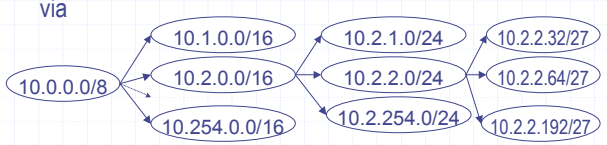
E-4: VLSM, Supernetting, NAT/PAT, Firewall

A. Memo

VLSM - Variable Length Subnet Masks

- 1987, esce l'**RFC 1009**, che specifica come una sottorete può utilizzare più *Subnet Mask*
- ammette lunghezze diverse dell'*extended-network-prefix*
- una rete viene prima divisa in sottoreti, poi alcune sottoreti sono ulteriormente suddivise in altre sotto-sottoreti, e così via



VLSM - Variable Length Subnet Masks

ATTENZIONE: tutte le tecniche descritte in questo modulo (VLSM, aggregamento delle reti, CIDR) funzionano solo se i protocolli di routing trasferiscono esplicitamente anche la subnet mask

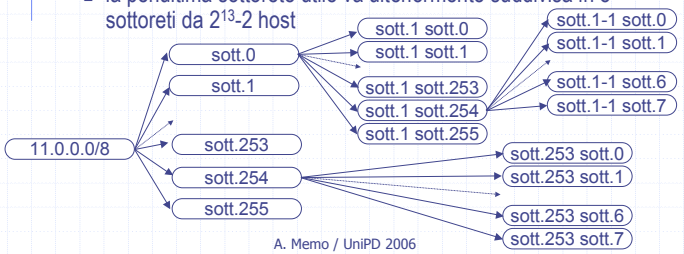
no RIP v.1 e no IGRP

quindi gestiscono anche le reti/sottoreti tutti i bit a 0 e tutti i bit a 1

Esempio VLSM

Si vuole suddividere la rete 11.0.0.0/8 in 256 sottoreti utili da 2^{16}-2 host, di cui

- la prima sottorete utile va ulteriormente suddivisa in 256 sottoreti da 2^8-2 host, di cui
  - la penultima sottorete utile va a sua volta suddivisa in 8 sottoreti utili da 2^5-2 host
- la penultima sottorete utile va ulteriormente suddivisa in 8 sottoreti da 2^{13}-2 host



Soluzione VLSM (1)

network-prefix

```
11.0.0.0/8 = 00001011.oooooooo.oooooooo.oooooooo
```

suddivisione in 256 (= 2^8) sottoreti

prima

```
11.0.0.0/16 = 00001011.00000000.oooooooo.oooooooo
11.1.0.0/16 = 00001011.00000001.oooooooo.oooooooo
11.2.0.0/16 = 00001011.00000010.oooooooo.oooooooo
11.3.0.0/16 = 00001011.00000011.oooooooo.oooooooo
:::::::::::   ::::::::.::::::::.::::::::.::::::::
11.254.0.0/16 = 00001011.11111110.oooooooo.oooooooo
11.255.0.0/16 = 00001011.11111111.oooooooo.oooooooo
```

extended-network-prefix

penultima

Soluzione VLSM (2)

extended-network-prefix

```
11.0.0.0/16 = 00001011.00000000.oooooooo.oooooooo
```

suddivisione della prima sottorete in 256 (=2^8) sottoreti

```
11.0.0.0/24 = 00001011.00000000.00000000.oooooooo
11.0.1.0/24 = 00001011.00000000.00000001.oooooooo
11.0.2.0/24 = 00001011.00000000.00000010.oooooooo
11.0.3.0/24 = 00001011.00000000.00000011.oooooooo
:::::::::::   ::::::::.::::::::.::::::::.::::::::
11.0.254.0/24 = 00001011.00000000.11111110.oooooooo
11.0.255.0/24 = 00001011.00000000.11111111.oooooooo
```

nuovo extended-network-prefix

penultima

Soluzione VLSM (3)

extended-network-prefix

```
11.0.254.0/24 = 00001011.00000000.11111110.oooooooo
```

suddivisione della penultima sottorete in 8 (= 2^3) sottoreti

```
11.0.254.0/27 = 00001011.00000000.11111110.000ooooo
11.0.254.32/27 = 00001011.00000000.11111110.001ooooo
11.0.254.64/27 = 00001011.00000000.11111110.010ooooo
11.0.254.96/27 = 00001011.00000000.11111110.011ooooo
11.0.254.128/27 = 00001011.00000000.11111110.100ooooo
11.0.254.160/27 = 00001011.00000000.11111110.110ooooo
11.0.254.192/27 = 00001011.00000000.11111110.101ooooo
11.0.254.224/27 = 00001011.00000000.11111110.110ooooo
```

nuovo extended-network-prefix

Soluzione VLSM (4)

