Progetto Scuola – U.S.R. Lombardia

Gruppo 1 – sottogruppo 2:

Marilù Bordieri

Maria Farinella

Liliana Liborio

Maurizio Lunardi

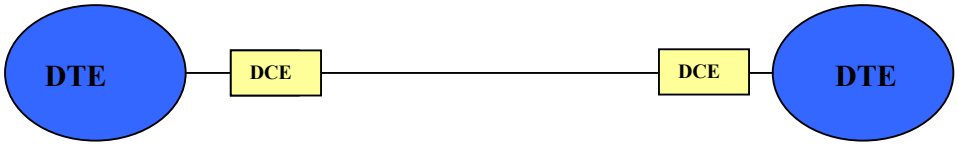
Maurizio Ruvutuso

I lavoro di gruppo – corso formazione Tutor C – Traccia 1

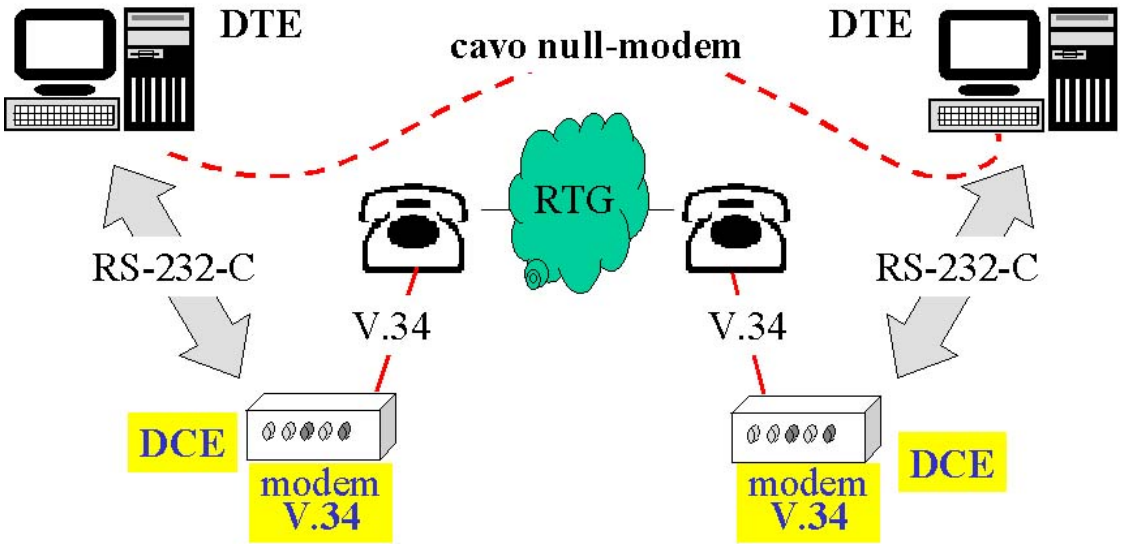
Definire la comunicazione tra le interfacce seriali di due router, attraverso la simulazione DCE/DTE
Gestire e configurare l'accesso al telnet e alla console di un router
Configurare le rotte statiche di una tabella di routing definendone vantaggi e svantaggi rispetto alle rotte generate dinamicamente
Spiegare il significato di Access Control List evidenziandone i tratti fondamentali e le applicazioni pratiche.

Definire la comunicazione tra le interfacce seriali di due router, attraverso la simulazione DCE/DTE

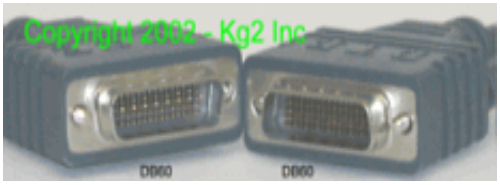
Per effettuare la comunicazione tra due router remoti è necessario effettuare una connessione del tipo DTE-DCE-DCE-DTE come evidenziato in figura



DTE è acronimo di Data Terminal Equipment = apparecchiatura terminale dati .
Solitamente DTE sono i computer, le stampanti , i terminali
DCE è acronimo di Data Communication Equipment = apparecchiatura per comunicazione dati . Solitamente sono i modem. Ma che differenza c'è tra i due ?
Molto semplicemente cambia la disposizione delle connessioni esterne. Per tale motivo un collegamento tra un DTE e un DCE deve essere effettuato con un cavo pin to pin , detto anche cavo MODEM.
Invece , per collegare DTE con DTE o DCE con DCE , che hanno le stesse disposizioni di pin sui connettori , occorre incrociare i conduttori (cavo NULL MODEM) , per collegarli in modo tale da creare la giusta connessione sui pin di handshake e dei dati .



