

ACCESS LIST

Pietro Nicoletti

www.studioreti.it



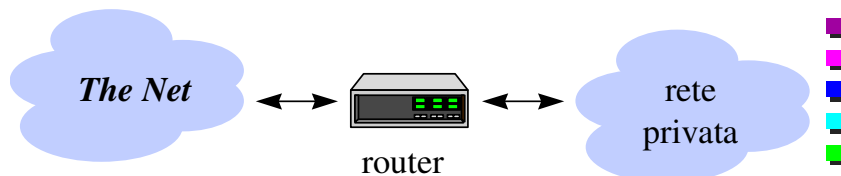
Nota di Copyright

- Questo insieme di trasparenze (detto nel seguito slides) è protetto dalle leggi sul copyright e dalle disposizioni dei trattati internazionali. Il titolo ed i copyright relativi alle slides (ivi inclusi, ma non limitatamente, ogni immagine, fotografia, animazione, video, audio, musica e testo) sono di proprietà degli autori indicati a pag. 1.
- Le slides possono essere riprodotte ed utilizzate liberamente dagli istituti di ricerca, scolastici ed universitari afferenti al Ministero della Pubblica Istruzione e al Ministero dell'Università e Ricerca Scientifica e Tecnologica, per scopi istituzionali, non a fine di lucro. In tal caso non è richiesta alcuna autorizzazione.
- Ogni altra utilizzazione o riproduzione (ivi incluse, ma non limitatamente, le riproduzioni su supporti magnetici, su reti di calcolatori e stampate) in toto o in parte è vietata, se non esplicitamente autorizzata per iscritto, a priori, da parte degli autori.
- L'informazione contenuta in queste slides è ritenuta essere accurata alla data della pubblicazione. Essa è fornita per scopi meramente didattici e non per essere utilizzata in progetti di impianti, prodotti, reti, ecc. In ogni caso essa è soggetta a cambiamenti senza preavviso. Gli autori non assumono alcuna responsabilità per il contenuto di queste slides (ivi incluse, ma non limitatamente, la correttezza, completezza, applicabilità, aggiornamento dell'informazione).
- In ogni caso non può essere dichiarata conformità all'informazione contenuta in queste slides.
- In ogni caso questa nota di copyright non deve mai essere rimossa e deve essere riportata anche in utilizzi parziali.



Liste di accesso

- Sui router possono essere definite “Liste di Accesso” (Access List) per controllare:
 - La trasmissione di pacchetti su un’interfaccia
 - La ricezione di pacchetti da un’interfaccia
 - L’accesso a linee “virtual terminal” (telnet)
 - L’aggiornamento delle tabelle di routing



Access List - 3

Copyright: si veda nota a pag. 2

Access List: filtri

- Le liste di accesso filtrano normalmente i pacchetti in base a:
 - indirizzo sorgente
 - indirizzo destinazione
 - port sorgente
 - port destinazione

Access List - 4

Copyright: si veda nota a pag. 2

Sicurezza da e verso Internet

- Il traffico che attraversa il router è controllato da una Access Control List, che permette di abilitare/negare il flusso dei pacchetti, in funzione degli host/servizi interessati.
- Per abilitare, ad esempio, la mail, un'ACL potrebbe avere il seguente formato:

Type	Src_IP	Dst_IP	Src_Port	Dst_Port	Action
tcp	*	192.106.248.*	*	25	permit
*	*	192.106.248.*	*	*	deny

Tutto quello che non è esplicitamente previsto è negato

Access List su router Cisco

- Per utilizzare le liste di accesso si deve:
 - 1) Definire la lista di accesso
 - una lista di accesso è una sequenza di condizioni di “**permit**” e “**deny**” che si applica ad **indirizzi IP** e **numeri di porta**
 - 2) Applicare la lista ad un'interfaccia o ad una linea virtual terminal:

```
interface Ethernet 0
  ip address 192.106.248.24 255.255.255.0
  ip access-group numero/nome [in/out]

line vty 0-4
  access-class numero [in/out]
```

Access List Cisco: protocolli

Protocollo	Range		
IP	1	to	99
Extended IP	100	to	199
Ethernet type code	200	to	299
DECnet and extended DECnet	300	to	399
XNS	400	to	499
Extended XNS	500	to	599
AppleTalk	600	to	699
Ethernet address	700	to	799
IPX	800	to	899
Extended IPX	900	to	999
IPX SAP	1000	to	1099
Extended transparent bridging	1100	to	1199

