

Capitolo 1. Generalità e configurazione di apparati Cisco

1.1. Per iniziare

1.1.1. Pre-requisiti

La fruizione ottimale di questo modulo richiede le seguenti conoscenze di base:

- Il protocollo IPv4, almeno per quanto riguarda le problematiche di base e di indirizzamento
- conoscenza delle problematiche e delle tecnologie di trasporto di livello 1-2 della pila OSI

E' inoltre richiesta la presenza di una certa dimestichezza con le esigenze di configurazione di una rete reale.

1.1.2. Obiettivi

Al termine di questo modulo il partecipante sarà in grado di padroneggiare i comandi fondamentali di configurazione degli apparati Cisco più comuni, quali router e switch. In particolare, questo comprende la configurazione dei principali parametri di sistema e delle principali tipologie di interfacce. La tecnologia ISDN verrà invece trattata compiutamente in un modulo distinto in quanto più ostica da configurare; verranno qui trattate solamente le parti fondamentali relative a tale tecnologia.

Questo modulo intende porsi come guida rapida di tali apparati senza porsi in alternativa ai manuali ufficiali; l'obiettivo consiste nell'offrire al lettore uno spunto di partenza strutturato per poter cominciare l'interazione in maniera più familiare con gli apparati Cisco. Questo modulo deve ovviamente intendersi come propedeutico ai successivi moduli di configurazione di apparati Cisco.

1.1.3. Struttura

In questo modulo si troverà l'elenco dei principali comandi di utilizzo comune e un cenno a come questi vengono impiegati. Gli argomenti principali sono:

- caratteristiche generali degli apparati
- configurazione di base necessaria all'attivazione di un router "spoglio"
- principali informazioni da conoscere a proposito dell'ambiente CLI (Command Line Interface) Cisco
- cenni sulle problematiche di debug
- configurazione delle interfacce più comuni

1.1.4. Sommario

Essendo questo modulo un "manuale di laboratorio", non è disponibile il sommario.

1.2. Cenni preliminari sui router Cisco

Gli apparati di rete (con particolare riferimento a router/switch Cisco) si possono scomporre nei seguenti componenti principali:

CPU

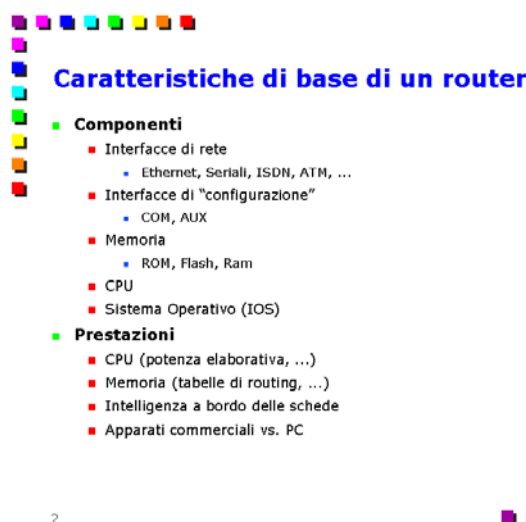
Componente che sovrintende al funzionamento dell'apparato, la cui potenza varia a seconda della classe della macchina. Su macchine di fascia alta possono coesistere anche più elementi di elaborazione (CPU oppure ASIC dedicati) specializzati in opportuni compiti. Il compito della CPU si può riassumere in:

- svolgimento del processo di forwarding (lettura dei pacchetti in arrivo dalle varie interfacce, determinazione dell'interfaccia di uscita, invio del pacchetto su tale interfaccia)
- calcolo delle tabelle in instradamento, aggiornamento dei dati di routing
- supervisione del router (gestione dei comandi dell'operatore, protocolli di gestione quali SNMP, ...)

Supporti di memorizzazione

Si dividono in:

- **ROM:** memoria nella quale è memorizzato il software di base del router (fondamentalmente quello necessario all'accensione). Include alcuni programmi di diagnostica ed alcuni comandi di base, necessari ad esempio per poter ripristinare il sistema operativo nel caso di cancellazione della memoria FLASH. Include anche il programma di bootstrap.



- **NVRAM:** è una particolare memoria non volatile dedicata esclusivamente al salvataggio del file di configurazione. L'utilizzo di una memoria distinta dalla FLASH offre la possibilità di sostituire integralmente la FLASH senza perdere la configurazione dell'apparato.
- **FLASH:** memoria di tipo "permanente", nella quale è memorizzato il sistema operativo (IOS). Rappresenta l'unità di memorizzazione di massa dell'apparato. Offre anche la possibilità di memorizzare files a scelta da parte dell'operatore (ad esempio file di configurazione di backup).
- **RAM:** è la memoria di lavoro, il cui contenuto viene perso allo spegnimento dell'apparato. Mantiene una copia del sistema operativo (che viene copiato dalla FLASH alla RAM nella fase di bootstrap, anche se non su tutti gli apparati), una copia del file di configurazione (che viene copiato dalla NVRAM nella fase di bootstrap), e tutte le strutture necessarie per l'operatività dell'apparato a run-time (es., routing table, ARP cache, ecc).

Interfacce di configurazione

Comprendono le interfacce fisiche necessarie alla configurazione del router. Sugli apparati Cisco si trovano solitamente le seguenti interfacce:

- **CONSOLE:** interfaccia seriale asincrona (RS232), usata per il collegamento di un terminale seriale per la configurazione del router. Spesso questa interfaccia viene utilizzata per la configurazione da locale dell'apparato, ossia attraverso un terminale (es. un PC con porta seriale) direttamente connesso all'apparato. Questo comporta la necessità per l'operatore di essere fisicamente presente nello stesso luogo dell'apparato.
- **AUX:** interfaccia seriale asincrona (RS232). Fisicamente è uguale alla porta console, ma funzionalmente viene utilizzata come porta di collegamento di altre periferiche, ad esempio un modem. Ad esempio, questa opzione permette ad un operatore di accedere ad una porta di configurazione attraverso la rete telefonica, consentendo di interagire con l'apparato anche senza essere fisicamente presente nel locale in cui risiede l'apparato. Si tenga presente che un apparato è configurabile anche via rete IP, ma in alcuni casi (es. rete malfunzionante con apparato irraggiungibile, oppure l'applicazione di qualche comando di configurazione errato che blocca il funzionamento dell'apparato) l'accesso ad una porta "console" rappresenta l'unica via d'uscita per ripristinarne il funzionamento.

Alloggiamenti per interfacce (*linecard*)

Sono normalmente delle schede di espansione che si inseriscono in appositi alloggiamenti e che ospitano vari tipi di interfacce fisiche (Ethernet, ...), la logica per il loro funzionamento, etc.; spesso il router viene venduto con un insieme minimale di interfacce di rete e sta all'utente decidere, in base ai propri bisogni, qual è l'insieme di schede più appropriate per le proprie esigenze.

Interfacce di rete

Comprendono le interfacce fisiche (i "connettori" destinati ad attacchi di rete); tra le principali si possono citare:

- **AUI:** interfaccia Ethernet di tipo AUI
- **10BaseT** (e superiori): interfaccia Ethernet di tipo 10BaseT

- **SERIAL:** interfacce seriali sincrone (da collegare, con apposito cavo proprietario, a modem sincroni con interfaccia V.35); sono utilizzate per collegamenti dedicati (CDN), reti X.25, Frame Relay, etc.
- **BRI:** interfaccia verso l'NT di un ISDN basic rate
- **ATM:** interfaccia ATM, in fibra ottica oppure in rame.

La potenza di un router (intesa in numero di pacchetti al secondo inoltrati) è variabile a seconda di alcune scelte architetturali del router:

- i router di fascia bassa hanno schede (interfacce) con bassa capacità di elaborazione e tutto il lavoro è fatto dall'unica CPU centrale la cui potenza può essere variabile a seconda delle prestazioni richieste
- i router di fascia media hanno schede intelligenti con a bordo CPU dedicate; queste svolgono autonomamente buona parte del processo di forwarding, mentre la CPU centrale si occupa del calcolo delle tabelle di instradamento e della gestione della macchina
- i router di fascia alta (layer 3-7 switch) hanno schede intelligenti con processo di forwarding in hardware, con prestazioni altissime; la CPU centrale si occupa del calcolo delle tabelle di instradamento e della gestione della macchina.



Il grosso punto di vantaggio di un apparato Cisco (ma la stessa cosa vale per altre case costruttrici) sta nel sistema operativo, tradizionalmente molto potente anche se ostico ad un primo impatto, che definisce tra le altre cose tutti i comandi per le varie funzionalità in modo omogeneo. Ad esempio, nonostante sia possibile utilizzare PC tradizionali carrozzati con opportuno software (routing, bridging, NAT, ...) in alternativa agli apparati commerciali, la configurazione dei vari moduli è spesso profondamente diversa, i moduli possono essere poco integrati tra loro, etc. Pertanto, nonostante i PC siano funzionalmente identici ad un apparato commerciale, hanno costi superiori dal punto di vista della gestione del parco apparati.

Sugli apparati Cisco, il sistema operativo (IOS) risiede nella memoria FLASH. Inoltre, il sistema operativo (tramite la CLI) acquisisce dall'operatore i comandi necessari alla configurazione della macchina e li mette in opera.