E’ possibile quindi, se necessario, definire, per esempio, la comunicazione tra le interfacce seriali di due router fisicamente vicini, attraverso una simulazione DCE/DTE facendo uso di tali cavi (vedi fig.)

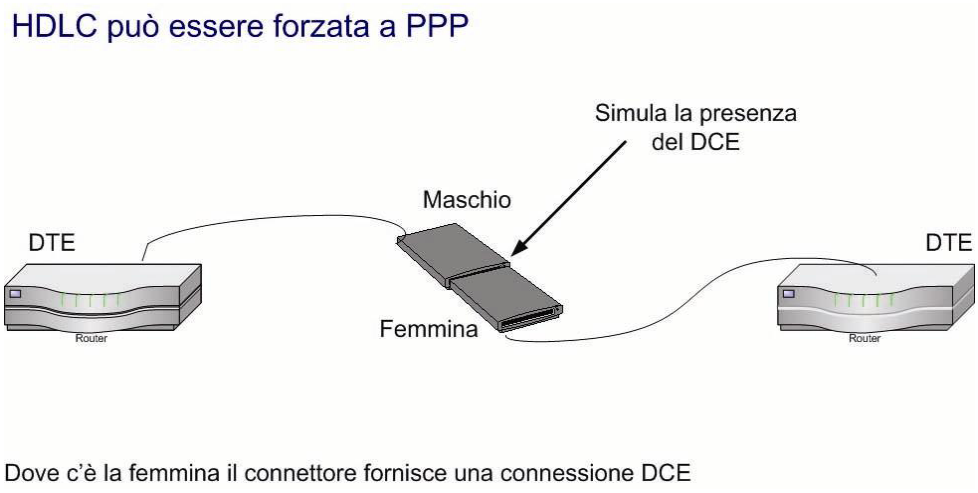


Supponiamo di avere due router da collegare tramite simulazione DCE/DTE (router A e B con ip. address 213.82.149.2 e 213.82.149.3)

Configurazione dell’interfaccia seriale dei router da collegare

E’ necessario, come prima cosa, configurare l’interfaccia seriale su ciascuno dei due router attraverso i seguenti comandi:

```
Router# configure terminal
Router(config)#interface serial 1
Router(config-if)#ip address 213.82.149.2   255.255.255.0      **per il router A**
Router(config-if)#ip address 213.82.149.3   255.255.255.0      **per il router B**
Router(config-if)#encapsulation ppp
Router(config-if)#no shutdown
```



Verifica tipo seriale

E' possibile capire dalla linea di comando se la seriale del router è DCE o DTE digitando il seguente comando dal Global configuration mode:

Router#show controllers serial 1

Configurazione del segnale di clock

Se la seriale del nostro router è di tipo DTE non occorrerà fare altro, se invece simula un DCE sarà necessario configurare un segnale di clock per sincronizzare la trasmissione dei dati. Questo perché stiamo simulando una connessione a distanza nella quale invece, di norma, il segnale viene automaticamente prodotto dai dispositivi DCE presenti effettivamente nel collegamento (per es. modem). I comandi per simulare tale segnale sono i seguenti :

Router#configure terminal
Router(config)#interface serial 1
Router)config-if)#clock rate 56000

Gestire e configurare l'accesso al telnet e alla console di un router

La configurazione di un router può avvenire collegandosi:

- dalla console terminale (un computer connesso al router attraverso la porta console) durante la sua installazione
- via modem utilizzando la porta ausiliaria del router
- da Terminali Virtuali 0-4 (Telnet)
- da un server TFTP sulla rete

Per connettersi ad un utente remoto è possibile utilizzare Telnet, un protocollo che è parte della suite tcp/ip e fornisce un terminale virtuale impostando, per esempio, la connessione tra un router ed un pc. Telnet permette di verificare il software a livello applicazione tra stazioni di origine e destinazione. Un router può avere fino a 5 connessioni simultanee in Telnet.

