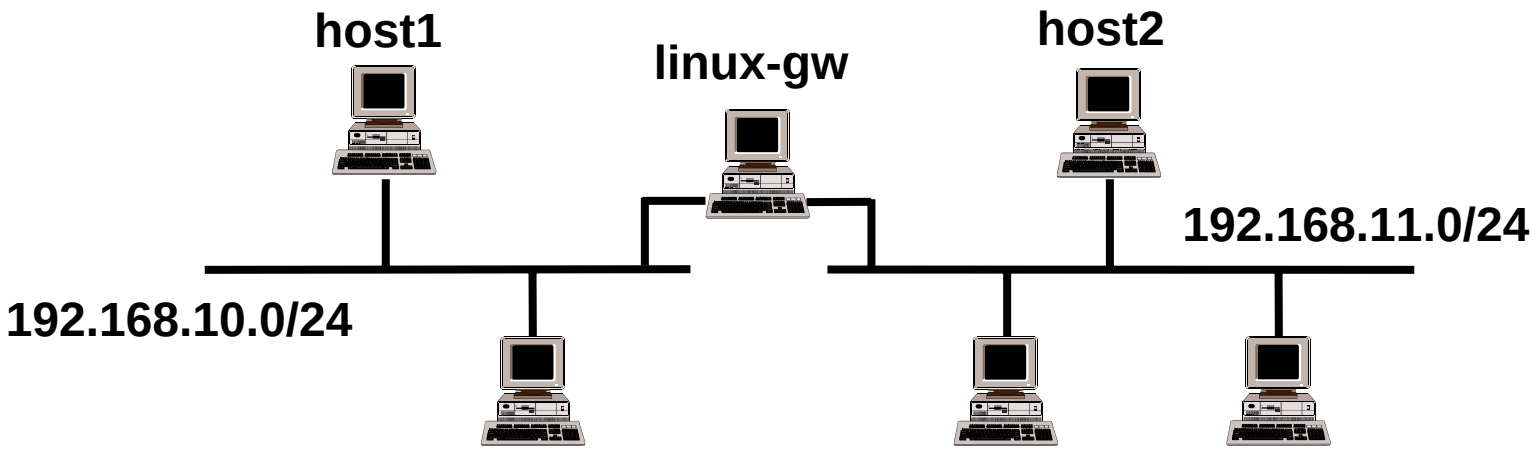
IP forwarding
Firewall e NAT

A.A. 2004/2005

Walter Cerroni

IP forwarding

Linux può funzionare da gateway tra due o più reti IP



Il kernel deve essere abilitato all'IP forwarding:

- verifica: **sysctl net.ipv4.ip_forward**
  oppure: **cat /proc/sys/net/ipv4/ip_forward**
  - restituisce **1** se abilitato, **0** altrimenti

- abilitazione: **sysctl –w net.ipv4.ip_forward=1**
  oppure: **echo 1 > /proc/sys/net/ipv4/ip_forward**

- disabilitazione: **sysctl –w net.ipv4.ip_forward=0**
  oppure: **echo 0 > /proc/sys/net/ipv4/ip_forward**

IP forwarding con aliasing

- Il forwarding è possibile anche tramite aliasing
  - bisogna però gestire i messaggi ICMP di tipo **redirect**
    - **host1** può consegnare direttamente a **host2** (1 hop) invece di passare attraverso **host3** (2 hop) → redirect
  - è possibile impostare l'invio dei redirect
    - verifica: **sysctl net.ipv4.conf.eth0.send_redirects**
      cat /proc/sys/net/ipv4/conf/eth0/send_redirects
    - abilitazione/disabilitazione:
      sysctl –w net.ipv4.conf.eth0.send_redirects=[1 | 0]
      echo [1 | 0] > /proc/sys/net/ipv4/conf/eth0/send_redirects