1.2.1. Accesso agli apparati

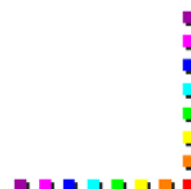
L'accesso all'apparato può avvenire via rete oppure collegando un terminale (o un PC) alla porta console dell'apparato; nel primo caso è possibile la gestione da remoto. L'accesso in locale è obbligatorio nella fase di configurazione iniziale del router; successivamente è possibile utilizzare un metodo che permette la configurazione remota, che rappresenta la tecnica preferenziale. In questa modalità viene prevalentemente utilizzato di un programma di emulazione terminale remoto (telnet o SSH; il secondo consente di criptare la comunicazione), che permette di configurare l'apparato con la solita interfaccia a linea di comando che rappresenta comunque la modalità preferita di configurazione di apparati Cisco. Tuttavia questa modalità di interazione richiede la presenza di un collegamento di rete attivo e funzionante a livello IP tra l'apparato e la macchina di gestione. In questo caso, siccome un apparato (in particolar modo un router) è tipicamente dotato di più interfacce e quindi più indirizzi IP, è possibile utilizzare un indirizzo qualunque tra questi per collegarvi. In altre parole, se l'apparato ha gli indirizzi A, B e C raggiungibili, sarà possibile digitare sia `telnet A`, che `telnet B`, che `telnet C`.



Accesso al router

- **Via terminale**
 - Parametri (emulazione terminale)
 - Configurazione iniziale, troubleshooting
 - SNMP
- **Via terminale virtuale (telnet)**
 - `telnet indirizzo_IP`
 - Sono ammessi gli indirizzi di tutte le interfacce attive non unnumbered del router (compreso il loopback), purchè esista una strada verso di essa
 - Attenzione alla presenza di indirizzi IP su interfacce non raggiungibili
 - Gestione remota
- **Via management (SNMP)**
 - Necessità di programmi appositi
- **Via web**
 - Funzionalità limitate

4

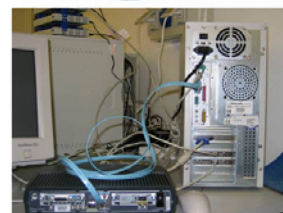


Altre modalità di interazione consistono nell'utilizzo del protocollo SNMP oppure attraverso un browser web (il servizio può essere abilitato tramite il comando `ip http server` dalla modalità di configurazione). Mentre SNMP offre anche possibilità di configurazione, sono ben pochi i gestori che utilizzano questa modalità. Viceversa, per quanto riguarda l'interazione via web, questa offre funzionalità estremamente limitate (status di ogni interfaccia, ...) ed è utilizzato più come controllo che come strumento di configurazione vero e proprio.

La modalità di interazione attraverso la rete presenta una criticità nel momento in cui l'indirizzo IP a cui si fa riferimento diventa irraggiungibile (ad esempio un'interfaccia con il cavo staccato). In questo caso quell'indirizzo IP non può essere utilizzato per accedere all'apparato ed è necessario far riferimento ad un altro indirizzo IP (ove raggiungibile). Questo è il motivo per cui spesso gli apparati commerciali hanno una ulteriore interfaccia virtuale configurata (l'interfaccia `loopback`) che ha la caratteristica di non essere legata ad alcuna interfaccia fisica, e pertanto risulta raggiungibile (fatto salvo che il routing esista per quell'indirizzo) purchè esista un percorso disponibile a livello IP.



Accesso tramite console



5

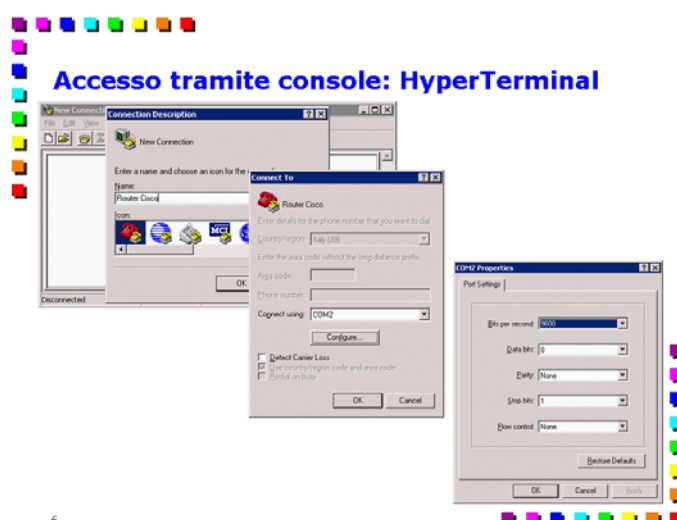


L'accesso tramite console non soffre di questi problemi di raggiungibilità; tuttavia, è necessario risiedere fisicamente in locale in quanto il router è collegato con il terminale di configurazione attraverso un cavo console. Nel passato per questa operazione era utilizzato un terminale VT100, ossia una sorta di terminale "stupido" in grado di inviare/ricevere dati verso un elaboratore attraverso un'interfaccia seriale. Questo dispositivo può essere emulato da un programma software quale l'HyperTerminal nel mondo Windows, il quale va configurato con gli opportuni parametri relativi all'interfaccia seriale:

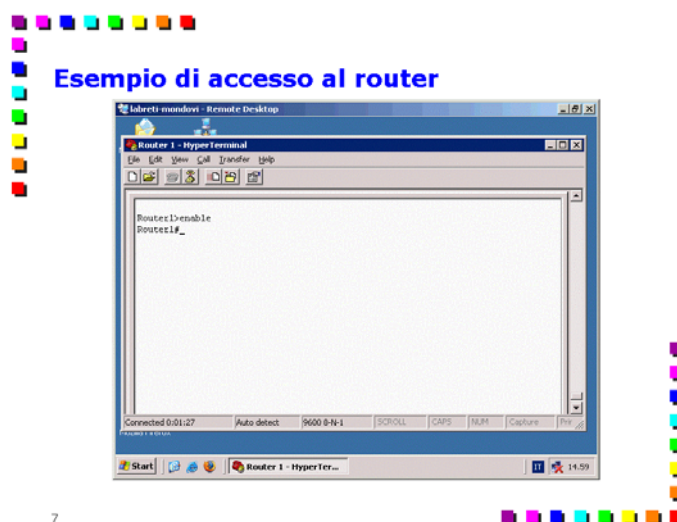
9600 bps, 8 bit, No Parity, Stop Bit 1, Flow Control Hardware

In alternativa, è possibile collegare la porta console (o AUX) ad un modem, con le stesse modalità di interazione già illustrate in precedenza. Tra il resto, nel momento in cui venga utilizzato un terminale seriale è possibile inviare all'apparato caratteri speciali, ad esempio il *break*. In Windows, il tasto Break si ottiene premendo contemporaneamente i tasti CTRL+&.

In figura è mostrata una possibile schermata di accesso ad un router attraverso una finestra HyperTerminal di Windows. In tale finestra è possibile digitare i comandi di configurazione secondo la sintassi a linea di comando degli apparati Cisco.



6



7

1.2.2. I files di configurazione

Un nuovo comando di configurazione impartito al router viene scritto in un file di configurazione chiamato `running-config`, memorizzato in RAM e immediatamente applicato dalla macchina. Tuttavia, questo file di configurazione viene perso allo spegnimento dell'apparato e l'effetto dei comandi in esso contenuti si esaurisce allo spegnimento del router.

Gli apparati mantengono per un secondo file di configurazione nella memoria NVRAM, chiamato `startup-config`, che viene utilizzato per impostare una configurazione sull'apparato alla sua accensione. I due file, in RAM e in NVRAM, possono non essere allineati. Ad esempio, nel caso dell'esempio precedente, i due file non sono allineati: per rendere effettiva anche la configurazione della RAM ad un successivo reboot è necessario salvare il file in NVRAM, da dove verrà letto all'accensione del router. Ne consegue che:

- non è detto che le configurazioni scritte in RAM e NVRAM siano allineate; in mancanza della configurazione RAM (ad esempio allo startup del router) viene letta quella della NVRAM
- la configurazione RAM viene trasferita in NVRAM solo in corrispondenza di uno specifico comando dell'operatore
- è possibile procedere ad una opportuna politica di backup, copiando la configurazione attiva dalla RAM in NVRAM solamente quando si è sicuri dalla correttezza della stessa (ad esempio si è verificato il corretto comportamento del router in queste condizioni per un certo tempo)
- tutte le modifiche di configurazione impartite dall'operatore vengono salvate esclusivamente sulla RAM, che quindi appare come se avesse la "precedenza" sulla NVRAM

La configurazione corrente del router può essere anche salvata (o letta) via rete attraverso il protocollo TFTP. È possibile quindi indicare al router di scrivere il file di configurazione in rete (anziché in NVRAM) su uno specifico TFTP server con il risultato di ottenere un file testuale con l'elenco di tutti i comandi di configurazione. Analogamente è possibile indicare al router di leggere un file di configurazione via rete anziché procedere alla configurazione manuale del tutto. Ovviamente tale modalità richiede che la rete sia funzionante e che vi sia la raggiungibilità del server TFTP a livello IP.

Gli apparati Cisco fanno largo uso di server TFTP; anche l'aggiornamento ad una nuova versione del sistema operativo fa uso di questi tipi di servers.

