

Netexpert.it

*Progettare e realizzare una rete dati con
router Cisco.*

Premessa

Con questo documento si desidera presentare una serie di step da seguire per progettare ed implementare una rete di trasmissione dati, la quale prevede l'instradamento fra diverse sedi e verso Internet dei dati informatici, per quanto concerne il protocollo TCP/IP (essendo notevolmente il più diffuso).

Si affronteranno le configurazioni riguardanti traffico IPX (Reti Novell) o SNA (Reti IBM) in altro documento.

Nell'affrontare i vari punti, si cercherà di chiarire il come e il perché delle scelte, per permettere al fruitore di poter gestire il più autonomamente possibile la propria infrastruttura.

Nel documento troverete:

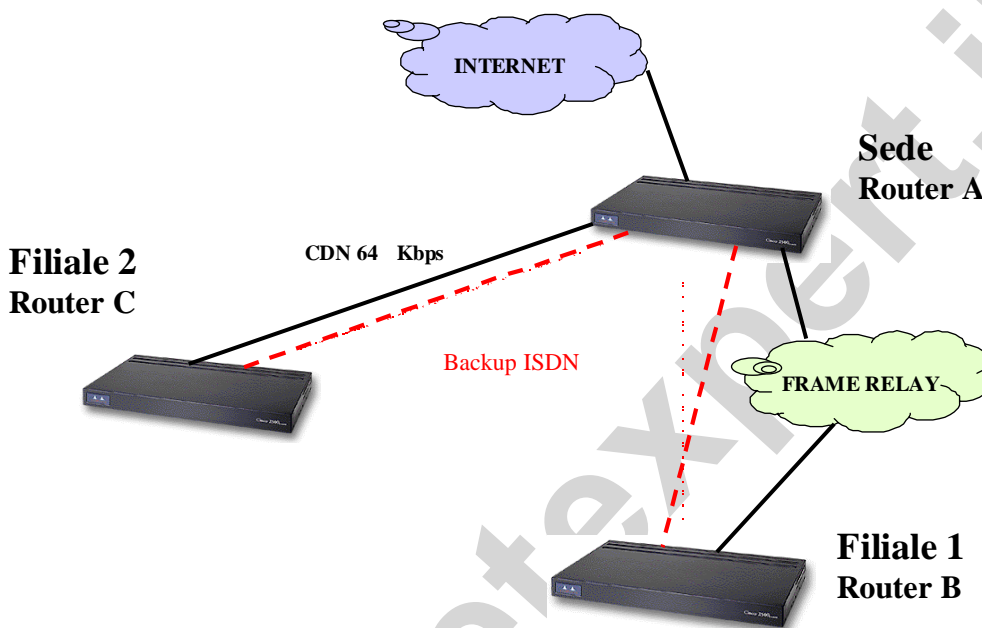
1	MODELLO	3
2	INDIRIZZI IP	3
2.1	Classe d'indirizzi	3
2.2	Indirizzi degli host e degli apparati	4
3	SCELTA DEGLI APPARATI	5
4	CONFIGURAZIONI	5
4.1	Accesso ai routers	5
4.2	Modalità di configurazione	8
4.3	Password	9
4.4	Interfacce Ethernet	10
4.5	Interfacce seriali	12
4.5.1	Linea CDN	12
4.5.2	Linea Frame Relay	13
4.6	Interfacce ISDN	15
4.7	Interfacce BRI	16
4.8	Interfacce Dialer	16
5	COLLEGAMENTO AD INTERNET	18
6	ROUTE	19
6.1	Route statiche	19
6.2	Routers remoti	20
6.3	Router centrale	21
7	CONFIGURAZIONI PARTICOLARI	21
7.1	Logon da remoto	21
8	CONSIDERAZIONI FINALI	22
9	CONFIGURAZIONI FINALI	23
10	SEDE (ROUTER A)	23
11	FILIALE 1 (ROUTER B)	25
12	FILIALE 2 (ROUTER C)	27

1 Modello

Il modello che adotteremo prevede la progettazione di una nuova rete, la quale sarà composta di tre sedi, delle quali una sarà considerata quella principale e le altre due, filiali remote.

Lo schema al quale faremo riferimento sarà il seguente:

Schema logico rete di trasmissione dati



Per la realizzazione delle connessioni geografiche, utilizzeremo tre router Cisco Systems (ad esempio della famiglia 2600), analizzando nel dettaglio le configurazioni che dovremo implementare per ottenere il collegamento.

2 Indirizzi IP

2.1 Classe d'indirizzi

Il primo passo da affrontare è decidere gli indirizzi che utilizzeremo per la nostra rete, siano essi pubblici o privati.

Normalmente, considerando che l'acquisto di indirizzi pubblici comporta un notevole costo, si decide che le macchine della rete privata utilizzino indirizzi privati per le connessioni interne (incluse quelle verso le filiali), mentre solo il router che dovrà connettersi verso l'esterno (Internet) dovrà necessariamente avere un indirizzo pubblico, per potersi connettere verso altre reti pubbliche. Questa soluzione non comporta alcun ostacolo per l'utilizzo di Internet da parte delle macchine private, in quanto sono integrate nei router funzioni di *NAT* e *PAT* (Network and Port Address Translation), che permettono, con un numero limitato di indirizzi, di "fare uscire" le macchine private "trasformando" gli indirizzi privati in pubblici, solo nel momento in cui è richiesta una connessione. Queste funzioni sono conosciute in ambito Unix/Linux come Masquerading, cioè mascherano i veri indirizzi, permettendo sia di avere meno indirizzi pubblici di quante sono le macchine, sia di nascondere all'esterno le workstations private.

Deciso che utilizzeremo indirizzi privati, resta da scegliere la classe da utilizzare.

Per reti di piccole dimensioni è uso comune scegliere indirizzi di Classe C (192.168.0.0 netmask 255.255.255.0), che consentiranno di avere 255 sottoreti e 254 host per ogni sottorete.

Lo standard ci lascia comunque molta libertà in merito a questo tipo di decisioni, permettendoci anche la scelta di indirizzi di Classe B (dalla rete 172.16.0.0 alla rete 172.31.0.0, netmask 255.255.0.0, 16 sottoreti per oltre 65.000 host ciascuna) o di classe A (10.0.0.0 netmask 255.0.0.0, oltre 16 milioni di host).

Per la nostra rete utilizzeremo indirizzi di classe C, ma è chiaro che per quanto concerne la configurazione della rete, questa decisione non cambia di molto le cose (si tratta solo di cambiare gli indirizzi IP alle interfacce).

2.2 Indirizzi degli host e degli apparati

Scelta la classe d'indirizzi, non rimane altro da fare che assegnare gli stessi agli hosts e, in prima istanza, agli apparati di networking che installeremo.