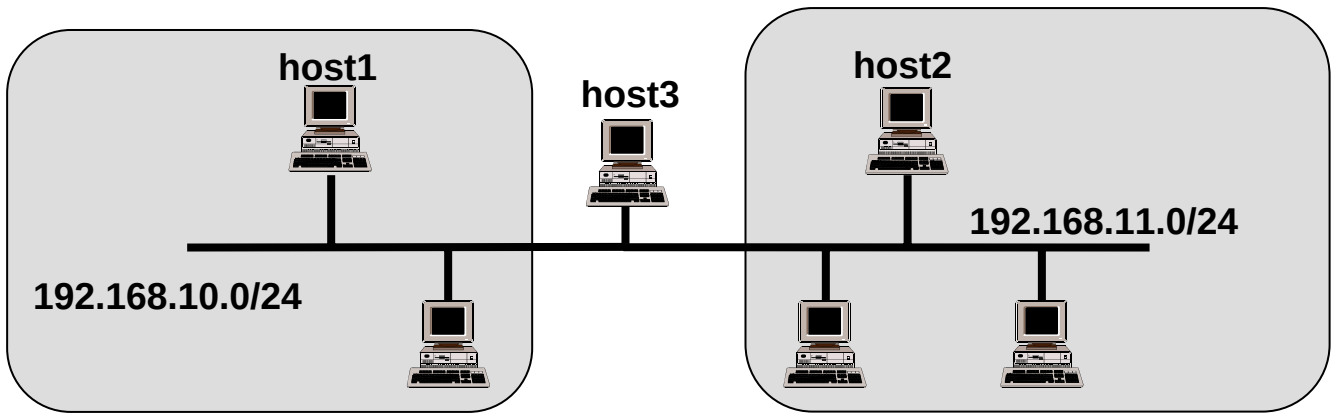


Tabella di instradamento

- Necessaria per sapere come come inoltrare i pacchetti
- Informazioni contenute in ciascuna riga:
  - **indirizzo di destinazione**: può essere un host o una network
  - **netmask**: utilizzata per verificare la corrispondenza con la destinazione
  - **gateway**: indica il tipo di consegna da effettuare (diretta o indiretta)
    - nel caso di consegna indiretta indica l'indirizzo del **next-hop**, cioè il gateway a cui inoltrare i pacchetti
  - **interfaccia di rete**: specifica quale interfaccia di rete utilizzare (loopback compreso)
  - **metrica**: specifica il "costo" di quella particolare route

- **Table lookup** eseguito per ogni datagramma
  - host: solo quelli provenienti dagli strati superiori
  - router: anche quelli in transito

Table lookup

- La ricerca nella tabella avviene utilizzando
  - l'indirizzo IP di destinazione del datagramma
  - l'indirizzo di destinazione e la netmask specificati in ciascuna riga della tabella
- Procedura:
  - si esegue un'operazione di **AND** bit per bit tra l'indirizzo di destinazione del datagramma e la netmask di ciascuna riga
  - il risultato viene confrontato con la destinazione specificata nella riga stessa: se coincidono, la riga è quella giusta
  - il controllo viene effettuato a partire dalla riga che presenta una netmask con un numero maggiore di bit a uno: priorità alle route più specifiche (prima host, poi reti piccole, poi reti grandi – **longest-prefix match**)
  - una volta trovata la riga corrispondente, il lookup si ferma e il datagramma viene instradato secondo la modalità specificata
  - se nessuna riga corrisponde, si usa il **default gateway**

Esempio di lookup – 1

	Destinazione	Netmask	Etc.
1	0.0.0.0	0.0.0.0	…
2	192.168.2.0	255.255.255.0	…
3	192.168.2.18	255.255.255.255	…

- Datagramma con IP dest. = 192.168.2.18
- Confronto prima con riga 3, poi con riga 2 e poi riga 1

192.168.002.018
255.255.255.255
192.168.002.018 == 192.168.002.018

bitwise AND

- La riga 3 è quella giusta (host specific)

Esempio di lookup – 2

	Destinazione	Netmask	Etc.
1	0.0.0.0	0.0.0.0	…
2	192.168.2.0	255.255.255.0	…
3	192.168.2.18	255.255.255.255	…

- Datagramma con IP dest. = 192.168.2.22

```
192.168.002.022
255.255.255.255
192.168.002.022 != 192.168.002.018

192.168.002.022
255.255.255.000
192.168.002.000 == 192.168.002.000
```

- La riga 2 è quella giusta (network specific)

Esempio di lookup – 3

	Destinazione	Netmask	Etc.
1	0.0.0.0	0.0.0.0	…
2	192.168.2.0	255.255.255.0	…
3	192.168.2.18	255.255.255.255	…

- Datagramma con IP dest. = 80.48.15.170

```
080.048.015.170
255.255.255.255
080.048.015.170 != 192.168.002.018

080.048.015.170
255.255.255.000
080.048.015.000 != 192.168.002.000

080.048.015.170
000.000.000.000
000.000.000.000 == 000.000.000.000
```

- La riga 1 è quella giusta (default gateway)