1.2.3. Menù e comandi



L'IOS ha interfaccia completamente testuale (CLI, Command Line Interface). Esistono dei tools grafici ma hanno caratteristiche estremamente limitate che ne rendono possibile l'utilizzo solamente con configurazioni molto semplici; di fatto, vengono utilizzati più spesso per la visualizzazione di alcuni parametri operativi.

I menù della linea di comandi di IOS seguono un'organizzazione gerarchica su N livelli annidati. E' possibile passare da un livello all'altro con specifiche parole chiave; per uscire dallo specifico sottomenù si usa la parola chiave `exit`. La parola chiave `end` permette invece il ritorno diretto da qualunque sottomenù di configurazione alla modalità privilegiata. I passaggi da una modalità all'altra sono evidenziati dalla diverso prompt che viene stampato dal router, ad esempio `Router>` in modalità utente, che diventa `Router#` in modalità privilegiata.

Le principali modalità operative sono le seguenti:

Modalità utente

Questa è la prima modalità a cui si ha accesso una volta collegati all'apparato. In essa è possibile visualizzare alcuni dati di funzionamento dell'apparato, anche se i privilegi in questo livello sono molto limitati. Il passaggio alla modalità successiva avviene attraverso la parola chiave `enable`. Per accedere a questa modalità può essere richiesta una fase di autenticazione.

Passaggio alle altre modalità operative: `enable` per passare alla modalità privilegiata; `exit` per abbandonare la sessione corrente con il router.

Modalità privilegiata

In questa modalità è possibile visualizzare tutti i dati di funzionamento del router ed è possibile azzerare alcune strutture che vengono utilizzate a run-time (es. cache, contatori di interfacce, ecc). Tuttavia, non è possibile cambiare la configurazione dell'apparato, anche se sono disponibili alcuni comandi che permettono di gestire i files di configurazione dell'apparato e, tramite questi, è possibile rimpiazzare un file con un altro. Curiosamente, mentre in questa modalità è possibile sostituire un intero file di configurazione con un altro, non è possibile digitare comandi di configurazione singoli, riferiti ad una specifica funzione.

Passaggio alle altre modalità operative: `configure terminal` per passare alla modalità di configurazione (Nota: esistono anche altri comandi per entrare in modalità configurazione, quali ad es. `configure network`); `exit` per tornare in modalità utente.

Modalità configurazione

In questa modalità è possibile variare i parametri di funzionamento del router e procedere alla sua configurazione.

Passaggio alle altre modalità operative: (comando specifico) per



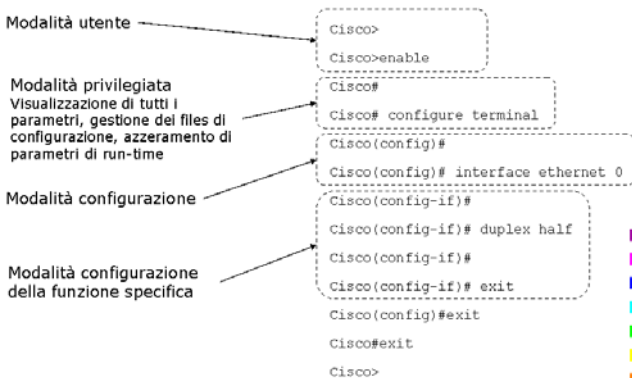
IOS e Menù

- **Interfaccia testuale (CLI - Command Line Interface)**
 - Tools grafici con funzionalità limitate
- **Modalità di accesso**
 - Utente
 - Privilegiata
 - Configurazione
 - Function-specific
- **Entrata nel menù**
 - Possibile con opportune parole chiave
- **Uscita dal menù**
 - Parola chiave `exit`: ritorna al livello precedente
 - Parola chiave `end`: ritorna alla modalità privilegiata
- **Accesso all'apparato**
 - Può essere richiesta una fase di autenticazione

9



IOS e menù: esempio



10

entrare nel sottomenù occorre utilizzare una parola chiave specifica che dipende dall'aspetto di configurazione che si vuole modificare; ad esempio, per entrare nella modalità di configurazione dell'interfaccia Ethernet0, è necessario digitare `interface ethernet 0`. Per tornare in modalità privilegiata: `exit`.

Modalità di configurazione della funzionalità specifica

In questa modalità è possibile configurare la funzionalità specifica. Nel caso dell'esempio precedente è possibile configurare i parametri di quell'interfaccia (ad esempio la modalità full/half duplex, l'indirizzo IP, ecc).

Passaggio alle altre modalità operative: normalmente non sono disponibili ulteriori sottomenù. Per tornare in modalità di configurazione: `exit`. Per tornare direttamente in modalità privilegiata: `end`.

In ogni momento l'IOS rende disponibile un help contestuale, richiamabile digitando il carattere "?". Vengono quindi elencati tutti i comandi disponibili in quella particolare modalità; per un help più specifico è possibile digitare "comando ?" in riferimento al comando desiderato. Questa tipologia di help è disponibile in maniera recursiva; pertanto, per sapere il significato e le possibili opzioni riferite all'opzione B del comando A, è possibile digitare `comandoA opzioneB ?` e così via.

Per velocizzare l'immissione dei comandi, l'IOS supporta anche comandi abbreviati: quando un particolare comando in un certo contesto non è più ambiguo, viene automaticamente riconosciuto dal sistema. Ad esempio è possibile digitare il comando abbreviato `sh` anziché la forma intera `show`. IOS dispone anche del completamento automatico: digitando un comando e premendo il tasto `TAB`, se l'IOS riconosce il comando questo viene completato automaticamente. In altre parole, digitando `sh` e premendo il tasto `TAB` comparirà sullo schermo il comando intero `show`. Questa modalità di autocompletamento è particolarmente utile per controllare che il comando (parziale) che si sta digitando è effettivamente quello voluto.

Ogni comando è disponibile in forma negata e affermata: è possibile abilitare una determinata funzione digitando `stringa_di_comando` e disabilitare la funzione stessa digitando `no stringa_di_comando`. Pertanto, per cancellare un comando esistente è sufficiente digitare il comando preceduto dalla parola `no`. Ad esempio, se il comando `shutdown` disabilita un'interfaccia di rete, il comando `no shutdown` effettua l'operazione opposta, riattivando l'interfaccia.

L'IOS ha seguito una certa evoluzione, anche nella sintassi dei comandi. Versioni nuove non solo inseriscono funzionalità nuove e quindi comandi nuovi, ma spesso vecchi comandi vengono sostituiti con sintassi diverse. Sarà quindi possibile che alcuni comandi citati in questi moduli non funzionino su alcuni router o perché la versione di IOS è troppo vecchia per supportarli, oppure addirittura perché alcune particolari famiglie non supportano quel comando specifico.

1.2.3.1. I comandi di default



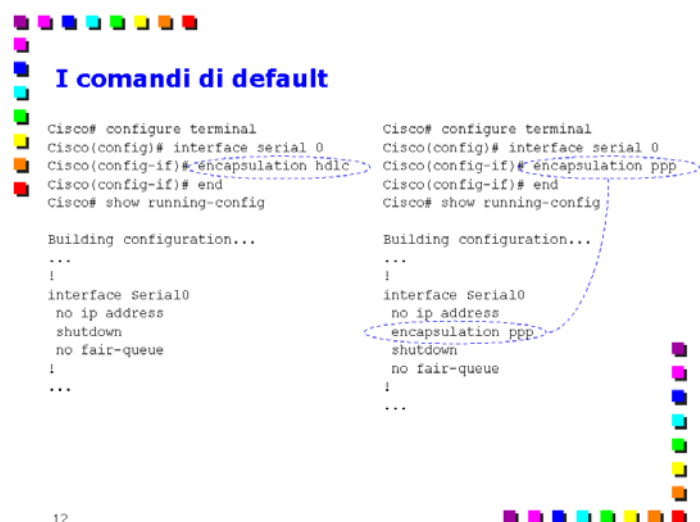
IOS: altre caratteristiche

- **Help**
 - ?
 - <comando> ?
 - <comando> <sottocomando> ... ?
- **Comandi parziali**
 - sh (anziché show)
 - sh[TAB] (per il completamento automatico)
- **Comandi in forma negata**
 - no ip address 1.1.1.1 255.255.255.0
- **Comandi in forma abbreviata**
 - sh ip rout [show ip routing]
- **Problematiche di versioni diverse di IOS**
 - Vecchie versioni possono non supportare le nuove sintassi
 - Alcune famiglie di apparati possono non supportare alcuni comandi

11



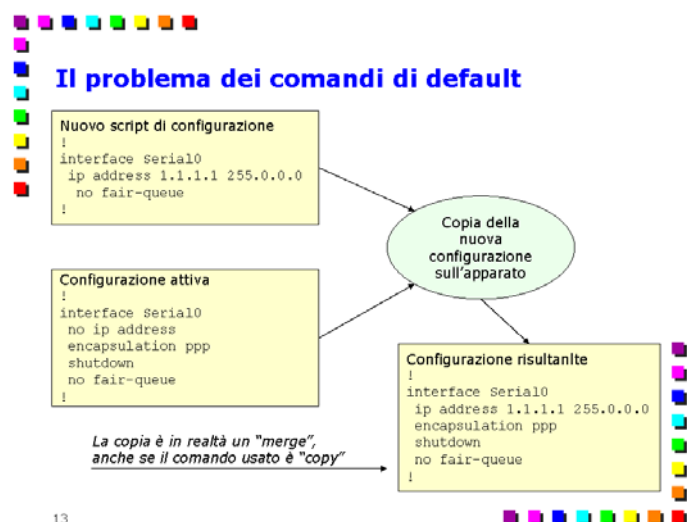
Gli apparati Cisco memorizzano la configurazione in un apposito file che può essere salvato sulla memoria NVRAM. La configurazione può essere visualizzata con opportuni comandi. Purtroppo, il file di configurazione non comprende esplicitamente tutti i parametri operativi configurati sul router. Ad esempio, nella figura si vede come nel primo caso l'interfaccia Serial0 venga configurata con un particolare tipo di protocollo di livello data-link con il comando `encapsulation hdlc`. Tuttavia questo comando non compare nella sezione della configurazione dedicata all'interfaccia seriale del router visualizzata attraverso un opportuno comando. Vice versa, se si ripete la procedura applicando il comando `encapsulation ppp` al posto del comando `encapsulation hdlc` (che rappresenta un protocollo di tipo data-link alternativo ad HDLC), questo viene poi visualizzato nella configurazione.



