IPTABLES

- IPTABLES implementa funzionalità di stateful packet filter nei kernel Linux 2.4 e successivi
- Lavora a livello di kernel ed ha il controllo dei pacchetti IP in transito sulle interfacce di rete (loopback compreso)
- I pacchetti IP processati da IPTABLES sono soggetti a diverse modalità di elaborazione chiamate **table** (o tabelle), ciascuna delle quali è composta da gruppi di regole denominate **chain**
- IPTABLES definisce quattro tabelle principali
  - **filter** (filtraggio di pacchetti)
  - **nat** (sostituzione di indirizzi IP)
  - **mangle** (manipolazione ulteriore dei pacchetti: TOS, TTL, …)
  - **raw** (esclusione di pacchetti dal connection tracking)

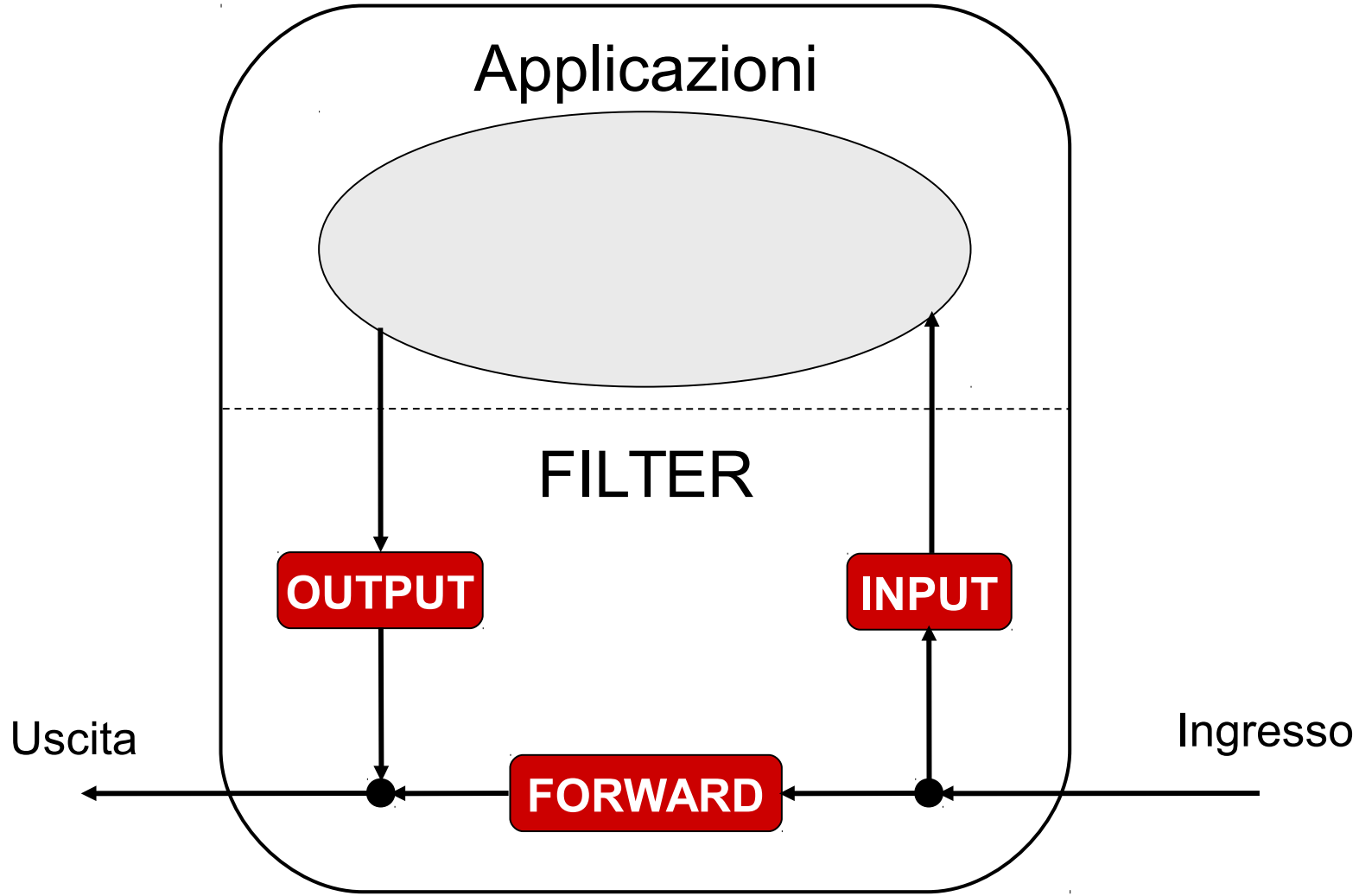
IPTABLES: la tabella FILTER

- Le funzionalità di firewall vere e proprie sono implementate dalla tabella **filter**, che si occupa di filtrare i pacchetti sulla base dell'interfaccia di provenienza e dei parametri contenuti nelle intestazioni IP e TCP

- Nella tabella filter sono presenti tre chain predefinite
  - **INPUT**: contiene le regole di filtraggio da usare sui pacchetti in arrivo al firewall (destinati all'host locale)
  - **OUTPUT**: contiene le regole da usare sui pacchetti in uscita dal firewall (originati dall'host locale)
  - **FORWARD**: contiene le regole da usare sui pacchetti in transito nel firewall (inoltrati tra interfacce diverse)

- E' possibile definire ulteriori chain

IPTABLES: chain della tabella FILTER



IPTABLES: regole della tabella FILTER

- Quando un pacchetto viene processato da una chain, esso è soggetto alle regole specificate in essa, **secondo l'ordine di inserimento**
- Una regola può stabilire se scartare (**DROP**), rifiutare esplicitamente (**REJECT**) o accettare (**ACCEPT**) un pacchetto in base a
