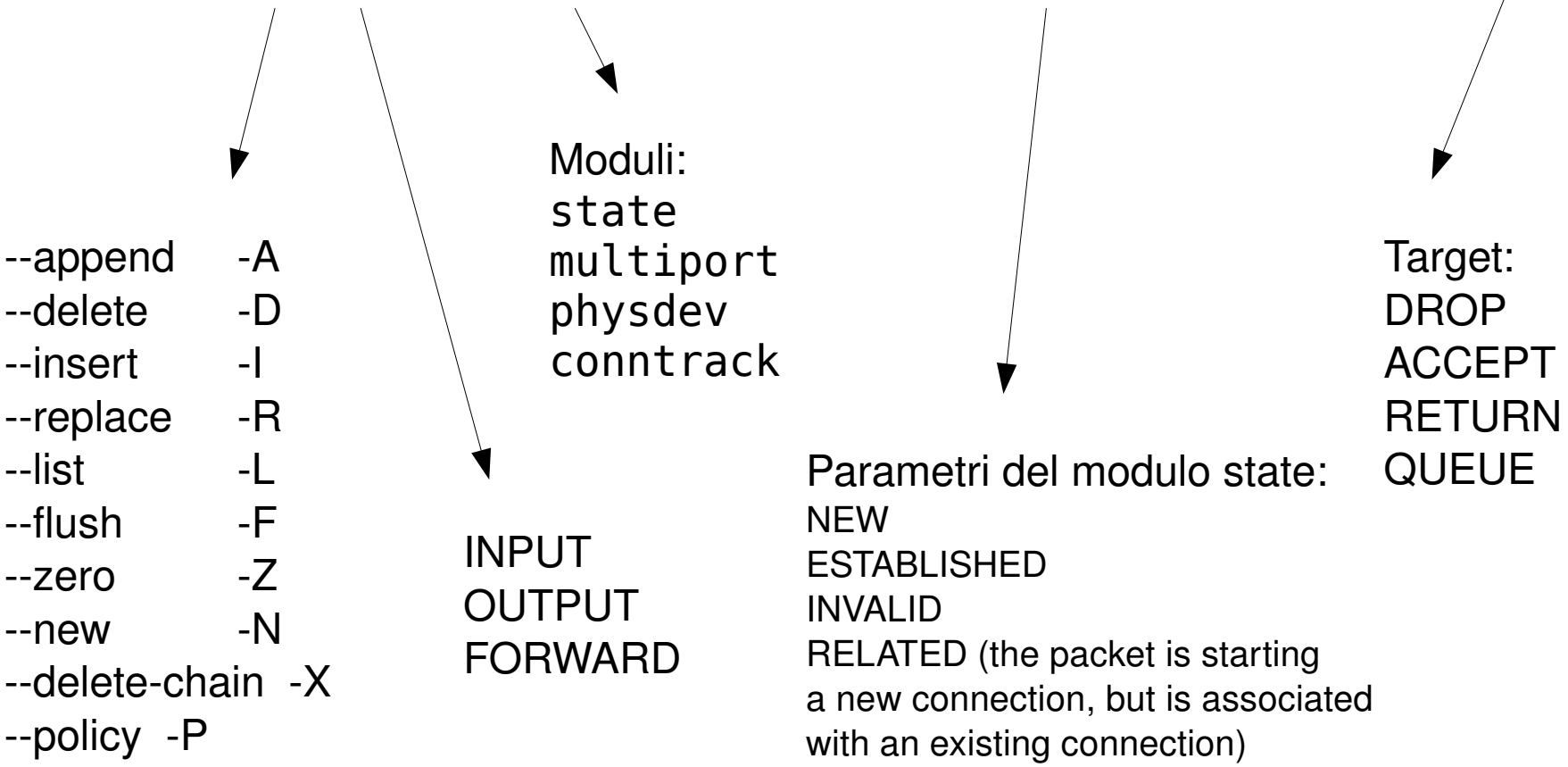
```
tcpdump -i ext -n  (
  tcp and src net 147.162/16
  and (
    dst port 80
    or dst port 443 )
  or (
    host 147.162.35.2 )


tcpdump -i ext -n -F filename
```