La ragione è che, per gli apparati Cisco, alcuni comandi sono considerati come scelta di default e pertanto non vengono visualizzati nel file di configurazione per evitare di farla diventare eccessivamente verbosa. Questo comportamento genera però due tipi di problemi:

- l'utente deve essere sufficientemente esperto da ricordare che alcune funzionalità sono presenti (oppure sono configurate in un certo modo di default) anche se non compare una riga esplicita nel file di configurazione
- la sostituzione della configurazione attuale attraverso la sua riscrittura con un nuovo file di configurazione rischia di creare dei problemi.

In particolare, il secondo punto merita un approfondimento. Gli apparati Cisco permettono di copiare un intero file di configurazione secondo diverse modalità (da un server TFTP al router, dalla memoria FLASH, oppure più banalmente attraverso un copia-e-incolla di una configurazione esistente via terminale, ecc.). Tuttavia, quello che viene indicato come "copia" dovrebbe essere più correttamente identificato come "unione". Infatti si supponga di avere un apparato con la configurazione attiva indicata in figura. Tale configurazione comprende la linea `encapsulation ppp`, che specifica un determinato protocollo di livello data-link sull'interfaccia seriale. Se, attraverso uno dei tanti comandi a disposizione, si vuole applicare sull'apparato una nuova configurazione (quella in alto) che non comprende la linea incriminata, il risultato è che l'apparato si troverà ancora il comando `encapsulation ppp` nella configurazione finale. Infatti, nella nuova configurazione il comando `encapsulation hdlc`, che rappresenta il comportamento di default, è omesso, e pertanto non può sovrapporsi (e sostituire) il comando alternativo `encapsulation ppp`.



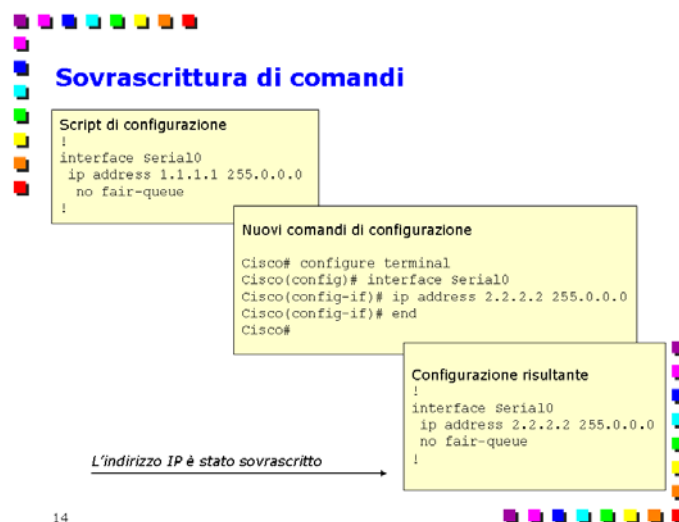
Si noti invece che questo problema non sussiste per la configurazione dell'indirizzo IP: nella vecchia configurazione non era presente alcun indirizzo IP configurato, e nella configurazione finale risulterà presente l'indirizzo IP definito sulla configurazione nuova, che annulla il precedente comando `no ip address`.

Un caso di errore molto frequente è relativo al comando `shutdown`, che disattiva un'interfaccia di rete. Il comando opposto, `no shutdown`, invece rende questa interfaccia operativa, ma viene omissso in quanto ritenuto un comando di default. Ora, si supponga che il router abbia una certa interfaccia di rete disabilitata: visualizzando il file di configurazione (comando `show running-config`), questa interfaccia includerà la direttiva `shutdown`. A questo punto, se si copia una nuova configurazione (che presuppone di avere l'interfaccia attiva, ma il cui comando `no shutdown` non viene visualizzato essendo quello di default) su quella attuale, lo stato dell'interfaccia non cambierà in quanto la nuova configurazione andrà *integrare* quella attuale. Per attivare l'interfaccia è quindi necessario impartire il comando di attivazione dell'interfaccia (`no shutdown`) in maniera esplicita.

E' pertanto necessario tenere conto di questi comandi di default nel momento in cui ci si trova ad applicare nuove configurazioni sugli apparati a partire da configurazioni esistenti. Viceversa, il problema non sussiste nel caso in cui l'apparato ha la configurazione iniziale, in quanto tale configurazione è, per definizione, quella con tutti i comandi di default.

1.2.3.2. Sovrascrittura di comandi

Gran parte dei comandi di configurazione degli apparati ammettono una sola istanza. Ad esempio, un solo indirizzo IP può essere configurato come primario su una interfaccia, oppure un'interfaccia può avere solamente una encapsulation attiva. L'IOS prevede che se un comando viene nuovamente digitato con altri parametri, la versione precedente viene persa. Ad esempio, la figura mostra una configurazione nella quale un'interfaccia seriale è configurata con un indirizzo IP uguale a 1.1.1.1. A seguito di un nuovo comando di configurazione che mira ad impostare il valore dell'indirizzo a 2.2.2.2, il primo indirizzo viene perso e sovrascritto dal secondo.

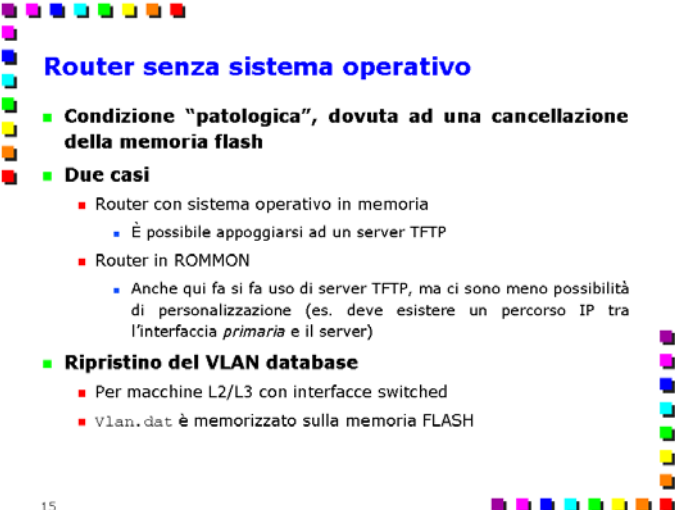


Pertanto, nella gran parte dei casi non è necessario annullare un precedente comando (digitandolo in forma negata, in questo caso `no ip address 1.1.1.1 255.0.0.0`) per poterne cambiare il valore, ma è sufficiente procedere a digitare un nuovo comando che va direttamente a sostituire quello precedente.

1.2.4. Ripristino del sistema operativo in caso di cancellazione della memoria FLASH

La memoria FLASH: è fondamentale in quanto contiene il sistema operativo. Tuttavia, questa memoria può venire cancellata da qualche comando maldestro (ad esempio `erase flash:`) e in questo caso è necessario ripristinarla copiandoci il sistema operativo.

Nel caso di cancellazione della memoria FLASH: possono verificarsi due casi a seconda che il router abbia fatto il reboot oppure no.



Router senza sistema operativo

- **Condizione "patologica", dovuta ad una cancellazione della memoria flash**
- **Due casi**
 - Router con sistema operativo in memoria
 - È possibile appoggiarsi ad un server TFTP
 - Router in ROMMON
 - Anche qui si fa uso di server TFTP, ma ci sono meno possibilità di personalizzazione (es. deve esistere un percorso IP tra l'interfaccia *primaria* e il server)
- **Ripristino del VLAN database**
 - Per macchine L2/L3 con interfacce switched
 - Vlan.dat è memorizzato sulla memoria FLASH

15

1.2.4.1. Router con sistema operativo

Il caso più semplice è quando ci si accorge di aver cancellato la memoria FLASH: senza che il router abbia effettuato un successivo reboot. In questo caso il sistema operativo è ancora attivo e pertanto il router accetta tutti i comandi previsti dall'IOS. Dalla modalità privilegiata è possibile lanciare il seguente comando:

```
copy tftp:nomefileIOS flash:
```

Questo comando scaricherà il file contenente il sistema operativo da un server TFTP e lo scriverà sulla memoria FLASH:. Completato questo punto, il router sarà pronto per un successivo reboot. Ovviamente deve esistere un server TFTP attivo e deve esistere una connettività a livello IP tra il router e questo server.