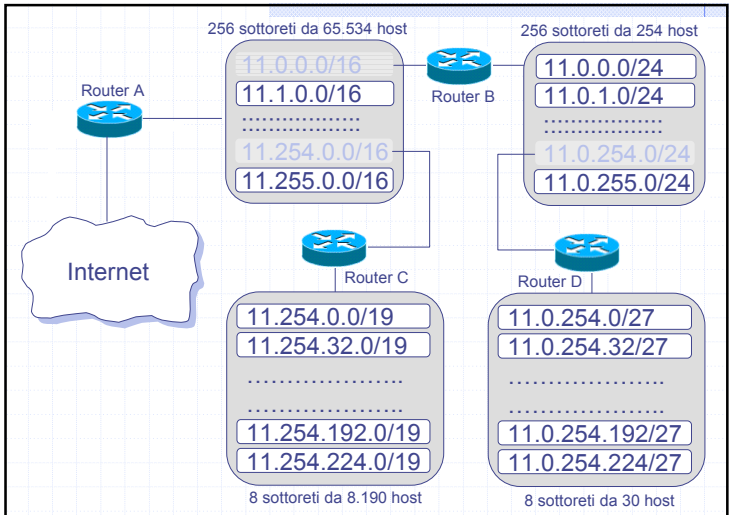
extended-network-prefix

```
11.254.0.0/16 = 00001011.11111110.oooooooo.oooooooo
```

suddivisione della prima sottorete in 8 (= 2^3) sottoreti

```
11.254.0.0/19 = 00001011.11111110.000ooooo.oooooooo
11.254.32.0/19 = 00001011.11111110.001ooooo.oooooooo
11.254.64.0/19 = 00001011.11111110.010ooooo.oooooooo
11.254.96.0/19 = 00001011.11111110.011ooooo.oooooooo
11.254.128.0/19 = 00001011.11111110.100ooooo.oooooooo
11.254.160.0/19 = 00001011.11111110.101ooooo.oooooooo
11.254.192.0/19 = 00001011.11111110.110ooooo.oooooooo
11.254.224.0/19 = 00001011.11111110.111ooooo.oooooooo
```

nuovo extended-network-prefix



Commento alla soluzione (1)

- siamo partiti da una rete di classe A
  - Host utili: $2^{24}-2=16.777.214$
- abbiamo creato

  (256-2)+(256-1)+8+8 = 525 sottoreti
- con un numero totale di host di

  (254x65.533)+(255x254)+(8x30)+(8x8.190)= 16.775.912

Commento alla soluzione (2)

- quante righe compongono la tabella di instradamento del Router A?
- attraverso l'interfaccia lato interno vede 254 + 255 + 8 + 8 = 525 reti !
- una tabella di instradamento grande implica
  - traffico elevato
  - lentezza di convergenza
  - grande mole di lavoro dei router

Aggregamento delle reti

il *Router D* instrada con Subnet Mask = /27 verso le sue sottoreti, e comunica ai router adiacenti solo la loro aggregazione

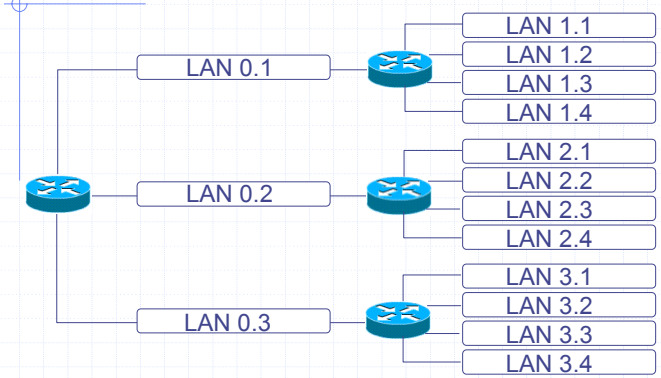
In tal modo si riducono di molto le righe delle tabelle di tutti i router, specialmente i *border*.