Configurazione dell'accesso al TELNET (Router Cisco 2600)

In ambiente Windows 2000 aprire il programma HyperTerminal:

- Fare ck sul tasto Start (o Avvio) a sinistra della Barra delle applicazioni.
- Scegliere Programmi.
- Nella tendina corrispondente scegliere Accessori.
- Nella tendina corrispondente scegliere Comunicazioni.
- Nella tendina corrispondente scegliere HyperTerminal.

Comparirà il prompt dei comandi

Router> Digitare Router>enable

Comparirà la parola

Password: Digitare Password: cisco (Si ipotizza che la password sia cisco)

Si entrerà in privilege mode attraverso la password digitata.

Comparirà il prompt dei comandi

Router#

Occorrerà ora entrare nel global configuration mode. Digitare

Router#configure terminal

Comparirà il prompt dei comandi

Router(config)#

Occorrerà ora configurare la password per l'accesso alle linee di TELNET (MAX 5).

Occorrerà prima entrare in line configuration mode. Digitare

Router(config)# line vty 0 4

Comparirà il prompt dei comandi

Router(config-line)#

Digitare

Router(config-line)#password telnet

(Si ipotizza che venga attribuita la password telnet)

Per ritornare a global configuration mode premere i tasti:

Router(config-line)# exit

Con questo comando si sale di un livello

Comparirà il prompt dei comandi

Router(config)#

Per ritornare a privilege mode digitare ancora:

Router(config)# exit

Comparirà il prompt dei comandi

Router#

Si sarebbe ottenuto lo stesso risultato digitando in line configuration mode:

Router(config-line)#CTRL + z

Comparirebbe subito il prompt dei comandi

Router#

Configurazione dell'accesso alla CONSOLE (Router Cisco 2600)

In ambiente Windows 2000 aprire il programma HyperTerminal:

- Fare ck sul tasto Start (o Avvio) a sinistra della Barra delle applicazioni.
- Scegliere Programmi.
- Nella tendina corrispondente scegliere Accessori.
- Nella tendina corrispondente scegliere Comunicazioni.
- Nella tendina corrispondente scegliere HyperTerminal.

Comparirà il prompt dei comandi Router>

Digitare Router>enable

Comparirà la parola Password:

Digitare Password: cisco (Si ipotizza che la password sia cisco)

Si entra in privilege mode attraverso la password digitata.

Comparirà il prompt dei comandi Router#

Occorre ora entrare nel global configuration mode. Digitare

Router#configure terminal

Comparirà il prompt dei comandi Router(config)#

Occorre ora configurare il nome del ROUTER. Digitare

Router(config)# hostname traccia1

(Si ipotizza di configurare il nome del ROUTER con traccia1)

Comparirà il prompt dei comandi

traccia1(config)#

Si configura ora la password di enable. Digitare

traccia1(config)#enable secret cisco

(Si ipotizza che venga attribuita la password cisco)

Si procede quindi a configurare la password per l'accesso alla CONSOLE.

Occorre prima entrare in line configuration mode. Digitare

traccia1(config)# line con 0

Comparirà il prompt dei comandi

traccia1(config-line)#

Digitare

traccia1(config-line)# password console

(Si ipotizza che venga attribuita la password console)

Per ritornare a global configuration mode digitare:

traccia1(config-line)#exit

Con questo comando si sale di un livello

Comparirà il prompt dei comandi

traccia1(config)#

Per ritornare a privilege mode digitare ancora:

traccia1(config)#exit

Comparirà il prompt dei comandi

traccia1#

Si sarebbe ottenuto lo stesso risultato digitando in line configuration mode:

traccia1(config-line)#CTRL + z

Comparirà il prompt dei comandi

traccia1#

Verificare e salvare la configurazione del ROUTER (Router Cisco 2600)

Dopo aver configurato l'accesso al telnet e alla console del router è possibile verificare la configurazione con il comando dato in stato di privilege mode.