1.2.4.2. Router in ROMMON (senza sistema operativo)

Questo caso è più complesso e si verifica quando il router ha già effettuato un reboot dopo la cancellazione della memoria FLASH. In questo caso, il router non troverà il sistema operativo ed entrerà in una speciale modalità operativa definita ROMMON. Questa può essere facilmente identificata dal prompt dei comandi che sarà, appunto, `rommon>`.

In questa modalità sono disponibili alcuni comandi basilari e non tutti quelli del sistema operativo. L'utility da utilizzare, in questo caso, è `tftpboot` per poter scaricare una nuova immagine del sistema operativo da un server TFTP. Al lancio dell'utility verrà richiesto di settare una serie di variabili di ambiente (es. l'indirizzo IP assegnato al router, etc), a cui farà seguito la sessione di richiesta del file indicato al server TFTP. Tuttavia in questo caso le scelte sono ridotte rispetto al caso precedente; ad esempio è necessaria la presenza di connettività IP tra l'interfaccia primaria del router e il server TFTP, mentre nel caso precedente era sufficiente un'interfaccia qualsiasi.

Al termine dello scaricamento del file, è possibile far ripartire il router lanciando il comando `boot`.

1.2.4.3. Ripristino del VLAN database in caso di cancellazione della memoria FLASH

A seguito della cancellazione della memoria FLASH, le macchine che hanno interfacce *switched* devono anche ripristinare il VLAN database in quanto questo è in realtà memorizzato come normale file (*vlan.dat*) sulla memoria FLASH.

Per il ripristino di questo file, è sufficiente digitare il comando `vlan database` (in modalità privilegiata) e impostare nuovamente tutte le VLAN attive sulla macchina. Per maggiori dettagli sull'impostazione del VLAN database, si consulti l'apposita sezione.

1.3. Configurazione di base

1.3.1. Passi principali per la configurazione

I principali passi necessari alla configurazione completa dei router Cisco possono essere così schematizzati:

- configurazione di base: parametri di sistema, password
- configurazione delle interfacce: configurazione a basso livello, imbustamento, velocità, indirizzi di rete
- configurazione del routing: route di default, attivazione dell'instradamento (forwarding), parametri propri di ciascun processo di routing (OSPF, ...)
- configurazione avanzata: access lists, etc.



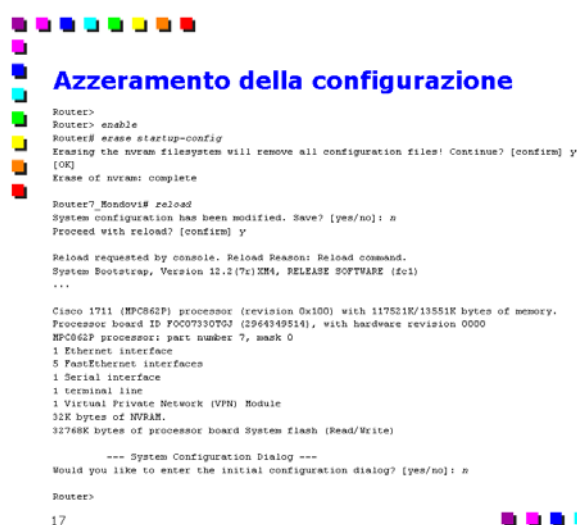
1.3.2. Azzeramento della configurazione

In figura è riportata la procedura da seguire per l'azzeramento della configurazione. In dettaglio, è necessario digitare i seguenti comandi:

```
Cisco> enable
      Entra in modalità privilegiata.

Cisco# erase startup-config
      Cancella la configurazione presente nella memoria NVRAM.
      A seguito di tale comando, l'apparato presenterà una domanda di conferma, a cui è necessario rispondere "y".

Cisco# reload
      Forza il reavvio del router. A seguito di questa domanda, il router effettua un controllo e si accorge che la configurazione attiva è diversa da quella presente nella NVRAM.
```



Pertanto, presenta una domanda che suggerisce all'utente di salvare la configurazione attuale nella NVRAM per evitare di perderla. A tale domanda è necessario rispondere `n`"; in quanto il nostro scopo è appunto quello di azzerare il router, e quindi farlo iniziare con una configurazione spoglia.

A seguito della nostra risposta, l'apparato presenterà una seconda domanda di conferma, a cui è necessario rispondere `y`". A questo punto il riavvio ha inizio.

...

Segue una fase in cui l'apparato procede al bootstrap. Al termine di questa fase, l'apparato presenterà una domanda nella quale suggerisce di entrare in una fase di configurazione guidata. A questa domanda è necessario rispondere `n`". A questo punto, l'apparato inizierà le sue interfacce e si posizionerà in modalità utente.

1.3.3. Configurazione di base

Anzichè presentare in questa sezione l'elenco dei principali comandi possibili, si presenta un esempio di configurazione reale a partire da un router spoglio.

Cisco> enable

Entra in modalità amministrazione (può richiedere una password, se è stata settata in precedenza).

Cisco# configure terminal

Entra in modalità di configurazione; l'apparato si attiene ora all'immissione di comandi dal terminale.

Cisco(config)# hostname *name*

Assegna un nome al router; questo verrà utilizzato come prompt (ad esempio `MioRouter>`).

Cisco(config)# enable password *ena_pwd*

Abilita (e imposta) la password necessaria per il passaggio dalla modalità utente a quella privilegiata (ossia la password richiesta a seguito della digitazione del comando `enable`). Si noti come la password impostata verrà visualizzata in chiaro nella configurazione corrente. **Attenzione:** si veda la nota al fondo del paragrafo.

Cisco(config)# username *name* password *passwd*

Associa password a singoli utenti del router. Può essere utilizzato sia per accedere ad un router, sia per configurare il router ad accedere in dial/up ad un altro apparato. Nel secondo caso, il router usa come password quella associata al proprio nome. **Attenzione:** si veda la nota al fondo del paragrafo.

Cisco(config)# line vty 0 4

Configura i terminali virtuali: il primo numero dopo il VTY indica il numero del primo terminale virtuale; il secondo indica il numero dell'ultimo terminale virtuale (in questo caso è stata configurata la possibilità di 5 accessi contemporanei al router).

Cisco(config-line)# login

Imposta l'obbligo di una fase di login nell'accesso via telnet (ma non impone una password).

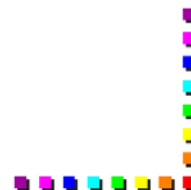


Configurazione di base

```
Cisco> enable
Cisco# configure terminal
Cisco(config)# hostname cisco
Cisco(config)# enable password ena_pwd
Cisco(config)# line vty 0 4
Cisco(config-line)# login
Cisco(config-line)# password telnet_pwd
Cisco(config-line)# exit
Cisco(config)# exit
```

Attenzione!

18




```
Cisco(config-line)# password telnet_pwd
```

Abilita (e configura) la password di accesso al router via telnet.

Attenzione: si veda la nota al fondo del paragrafo.

```
Cisco(config-line)# exit
```

Esce dalla modalità di configurazione dei terminali virtuali.

```
Cisco(config)# exit
```

Esce dalla modalità di configurazione.

Nota importante Nelle esercitazioni di laboratorio si faccia attenzione a non impostare password di nessun tipo. Infatti, nel momento in cui la password non sia conosciuta, è necessario procedere ad una operazione di password recovery che è relativamente complessa. Pertanto, ai fini di laboratorio si consiglia caldamente di non impostare password.

NOTA: Nella visualizzazione di una configurazione (ad esempio `show run`) vengono riportate solo le opzioni che non sono al valore standard.

1.3.4. Gestione e visualizzazione dei files di configurazione

Negli apparati Cisco è fondamentale avere chiari i comandi per la visualizzazione e la gestione della configurazione. In particolare, la visualizzazione della configurazione è fondamentale per verificare che eventuali comandi impartiti siano effettivamente stati applicati dall'apparato. I comandi più importanti sono i seguenti:

```
Cisco# show running-config
```

Visualizza l'attuale configurazione (RAM) dell'apparato.

```
Cisco# copy running-config startup-config
```

Salva nella NVRAM la configurazione attiva.

```
Cisco# copy running-config flash:myconfig
```

Salva l'attuale configurazione in un file chiamato `myconfig` e memorizzato nella memoria FLASH. Analogamente, è possibile salvare la configurazione in un file su un server TFTP (`copy running-config tftp:myconfig`); in questo caso il server TFTP deve essere attivo e raggiungibile a livello IP.

!!Attenzione!! All'atto della digitazione di questo comando, il router chiederà di confermare la formattazione della memoria FLASH prima di memorizzare la configurazione. Digitare, altrimenti tutte le informazioni sulla FLASH: verranno perse. Nel caso in cui questo si verifichi è necessario ripristinare il sistema operativo sulla memoria FLASH con l'apposita procedura.

```
Cisco# show startup-config
```

Visualizza la configurazione salvata su NVRAM.

```
Cisco# show configuration
```

Attenzione: contrariamente a quanto sembrerebbe intuitivo, questa configurazione NON è quella attualmente attiva sul router, ma quella salvata su NVRAM. Pertanto, si consiglia a scanso di equivoci di utilizzare i comandi che fanno uso delle parole chiave `running-config` e `startup-config`

```
Cisco# erase startup-config
```

Gestione e visualizzazione della configurazione

```
Cisco# show running-config
Building configuration...

Current configuration : 919 bytes
!
version 12.3
service timestamps debug datetime msec
no service password-encryption
!
hostname Cisco
...

Cisco#
Cisco# copy running-config startup-config...
Cisco# copy running-config flash:config-prova
Cisco# show startup-config
...
Cisco# erase startup-config
Cisco#
Cisco# dir flash:
```

Attenzione!