  - interfaccia di rete coinvolta
  - indirizzo IP di origine e/o destinazione
  - protocollo (TCP, UDP, ICMP)
  - porta TCP o UDP di origine e/o destinazione
  - tipo di messaggio ICMP
  - ecc...
- Se un pacchetto non soddisfa nessuna regola, viene applicata la regola di default, o **policy**, di quella chain

IPTABLES: gestione della tabella FILTER

- Per visualizzare le regole attualmente in uso da ogni chain della tabella filter:
  iptables -L [-nv --line-num]
- Per visualizzare le regole attualmente in uso da una chain specifica:
  iptables -L <chain>
- Per impostare la policy di default di una chain:
  iptables -P <chain> <policy>
- Per aggiungere una regola in coda ad una chain:
  iptables -A <chain> <options> -j <policy>

dove: **<chain> = INPUT | OUTPUT | FORWARD | …**
<policy> = ACCEPT | DROP | REJECT | …

Nota: **REJECT** non è ammessa come policy di default

IPTABLES: gestione della tabella FILTER

- Per inserire una regola in una chain nella posizione **<N>**:
  iptables -I <chain> <N> <options> -j <policy>

- Per sostituire la regola nella posizione **<N>** di una chain:
  iptables -R <chain> <N> <options> -j <policy>

- Per eliminare la regola nella posizione **<N>** di una chain:
  iptables -D <chain> <N>

- Per eliminare (flush) tutte le regole da una specifica chain o da tutte le chain (non agisce sulla policy di default):
  iptables -F <chain>
  iptables -F

IPTABLES: opzioni per specificare le regole

- Per specificare l'interfaccia di ingresso o di uscita:
  -i <interface> **-o <interface>**

- Per specificare l'IP (host o rete) di origine o destinazione:
  -s <address>/<netmask>
  -d <address>/<netmask>

  * la netmask può essere in formato decimale puntato o CIDR

- Per specificare il protocollo:
  -p tcp | udp | icmp | ...