Di seguito trovate una tabella con un esempio di scelte possibili:

Tabella A

Rete	Netmask	Sede	Macchina	Indirizzo IP
192.168.1.0	255.255.255.0	Sede	Router A	192.168.1.1
			PDC	192.168.1.2
			BDC	192.168.1.3
			Mail Server	192.168.1.4
			Client	192.168.1.5 ÷ 192.168.1.254
192.168.2.0	255.255.255.0	Filiale 1	Router B	192.168.2.1
			PDC	192.168.2.2
			BDC	192.168.2.3
			Mail Server	192.168.2.4
			Client	192.168.2.5 ÷ 192.168.2.254
192.168.3.0	255.255.255.0	Filiale 2	Router C	192.168.3.1
			Client	192.168.3.2 ÷ 192.168.3.254
192.168.254.0	255.255.255.252	Frame-Relay Sede-Filiale 1	Router A	192.168.254.1
192.168.254.4	255.255.255.252	CDN 64 kbps Sede-Filiale 2	Router B	192.168.254.2
			Router A	192.168.254.5
192.168.254.8	255.255.255.252	Backup ISDN Sede-Filiale 1	Router C	192.168.254.6
			Router A	192.168.254.9
192.168.254.12	255.255.255.252	Backup ISDN Sede-Filiale 2	Router B	192.168.254.10
			Router A	192.168.254.13
			Router C	192.168.254.14

Per rendere più completo possibile l'esempio, adotteremo le seguenti scelte:

- La connessione ad Internet della sede sarà realizzata mediante il collegamento ISDN verso un ISP (Internet Service Provider), per poter commentare una configurazione con indirizzo IP assegnato al momento del collegamento;

- Nella sede e nella filiale 1 sono presenti i server, sia di dominio (PDC, BDC nell'ipotesi Windows NT), sia di posta (Mail Server), mentre nella filiale 2 sono presenti solo client, i quali dovranno necessariamente autenticarsi al PDC (o al BDC) della sede;

3 Scelta degli apparati

Il passo successivo è quello di decidere il tipo di apparati da acquistare per realizzare la nostra rete. Nelle nostre scelte decidiamo i tre routers da adottare, lasciando ad altra sede il compito di scegliere i vari server e gli apparati di livello 2 per collegare gli host alla rete (hub o preferibilmente switch). Nella scelta dobbiamo tenere in considerazione vari parametri:

- Il numero di hosts da collegare alla rete Ethernet;
- Il livello di sicurezza che desideriamo ottenere, per decidere il numero di interfacce Ethernet di cui avremo bisogno;
- Il numero e il tipo di servizi che vorremo gestire (per esempio se desideriamo pubblicare un sito Web all'interno della nostra rete);
- Il numero di collegamenti geografici ai quali andrà connesso il router (ISDN, CDN, Frame-Relay, ecc.);
- La necessità di scalabilità futura della rete.

In base a queste considerazioni, essendo la nostra rete molto semplice e non avendo bisogno di configurazioni particolari, scegliamo 3 routers Cisco della famiglia 2600, che ci permettono comunque, grazie alla loro modularità, di lasciarci notevole spazio in futuro per eventuali ampliamenti.

Inizialmente inseriamo i moduli e le interfacce necessarie, che ci permettono di avere le porte Ethernet per il collegamento alla LAN locale, porte seriali per il collegamento alla rete geografica (CDN o Frame Relay) e interfacce ISDN per l'interfacciamento alla linea telefonica digitale (per realizzare collegamenti di backup).

I due routers delle filiali hanno bisogno di una scheda con un'interfaccia seriale per il collegamento alla rete geografica "always-on" (CDN e Frame-Relay) e di una scheda BRI (Basic Rate Interface), per il collegamento alla rete ISDN (Backup).

Nel router della sede principale c'è bisogno di due interfacce seriali, per il collegamento con le due filiali, di 1 scheda BRI per il backup delle due filiali (considerando che un collegamento ISDN base consta di due canali a 64kbps), nonché di un'ulteriore scheda BRI per il collegamento ad Internet.

4 Configurazioni

Una volta acquistati gli apparati e installate le tre reti locali (LAN), si tratta di configurare i tre routers per permettere la comunicazione fra le tre sedi.

4.1 Accesso ai routers

La prima configurazione del router si deve realizzare mediante una connessione seriale alla sua porta di console, non avendo ancora un indirizzo IP valido sulla sua porta Ethernet. In seguito, per verifiche, controlli e modifiche alla configurazione, potremo raggiungere il router con una semplice connessione Telnet.

Per collegarsi alla porta di console è sufficiente un PC con un programma di emulazione di terminale (il comune Hyper Terminal è quanto serve), configurandolo per una connessione locale (porta seriale COM1 ad esempio), con i seguenti parametri:

- 9.600 bit per secondo
- 8 data bits
- N (disabilitata) parità

- 1 bit di stop
- N (disabilitato) controllo di flusso

Realizzata la connessione possiamo iniziare a configurare il router.
Ci troviamo presumibilmente in questa situazione:

Router>

Con questa notazione (simbolo di maggiore dopo il nome del router), il router ci indica che ci troviamo in User EXEC Mode (modalità utente), situazione nella quale siamo limitati a poche semplici operazioni; dobbiamo quindi spostarci nella modalità privilegiata (Privileged EXEC Mode), mediante il comando

Router>enable
Router#

Il router ci indica, cambiando il prompt in cancelletto (#), che siamo nella modalità privilegiata. In questa situazione possiamo accedere a tutte le funzioni del router, ma non cambiare la sua configurazione.

Possiamo, ad esempio, visualizzare la configurazione attiva in questo momento nel router, mediante il comando

Router#show running-configuration

Building configuration...

Current configuration:

!
version 12.0
service udp-small-servers
service tcp-small-servers
!
hostname Router
!
interface Ethernet0
no ip address
no ip directed-broadcast
shutdown
!
!
interface Serial0/0
no ip address
no ip directed-broadcast
shutdown
!
interface Serial0/1
no ip address
no ip directed-broadcast
shutdown
!
interface BRI1/0
no ip address

```

no ip directed-broadcast
shutdown
!
interface BRI1/1
no ip address
no ip directed-broadcast
shutdown
!
line con 0
transport input none
line aux 0
transport input all
line vty 0 4
!
end

```

Analizzando l'output notiamo che le varie interfacce sono tutte in stato di *shutdown* amministrativo e che non ci sono configurazioni particolari attive.

Per visualizzare la configurazione attualmente salvata in memoria non volatile (NVRAM), dobbiamo utilizzare il comando *show startup-configuration*. L'output del comando è, nella forma, identico a *show running-configuration*, la differenza sta nel modo in cui il router utilizza le due configurazioni.

All'accensione, dopo aver caricato il sistema operativo (IOS), verifica se nella memoria non volatile esiste una configurazione (*startup-configuration*), dopo di che la carica nella RAM e la esegue (*running-configuration*).

Le modifiche effettuate alla configurazione si ripercuotono su quella attualmente operativa (*running*), per questo se vogliamo rendere definitive eventuali modifiche, dobbiamo salvare in memoria non volatile la configurazione, con il comando:

```
Router#copy running-configuration startup-configuration
```

il quale indica al router di salvare in memoria la configurazione che sta attualmente utilizzando.

Per entrare in modalità di configurazione dobbiamo inserire un ulteriore comando

```
Router#configuration terminal
Router(conf)#
```

che indica al router di accettare i comandi di configurazione che inseriremo dal terminale.

Notazioni sulla filosofia dell'IOS

Quando il router è nuovo, ci permette di accedere a tutte le sue funzionalità senza richiedere alcuna password di protezione; spetta a noi inserirle nella configurazione.

- L'IOS implementa la funzione di completamento dei comandi, che ci permette sia di completarli con il tasto <TAB>

```
Router#conf <TAB>
Router#configuration
```

Sia di non scriverli completamente, nel caso siano già univoci

Router>en (è sottinteso che si tratti del comando di *enable*)

- L'IOS implementa la funzionalità di help, mediante l'uso del carattere punto interrogativo (?)