Visualizzazione tabella di routing

route print (Windows)

```
===========================================================================
Elenco interfacce
0x1 ........................... MS TCP Loopback interface
0x1000003 ...00 d0 59 ce 68 16 ...... Intel 8255x-based Integrated Fast Ethernet
===========================================================================
===========================================================================
Route attive:
Indirizzo rete             Mask             Gateway       Interfac.  Metric
          0.0.0.0          0.0.0.0    192.168.10.76   192.168.10.90       1
        127.0.0.0        255.0.0.0        127.0.0.1       127.0.0.1       1
    192.168.10.0    255.255.255.0    192.168.10.90   192.168.10.90       1
   192.168.10.90  255.255.255.255        127.0.0.1       127.0.0.1       1
  192.168.10.255  255.255.255.255    192.168.10.90   192.168.10.90       1
        224.0.0.0        224.0.0.0    192.168.10.90   192.168.10.90       1
  255.255.255.255  255.255.255.255    192.168.10.90   192.168.10.90       1
Gateway predefinito:     192.168.10.76
===========================================================================
Route persistenti:
  Nessuno
```

Gateway = IP locale → consegna diretta

Gateway = loopback → consegna agli strati superiori

Altrimenti → consegna indiretta tramite il gateway indicato

Visualizzazione tabella di routing

route -n (Linux)

```
[walter@deis73 walter]$ /sbin/route -n
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
192.168.10.0    0.0.0.0         255.255.255.0   U     0      0        0 eth0
127.0.0.0       0.0.0.0         255.0.0.0       U     0      0        0 lo
0.0.0.0         192.168.10.76   0.0.0.0         UG    0      0        0 eth0
[walter@deis73 walter]$
```

Gateway = 0.0.0.0 & Iface = eth*n* → consegna diretta

Gateway = 0.0.0.0 & Iface = lo → agli strati superiori

Altrimenti → consegna indiretta tramite il gateway indicato

Multi-homed host

- Se sono presenti più interfacce, c'è una entry per ogni rete IP a cui si è connessi
  - necessaria per eseguire correttamente la consegna diretta

```
[walter@deis76 walter]$ /sbin/route  -n
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
137.204.57.0    0.0.0.0         255.255.255.0   U     0      0        0 eth0
192.168.10.0    0.0.0.0         255.255.255.0   U     0      0        0 eth1
127.0.0.0       0.0.0.0         255.0.0.0       U     0      0        0 lo
0.0.0.0         137.204.57.254  0.0.0.0         UG    0      0        0 eth0
[walter@deis76 walter]$
```

Modifica della tabella di routing

route add default gw <gateway>

aggiunge il default gateway alla tabella di routing

route add –net <dest> netmask <mask> gw <gateway> dev <interface>

route add –host <dest> gw <gateway> dev <interface>

aggiunge una entry alla tabella di routing specificandone i parametri (si omette **gw <gateway>** per forzare la consegna diretta)