* l'elenco dei protocolli supportati è in **/etc/protocols**

- Per specificare la porta (TCP/UDP) di origine o destinazione:
  --sport <port> **--dport <port>**

* l'elenco delle porte con i corrispondenti servizi è in **/etc/services**

IPTABLES: opzioni per specificare le regole

- Per specificare il tipo di messaggio ICMP:
  --icmp-type <typename>
  * l'elenco dei tipi di messaggi ICMP riconosciuti da IPTABLES è visualizzabile con: **iptables -p icmp -h**

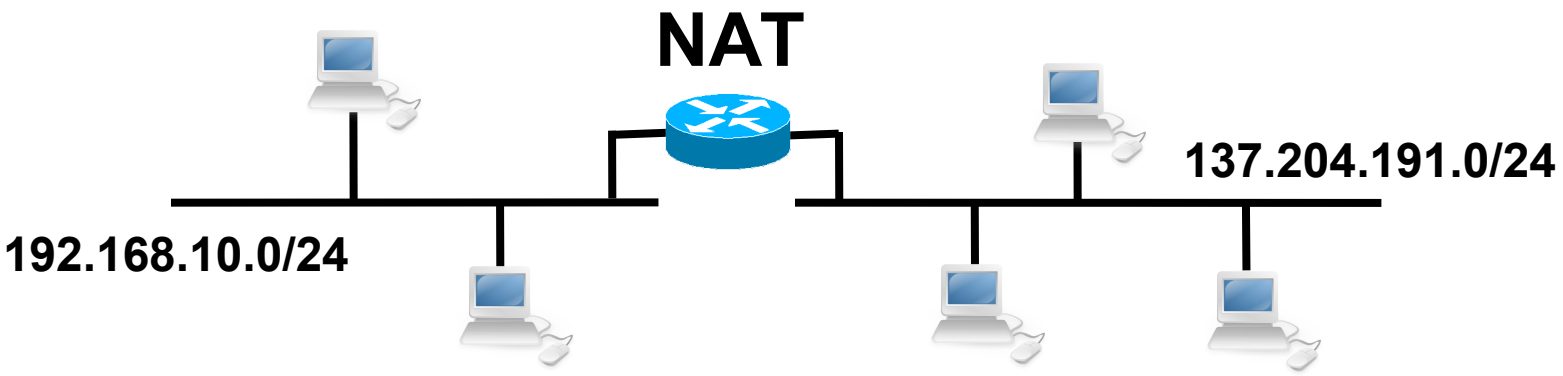
- Per specificare l'indirizzo MAC di origine:
  --mac-source <MAC_address>

- E' possibile specificare il negato di un'opzione tramite l'operatore **!**
  es. **-s ! <address>/<netmask>**

- Per specificare pacchetti di connessioni TCP o flussi UDP nuovi o già attivi (stateful packet filter):
  -m state --state NEW
  -m state --state ESTABLISHED

Network Address Translation (NAT)

- Tecnica per il filtraggio di pacchetti IP con sostituzione degli indirizzi o mascheramento
- Definito nella RFC 3022 per permettere a host appartenenti a reti IP private l'accesso a reti IP pubbliche tramite un apposito gateway
- Utile per il risparmio di indirizzi IP pubblici e il riutilizzo di indirizzi IP privati



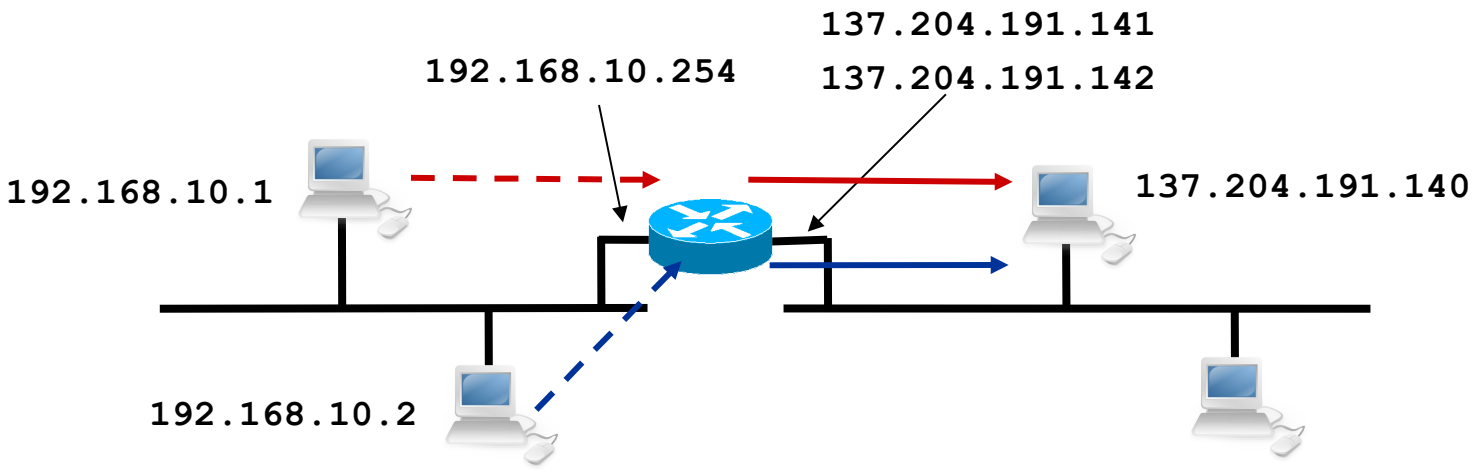
Reti IP private (RFC 1918)