Questo carattere può essere digitato sia da solo (senza battere il tasto <ENTER>), elencandoci tutti i comandi disponibili

Router>?

sia seguito da una parte di comando, elencandoci tutti i comandi che iniziano con la parte da noi digitata

Router>en?

enable

Router>en

sia staccati dal comando, dandoci una breve descrizione di cosa fa lo stesso, nonché indicandoci ulteriori parametri da indicare

Router>enable ?

<0-15> Enable level

<cr>

Router>enable

A questo punto possiamo inserire i comandi di configurazione uno di seguito all'altro.

Da notare che l'output del comando *show running-configuration* indica esattamente i comandi da digitare nella configurazione, dandoci un aiuto nel realizzare la stessa.

Inoltre i comandi sono indicati a colonne sfalsate, quelli allineati più a sinistra sono da inserire in modalità di configurazione generale

Router(conf)#

Mentre quelli allineati più a destra sono da inserire in particolari modalità di configurazione, ad esempio quelli indicati di seguito

interface Ethernet0

no ip address

no ip directed-broadcast

shutdown

sono da inserire nella modalità di configurazione dell'interfaccia Ethernet.

4.2 Modalità di configurazione

Ognuno può adottare il metodo che preferisce per realizzare una corretta configurazione, la cosa importante è seguire una traccia che possibilmente sia sempre la stessa: si eviterà di dimenticare delle parti importanti.

A titolo d'esempio ne sarà adottato uno, si tenga comunque presente che non è assolutamente obbligatorio seguirlo alla lettera, l'importante è realizzare tutti i passi, nell'ordine che si preferisce.

4.3 Password

Iniziamo con la configurazione delle password.

Si è già detto di come i livelli di accesso al router siano diversi, così anche le password si associano ai livelli.

Sicuramente la password più importante è quella che ci viene richiesta per accedere in modalità comandi privilegiata, dalla quale si può controllare completamente il router, fino ad arrivare a poter cancellare la memoria o anche il sistema operativo.

Per impostarla bisogna essere in modalità privilegiata ed entrare in modalità di configurazione generale, dopo di che digitare il comando *enable password* seguito dalla password che desideriamo impostare.

Si può anche impostare una password *secret*, la quale ha sempre priorità rispetto a quella normale (in pratica, se sono impostate entrambe, quella corretta da digitare è *secret*).

La differenza fondamentale tra le due è che, nella visualizzazione della configurazione (con il comando *show running-config* piuttosto che *show startup-config*), quella di *secret* è mostrata criptata.

È comunque possibile visualizzare tutte le password come criptate, semplicemente attivando il servizio di *password-encryption*.

```
Router>enable
Password: *****
Router#configure terminal
Router(config)#service password-encryption
```

È sufficiente impostarne una sola perché ci venga richiesta.

La sequenza di comandi è la seguente:

```
Router>enable
Password: *****
Router#configure terminal
Router(config)#enable password cisco
Router(config)#enable secret cisco
Router(config)#
```

Impostata la password di *enable* (o di *secret*), possiamo passare alle password di accesso del router in modalità utente.

Visto che al router si può accedere o fisicamente tramite la porta di console, oppure tramite il protocollo telnet sulle porte virtuali, dovremo impostare le password per entrambi i tipi di accesso.

Per fare questo dobbiamo entrare in modalità di configurazione delle porte (*line*) e indicare al router che ci richieda il *login* ad ogni tentativo d'accesso.

La sequenza di comandi da dare è la seguente:

```
Router(config)#line console 0
Router(config-line)#login
Router(config-line)#password cisco
Router(config)#line vty 0 4
Router(config-line)#login
Router(config-line)#password cisco
```

Router(config)#

Ovviamente *cisco* è la password usata come esempio, da sostituire a discrezione dell'amministratore di rete. Si tenga in considerazione che è molto importante, a livello di sicurezza, un buon controllo (e scelta) delle password di accesso. Ad esempio si può decidere di cambiarle ad intervalli di tempo prestabiliti.

Lasciamo ad altri il compito di descrivere nel dettaglio funzionalità e politiche per la sicurezza.

4.4 Interfacce Ethernet

A questo punto possiamo passare alla configurazione dell'interfaccia Ethernet, che ci permetterà di comunicare con il router sulla rete locale, nonché di abbandonare la configurazione da console per passare a quella più pratica via telnet.

Per configurare la porta Ethernet dobbiamo entrare in modalità di configurazione generale, da qui passare alla configurazione dell'interfaccia.

I comandi indispensabili affinché la porta si attivi, sono quelli con i quali assegniamo l'indirizzo IP e quelli per disabilitare lo stato di *shutdown* amministrativo.

Per ora tralasciamo ulteriori possibili comandi, che in generale permettono di ottimizzare il funzionamento o di realizzare funzioni particolari, ma del tutto superflui per l'attivazione.

Da qui in avanti utilizzeremo i comandi nella loro forma completa solo la prima volta che verranno indicati, dopo di che saranno usati quelli nella forma ridotta, per permettere al lettore di prendere confidenza con quelli che verranno effettivamente utilizzati, essendo i comandi ridotti decisamente più comodi di quelli completi.

Per esempio il comando *int eth 0* corrisponde a *interface ethernet 0*.

La sequenza di comandi da digitare è la seguente:

```
Router>enable
Password:*****
Router#conf t
Router(config)#interface ethernet 0
Router(config-if)#description Interfaccia Ethernet verso rete LAN locale
Router(config-if)#ip address 192.168.1.1
Router(config-if)#no shutdown
Router(config-if)#
```

Il comando *description* è di tipo esclusivamente descrittivo (come suggerisce il nome) e ci aiuterà in futuro, quando visualizzeremo l'output della configurazione, a ricordarci il tipo di interfaccia .

Nel nostro caso non è indispensabile, ma per configurazioni più complesse può risultare molto utile. Per l'esempio abbiamo preso in considerazione la porta Ethernet del Router A (sede); per la configurazione delle porte Ethernet dei Router B e C delle Filiali 1 e 2 i comandi sono gli stessi, con la differenza dell'indirizzo IP (*ip address*), che troviamo nella tabella A.

A questo punto possiamo collegare fisicamente la porta Ethernet alla nostra rete, con un cavo straight verso un apparato attivo, che sia esso uno switch o un hub.

Dopodiché possiamo verificare che tutto sia andato nel modo corretto, utilizzando il comando di stato *show interface ethernet 0*, il cui output ci indica lo stato della porta.

Ad esempio un output corretto è il seguente:

```
Router#show int eth 0
Ethernet0 is up, line protocol is up
Hardware is Lance, address is 00e0.1e3e.ae9b (bia 00e0.1e3e.ae9b)
Internet address is 192.168.1.1/24
MTU 1500 bytes, BW 10000 Kbit, DLY 1000 usec, rely 255/255, load 1/255
Encapsulation ARPA, loopback not set, keepalive set (10 sec)
ARP type: ARPA, ARP Timeout 04:00:00
Last input 00:00:00, output 00:00:00, output hang never
Last clearing of "show interface" counters never
Queueing strategy: fifo
Output queue 0/40, 0 drops; input queue 1/75, 0 drops
5 minute input rate 1000 bits/sec, 1 packets/sec
5 minute output rate 1000 bits/sec, 1 packets/sec
 393015 packets input, 60916476 bytes, 0 no buffer
 Received 30979 broadcasts, 0 runts, 0 giants, 0 throttles
  1 input errors, 0 CRC, 0 frame, 0 overrun, 1 ignored, 0 abort
 0 input packets with dribble condition detected
635814 packets output, 438334976 bytes, 0 underruns
 0 output errors, 1079 collisions, 15 interface resets
 0 babbles, 0 late collision, 808 deferred
 0 lost carrier, 0 no carrier
 0 output buffer failures, 0 output buffers swapped out
```

Notiamo che lo stato dell'interfaccia è *up* (attiva), questo si riferisce allo stato fisico dell'interfaccia. Inoltre anche il protocollo è *up* e questo si riferisce al fatto che il router rileva il carrier dell'Ethernet (in pratica il cavo è attaccato, nel caso non fosse così lo stato sarebbe *up* mentre il protocollo sarebbe *down*).