route del default

route del –net <dest> netmask <mask>

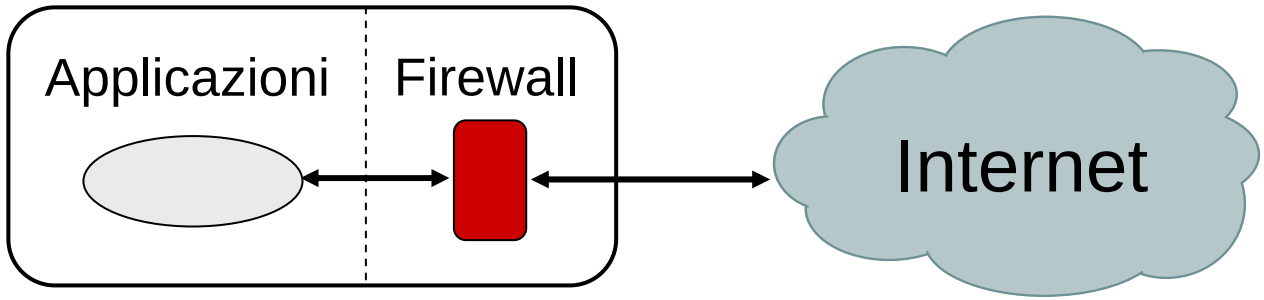
route del –host <dest>

elimina le corrispondenti entry dalla tabella

Protezione di host: personal firewall

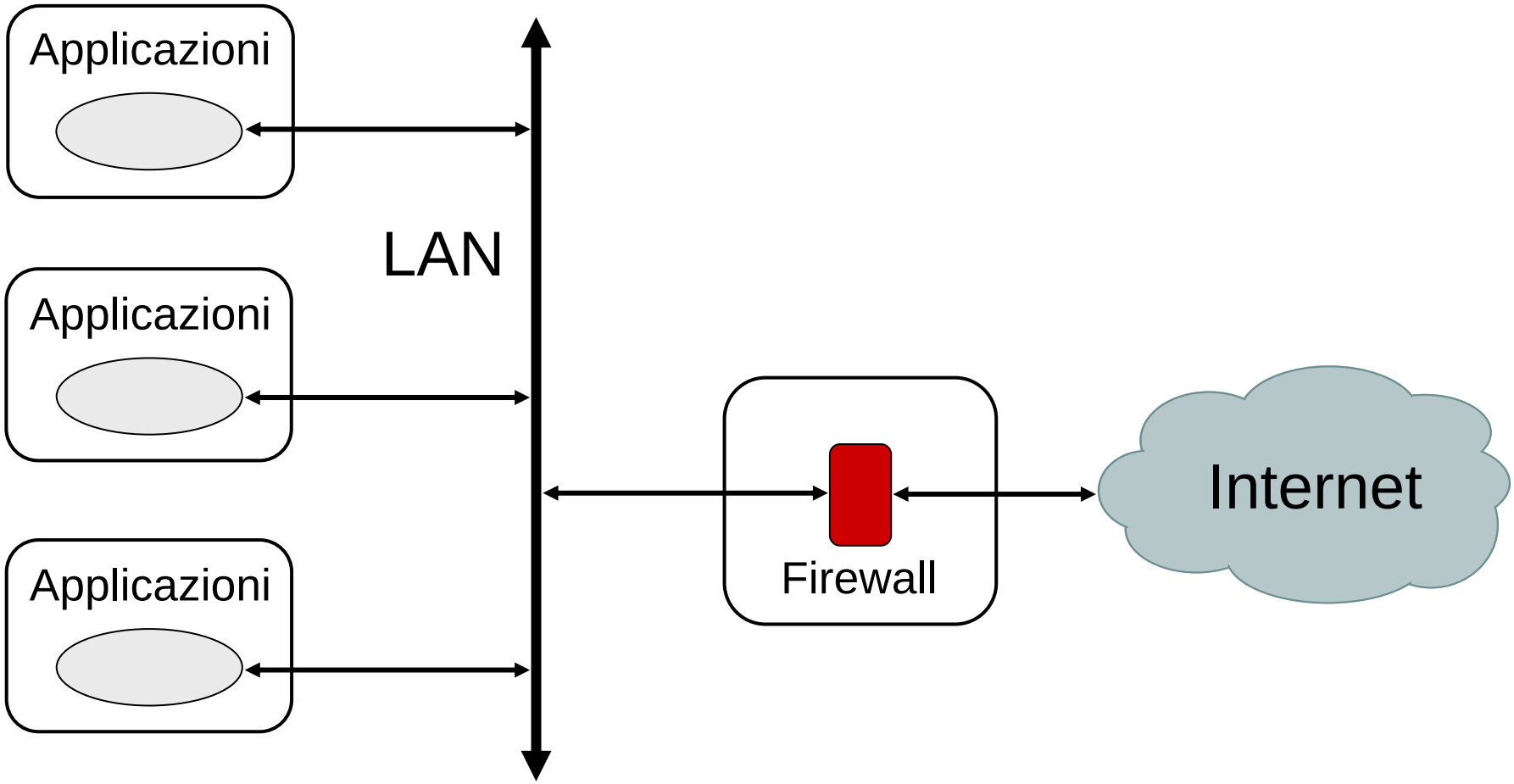
- Un firewall è un filtro software che serve a proteggersi da accessi indesiderati provenienti dall'esterno della rete

- Può essere semplicemente un programma installato sul proprio PC che protegge quest'ultimo da attacchi esterni



Protezione di rete: firewall

- Oppure può essere una macchina dedicata che filtra tutto il traffico da e per una rete locale



Firewall: caratteristiche

- Tutto il traffico fra la rete locale ed Internet deve essere filtrato dal firewall
- Solo il traffico autorizzato deve attraversare il firewall
- Si deve comunque permettere che i servizi di rete ritenuti necessari siano mantenuti
- Il firewall deve essere per quanto possibile immune da problemi di sicurezza sull'host
- In fase di configurazione di un firewall, per prima cosa si deve decidere la politica di default per i servizi di rete
  - **default deny**: tutti servizi non esplicitamente permessi sono negati
  - **default allow**: tutti i servizi non esplicitamente negati sono permessi

Livelli di implementazione

- Un firewall può essere implementato come
  - **Packet filter**
    - si interpone un router fra la rete locale ed Internet
    - sul router si configura un filtro sui datagrammi IP da trasferire attraverso le varie interfacce
    - il filtro scarta i datagrammi sulla base di
      - indirizzo IP e/o MAC sorgente o destinazione
      - tipo di servizio (campo PROTOCOL o porta TCP/UDP)
      - interfaccia di provenienza o destinazione
  - **Proxy server**
    - nella rete protetta l'accesso diretto ad Internet non è consentito a tutti gli host
    - si interpone un server apposito detto proxy server per controllare gli accessi alla rete esterna
    - il proxy server evita un flusso diretto di datagrammi fra Internet e le macchine della rete locale

Utilizzo di packet filter e proxy server