Dal prompt dei comandi

Router#

Digitare

Router#show running-config

Per copiare la configurazione nella flash occorre dare il seguente comando in stato di privilege mode.

Dal prompt dei comandi

Router#

Digitare

Router#copy running-config startup-config

oppure

Router#write memory

Configurare le rotte statiche di una tabella di routing definendone vantaggi e svantaggi rispetto alle rotte generate dinamicamente

Uno dei compiti assolti dal router è la costruzione della Tabella d'Instradamento attraverso la quale decide di instradare il pacchetto sulla base delle caratteristiche configurate per quel preciso traffico/protocollo su una porta specifica.

Sono molteplici le modalita' tramite cui queste decisioni vengono gestite e mediante cui le tabelle d'instradamento vengono create e mantenute all'interno del Router. Tutto cio' e' strettamente legato alla conformazione dell'hardware, al tipo di traffico e al disegno di rete.

Pertanto la modalita' con cui il Router è configurato ha effetti sulle performance d'instradamento dei pacchetti.

Rotte

In pratica bisogna configurare sui router le cosiddette rotte che indicano al router su quale interfaccia deve trasmettere il pacchetto in base all'indirizzo IP di destinazione del pacchetto stesso.

Ci sono due modi per "insegnare" al router le rotte: in modo statico e in modo dinamico.

Per reti di piccole dimensioni è consigliabile l'utilizzo delle rotte statiche; questo perché le istruzioni da dare sono abbastanza limitate (si utilizzano poche subnet) e chi le configura può decidere in modo deterministico quali percorsi far seguire ai dati (questo implica anche una maggior sicurezza, visto che il router non può "imparare" route da nessun'altra fonte).

Nel caso di reti di dimensioni maggiori, è praticamente indispensabile utilizzare le rotte dinamiche; in sostanza si indica al router quali reti conosce (quelle direttamente connesse); sarà suo compito comunicarle ai router vicini che le comunicheranno a loro volta ai loro vicini e così via.

In questo modo anche in caso di modifiche alla rete, i router si occuperanno di tenere aggiornate autonomamente le loro tabelle di routing.

Rotte statiche

I comandi da dare devono indicare al router quali pacchetti instradare attraverso una certa interfaccia in base all'indirizzo IP di destinazione del pacchetto.

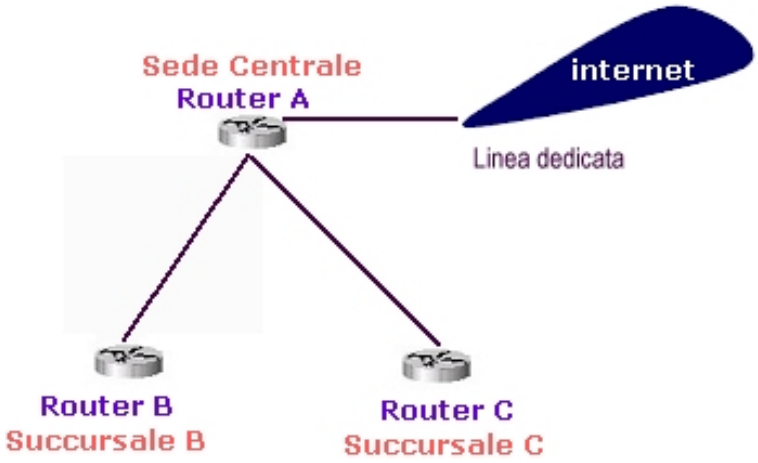
Per indicare al router attraverso quale interfaccia far transitare i dati si indica normalmente il cosiddetto next hop ovvero il prossimo router attraverso il quale i pacchetti devono transitare per giungere a destinazione.

Cosa succede quando un utente attiva un trasferimento dati?