Iptables: sintassi

- Esempio: accetta le connessioni established

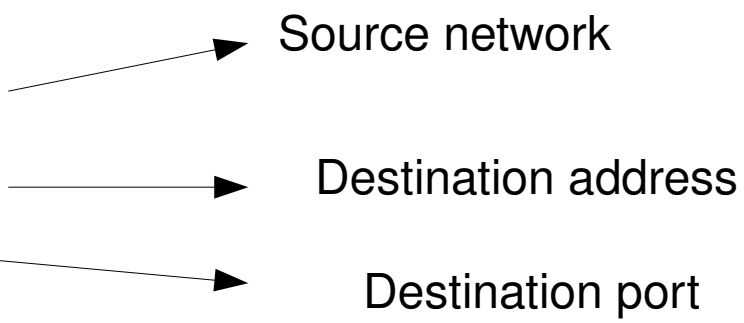
```
iptables -A INPUT -m state --state RELATED,ESTABLISHED -j ACCEPT
```



Iptables: sintassi

- Esempio: accetta le connessioni destinate al server web dall'interno dell'Ateneo

```
iptables -A FORWARD
  -p tcp
  -s 147.162.0.0/16
  -d 147/162.35.218
  --dport 80
  -j ACCEPT
```



Iptables: sintassi

- Elimina le connessioni invalide, con log

```
iptables -A FORWARD -m state --state INVALID
  -j LOG --log-prefix "DROP INVALID "
iptables -A FORWARD -m state --state INVALID
  -j DROP
```

Iptables: sintassi

- pacchetti UDP

```
iptables -A INPUT -i ext -p udp -j DROP

iptables -A FORWARD -d 147.162.35.1/32
   -p udp -m multiport --dports 53
   -i ext -j ACCEPT
```

- policy di default della chain

```
iptables -P FORWARD DROP

iptables -P FORWARD ACCEPT
```

- accetta conenssioni http in ingresso

```
iptables -A FORWARD
   -d 147.162.35.218/32 -i ext
   -p tcp -m multiport --dports 80,443
   -j ACCEPT
   --comment “accetta connessioni sul server web dall'esterno”
```

Farsi un'idea del traffico

Per non interrompere il servizio e la connettivita'

- Procedimento a imbuto:
  - Analizzare il traffico in ingresso/uscita
  - Escudere il traffico regolare --> regole ALLOW
  - Resta quello “strano” --> regole DROP/LOG
- Applicare le regole con policy ALLOW
- Applicare le regole con policy DROP

FAQ

http://www.netfilter.org/documentation/FAQ/netfilter-faq-3.html

3.13 How do I build a transparent proxy using squid and iptables?

```
iptables -t nat -A PREROUTING -p tcp --dport 80 -j DNAT --to
192.168.22.33:3128
```

The squid.conf for Squid 2.4

```
http_port 3128
httpd_accel_host virtual
httpd_accel_port 80
httpd_accel_with_proxy  on
httpd_accel_uses_host_header on
httpd_accel_single_host off
```

FAQ

http://www.netfilter.org/documentation/HOWTO

I Just want masquerading

```
# Load the NAT module (this pulls in all the others).
modprobe iptable_nat


# In the NAT table (-t nat), Append a rule (-A) after routing
# (POSTROUTING) for all packets going out ppp0 (-o ppp0) which says to
# MASQUERADE the connection (-j MASQUERADE).

iptables -t nat -A POSTROUTING -o ppp0 -j MASQUERADE


# Turn on IP forwarding
echo 1 > /proc/sys/net/ipv4/ip_forward
```