Esercizio

Un'azienda è strutturata in 3 sedi staccate che fanno capo allo stesso router, ciascuna con un massimo di 4 reparti, ed ogni reparto è una LAN distinta, con un massimo di 50 utenti.

Proporre una possibile pianificazione degli indirizzi IP.

Traccia di soluzione



Traccia di soluzione

- almeno 6 bit per i 50 host dei laboratori/uffici di ogni reparto + una porta del router
- almeno 2 bit per i 4 reparti
- almeno 2 bit per le 3 sedi e per le sottoreti di interconnessione tra i router

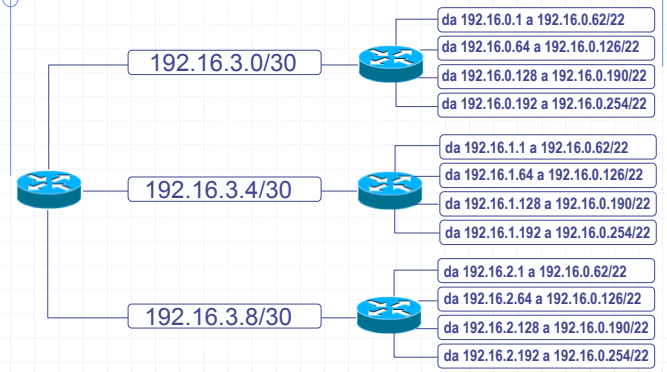
per un totale di 10 bit.

È quindi sufficiente un indirizzo di classe B. Partiamo ad esempio dalla sottorete 172.16.0.0/22.

```
172.16.0.0/22 = 10101100.00010000.000000oo.oooooooo
```

sedi+ interc. | reparti | host

Traccia di soluzione



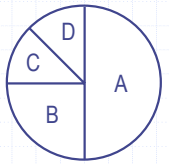
Classless Inter-Domain Routing

- Non instrada in base alla classe (campo *network-prefix*) dell'indirizzo, ma solo in base ai bit più significativi (campo *IP-prefix*) dell'intero indirizzo IP
- si utilizza una *Network Mask* per individuare l'IP-prefix
- la Network Mask può essere più corta della maschera standard di quella classe (**supernetting**)

Esempio CIDR

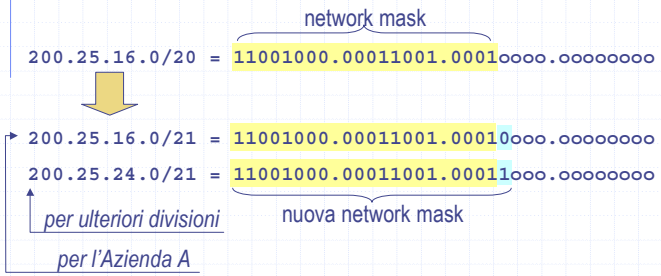
Un ISP possiede il blocco di indirizzi 200.25.16.0\20, e vuole distribuire questi indirizzi tra 4 aziende con le seguenti caratteristiche:

azienda A: 2000 host
azienda B: 1000 host
azienda C: 500 host
azienda D: 500 host



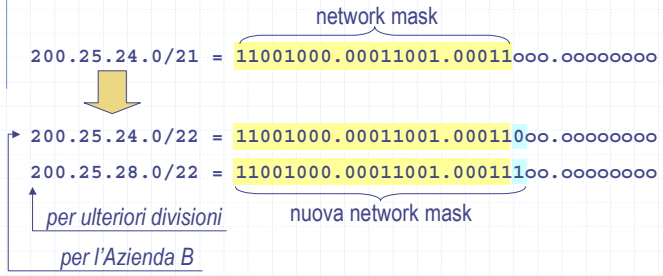
Soluzione (1)

1. suddividere il blocco di indirizzi in due fette: (A) e (B+C+D)



Soluzione (2)

- suddividere il secondo blocco in due fette uguali: (B) e (C+D)



Soluzione (3)