- Un utente decide di inviare un dato (per esempio un'e-mail)
- L'applicazione verifica che il destinatario non è nella subnet dell'host, utilizzando la netmask e l'indirizzo IP
- Il "pacchetto" viene quindi inviato al proprio default gateway (il router)
- Il router riceve il pacchetto e estrae l'indirizzo di destinazione dello stesso
- Il router controlla nella propria tabella di routing se conosce un percorso per raggiungere la rete destinataria
- Se esiste questo percorso il router instrada il pacchetto verso il next hop indicato nella route
- Se non esiste, verifica se è stata impostata una route di default, che utilizzerà per instradare il pacchetto stesso
- Viceversa il pacchetto viene scartato

Esempio di configurazione

Supponiamo di avere due router in due succursali (router B e C – ip. 213.82.149.2 e 213.82.149.3); la loro unica connessione geografica è verso un router posto nella sede centrale (router A – ip. 213.82.149.1) e anche per comunicare fra loro devono transitare da lì.



Sarà necessario indicare ai router delle succursali di instradare tutto il traffico verso il router della sede centrale.

Ci sono due modi per indicare questo al router: possiamo indicargli il suo default gateway oppure indicare che tutte le reti sono raggiungibili tramite il Router A.

- Configurazione del default gateway sui router delle succursali

```
RouterB>enable
Password:*****
RouterB#configure terminal
RouterB(config)#ip default-gateway 213.82.149.1
RouterB(config)#
```

oppure

```
RouterB>enable
Password:*****
RouterB# configure terminal
RouterB(config)#ip route 0.0.0.0  0.0.0.0  213.82.149.1
RouterB(config)#
```

Il primo comando (ip default-gateway) è abbastanza esplicativo: indica al router qual'è il proprio default-gateway.

Nel secondo caso invece indicando come destinazione 0.0.0.0 con netmask 0.0.0.0 diciamo al router che tutte le reti esistenti sono raggiungibili tramite il 213.82.149.1.

- Configurazione del router delle sede centrale

Per quanto riguarda il router della sede, dobbiamo innanzi tutto istruirlo sul come raggiungere le due succursali, indicando l'indirizzo delle due reti come destinazione e quello del router della succursale interessata come next-hop.

Bisogna inoltre indicare al router i percorsi alternativi da seguire in caso di caduta di uno dei link dedicati. In questo caso, infatti, dobbiamo utilizzare le interfacce ISDN di backup, le quali verranno configurate come next-hop nelle route allo stesso modo di quelle principali, ma ad un costo superiore. Infatti al router si possono indicare più route con la stessa destinazione, differenziandole per il costo che comporta la loro percorrenza.

Il router utilizzerà sempre la strada di minor costo, se attiva, ma se essa dovesse venir meno per un guasto, verrebbe utilizzata la strada di backup. Nel momento in cui venisse ripristinata la strada di minor costo, il router ricomincerebbe ad usarla, in maniera assolutamente trasparente per la rete.

Queste configurazioni si realizzano con i seguenti comandi:

```
RouterA>enable
RouterA#configure terminal
```

```
RouterA(config)#ip route 213.82.101.0 255.255.255.0 213.82.149.2
RouterA(config)#ip route 213.82.102.0 255.255.255.0 213.82.149.3
RouterA(config)#ip route 213.82.101.0 255.255.255.0 213.82.149.10 200
RouterA(config)#ip route 213.82.102.0 255.255.255.0 213.82.149.14 200
RouterA(config)#
```

Inoltre dobbiamo indicare qual'è la rotta di default da utilizzare per tutto il traffico non conosciuto (in pratica, tutte le connessioni verso Internet). Si presuppone come default gateway un'interfaccia (Dialer3), connessa all'Internet Service Provider.

```
RouterA(config)#ip route 0.0.0.0 0.0.0.0 Dialer3
RouterA(config)#
```

Spiegare il significato di Access Control List evidenziandone i tratti fondamentali e le applicazioni pratiche.

ACL cosa sono e a cosa servono

Servono a limitare il traffico indesiderato proveniente o destinato ad altre reti.