- Alcuni gruppi di indirizzi sono riservati a reti IP private
- Essi non sono raggiungibili dalla rete pubblica
- I router di Internet non instradano datagrammi destinati a tali indirizzi
- Possono essere riutilizzati in reti isolate

- da **10.0.0.0** a **10.255.255.255** = **10.0.0.0/8**
- da **172.16.0.0** a **172.31.255.255** = **172.16.0.0/12**
- da **192.168.0.0** a **192.168.255.255** = **192.168.0.0/16**

Basic NAT – Conversione di indirizzo

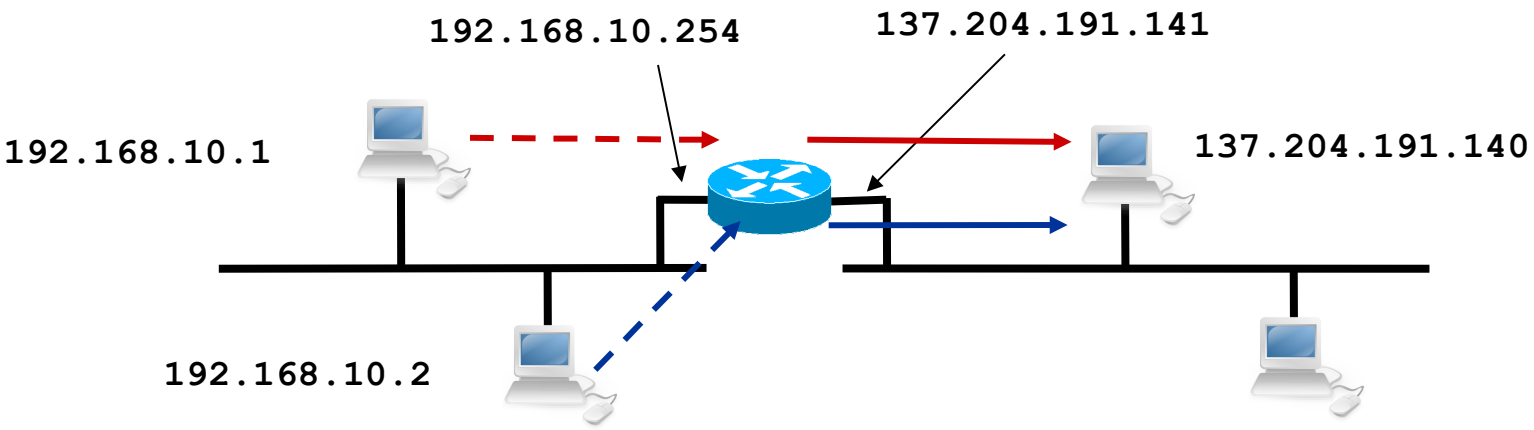
- Il NAT può fornire una semplice conversione di indirizzo IP (statica o dinamica)
- Conversioni contemporanee limitate dal numero di indirizzi IP pubblici a disposizione del gateway NAT



192.168.10.1	--->	137.204.191.140
137.204.191.141	--->	137.204.191.140
192.168.10.2	--->	137.204.191.140
137.204.191.142	--->	137.204.191.140