Possiamo comunque verificare la connettività con un semplice comando di *ping*, o dal router verso una macchina della LAN o viceversa.

Ad esempio, da un prompt di DOS digitiamo:

```
C:\>ping 192.168.1.1
```

```
pinging 192.168.1.1 with 32 byte of data
```

```
Reply from 192.168.1.1: bytes=32 time<10ms TTL=128
Reply from 192.168.1.1: bytes=32 time<10ms TTL=128
Reply from 192.168.1.1: bytes=32 time<10ms TTL=128
Reply from 192.168.1.1: bytes=32 time<10ms TTL=128
```

```
Ping statistics for 192.168.1.1:
```

```
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
```

```
Approximate round trip times in milli-seconds:
```

```
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

In questo caso l'output del comando ci indica che esiste connettività fra l'host e il router.

“Risposte” differenti (ad esempio Destination host unreachable) ci indicherebbero che non si riesce a raggiungere il router, per motivi che potrebbero essere di vario genere.

4.5 Interfacce seriali

A questo punto, stabilita una connessione attiva tra il router e la rete LAN locale attivando l'interfaccia Ethernet, possiamo passare a stabilire le connessioni geografiche tra la sede e le filiali, attivando le interfacce seriali.

A seconda della connessione geografica disponibile, varierà la configurazione dell'interfaccia seriale (per il nostro esempio abbiamo preso in considerazione una connessione su linea dedicata CDN e una su linea Frame Relay).

4.5.1 Linea CDN

La configurazione di una connessione geografica su linea dedicata CDN è veramente semplice. In pratica, come per la Ethernet, è sufficiente indicare l'indirizzo IP e togliere dallo stato di *shutdown* amministrativo l'interfaccia.

I comandi da dare sono i seguenti (per il nostro esempio della connessione fra la sede e la filiale 2):

```
RouterA>enable
Password:*****
RouterA#conf t
RouterA(config)#int serial 0/1
RouterA(config-if)#ip address 192.168.254.5 255.255.255.252
RouterA(config-if)#no shutdown
```

Una volta che su entrambi i router sono state attivate le interfacce seriali, dando a queste un indirizzo della stessa rete (192.168.254.4), la connessione fra i due è stabilita.

Possiamo verificarlo prima con il comando di stato *show ip int brief*, poi eseguendo un comando *ping* da un router, verso l'interfaccia seriale dell'altro.

```
Router#show ip int brief
```

Interface	IP-Address	OK?	Method	Status	Protocol
Ethernet0	192.168.1.1	YES	NVRAM	up	up
Serial0/0	unassigned	YES	unset	up	up
Serial0/0.1	192.168.254.1	YES	NVRAM	up	up
Serial0/1	192.168.254.5	YES	unset	up	up
BR1/0	unassigned	YES	unset	administratively down	down
BR1/1	unassigned	YES	unset	administratively down	down

```
Router#ping 192.168.254.6
```

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 192.168.254.6, timeout is 2 seconds:

!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 1/4/8 ms

```
Router#
```

Questo comando (*show ip int brief*) è molto utile, perché ci indica in maniera concisa (*brief*=riassunto), lo stato fisico di tutte le interfacce (con i loro protocolli), permettendoci con un veloce colpo d'occhio di verificare quali siano attive e quali no.

In questo caso il protocollo di *encapsulation* utilizzato dai due end-point per comunicare è quello proprietario Cisco, il *HDLC*.

È preferibile cambiarlo in *point-to-point* (ppp), più performante e con più possibilità del HDLC (ad esempio l'autenticazione).

I comandi per settarlo sono i seguenti:

```
RouterB>enable
Password:*****
RouterB#conf t
RouterB(config)#int serial 0/1
RouterB(config-if)#encapsulation ppp
RouterB(config-if)#
```

Ovviamente è una configurazione da realizzare su entrambi i router, quindi si ponga attenzione a come si imposta.

Ad esempio, se fossimo fisicamente in sede e desiderassimo cambiare la configurazione del router della filiale, senza necessariamente andare là, i passi da seguire dovrebbero essere:

- Collegarsi con una sessione telnet al router della filiale
- Cambiare nel router della filiale l'*encapsulation* (a questo punto la sessione di telnet cadrà, visto che nel router locale è ancora attiva l'*encapsulation HDLC*)
- Cambiare nel router locale l'*encapsulation* sulla seriale
- Verificare la connettività, che dovrà a questo punto essere attiva

Si tenga presente che, se si cambiasse l'*encapsulation* prima sul router al quale siamo connessi localmente, la connessione con quello remoto non sarebbe più possibile. Ma non ci preoccupiamo, basterebbe ripristinare la configurazione di prima ed ecco che la connessione sarebbe ripristinata.

4.5.2 Linea Frame Relay

Per attivare una connessione geografica su linea Frame Relay abbiamo bisogno di alcuni parametri di linea, che ci vengono normalmente comunicati dal fornitore della linea stessa.

Una linea Frame Relay si “appoggia” ad uno switch Frame Relay, al quale possono essere connesse 1024 linee, per questo dobbiamo sapere l'indirizzo di livello 2 della linea alla quale siamo connessi, Questo parametro si chiama *dlci* (data-link connection identifier) e deve essere unico in ogni switch, quindi nella nostra sede e nella filiale potremmo avere lo stesso *dlci*, come potrebbero anche essere diversi.

Inoltre i due estremi della connessione Frame Relay (DCE e DTE), per controllare la funzionalità della stessa, utilizzano un protocollo che si chiama *LMI* (Local Management Interface), il quale esiste in vari formati (cisco, ansi, q933a).

La differenza principale fra i vari tipi di *LMI* sta nel *dlci* che utilizzano i due end-point per scambiarsi i messaggi (il 1023 cisco e q933a, lo 0 ansi), oltre al formato degli stessi messaggi; risulta quindi indispensabile indicare nella configurazione anche questo parametro.

A partire dalla versione di IOS 11.2 è supportato l'*LMI autosensing*, in ogni caso per evitare confusioni è preferibile indicare in modo univoco il tipo.

Stabiliti i parametri indispensabili per poter attivare la connessione, possiamo configurare il router. È consigliabile configurare delle sotto-interfacce, visto che le linee frame-relay sono di tipo logico, quindi è possibile con lo stesso modem fisico realizzare più connessioni logiche.

Realizzando delle sotto-interfacce sarà possibile in futuro, utilizzando la stessa interfaccia fisica, collegare ulteriori linee al router.

I parametri fisici vanno settati sull'interfaccia reale (tipo di *encapsulation*, *lmi-type*), mentre quelli logici sulla sotto-interfaccia (indirizzo IP, *dlci*).

I comandi in sequenza sono i seguenti:

```
RouterA>enable
Password:*****
RouterA#conf t
RouterA(config)#int serial 0/0
RouterA(config-if)#description Interfaccia seriale su linea Frame-Relay (fisica)
RouterA(config-if)#encapsulation frame-relay
RouterA(config-if)#frame-relay lmi-type ansi
RouterA(config-if)#no shutdown
RouterA(config-if)#int serial 0/0.1
RouterA(config-subif)#description Interfaccia verso Filiale 1 (logica)
RouterA(config-subif)#ip address 192.168.254.1 255.255.255.252
RouterA(config-subif)#frame-relay interface-dlci 10
RouterA(config-subif)#
```

Le cose fondamentali che si notano sono il tipo di *encapsulation* (che potrebbe anche essere del tipo *IETF*, in questo caso si tratterebbe di usare il comando *encapsulation frame-relay ietf*), il tipo di *lmi* (di cui si è detto in precedenza), l'indirizzo IP e il *dlci*.

A questo punto, se tutto è stato eseguito correttamente (soprattutto se i parametri sono giusti!! non facciamoci ingannare se la linea non funziona, prima verifichiamo che ci siano stati detti quelli corretti!!), la linea dovrebbe passare allo stato attivo.

Lo possiamo verificare con il comando:

```
Router#show ip int brief
Interface      IP-Address      OK? Method      Status          Protocol
Ethernet0      192.168.1.1     YES NVRAM          up              up
Serial0/0      unassigned      YES unset         up              up
Serial0/0.1    192.168.254.1  YES NVRAM          down            down
Serial0/1      unassigned      YES unset         administratively down down
BR11/0         unassigned      YES unset         administratively down down
BR11/1         unassigned      YES unset         administratively down down
Router#
```

L'output precedente ci indica che l'interfaccia fisica si è attivata correttamente (Serial 0/0), mentre l'interfaccia logica è ancora "down", visto che l'altro end-point (RouterB della filiale remota) non è ancora stato configurato.

Una volta che sull'altra estremità del collegamento attiveremo la configurazione corretta, troveremo il seguente output:

```
Router#show ip int brief
Interface      IP-Address      OK? Method      Status          Protocol
Ethernet0      192.168.1.1     YES NVRAM          up              up
Serial0/0      unassigned      YES unset         up              up
Serial0/0.1    192.168.254.1  YES NVRAM          up              up
Serial0/1      unassigned      YES unset         administratively down down
BR11/0         unassigned      YES unset         administratively down down
```

```
BRI1/1      unassigned  YES  unset      administratively down  down
Router#
```

che indica il collegamento (fisico e logico) realmente attivo.

Ovviamente rimangono disattivate le interfacce che non abbiamo ancora configurato.

Possiamo verificare la connettività con il solito comando *ping* dal RouterA, verso il RouterB:

```
Router#ping 192.168.254.2
```

```
Type escape sequence to abort.
```

```
Sending 5, 100-byte ICMP Echos to 192.168.254.2, timeout is 2 seconds:
```

```
!!!!
```

```
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/4/8 ms
```

```
Router#
```

I punti esclamativi indicano che i pacchetti sono stati correttamente ricevuti.

Abbiamo raggiunto il primo risultato, la sede è connessa a livello geografico, tramite il protocollo IP, con la prima filiale!!

A questo punto abbiamo stabilito le connessioni fra le sedi, ci resta da configurare quelle di backup e verso Internet su linea ISDN.

4.6 Interfacce ISDN

La prima cosa da fare quando si configurano interfacce su linea pubblica ISDN, è indicare al router a che tipo di linea viene collegato.

Per l'Europa i due tipi possibili sono il *basic-net3* (per le BRI, vedi sotto) e il *primary-net5* (per le PRI), e lo dobbiamo impostare dalla configurazione generale, nel seguente modo:

```
RouterA>enable
```

```
password: *****
```

```
RouterA#conf t
```

```
RouterA(config)#isdn switch-type basic-net3
```

```
RouterA(config)#
```

Dobbiamo inoltre indicare al router di “negoziare” con la centrale telefonica l'identificativo della chiamata (TEI), quando effettua la prima chiamata, con il comando

```
RouterA(config)#isdn tei-negotiation first-call
```

Una volta indicati questi parametri, possiamo passare alla configurazione delle interfacce vere e proprie.

Le interfacce fisiche (quelle che vengono collegate con un cavetto RJ45 alla borchia telefonica), sono indicate nel router come BRI (Basic Rate Interface) per quelle a due canali e PRI (Primary Rate Interface) per quelle a 31 canali.

Siccome l'interfaccia BRI (quella che analizzeremo nel nostro caso, ma si tenga in considerazione che per le PRI il discorso non è molto diverso, cambiando solo il numero di canali) può gestire due canali, è conveniente realizzare la configurazione realizzando delle interfacce logiche, che vengono chiamate *Dialer*.

In questo modo è possibile, sfruttando la stessa interfaccia fisica, realizzare connessioni verso punti differenti.

Nello specifico ciò risulta molto utile, potendo usare una BRI per la connessione di backup verso le filiali (due canali), e l'altra per la connessione ad Internet (scegliendo di usare o 64kbps o 128kbps, usando entrambi i canali).

4.7 Interfacce BRI

Sull'interfaccia fisica dobbiamo indicare il tipo di *encapsulation* (in questo caso *ppp*, trattandosi di un collegamento punto-punto), il *dialer pool* di cui fa parte (dello stesso *dialer pool* faranno parte le interfacce *Dialer* che la utilizzano) ed il tipo di protocollo da utilizzare per l'autenticazione (*PAP* o *CHAP*).

```
RouterA(config)#int bri1/0
RouterA(config-if)#description "Interfaccia ISDN"
RouterA(config-if)#encapsulation ppp
RouterA(config)#dialer pool-member 1
RouterA(config)#ppp authentication chap
RouterA(config)#
```

4.8 Interfacce Dialer

Per configurare correttamente le interfacce Dialer (dopo averle create con il comando *interface Dialer*), la prima cosa da fare è associarle all'interfaccia fisica (BRI) che utilizzano per effettuare la chiamata (*dialer pool*).

```
RouterA(config-if)#int dialer1
RouterA(config-if)#dialer pool 1
RouterA(config-if)#
```

Dobbiamo poi indicare l'indirizzo IP ed il numero di telefono da chiamare (*dialer-string*). Inoltre, con il comando *dialer idle-timeout*, indichiamo al router dopo quanto tempo di inattività della linea deve "abbattere" la connessione. Senza questa configurazione la chiamata rimarrebbe attiva.

```
RouterA(config-if)#description "Interfaccia di backup verso Filiale1"
RouterA(config-if)#ip address 192.168.254.9 255.255.255.252
RouterA(config-if)#dialer string 01234567
RouterA(config-if)#dialer idle-timeout 300
RouterA(config-if)#dialer-group 1
RouterA(config-if)#
```

Discorso a parte merita il comando *dialer-group*: esso si associa con una *dialer-list*, che viene creata "al di fuori" dell'interfaccia, ed indica al router il traffico da considerare "interessante" per attivare la chiamata. Non bisogna confonderla con un'*access-list*, visto che con quest'ultima possiamo permettere o negare il transito di un determinato traffico, mentre la *dialer-list* indica solo il traffico che deve "alzare" la linea telefonica. Una volta che la linea è up, il traffico da instradare non viene più influenzato dalla *dialer-list*, ma eventualmente, da un'*access-list*.