Come si configurano:

La configurazione delle access-list prevede due separate fasi:
definizione e applicazione.
Si effettua prima la definizione della access list necessarie; poi le ACL si applicano alle relative interfacce.

1. In global configuration mode:
   Definiamo la access-list 10 che blocca il traffico dall'host 172.30.24.12
   Router(config)# *access-list 10 deny host 172.30.24.12*
   Router(config)# *access-list 10 permit any*
2. In interface configuration mode:
   Applichiamo questo gruppo di access-list all'interfaccia Ethernet:
   Router(config-if)# *ip access-group 10*

Access-list number convenzioni Cisco

Per identificatore numerico si usa normalmente un numero appartenente ad un range che individua il tipo di ACL in base alla seguente convenzione.

1-99	IP standard access list
100-199	IP extended access list
1000-1099	IPX SAP access list
1100-1199	Extended 48-bit MAC address access list
1200-1299	IPX summary address access list

200-299	Protocol type-code access list
300-399	DECnet access list
600-699	Appletalk access list
700-799	48-bit MAC address access list
800-899	IPX standard access list
900-999	IPX extended access list

Uso di identificatore mnemonico:

E' possibile definire e applicare una access-list con identificatore non numerico, ad esempio è possibile definire la access-list "pippo":

1. In global configuration mode:
   Definiamo la access-list pippo che blocca il traffico dall'host 172.30.24.12
   Router(config)# *access-list pippo deny host 172.30.24.12*
   Router(config)# *access-list pippo permit any*
2. In interface configuration mode:
   Applichiamo questo gruppo di access-list all'interfaccia Ethernet:
   Router(config-if)# *ip access-group pippo*

Applicazione di una ACL ad un'interfaccia in entrata o in uscita

Nell'applicare un gruppo di access-list ad una interfaccia viene definito se il filtro deve essere applicato in entrata o in uscita.

Router(config-if)# *ip access-group 10 in*

La ACL viene effettuata prima del routing

Router(config-if)# *ip access-group 10 out*

La ACL viene effettuata dopo il routing (impostazione di default)

Wildcard

Nel caso in cui occorra gestire l'accesso non più di un singolo host ma di una rete nella access-list bisogna ricorrere ad una mascheratura con una wildcard mask.
La mascheratura con Wildcard mask avviene all'inverso rispetto alla subnet mask.

Mascheriamo un singolo Host:
l'istruzione: ***Router(config)#*** *access-list pippo deny host 172.30.24.12*

diventa:	*Router(config)# access-list pippo deny 172.30.24.12*	*0.0.0.0*
Mascheriamo la rete 172.30.24.0:	*172.30.24.0*	*0.0.0.255*
La rete da 172.30.24.12 a 172.30.24.18:	*172.30.24.12*	*0.0.0.7*
Tutto (any):	*0.0.0.0*	*255.255.255.255*

0.0.0.0: corrispondenza esatta rispetto all'indirizzo indicato (host)
0.0.0.255: controlla che i primi 3 bytes dell'indirizzo corrispondano (rete di classe C)
0.0.0.7: controlla che i primi tre corrispondano (porzione di classe C)
255.255.255.255: qualunque indirizzo soddisfa il criterio

ACL standard ed estese differenze:

Nelle access-list standard il controllo viene effettuato solo sull'indirizzo sorgente
Nelle access-list estese il controllo può essere effettuato sia sull'indirizzo sorgente che destinatario.
Inoltre è possibile effettuare controlli su protocollo, numero di porta, e altri parametri.