- suddividere il secondo blocco in due fette uguali: (C) e (D)

network mask

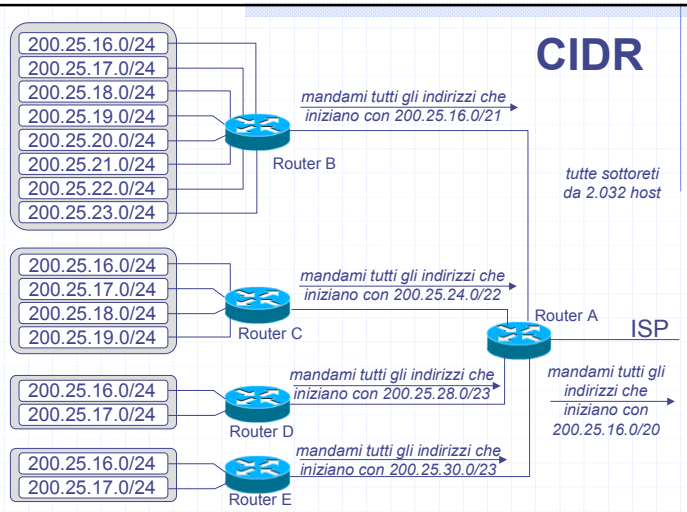
```
200.25.28.0/22 = 11001000.00011001.000111oo.oooooooo

200.25.28.0/23 = 11001000.00011001.0001110o.oooooooo
200.25.30.0/23 = 11001000.00011001.0001111o.oooooooo
```

nuova network mask

per l'Azienda D

per l'Azienda C

CIDR



Indirizzi pubblici e privati

IANA ha suddiviso gli indirizzi IP in:

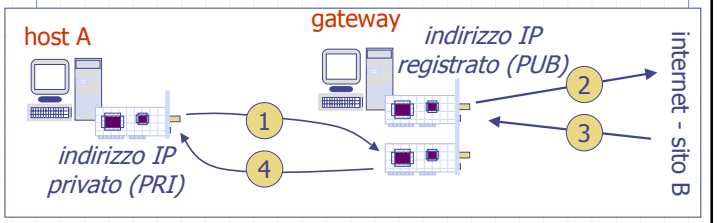
- **registrati** o **pubblici**, se vengono attribuiti formalmente e forniti staticamente o dinamicamente dall'ISP
- **privati**, solo ad uso interno, di valore compreso tra

10.0.0.0 - 10.255.255.255 *1 rete di classe A*

172.16.0.0 - 172.31.255.255 *16 reti di classe B*

192.168.0.0 - 192.168.255.255 *255 reti di classe C*

traduzione degli indirizzi



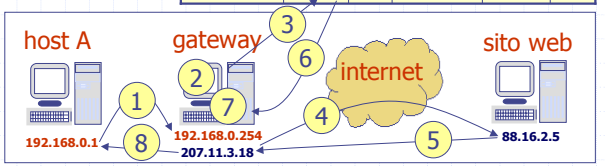
1= richiesta da host A (PRI) a gateway (PRI) per sito B (PUB)
2= richiesta da gateway (PUB) ad sito B (PUB)
3= risposta da sito B (PUB) a gateway (PUB)
4= risposta da gateway (PRI) a host A (PRI)

Tecniche di traduzione

- La traduzione di indirizzi può avvenire in diversi modi:
  - UNIVOCO, un indirizzo privato per ogni indirizzo fisico, e questa associazione può essere (NAT):
    - statica (usato in genere per i server)
    - dinamica
  - NON UNIVOCO, in base alla coppia IP-PortNumber, con tecnica NAT-PAT, detta anche NAPT (Network Address Port Traslation) o IP Masquerading; permette di condividere un indirizzo pubblico tra molti utenti con indirizzi privati

NAT/PAT

Tabella dinamica NAT					
interno			esterno		
192.168.0.1	29011	TCP	88.16.2.5	1025	TCP



#	sorgente			destinazione			commenti
1	192.168.0.1	29011	TCP	88.16.2.5	80	TCP	invio dall'host
2	207.11.3.18	1025	TCP	88.16.2.5	80	TCP	traduzione
3	207.11.3.18	1025	TCP	88.16.2.5	80	TCP	aggiorna NAT tabel
4	207.11.3.18	1025	TCP	88.16.2.5	80	TCP	invio al sito
5	88.16.2.5	80	TCP	207.11.3.18	1025	TCP	risposta del sito
6	88.16.2.5	80	TCP	207.11.3.18	1025	TCP	consulta NAT tabel
7	88.16.2.5	80	TCP	192.168.0.1	29011	TCP	traduzione
8	88.16.2.5	80	TCP	192.168.0.1	29011	TCP	arriva all'host