```
RouterA(config)#dialer-list 1 protocol ip permit
RouterA(config)#
```

In questo modo solo il traffico IP potrà attivare una connessione ISDN.

Inoltre è conveniente (ma non indispensabile) utilizzare un protocollo di autenticazione, che permetta al router di identificare l'altro router che lo chiama. Per fare questo dobbiamo indicare il tipo di *authentication* da utilizzare (conviene utilizzare *CHAP*) e il nome e la password da utilizzare per la connessione.

Autenticazioni

I due tipi di autenticazione che ci permette di usare il protocollo *ppp* sono il *PAP* (Password Authentication Protocol) e il *CHAP* (Challenge Handshake Authentication Protocol).

L'idea di tutti e due i protocolli è quella che il router che effettua la chiamata invii all'altro router un'identificativo (*username*) e una *password*, in modo da permettere il riconoscimento.

La differenza maggiore tra i due protocolli (che rende il *CHAP* quello preferibile da usare) è che il *PAP* trasmette *username* e *password* in chiaro sulla linea, mentre il *CHAP* utilizza il protocollo di *encryption* MD5 (Message Digest 5) per scambiare le informazioni.

In pratica la sequenza che si verifica è la seguente:

- il router chiamante effettua la chiamata;
- il router chiamato "chiede" al router chiamante di inviargli *username* e *password*, insieme alla richiesta invia un numero casuale (*challenge*);
- il router chiamante effettua una funzione (*hash*) fra lo *username*, la *password* e il numero casuale ricevuto, ottenendo una stringa criptata che invia al router chiamato;
- il router chiamato effettua la stessa operazione, per verificare che il chiamante sia autorizzato alla connessione, che a questo punto viene stabilita.

Considerando che nel nostro caso vogliamo dare l'opportunità sia al router centrale sia ai due periferici di effettuare la chiamata, in caso di *failure* del link *always-on*, dobbiamo indicare nella configurazione sia come autenticarsi quando è il chiamante, sia come autenticare il router remoto quando riceve la chiamata.

Per semplicità si utilizzano come *username* l'*hostname* del router, come *password* quella di *enable*.

Quindi resta solo da indicare al router quali altri router hanno il permesso di collegarsi con lui.

Questo viene fatto in modalità di configurazione generale, indicando *username* e *password* dei router remoti.

```
RouterA>en
Password:*****
RouterA#conf t
RouterA(config)#username RouterB password cisco
RouterA(config)#username RouterC password cisco
RouterA(config)#
```

Questa configurazione va realizzata anche sui router remoti, indicando *username* e *password* di quello principale.

```
RouterB>en
Password:*****
RouterB#conf t
RouterB(config)#username RouterA password cisco
RouterB(config)#
```

A questo punto i router sono in grado di instaurare una connessione su linea ISDN tra di loro, resta da indicare quale interfaccia utilizzare quando esiste traffico da instradare. Come indicarlo al router è spiegato nella sezione Route.

5 Collegamento ad Internet

Per il collegamento ad Internet dobbiamo configurare la seconda interfaccia BRI (ISDN), per poterci collegare all'ISP (Internet Service Provider).

Una volta che il router sarà collegato con l'ISP, questi assegnerà un indirizzo IP (*ip address negotiated*); questa è l'unica grossa differenza nella configurazione della BRI verso Internet da quella verso le sedi remote.

La configurazione da realizzare è la seguente:

```
RouterA>en
Password:*****
RouterA#conf t
RouterA(config)#int bri 1/1
RouterA(config-if)#description "Interfaccia ISDN"
RouterA(config-if)#encapsulation ppp
RouterA(config-if)#dialer pool-member 2
RouterA(config-if)#ppp authentication chap
RouterA(config-if)#int dialer 3
RouterA(config-if)#ip address negotiated
RouterA(config-if)#dialer pool 2
RouterA(config-if)#dialer string 0123123
RouterA(config-if)#ppp chap hostname UTENTE
RouterA(config-if)#ppp chap password PASSWORD
RouterA(config-if)#
```

Con le istruzioni *ppp chap hostname UTENTE* e *ppp chap password PASSWORD*, indichiamo al router lo username e la password con le quali l'ISP autentica la nostra connessione.

Realizzata la connessione, si tratta di dividerla con il resto della rete.

Per fare questo dobbiamo configurare il NAT (Network Address Translation), visto che i PC interni hanno indirizzi privati, con i quali non potrebbero comunicare con siti pubblici.

Più precisamente configureremo il PAT (Port Address Translation), che permetterà di utilizzare l'unico indirizzo IP pubblico (quello che l'ISP ha assegnato al router) a tutte le macchine della rete. Il principio del PAT è molto semplice: quando un PC con un indirizzo privato richiede di comunicare verso l'esterno, il router, in una propria tabella interna, crea un'associazione tra una propria porta TCP e l'indirizzo privato; in questo modo è in grado di attivare molte sessioni verso l'esterno, nello stesso tempo tenere traccia da quale host erano state aperte.

Per configurarlo correttamente, dobbiamo definire il pool di indirizzi privati che hanno l'accesso alle funzionalità di NAT, con un'access list, nel seguente modo:

```
RouterA>en
RouterA#conf t
RouterA(config)#access-list 1 permit 192.168.1.0 0.0.0.255
RouterA(config)#access-list 1 permit 192.168.2.0 0.0.0.255
RouterA(config)#access-list 1 permit 192.168.3.0 0.0.0.255
RouterA(config)#
```

In questo modo definiamo le tre reti (sede e due filiali) che potranno utilizzare il PAT.

A questo punto dobbiamo associare questa lista al NAT, insieme all'interfaccia che utilizzeremo per il collegamento ad Internet (la Dialer3).

Infine indichiamo al Router in quali interfacce deve usare il PAT, in ingresso (porta Ethernet) e in uscita (Dialer3).

I comandi per la configurazione sono:

```
RouterA(config)#ip nat inside source list 1 interface Dialer3 overload
RouterA(config)#int eth0
RouterA(config-if)#ip nat inside
RouterA(config-if)#int dailer3
RouterA(config-if)#ip nat outside
RouterA(config-if)#int ser0/0.1
RouterA(config-if)#ip nat inside
RouterA(config-if)#int ser0/1
RouterA(config-if)#ip nat inside
RouterA(config-if)#
```

In questo modo il router utilizzerà l'indirizzo assegnato dal provider (che verrà acquisito dall'interfaccia Dialer3), per “traslare” gli indirizzi reali delle 3 reti.

Con i comandi *ip nat inside* e *ip nat outside* indichiamo al router quale è la rete interna e quale quella esterna.

Dobbiamo indicare che anche sulle interfacce seriali venga utilizzato il NAT, in modo che anche le filiali remote possano utilizzare questa funzionalità.

6 Route

Una volta attivate tutte le interfacce su tutti i router, si tratta di indicare agli stessi i “percorsi” da far seguire ai dati che vengono trasmessi al di fuori della rete (questo è il “compito” di un router).

L'operazione è piuttosto semplice e lineare, se non si pretendono configurazioni particolari (per esempio limitare il traffico a dati computer o per certi dati con apposite access-list).

Ci sono due modi per “insegnare” al router i percorsi (route): il modo statico e quello dinamico.

Per reti di piccole dimensioni (come quella che utilizziamo come esempio) è consigliabile l'utilizzo delle route statiche; questo perché le istruzioni da dare sono abbastanza limitate e chi le configura può decidere 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 più pratico utilizzare le route dinamiche; in sostanza si indica al router quali reti conosce (quelle direttamente connesse); sarà suo compito “insegnarle” ai router vicini.

In questo modo, se viene aggiunto alla topografia della rete un nuovo router, o anche semplicemente una nuova rete, i router si occupano di tenere aggiornate autonomamente le loro tabelle di routing, inviando pacchetti di update ai routers che conoscono.

Nel nostro caso analizziamo le route statiche.

6.1 Route statiche

I comandi da dare devono indicare al router quali dati instradare verso quale destinazione.

In parole semplici, si indica al router la rete destinataria e il “passo” successivo da far prendere ai dati.

Le sequenze di eventi che possono accadere sono le seguenti:

- Un utente decide di inviare un dato (per esempio un'e-mail);

- L'applicazione verifica che il destinatario non è nella propria rete, utilizzando la netmask e l'indirizzo IP;
- Decide di inviare il "pacchetto" utilizzando il proprio default gateway (il router);
- Il router riceve il pacchetto e lo analizza, per verificare a quale rete è destinato;
- Il router controlla nella propria tabella di routing se conosce un percorso per raggiungere la rete destinataria;
- Se esiste lo instrada verso il next hop indicato nella route;
- Se non esiste, verifica se è stata impostata una route di default, che utilizza per instradarlo;
- Se non esiste modo per instradarlo scarta il pacchetto.

6.2 Router remoti

Nel caso della rete che stiamo analizzando, per i router delle filiali si tratta semplicemente di indicare ai router delle filiali di instradare tutto il traffico verso il router della sede centrale, visto che gli stessi non hanno altra possibilità (la loro unica connessione geografica è appunto verso il router della sede, e anche per comunicare fra loro devono "transitare" da lì).

Ci sono diversi modi con cui indicare questo al router: per esempio possiamo indicargli il suo default gateway oppure indicargli che tutte le reti sono raggiungibili tramite il router "A".