NAPT – Conversione di indirizzo e porta

- Il NAT può fornire anche conversione di indirizzo IP e porta TCP o UDP (anche noto come PAT)
- Conversioni contemporanee possibili anche con un unico indirizzo IP pubblico del gateway NAT



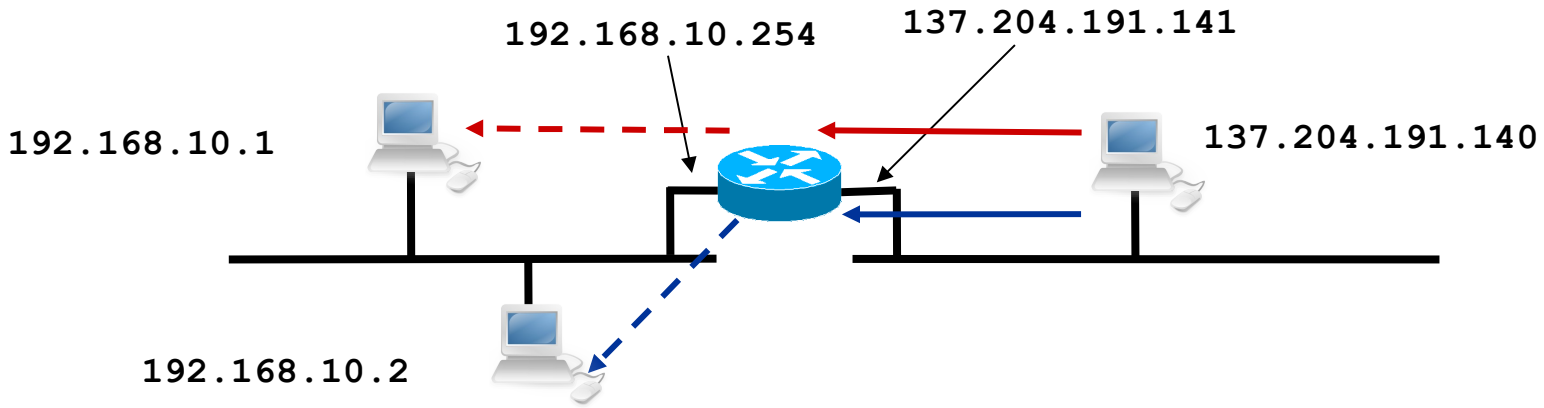
192.168.10.1:3123	⇢	137.204.191.140:80
137.204.191.141:3123	→	137.204.191.140:80
192.168.10.2:3123	⇢	137.204.191.140:80
137.204.191.141:4135	→	137.204.191.140:80

Direzione delle connessioni

- Il NAT si applica generalmente da rete privata verso rete pubblica (**Outbound NAT**)
  - tiene memoria delle connessioni e/o dei flussi di traffico che lo attraversano (stateful)
  - registra le traduzioni in corso in una cache
    - traduzioni con tempo di vita limitato
  - si preoccupa di effettuare la conversione inversa quando arrivano pacchetti in direzione opposta

Direzione delle connessioni

- E' anche possibile contattare dalla rete pubblica un host sulla rete privata (**Bi-directional NAT**)
  - bisogna configurare esplicitamente il NAT (**Port Forwarding**)
  - bisogna utilizzare porte diverse se gli indirizzi sono limitati