Una buona pratica di backup per il salvataggio delle configurazioni è quella di fare "cut-and-paste" della configurazione visualizzata su schermo e salvarla sul proprio hard disk

Cancella la configurazione presente nella memoria NVRAM.

A seguito di tale comando, l'apparato presenterà una domanda di conferma, a cui è necessario rispondere "Y".

!!Attenzione!! Si faccia attenzione al comando `erase` in quanto potrebbe essere utilizzato per cancellare anche altre zone di memoria. In particolare, potrebbe essere utilizzato per cancellare la memoria FLASH, con la conseguente cancellazione del sistema operativo (e il conseguente blocco dell'apparato al successivo riavvio).

```
Cisco# dir flash
```

Visualizza l'elenco dei files contenuti nella memoria FLASH.

Una buona pratica di backup per il salvataggio delle configurazioni è quella di fare "cut-and-paste" della configurazione visualizzata su schermo e salvarla sul proprio hard disk. In questo modo sarà possibile riapplicare la configurazione direttamente da terminale, dopo aver eventualmente riavviato il router con l'apposita procedura.

Il comando fondamentale è perciò il comando `show`

1.4. Problematiche di controllo e debugging

1.4.1. Controllo dell'apparato

I principali comandi di utilità, controllo e debugging sono solitamente disponibili solo in modalità privilegiata. I comandi fondamentali ricadono sotto le seguenti categorie:

- `copy`: per la copia dei files di configurazione
- `show`: per la visualizzazione in generale. Può essere utilizzato per visualizzare files di configurazione, lo stato delle interfacce, lo stato del routing, lo stato delle cache (es. `show ip arp`), e altro.
- `erase` per la cancellazione di file.
- `clear`: per l'azzeramento di strutture calcolate a run-time (es. le cache, i contatori delle interfacce, ecc).
- `debug`: per attivare informazioni di debug sul monitor a seguito di determinati eventi, specificati nel proseguo del comando stesso.



Controllo e debugging dell'apparato

Principali categorie di comandi

- Copy
- Show
- Erase
- Clear
- Debug

Per quanto riguarda il debug

- Selezionare accuratamente la grandezza di cui impostare il debug, pena l'overflow di informazioni sulla console
- Debug poco selettivi possono saturare il router (CPU e banda)

```
Cisco# show interfaces
Cisco# show ?
Cisco#
Cisco# clear arp-cache
Cisco# clear ?
Cisco#
Cisco# term mon
Cisco# debug <debug desiderato>
Cisco# debug ?
Cisco# no debug all
Cisco# debug ip packet dump
Cisco# term no mon
```



Alcuni esempi di comando sono i seguenti:

```
Cisco# show comando
```

Visualizza i parametri relativi a *comando*.

```
Cisco# show interfaces
```

Visualizza lo stato delle interfacce di rete.

```
Cisco# show ? (oppure show ip ?)
```

Elenca i parametri visualizzabili.

```
Cisco# clear arp-cache
```

Cancella tutti i valori contenuti nella ARP cache dell'apparato.

```
Cisco# debug comando
```

Attiva il debug su una funzione specifica.

```
Cisco# debug ?
Mostra le attività su cui il debugging può essere attivato.

Cisco# debug ip packet dump
Stampa su monitoring il dump esadecimale dei pacchetti che
passano nel router; è un comando molto pericoloso per la sua
capacità di saturare il router.

Cisco# no debug all
Per disabilitare tutti i comandi debug attivati in precedenza.

Cisco# term mon (term no mon per la sua disattivazione)
Attiva il debugging sul monitor (necessario solo via telnet, per
attivare l'output su terminale locale e non sulla console del router).
```

Il debug deve essere lanciato con cura evitando di saturare la CPU e la capacità trasmissiva (nel caso di debug remoto) a disposizione del router. Non è infrequente che il router risulti saturato dalla gestione dei messaggi di debug e che non riesca più ad accettare altri comandi di nessun tipo. In queste condizioni il debug provoca la totale perdita di controllo sul router che può essere riattivato solamente attraverso l'utilizzo della console dello stesso.

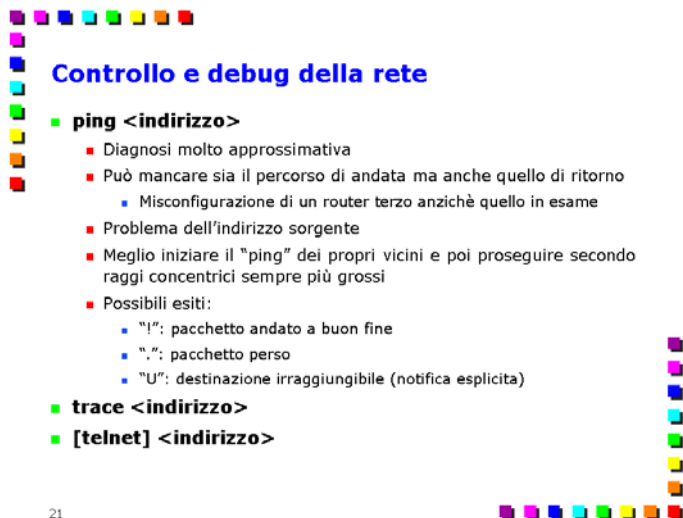
1.4.2. Controllo operativo della configurazione

Altri comandi utili per il controllo dell'operabilità del router sono quelli classici dell'ambiente TCP/IP, e cioè:

ping *indirizzo*

Controlla la raggiungibilità di indirizzo. Normalmente vengono inviati 5 pacchetti e il risultato viene visualizzato sullo schermo con i seguenti simboli:

- "!" : la risposta ha avuto esito positivo
- "U" : il router ha ricevuto una notific di irraggiungibilità (es. un pacchetto ICMP di errore)
- ". " : la risposta non è pervenuta in tempo. Si consideri che, nel caso di apparati poco performanti, il primo PING può essere perso a causa del tempo necessario per riempire le strutture dati interne agli apparati.



Controllo e debug della rete

- **ping <indirizzo>**
 - Diagnosi molto approssimativa
 - Può mancare sia il percorso di andata ma anche quello di ritorno
 - Misconfigurazione di un router terzo anzichè quello in esame
 - Problema dell'indirizzo sorgente
 - Meglio iniziare il "ping" dei propri vicini e poi proseguire secondo raggi concentrici sempre più grossi
 - Possibili esiti:
 - "I": pacchetto andato a buon fine
 - ".": pacchetto perso
 - "U": destinazione irraggiungibile (notifica esplicita)
- **trace <indirizzo>**
- **[telnet] <indirizzo>**

21

Si noti come in taluni casi la mancanza di risposta del PING sia dovuto al mancato recapito del pacchetto di risposta. Questo è dovuto al fatto che l'indirizzo sorgente del pacchetto viene deciso autonomamente dall'apparato (ad esempio un router ha tipicamente più di un indirizzo IP e, in mancanza di un indirizzo di loopback, può scegliere un indirizzo a caso come sorgente) e potrebbe non esistere una route per quel particolare indirizzo. In questi casi conviene digitare il comando PING senza parametri, che fa sì che il router chieda interattivamente i vari parametri da usare, tra i quali anche l'indirizzo sorgente.

trace *indirizzo*

Visualizza il percorso verso la destinazione; nel caso di più percorsi, li visualizza tutti

[telnet] indirizzo

Apri un terminale virtuale con la destinazione

Può essere importante ricordare che questi strumenti di diagnostica sono molto approssimativi. Ad esempio una mancanza di risposta al comando *ping* non implica automaticamente la mancanza di una route per raggiungere la destinazione, ma può anche essere l'eventuale mancanza di una route per il ritorno. E' quindi importante accertarsi in prima battuta che i vicini al router in esame siano raggiungibili, per poi proseguire il debug secondo cerchi concentrici a raggio sempre maggiore.

1.5. Configurazione e controllo delle interfacce

L'IOS assegna ad ogni interfaccia fisica di rete un identificativo univoco all'interno del sistema. Questo identificativo è formato dalla tipologia dell'interfaccia (ad esempio, le interfacce Ethernet avranno un nome che inizierà con `Ethernet`, le interfacce Fast Ethernet con `FastEthernet`, la console con `CON`, e così via) seguito da un identificativo numerico (quindi si troveranno `Ethernet0`, `Ethernet1`, `Serial0`, `Serial1`) in ordine crescente. Nel caso di apparati composti da chassis, il numero dell'interfaccia comprende anche il numero della linecard (ad esempio `Ethernet0/1` indica la seconda Ethernet della prima linecard). In certi casi, alcuni apparati hanno nomi anche su tre livelli numerici (es. `Ethernet0/0/1`).

Da questo punto in poi si seguiranno le seguenti regole:

- i comandi, eccetto quando chiaramente specificato, saranno comandi disponibili solamente da in modalità configurazione (o da un suo sottomenu)
- a questa regola fanno eccezione i comandi di tipo `show`, i quali sono disponibili esclusivamente in modalità privilegiata.