Limiti del NAT/PAT

NAT:

- mancanza della connessione diretta tra gli end-point
- malfunzionamento delle applicazioni che veicolano indirizzi IP al loro interno (anche il TCP)
- in IPSec occorre ricalcolare il checksum

PAT:

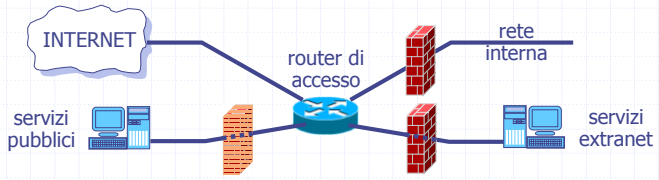
- impossibilità di associare dall'esterno il solo indirizzo IP pubblico a più host (gaming multi player o più server web interni)

entrambi:

- collo di bottiglia per il traffico (criticità per i guasti)

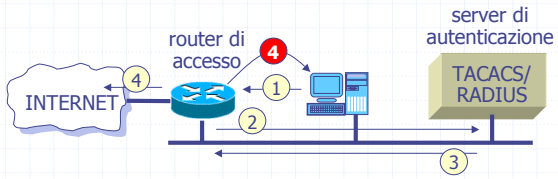
Sicurezza: firewall

- un firewall è un dispositivo che governa il traffico tra due reti distinte, permettendo solo quello autorizzato e registrando eventuali tentativi di effrazione
- l'autorizzazione deriva dall'identificazione e accettazione degli utenti/sistemi che effettuano la richiesta e dalla congruità delle relative risposte



Sicurezza: autenticazione

- la distribuzione degli accessi ad Internet va regolamentata con uno schema di autenticazione personalizzata
- bloccano le richieste non autorizzate
- esempio di autenticazione interna:



Firewall

- un firewall può operare
  - a livello rete (*packet filtering*)
  - a livello trasporto (*circuit gateway*)
  - a livello applicazione (*application*)
  - basandosi sui contenuti

Livello Applicazione
Livello Trasporto
Livello Rete
Livello Collegamento Dati
Livello Fisico

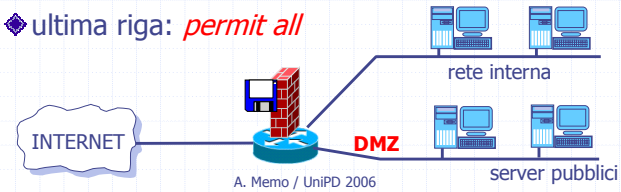
Firewall: classificazioni

classificazione in base all'architettura esterna:
- screening router firewall
- computer-based firewall
- firewall dedicati e/o integrati
- firewall interno
- host firewall
- screened host gateway

classificazione in base alle tecnologie di filtraggio:
- static packet filter firewall
- stateful firewall
- NAT per IP masquerading
- application firewall

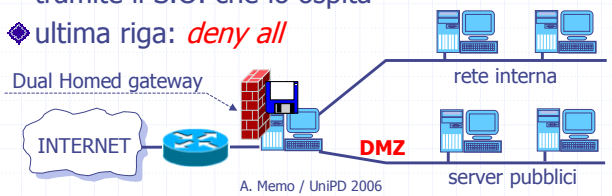
Screening router firewall

- pacchetto software aggiunto al S.O. del router
- generalmente costoso (patch aggiuntiva)
- consuma risorsa hardware
- intercetta attacchi semplici (scrematura a livello IP)
- riduce il lavori di altri firewall
- ultima riga: *permit all*



Computer-based firewall

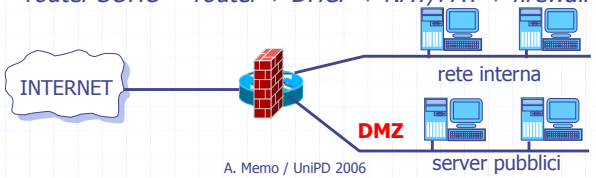
- pacchetto software aggiunto al S.O. del server di condivisione degli accessi
- generalmente poco costoso
- generalmente l'hardware è sufficiente
- attaccabile non solo come firewall, ma anche tramite il S.O. che lo ospita
- ultima riga: *deny all*