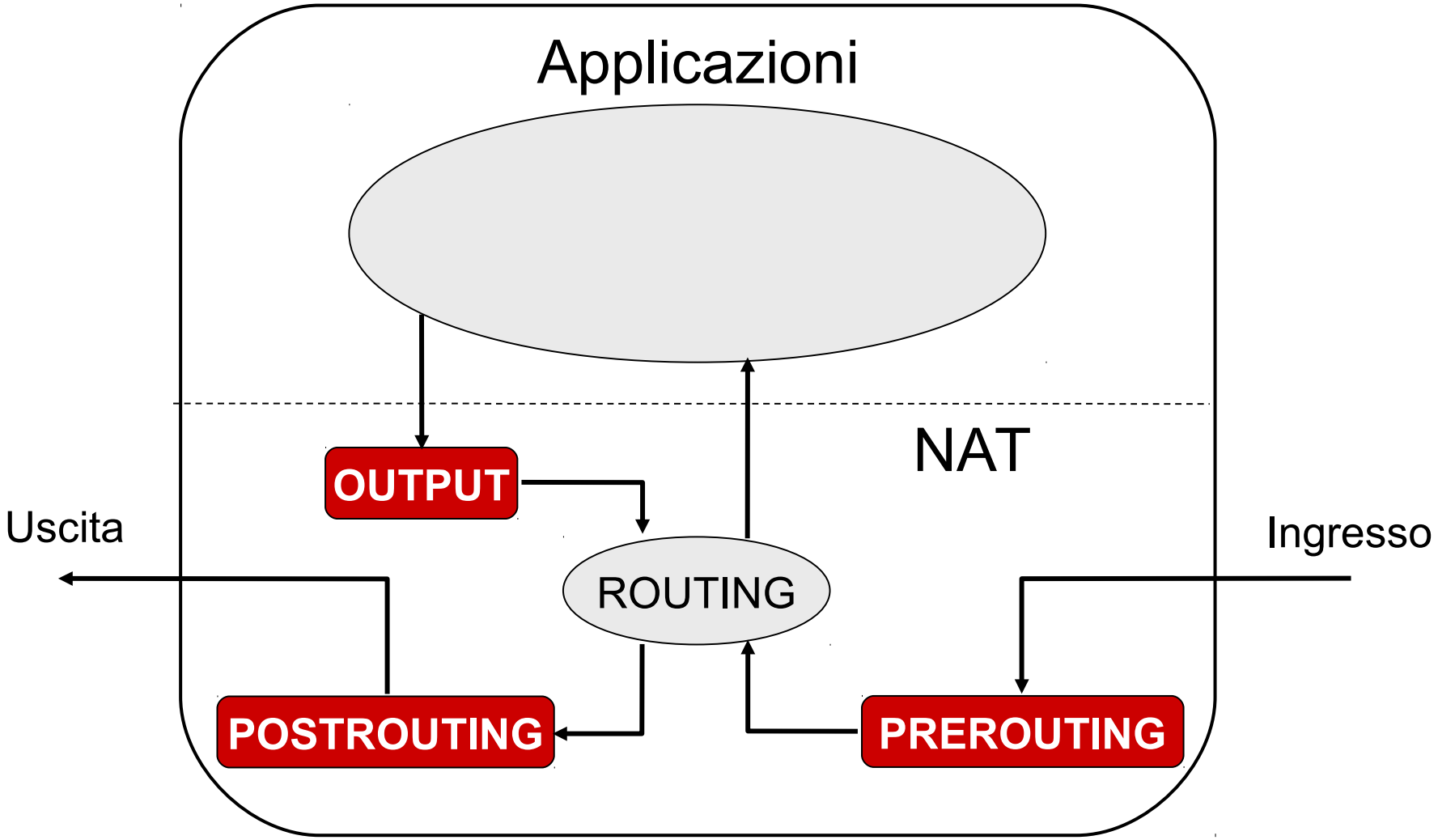


137.204.191.141:80	←	137.204.191.140:4014
192.168.10.1:80	←	137.204.191.140:4014
137.204.191.141:8080	←	137.204.191.140:4015
192.168.10.2:80	←	137.204.191.140:4015

IPTABLES: la tabella NAT

- Le funzionalità di NAT sono implementate da IPTABLES tramite la tabella **nat**
- Nella tabella nat sono presenti tre chain predefinite
  - **PREROUTING**: contiene le regole da usare prima dell'instradamento per sostituire l'indirizzo di destinazione dei pacchetti (policy = Destination NAT o **DNAT**)
  - **POSTROUTING**: contiene le regole da usare dopo l'instradamento per sostituire l'indirizzo di origine dei pacchetti (policy = Source NAT o **SNAT**)
  - **OUTPUT**: contiene le regole da usare per sostituire l'indirizzo di destinazione dei pacchetti generati localmente (policy = **DNAT**)
- La policy **ACCEPT** vuol dire assenza di conversione
- La policy **MASQUERADE** vuol dire conversione implicita nell'indirizzo IP assegnato all'interfaccia di uscita