ACL IP standard Cisco

```
ip access-list          numero permit/deny src.addr src.wildcard
ip access-list standard nome permit/deny src.addr src.wildcard
```

wildcard: n bit a 0 e 32-n ad 1
es: 0.0.0.255 indica che l'ultimo byte può assumere qualsiasi valore se non specificata si sottintende la wildcard 0.0.0.0

abbreviazioni e alias:
 host equivale alla wildcard 0.0.0.0
 any equivale a 0.0.0.0 255.255.255.255

ACL IP estese

```
ip access-list numero permit/deny protocol
    src.addr src.wildcard dst.addr dst. Wildcard
    [eq port] [established] [log]

ip access-list extended nome permit/deny protocol
    src.addr src.wildcard dst.addr dst. Wildcard
    [eq port] [established] [log]
```

- Il parametro protocol tipicamente varrà: IP/ICMP/TCP/UDP
- Il valore port può essere sostituito dal nome del servizio (FTP, Telnet, etc.)
- Il parametro opzionale *established*, valido solo per TCP, indica l'accettazione dei messaggi di ritorno per connessioni TCP già instaurate
- Il parametro opzionale log, provoca il logging della riga

Esecuzione Access List su Cisco

- Alla ricezione di un pacchetto il router Cisco:
 - scorre la lista di accesso dalla prima riga in ordine sequenziale
 - se trova una riga che corrisponde ad indirizzo/protocollo/port del pacchetto scarta/accetta (deny/permit) il pacchetto
 - se a fine lista non è stata trovata nessuna corrispondenza il pacchetto viene scartato; cioè ad ogni fine lista si considera una riga implicita del tipo:

```
deny ip any any
```

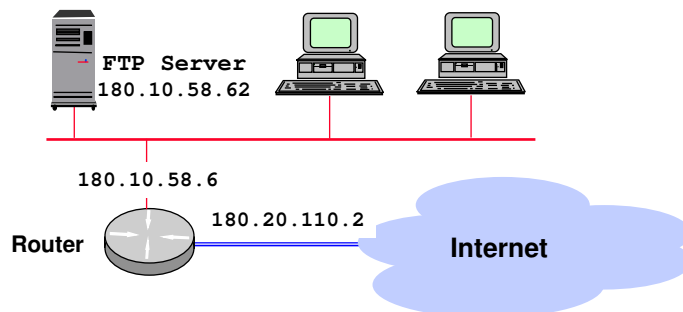
ACL IP standard e estese

■ Configurazione di ACL IP estese:

- è indispensabile conoscere l'impiego delle porte da parte degli applicativi a seconda che la comunicazione sia da client a server o viceversa
- Nei router l'aggiunta di righe alle access list non è problematica
 - bisogna però considerare che vengono messe in fondo alla lista esistente
- La cancellazione di una riga della lista provoca la cancellazione di tutta lista

Caso di esempio

- Si vuole uscire verso Internet per:
 - WWW, FTP verso altri siti, ricevere la posta
- Si permette da internet:
 - FTP al solo Server 180.10.58.62



Esempio di access list

```
Interface serial 0
ip address 180.20.110.2 255.255.255.252
ip access-group 101 in
ip access-group 102 out
!
access-list 101 permit tcp any any established
access-list 101 permit udp any eq domain any
access-list 101 permit tcp any host 180.10.58.62 eq ftp
access-list 101 permit tcp any host 180.10.58.62 eq ftp-data
access-list 101 permit tcp any eq ftp-data any
access-list 101 deny ip any any
access-list 102 permit udp 180.10.58.0 0.0.0.255 any eq domain
access-list 102 permit tcp 180.10.58.0 0.0.0.255 any eq www
access-list 102 permit tcp 180.10.58.0 0.0.0.255 any eq ftp
access-list 102 permit tcp 180.10.58.0 0.0.0.255 any eq ftp-data
access-list 102 permit tcp host 180.10.58.62 eq ftp-data any
access-list 102 permit tcp 180.10.58.0 0.0.0.255 any eq smtp
access-list 102 permit tcp 180.10.58.0 0.0.0.255 any eq pop3
access-list 102 permit tcp any any established
access-list 102 deny ip any any
```

Access List - 13

Copyright: si veda nota a pag. 2