```
RouterB>en
Password:*****
RouterB#conf t
RouterB(config)#ip default-gateway 192.168.254.1
RouterB(config)#
```

oppure

```
RouterB>en
Password:*****
RouterB#conf t
RouterB(config)#ip route 0.0.0.0 0.0.0.0 192.168.254.1
RouterB(config)#
```

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

Il secondo potrebbe non essere così chiaro: indicando come destinazione *0.0.0.0* con *netmask 0.0.0.0* vogliamo indicare tutte le reti possibili.

In ogni caso dobbiamo aggiungere un ulteriore comando: *ip classless*. Con questo comando indichiamo al router che, con i pacchetti per i quali non conosce la destinazione, deve utilizzare una route che li include.

Ad esempio il router potrebbe conoscere come instradare i pacchetti per la rete *10.0.0.0* netmask *255.0.0.0*. Se il router ricevesse un pacchetto per la rete *10.1.1.0* netmask *255.255.255.0* (la quale è una sottorete della *10.0.0.0* netmask *255.255.255.0*), potrebbe instradarlo verso la route indicata per la rete di classe superiore.

Questo vale anche per la route verso la rete *0.0.0.0* netmask *0.0.0.0*: se non indicassimo al router che può utilizzarla per pacchetti per i quali non conosce una route precisa, lui li scarterebbe, mentre con il comando *ip classless* potrebbe utilizzare tale route.

```
RouterB(config)#ip classless
RouterB(config)#
```

6.3 Router centrale

Per quanto riguarda il router della sede, dobbiamo innanzi tutto “istruirlo” su come raggiungere le due filiali, indicando l’indirizzo delle due reti come destinazione e quello del router della filiale interessata come next-hop.

Bisogna inoltre indicare al router i percorsi “alternativi” da seguire, in caso di caduta di una connessione. A questo punto entrano in gioco 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 percorrerle.

Spetterà al router decidere quale usare: quella con minor costo, se sono tutte attive, mentre se quella con minor costo dovesse venire meno, potrebbe utilizzare quella di backup.

Nel momento in cui venisse ripristinata quella principale, ricomincerebbe ad usarla, in maniera assolutamente trasparente per la rete.

Queste configurazioni le realizziamo con i seguenti comandi:

```
RouterA>en
RouterA#conf t
RouterA(config)#ip route 192.168.2.0 255.255.255.0 192.168.254.2
RouterA(config)#ip route 192.168.3.0 255.255.255.0 192.168.254.6
RouterA(config)#ip route 192.168.2.0 255.255.255.0 192.168.254.10 200
RouterA(config)#ip route 192.168.3.0 255.255.255.0 192.168.254.14 200
RouterA(config)#
```

Inoltre dobbiamo indicare qual’è la route di default da usare per tutto il traffico non conosciuto (in pratica, tutte le connessioni verso Internet).

Questo lo facciamo indicando come default gateway l’interfaccia Dialer3, quella connessa al Internet Service Provider.

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

7 Configurazioni particolari

Di seguito elenchiamo alcuni casi che si potrebbero presentare, generando la necessità di configurazioni particolari sui Router.

7.1 Logon da remoto

Per permettere a dei client di effettuare il logon ad un server Windows NT che si trova su un’altra rete che non sia la propria, si rende necessario permettere il passaggio sulla rete geografica dei pacchetti *bootp* che vengono appunto usati per autenticarsi ad un dominio.

Per fare questo dobbiamo indicare al router innanzi tutto di far passare i pacchetti bootp, con il comando *ip bootp server*.

In più è necessario lasciar passare, in alcuni casi, i pacchetti di *broadcast*, che normalmente verrebbero bloccati alla rete locale.

Per fare questo utilizziamo il comando *ip helper-address*, il quale indica al router a quale indirizzo (può anche essere un’intera rete), indirizzare gli eventuali pacchetti broadcast ricevuti.

Per esempio possiamo usare come *ip helper-address* l’indirizzo del server NT di dominio, in modo che questi riceva le richieste di logon.

Per esempio:

```
RouterC>en
Password: *****
RouterC#conf t
RouterC(config)#int eth0
RouterC(config-if)#ip helper-address 192.168.1.2
RouterC(config-if)#ip helper-address 192.168.1.3
RouterC(config-if)#
```

Gli indirizzi 192.168.1.2 e 192.168.1.3 sono quelli dei server PDC e BDC.

Inoltre, nella sede principale, è necessario abilitare il passaggio del *directed-broadcast* nella configurazione dell'interfaccia Ethernet. Questo è proprio il meccanismo che viene utilizzato dal router per propagare sulla rete geografica il broadcast: quando al primo router (RouterC) arriva un pacchetto di broadcast sull'interfaccia Ethernet, lo "trasforma" in un pacchetto "*unicast*" diretto al RouterA, il quale lo reindirizza verso l'*ip helper-address* indicato dal primo Router, mediante il *directed-broadcast*.

Bisogna ricordarsi che di default il router ha disabilitato il *directed-broadcast*, bisogna quindi abilitarlo.