1.5.1. Comandi di configurazione

1.5.1.1. Stato delle interfacce

L'interfaccia fisica di un apparato Cisco può trovarsi nei seguenti tre stati:

- *Administratively Down*: l'interfaccia è stata disabilitata da management (ad esempio mediante un comando `shutdown`) e non può né inviare né ricevere i pacchetti;
- *Down*: l'interfaccia è abilitata a funzionare, ma qualcosa ne impedisce il funzionamento e il router non rileva la presenza del segnale di portante sull'interfaccia. Ad esempio, può capitare su una interfaccia seriale in modalità DCE senza il *clockrate* attivato.
- *Up*: l'interfaccia è abilitata a funzionare e il segnale di portante è correttamente rilevato. Questo non vuole necessariamente dire che l'interfaccia sia completamente funzionante: ad esempio un link seriale



Interfacce: status

Le interfacce possono essere:

- Administratively Down
- Down (non c'è il segnale della portante)
- Up

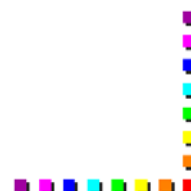
Il protocollo di linea su di esso, invece può essere:

- Up
- Down

Comando:

```
Cisco# show interface
```

22



- potrebbe non funzionare a causa dell'encapsulation, magari PPP da un lato e HDLC dall'altro.

Il protocollo di linea rappresenta invece lo stato della connessione sulla rete e può assumere i seguenti valori:

- **Downn**: il protocollo di linea non è attivo (ad esempio l'encapsulation è errata, etc).
- **Up**: il protocollo di linea è attivo e l'interfaccia è pertanto in grado di inviare i propri dati verso sul canale fisico.

1.5.1.2. Comandi generali di configurazione

Sono quei comandi che possono essere sostanzialmente applicati su tutte le interfacce fisiche. Si riporta una traccia di configurazione che fa uso di questi comandi (si noti che non tutti questi comandi vengono utilizzati in una configurazione normale)..

Cisco# configure terminal
Entra in modalità configurazione.

Cisco(config)# ip subnet-zero
Abilita l'uso della subnet zero sulle interfacce e sulle routing updates. In mancanza di questo comando le reti terminanti con "0" non sono ammesse se non con netmask "naturali" (/24, /16 e /8); ad esempio non è ammessa la rete 130.192.1.0/30, mentre lo è la 130.192.1.4/30.

Cisco(config)# interface name

Entra nel sottomenù di configurazione dell'interfaccia name. Questo comando permette l'entrata nel sottomenu di configurazione delle interfacce abilitando quindi la digitazione dei comandi successivi.

Cisco(config-if)# ip addressindirizzo maschera

Assegna all'interfaccia l'indirizzo e la maschera indicati.

Cisco(config-if)# ip addressindirizzo maschera secondary

L'opzione secondary indica che l'indirizzo è secondario e permette la configurazione di più indirizzi IP sulla stessa interfaccia fisica. Si ricordi che senza questa opzione secondary l'indirizzo IP verrebbe sovrascritto all'indirizzo precedente.

Cisco(config-if)# descriptiondescrizione_interfaccia

Assegna una stringa letterale per la descrizione dell'interfaccia.

Cisco(config-if)# no shutdown

Abilita il funzionamento di quell'interfaccia (può essere utilizzato ad esempio dalle interfacce ISDN per forzare la terminazione della chiamata corrente); per riattivare l'interfaccia è necessario digitare no shutdown.

Cisco(config-if)# mtu valore

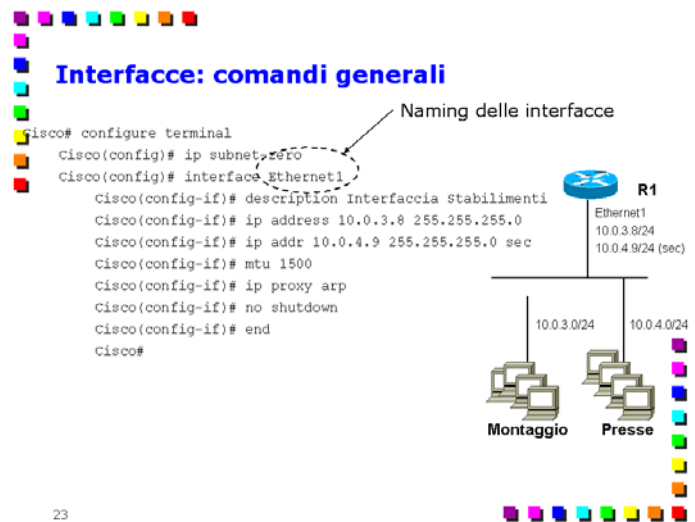
Definisce una MTU diversa rispetto a quella standard.

Cisco(config-if)# ip proxy arp

Abilita il proxy arp su quell'interfaccia.

Cisco(config-if)# end

Esce dal menù di configurazione e ritorna in modalità privilegiata.



1.5.1.3. Comandi di visualizzazione e controllo

I comandi di controllo sono attivabili in modalità privilegiata e sono normalmente dei comandi di tipo *show*.

`show interface [nome]`

Visualizza gli attuali dati relativi alle interfacce del router; se viene specificato *nome* vengono visualizzati solamente i dati relativi a quell'interfaccia. Questo comando visualizza, tra gli altri dati, lo stato dell'interfaccia e quello del suo protocollo di linea.

`show interfaces [type]`

Visualizza gli attuali dati relativi ad un particolare tipo di interfacce del router (ad esempio tutte le interfacce Ethernet).

`show controllers [interface]`

Visualizza tutte le informazioni relative ad un controller di interfaccia; è utilizzato soprattutto per il debug dal personale tecnico per visualizzare dati interni all'interfaccia che potrebbero segnalare un malfunzionamento. Ad esempio, nel caso di link seriale, questo visualizza se la seriale è utilizzata in modalità DTE o DCE, il valore dell'eventuale clockrate, etc.

`show cdp neighbors`

Visualizza l'elenco dei router vicini a quello in esame; questa informazione è ottenuta grazie ad un protocollo proprietario Cisco (Cisco Discovery Protocol), abilitato di default su tutti i router.

`show process cpu`

Visualizza i dati di occupazione della CPU corrente e i processi attualmente attivi; è utile per verificare il grado di carico attuale sul router.

`clear interface name`

Effettua un reset hardware dell'interfaccia selezionata.

`clear counters`

Azzera i contatori (ad esempio il numero di pacchetti trasmessi, ...) relativi all'interfaccia selezionata.



Comandi di visualizzazione e controllo

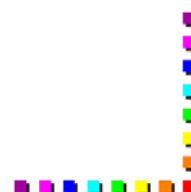
Comandi "show"

```
Cisco# show interfaces
Cisco# show interfaces ethernet0
Cisco# show interfaces ethernet
Cisco# show controllers serial 1 [notare lo spazio]
Cisco# show cdp neighbors
Cisco# show process CPU
```

Comandi "clear"

```
Cisco# clear interface ethernet0
Cisco# clear counters ethernet0
```

24



1.5.2. Esempio di configurazione di interfaccia FastEthernet

Si riporta un esempio di configurazione tipico di un'interfaccia Ethernet.

```
Cisco> enable
```

Entra in modalità privilegiata.

```
Cisco# configure terminal
```

Entra in modalità di configurazione

```
Cisco(config)# interface FastEthernet0
```

Entra nella modalità di configurazione dell'interfaccia FastEthernet0.

Nota: questa interfaccia è di tipo tradizionale (non switched), pertanto la configurazione degli indirizzi IP va fatta direttamente sull'interfaccia stessa.

```
Cisco(config-if)# ip address
192.168.100.2 255.255.255.0
```

Assegnazione dell'indirizzo IP (e netmask) all'interfaccia.

```
Cisco(config-if)# no shutdown
```

Attiva l'interfaccia, cancellandola dallo stato *shutdown* (spegnimento amministrativo).

```
Cisco(config-if)# end
```

Esce dal menù di configurazione e ritorna in modalità privilegiata.