IPTABLES: chain della tabella NAT

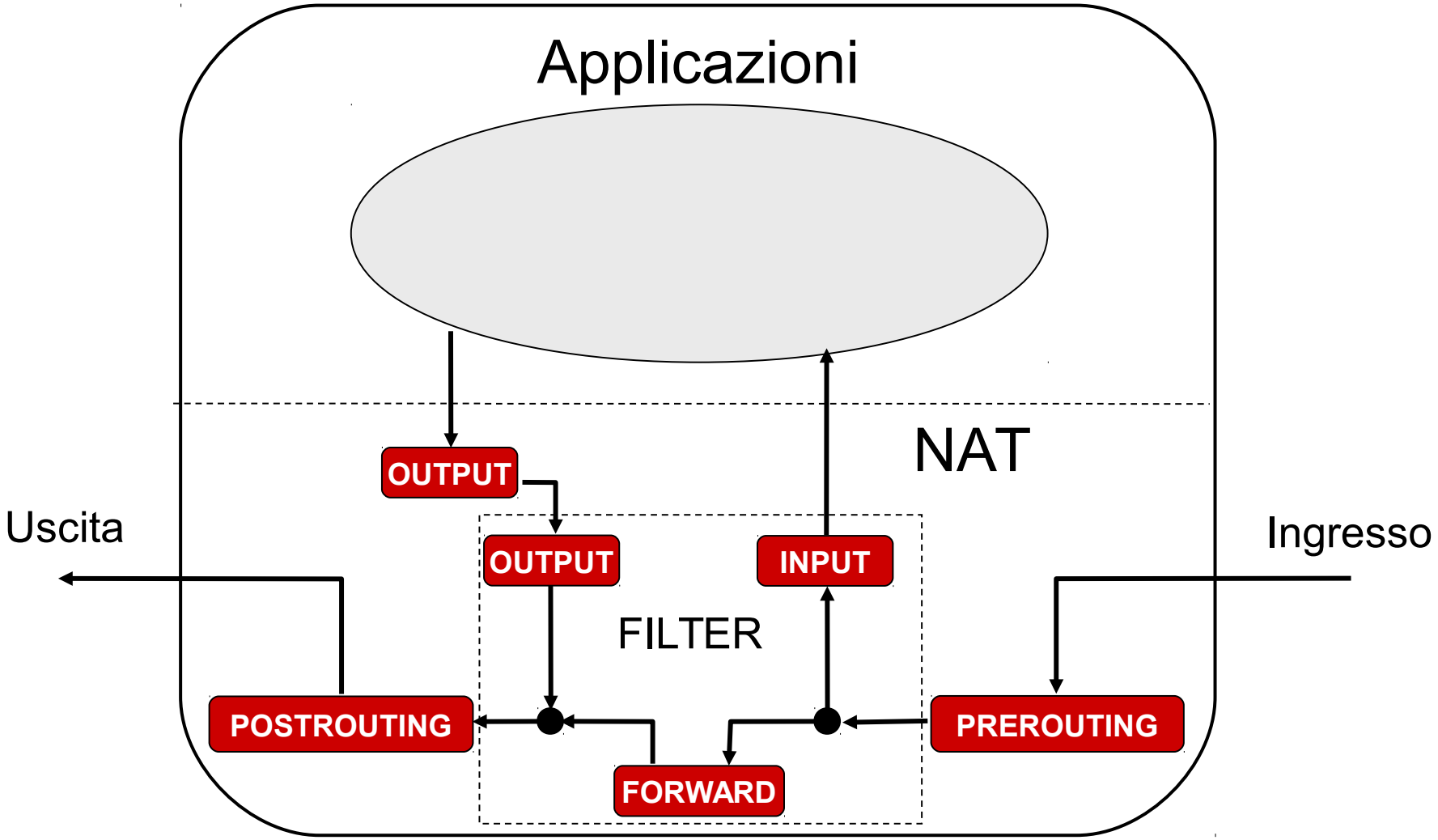


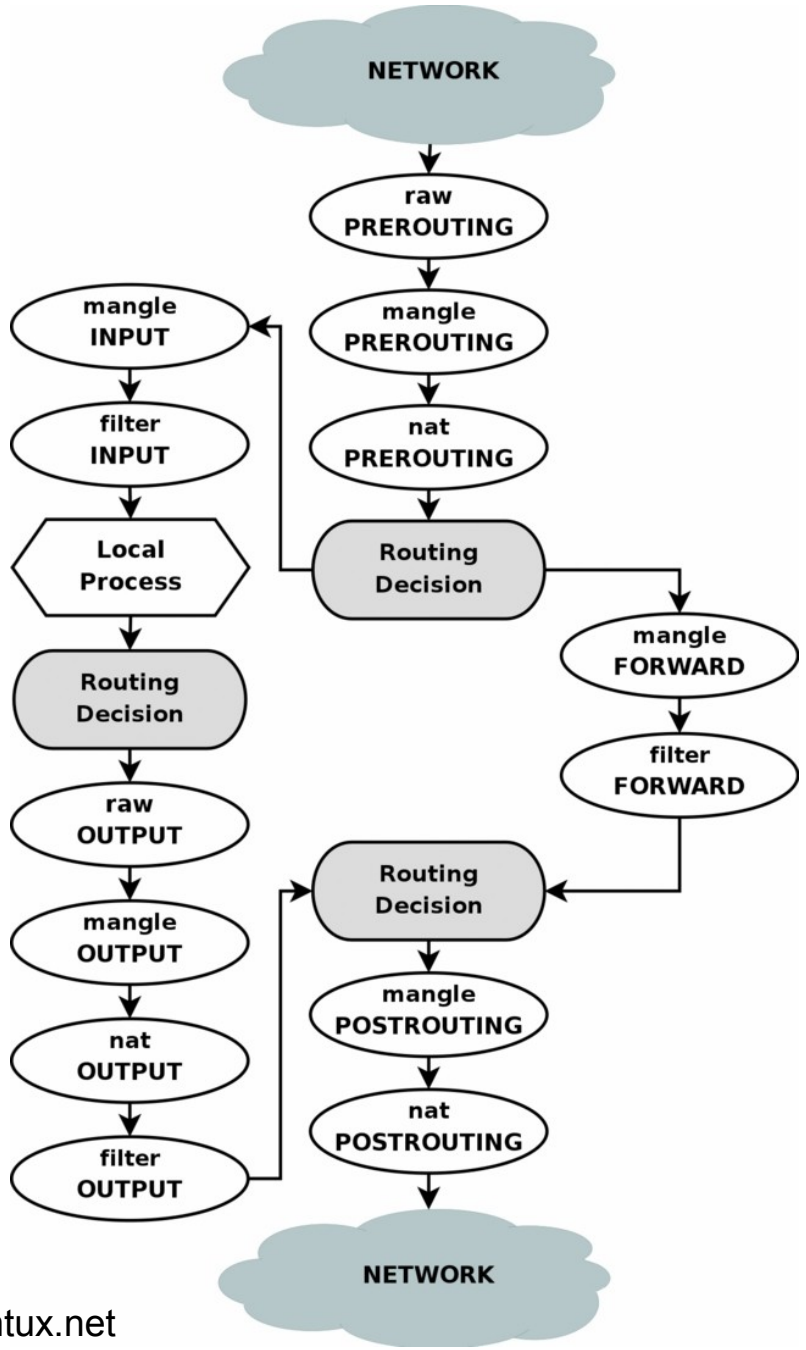
IPTABLES: gestione della tabella NAT

- Per visualizzare le regole attualmente in uso da ogni chain della tabella nat:
  iptables -t nat -L [-nv --line-num]
- Per visualizzare le regole attualmente in uso da una chain specifica:
  iptables -t nat -L <chain>
- Per aggiungere una regola in coda ad una chain:
  iptables -t nat -A <chain> <options> -j <policy>

dove:
<chain> = **POSTROUTING** | **PREROUTING** | **OUTPUT** | …
<policy> = **ACCEPT** | **MASQUERADE** |
SNAT --to-source <addr> |
DNAT --to-destination <addr>
<addr> = **<address>** | **<address>:<port>**
<options> = come per la tabella filter

IPTABLES: FILTER + NAT





da http://iptables-tutorial.frozentux.net