Firewall integrati e/o dedicati

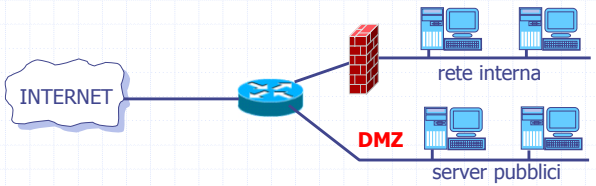
- dispositivi autonomi indipendenti
- S.O. minimo (e quindi più sicuro)
- generalmente più costoso
- avviamento e manutenzione minimizzati
- richiede aggiornamenti (flash o patch)

router SOHO = router + DHCP + NAT/PAT + firewall



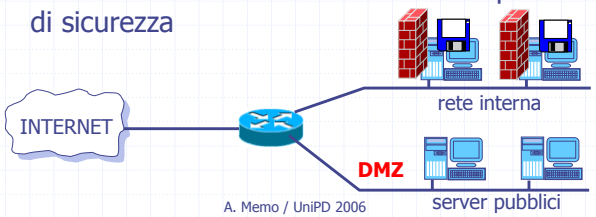
Firewall interno

- posizionato tra router esterno e rete interna
- blocca con più sicurezza gli accessi alla rete interna



Host firewall

- pacchetto software installato nei client
- garantisce una protezione più dettagliata ed approfondita, ma limitata al solo client che lo ospita
- mancanza di un coordinamento delle politiche di sicurezza

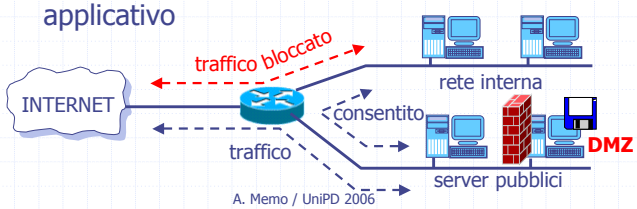


DMZ

- DeMilitarized Zone, zona accessibile dall'esterno, contenente servizi pubblici
- il firewall impedisce anche che traffico prodotto dalla DMZ entri nella rete interna
- nella DMZ può essere installato anche un host con funzioni di *application firewall*
  - controlla le richieste all'interno delle sessioni applicative
  - cerca di respingere attacchi via browser e HTTP
  - opera a livello applicazione
- gli host della DMZ vengono chiamati *Bastion Host*

Screened host gateway

- pacchetto software installato in un host della rete DMZ (bastion host)
- lo *screening router* impedisce il traffico diretto tra rete esterna e rete interna
- il *bastion host* governa il traffico a livello applicativo



Caratteristiche di un firewall

- prestazioni di filtraggio
- esigenze di calcolo
- complessità di filtraggio vs volume di traffico
- scelta e limitazione delle regole

Static packet filter firewall

- tipicamente attivo nei router
- opera a livello rete, in base a:
  - indirizzo IP
  - indirizzo della porta
  - protocollo
- indipendente dalle applicazioni
- configurazione difficile
- facilmente aggirabile
- costo contenuto, prestazioni buone

Stateful firewall (dynamic)

- come il packet statico, ma basato sullo stato dei vari livelli
- il primo pacchetto di una connessione IP passa attraverso tutte le regole, se ne ha il permesso
- il firewall identifica la connessione e permette il passaggio a tutti i suoi pacchetti in entrambe le direzioni
- prestazioni migliori del packet statico

NAT per IP Masquerading

- la NAT permette di connettere più computer ad Internet usando un host con un solo indirizzo IP pubblico
- come effetto gli host interni vengono mascherati all'esterno

Application firewall gateway

- effettua filtraggio a livello applicazione
- un proxy è un application firewall gateway, e può offrire
  - connettività
  - caching
  - auditing
  - sicurezza e privacy
- spesso svolge anche funzioni di IDS (*Intrusion Detection System*)

Riassumendo

- classful
- subnetting FLSM
- subnetting VLSM
- aggregazione
- classless CIDR
- NAT/PAT