```
RouterA>en
Password: *****
RouterA#conf t
RouterA(config)#int eth0
RouterA(config-if)#ip directed-broadcast
RouterA(config-if)#
```

8 Considerazioni finali

A questo punto la configurazione dei tre router è completa: sono state realizzate le connessioni tra le sedi, quelle di backup, quella verso Internet (condivisa) ed inoltre sono state definite le route che i dati dovranno seguire.

Naturalmente questo non vuol essere un documento esaustivo, in quanto le possibili configurazioni possono essere numerosissime. Può essere comunque un ottimo punto di partenza per comprendere la filosofia del sistema operativo che gestisce i routers (IOS) e con piccole modifiche può essere utilizzato in una rete di piccole/medie dimensioni per realizzare le configurazioni.

9 Configurazioni finali

Nelle pagine seguenti indichiamo le configurazioni finali e complete dei tre Router.

Sede (Router A)

Current configuration:

```
!  
!  
version 12.0  
service udp-small-servers  
service tcp-small-servers  
service password-encryption  
!  
!  
hostname RouterA  
!  
enable password cisco  
enable secret 5 $1$T6f0$XCbv3CEwGGNv4QxQ6  
!  
!  
username RouterB password cisco  
username RouterC password cisco  
!  
isdn switch-type basic-net3  
isdn tei-negotiation first-call  
!  
!  
interface Ethernet0  
  description Interfaccia Ethernet verso rete LAN locale  
  ip address 192.168.1.1 255.255.255.0  
  ip nat inside  
  ip directed-broadcast  
!  
interface Serial0/0  
  description Interfaccia seriale su linea Frame-Relay (fisica)  
  no ip address  
  encapsulation frame-relay  
  frame-relay lmi-type ansi  
  no ip directed-broadcast  
!  
interface Serial0/0.1  
  description Interfaccia verso Filiale 1 (logica)  
  ip address 192.168.254.1 255.255.255.252  
  frame-relay interface-dlci 10  
  no ip directed-broadcast  
  ip nat inside  
!  
interface Serial0/1  
  description Interfaccia seriale su linea CDN verso Filiale 2  
  ip address 192.168.254.5 255.255.255.252
```

```

encapsulation ppp
no ip directed-broadcast
ip nat inside
!
!
interface BRI1/0
description "Interfaccia ISDN"
encapsulation ppp
dialer pool-member 1
ppp authentication chap
!
Interface BRI1/1
description "Interfaccia ISDN per Internet"
encapsulation ppp
dialer pool-member 2
ppp authentication chap
!
Interface Dialer1
dialer pool 1
description "Interfaccia di backup verso Filiale1"
ip address 192.168.254.9 255.255.255.252
dialer string 01234567
dialer idle-timeout 300
dialer-group 1
!
Interface Dialer2
dialer pool 1
description "Interfaccia di backup verso Filiale2"
ip address 192.168.254.13 255.255.255.252
dialer string 01234568
dialer idle-timeout 300
dialer-group 1
!
Interface Dialer3
ip address negotiated
dialer pool 2
dialer string 0123123
ppp chap hostname UTENTE
ppp chap password PASSWORD
dialer-group 1
ip nat outside!
!
!
dialer-list protocol ip permit
access-list 1 permit 192.168.1.0 0.0.0.255
access-list 1 permit 192.168.2.0 0.0.0.255
access-list 1 permit 192.168.3.0 0.0.0.255
!
ip classless
ip route 0.0.0.0 0.0.0.0 Dailer3
ip route 192.168.2.0 255.255.255.0 192.168.254.2

```

```

ip route 192.168.2.0 255.255.255.0 192.168.254.10 200
ip route 192.168.3.0 255.255.255.0 192.168.254.6
ip route 192.168.3.0 255.255.255.0 192.168.254.14 200
!
!
line con 0
  transport input none
  login
password cisco
line aux 0
  transport input all
line vty 0 4
  login
password cisco
!

```

10 Filiale 1 (Router B)

Current configuration:

```

!
!
version 12.0
service udp-small-servers
service tcp-small-servers
service password-encryption
!
!
hostname RouterB
!
enable password cisco
enable secret 5 $1$T6f0$XCbv3CEwGGNv4QxQ6
!
!
username RouterA password cisco
!
isdn switch-type basic-net3
isdn tei-negotiation first-call
!
!
interface Ethernet0
  description Interfaccia Ethernet verso rete LAN locale
  ip address 192.161.2.1 255.255.255.0
  no ip directed-broadcast
!
interface Serial0/0
  description Interfaccia seriale su linea Frame-Relay (fisica)
  no ip address
  encapsulation frame-relay
  frame-relay lmi-type ansi
  no ip directed-broadcast

```

```

!  

interface Serial0/0.1 point-to-point  

  description Interfaccia verso Sede (logica)  

  ip address 192.168.254.2 255.255.255.252  

  frame-relay interface-dlci 15  

  no ip directed-broadcast  

!  

interface Serial0/1  

  description Seriale non utilizzata  

  no ip address  

  no ip directed-broadcast  

  shutdown  

!  

interface BRI1/0  

  description "Interfaccia ISDN"  

  encapsulation ppp  

  dialer pool-member 1  

  ppp authentication chap  

  dialer-group 1  

!  

interface BRI1/1  

  description "Interfaccia non utilizzata"  

  no ip address  

  no ip directed-broadcast  

  shutdown  

  dialer-group 1  

!  

Interface Dialer1  

  dialer pool 1  

  description "Interfaccia di backup verso Sede"  

  ip address 192.168.254.10 255.255.255.252  

  dialer string 01234569  

  dialer idle-timeout 300  

!  

!  

dialer-list protocol ip permit  

!  

ip classless  

ip route 0.0.0.0 0.0.0.0 192.168.254.1  

ip route 0.0.0.0 0.0.0.0 192.168.254.9 200  

!  

!  

line con 0  

  transport input none  

  login  

password cisco  

line aux 0  

  transport input all  

line vty 0 4  

  login  

password cisco

```

!

11 Filiale 2 (Router C)

Current configuration:

```
!  
!  
version 12.0  
service udp-small-servers  
service tcp-small-servers  
service password-encryption  
!  
!  
hostname RouterC  
!  
enable password cisco  
enable secret 5 $1$T6f0$XCbv3CEwGGNv4QxQ6  
!  
username RouterA password cisco  
!  
isdn switch-type basic-net3  
isdn tei-negotiation first-call  
!  
!  
interface Ethernet0  
  description Interfaccia Ethernet verso rete LAN locale  
  ip address 192.161.3.1 255.255.255.0  
  no ip directed-broadcast  
  ip helper-address 192.168.1.2  
  ip helper-address 192.168.1.3  
!  
interface Serial0/0  
  description Interfaccia seriale su linea CDN verso Sede  
  ip address 192.168.254.6 255.255.255.252  
  encapsulation ppp  
  no ip directed-broadcast  
!  
interface Serial0/1  
  description Interfaccia non utilizzata  
  no ip address  
  no ip directed-broadcast  
  shutdown  
!  
interface BRI1/0  
  description "Interfaccia ISDN"  
  encapsulation ppp  
  dialer pool-member 1  
  ppp authentication chap  
!  
interface BRI1/1
```

```
description "Interfaccia non utilizzata"
no ip address
no ip directed-broadcast
shutdown
!
!
Interface Dialer1
dialer pool 1
description "Interfaccia di backup verso Sede"
ip address 192.168.254.10 255.255.255.252
dialer string 01234569
dialer idle-timeout 300
dialer-group 1
!
!
dialer-list protocol ip permit
!
ip classless
ip route 0.0.0.0 0.0.0.0 192.168.254.5
ip route 0.0.0.0 0.0.0.0 192.168.254.13 200
!
!
line con 0
transport input none
login
password cisco
line aux 0
transport input all
line vty 0 4
login
password cisco
!
```

Daniele Gallarato

Documentazione prodotta dallo staff Netexpert.it. Tutti i diritti riservati.

La documentazione può essere riprodotta ed utilizzata liberamente per scopi istituzionali e formativi, e altresì rigorosamente vietato l'uso a fine di lucro. Gli autori non sono responsabili per danni recati a software o hardware causati da eventuali informazioni errate presenti in questo documento. Tutti i nomi o marchi registrati sono proprietà delle rispettive aziende.

Chiunque voglia segnalare errori, omissioni o suggerimenti può farlo all'indirizzo staff@netexpert.it