Configurazione di ACL estesa:

Access-list {100-199}{deny-Permit}{Protocol}{Source}{SourceWildcard}
{Destination}{DestinationWildcard}{Equivalence}{PortNumber}
Il parametro equivalence Controlla il flusso dei pacchetti su una data "porta", di seguito si riportano alcuni parametri:

0-65535	Port number	finger	Finger (79)
bgp	Border Gateway Protocol (179)	ftp	File Transfer Protocol (21)
chargen	Character generator (19)	ftp-data	FTP data connections (used
cmd	Remote commands(rcmd, 514)		infrequently, 20)
daytime	Daytime (13)	gopher	Gopher (70)
discard	Discard (9)	hostname	NIC hostname server (101)
domain	Domain Name Service (53)	iden	Ident Protocol (113)
echo	Echo (7)	irc	Internet Relay Chat (194)
exec	Exec (rsh, 512)	klogin	Kerberos login (543)

kshell	Kerberos shell (544)	sunrpc	Sun Remote Procedure Call (111)
login	Login (rlogin, 513)	syslog	Syslog (514)
lpd	Printer service (515)	tacacs	TAC Access Control System (49)
nntp	Network News Transport Protocol (119)	talk	Talk (517)
pim-auto-rp	PIM Auto-RP (496)	telnet	Telnet (23)
pop2	Post Office Protocol v2 (109)	time	Time (37)
pop3	Post Office Protocol v3 (110)	uucp	Unix-to-Unix Copy Program(540)
smtp	Simple Mail Transport Protocol (25)	whois	Nicname (43)

1. www World Wide Web (HTTP, 80)In global configuration mode:

Definiamo la ACL 102 che applicheremo alla porta Ethernet in modo che la rete 172.30.24.12 / 172.30.24.18 sia destinataria di ip e tcp da parte di tutti.

Router(config)# *access-list 102 deny ip 172.30.24.12 0.0.0.7 any*

Router(config)# *access-list 102 permit tcp any 172.30.24.12 0.0.0.7 established*

Router(config)#*access-list 102 permit ip any 172.30.24.12 0.0.0.7*

Definiamo la ACL 103 che applicheremo alla porta seriale in modo che la rete 172.30.24.12 / 172.30.24.18 sia mittente di udp – tcp – icmp verso una specifica rete e di ip verso tutti tranne gli indirizzi specificati.

Router(config)# *access-list 103 permit udp 172.30.24.12 0.0.0.7 150.50.125.0 0.0.0.31 eq domain*

Router(config)# *access-list 103 permit tcp 172.30.24.12 0.0.0.7 150.50.125.0 0.0.0.31 gt 1023*

Router(config)# *access-list 103 permit tcp 172.30.24.12 0.0.0.7 host 150.50.126.5 eq www*

Router(config)# *access-list 103 permit icmp 172.30.24.12 0.0.0.7 150.50.0.0 0.0.127.255*

Router(config)# *access-list 103 permit icmp 172.30.24.12 0.0.0.7 199.33.0.0 0.0.127.255*

Router(config)# *access-list 103 deny ip 172.30.24.12 0.0.0.7 150.50.0.0 0.0.127.255*

Router(config)# access-list 103 deny ip 172.30.24.12 0.0.0.7 199.33.0.0 0.0.127.255

Router(config)# access-list 103 permit ip 172.30.24.12 0.0.0.7 any

2. In interface configuration mode:
   Applichiamo il gruppo di access-list 102 all'interfaccia Ethernet:
   Router(config-if)# ip access-group 102 out

   In interface configuration mode:
   Applichiamo il gruppo di access-list 103 all'interfaccia seriale:
   Router(config-if)# ip access-group 103 out

Cancellare una access-list:

La cancellazione della access-list deve essere sempre preceduta dalla rimozione da ogni interfaccia:

1. In interface configuration mode:
   Rimuoviamo la access-list dall'interfaccia Ethernet:
   Router(config-if)# no ip access-group 10
2. In global configuration mode:
   Cancelliamo la access-list 10
   Router(config)# no access-list 10

Modalità di filtering

Tutte le entry vengono esaminate sequenzialmente. E' quindi importante l'ordine in cui vengono definite.
Il passaggio alla entry successiva avviene solo se il test precedente non è soddisfatto.
Il sistema operativo cisco pone implicitamente la entry deny any alla fine di ogni ACL.
E' necessario perciò ricordarsi, nel caso si voglia negare alcuni hosts e permettere tutto il resto, di porre la entry "Permit Any" alla fine dell'access-list.