Esempio di configurazione Ethernet



```
Cisco> enable
Cisco# configure terminal
Cisco(config)# interface FastEthernet0
Cisco(config-if)# ip address 192.168.100.2 255.255.255.0
Cisco(config-if)# no shutdown
Cisco(config-if)# end
Cisco#
```

1.5.3. Esempio di configurazione di interfaccia FastEthernet switched in modalità *routed*

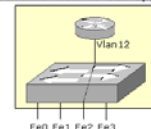
Le interfacce *switched* possono essere usate sia come interfaccia di livello data-link (su una rete switched, appunto), oppure come interfacce di livello network (ossia come interfacce di un router), a seconda della configurazione sull'interfaccia stessa. Nel momento in cui si vuole utilizzare una interfaccia *switched* in modalità *routed*, la configurazione è leggermente diversa da quella di una interfaccia *routed* nativa, principalmente perchè IOS non consente di assegnare l'indirizzo IP direttamente all'interfaccia, ma l'indirizzo IP va assegnato ad una interfaccia virtuale VLAN, la quale deve essere a sua volta associata all'interfaccia fisica. Un esempio è riportato in figura: si vuole collegare 2 apparati attraverso un cavo diretto. Una estremità del cavo viene però terminata su una interfaccia *switched*. Tuttavia, dal punto di vista della configurazione "esterna", deve apparire come se l'interfaccia in esame risponda all'indirizzo 192.168.100.2. Si riporta a questo punto una possibile configurazione dell'apparato in esame:

Esempio di configurazione FastEthernet Switched

Topologia logica



Schema interno dell'apparato



```
Cisco> enable
Cisco# configure terminal
Cisco(config)# interface FastEthernet2
Cisco(config-if)# switchport access vlan 12
Cisco(config-if)# no ip address
Cisco(config-if)# no shutdown
Cisco(config-if)# exit
Cisco(config)# interface Vlan12
Cisco(config-if)# ip address 192.168.100.2 255.255.255.0
Cisco(config-if)# end
Cisco#
```

Default: access mode, VLAN 1

```
Cisco(config)# interface FastEthernet2
```

Entra nella modalità di configurazione dell'interfaccia fisica FastEthernet2

Nota: questa interfaccia è di tipo switched, pertanto la configurazione degli indirizzi IP va fatta assegnando l'interfaccia ad una determinata VLAN, ed assegnando l'indirizzo IP alla VLAN stessa.

```

Cisco(config-if)# switchport access vlan 12
    Assegnazione dell'interfaccia alla VLAN 12 in modalità access. Dal
    momento che in questa modalità le trame ethernet non vengono
    taggate con il VLAN-ID, il valore 12 ha validità puramente interna
    all'apparato, e deve essere uguale al corrispondente numero
    presente nel comando interface vlan

Cisco(config-if)# no ip address
    Nessun indirizzo IP è assegnato all'interfaccia FastEthernet fisica.

Cisco(config-if)# no shutdown
    Attiva l'interfaccia, cancellandola dallo stato di shutdown
    (spegnimento amministrativo).

Cisco(config-if)# exit
    Esce dal contesto di configurazione dell'interfaccia FastEthernet2.

Cisco(config)# interface Vlan12
    Entra nella modalità di configurazione dell'interfaccia virtuale Vlan12.
    Questa interfaccia è necessaria per attivare un'indirizzo di livello 3
    (routed) sull'intera VLAN.
    Nota: questa interfaccia è di tipo virtuale e può venire creata/
    cancellata dinamicamente a seconda delle assegnazioni delle VLAN
    alle interfacce Ethernet switched. In particolare, questo comando
    non solo permette di entrare nella configurazione della interfaccia
    VLAN12, ma impartisce anche all'IOS il comando di creazione di tale
    interfaccia virtuale. Il numero "12" deve essere uguale a quello
    associato al comando switchport presente nell'interfaccia
    FastEthernet reale.
    Nota: una volta create, le interfacce VLAN sono attive
    automaticamente; pertanto non è necessario digitare esplicitamente
    il comando no shutdown

Cisco(config-if)# ip address 192.168.12.2 255.255.255.0
    Assegnazione dell'indirizzo IP (e netmask) all'interfaccia virtuale.

Cisco(config-if)# end
    Esce dal menù di configurazione e ritorna in modalità privilegiata.

```

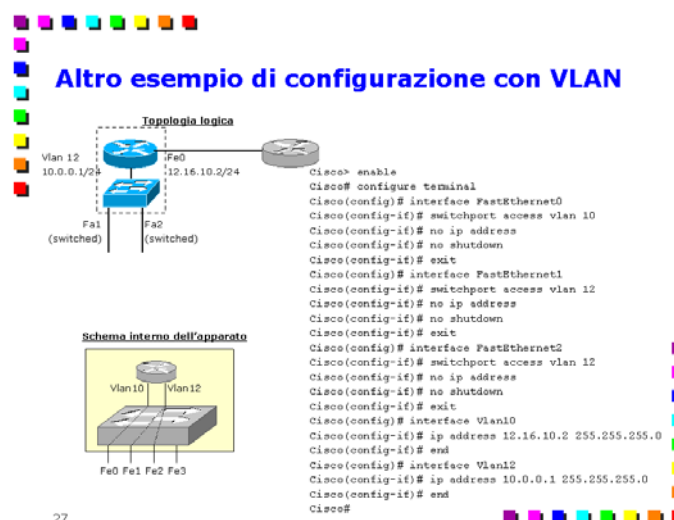
E' importante ricordare come l'interfaccia VLAN sia di tipo virtuale, quindi viene creata dinamicamente a seconda dei comandi dell'operatore. In altre parole, in un apparato appena inizializzato questa interfaccia non verrà visualizzata dal comando `show running-config`. Tuttavia, a seguito della creazione dell'interfaccia stessa, lo stesso comando `show running-config` visualizzerà questa nuova interfaccia nel file di configurazione.

Le interfacce *switched* sono sempre associate ad una VLAN. Qualora il comando `switchport` non sia presente esplicitamente, la porta viene configurata automaticamente in modalità accesso ed associata alla VLAN 1.

1.5.3.1. Esempio complesso di configurazione

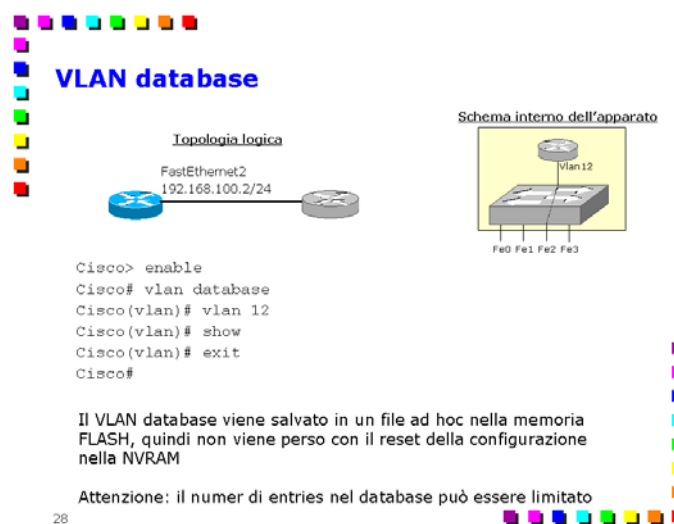
In figura è riportato un possibile scenario di configurazione maggiormente complesso rispetto al precedente. Tralasciando i dettagli relativi ai comandi impartiti, in tale esempio l'apparato avrà una interfaccia (FastEthernet0) utilizzata solamente in modalità *routed*, mentre altre due (FastEthernet1 e FastEthernet2) vengono utilizzate in modalità *switched*. Tuttavia, le ultime due interfacce sono associate ad un indirizzo IP che rappresenta il default gateway per le stazioni collegate alle interfacce in esame.

La configurazione precede quindi la creazione di due VLAN, la prima associata ad una sola interfaccia *switched*, la seconda associata alle ulteriori due interfacce in esame.



1.5.3.2. II VLAN database

Per quanto riguarda le interfacce VLAN, è necessario ricordare che alcuni apparati (tra cui quelli presenti nel laboratorio al Politecnico di Torino) attivano le VLAN solo a fronte di una esplicita configurazione del VLAN database **che non è fatto automaticamente** digitando la configurazione nella modalità tradizionale del router. Pertanto, è necessario accertarsi della configurazione delle VLAN utilizzando i seguenti comandi:



Cisco> enable
Entra in modalità privilegiata.

Cisco# vlan database
Entra nel menù di gestione del VLAN database.
Nota: i comandi riportati in seguito non devono essere digitati tutti: è necessario digitare solamente quelli relativi all'azione (visualizzazione delle VLAN attive, aggiunta di una nuova VLAN, cancellazione di una VLAN esistente) che si vuole intraprendere.

Cisco(vlan)# vlan45
Attiva una nuova VLAN (contraddistinta dal numero 45).

Cisco(vlan)# no vlan44
Elimina una VLAN precedentemente attiva (contraddistinta dal numero 44).

Cisco(vlan)# show
Visualizza le VLAN attualmente configurate nel VLAN database.

Cisco(vlan)# exit
Esce dalla modalità di gestione del VLAN database e rende attivi i cambiamenti impostati.
Nota: mentre i comandi di configurazione (in modalità *configure terminal*) sono immediatamente attivi, i comandi relativi al VLAN database vengono applicati solamente all'atto del comando *exit*.

La configurazione del VLAN database viene salvata sulla memoria FLASH, pertanto viene automaticamente riattivata al successivo reboot del router.

Normalmente (per quanto riguarda i router di laboratorio al Politecnico di Torino) non è necessario configurare il VLAN database in quanto già configurato prima delle esercitazioni.

E' importante ricordare che la dimensione del VLAN database può essere limitata su alcuni apparati (ad es 4 VLAN nel caso di piccoli apparati). In questo caso è necessario eventualmente limitare alcune VLAN presenti nel database prima di poter configurare nuovi valori.

1.5.4. Interfacce seriali

Si riportano alcuni comandi specifici per interfacce seriali:

`encapsulation ppp | hdlc | x25 | frame-relay`

Definisce il tipo di protocollo sul link fisico. A differenza dei link Ethernet, sui link punto-punto esistono numerosi protocolli di livello 2 che possono essere usati; questo comando serve a specificare quello in uso sul link in esame. HDLC è una versione proprietaria CISCO (permette il multiprotocol), per cui è necessario usare il PPP quando è necessaria l'interoperabilità con altri costruttori. HDLC non prevede autenticazione. Le encapsulations di tipo X.25 - Frame Relay sono utilizzate quando l'interfaccia seriale è collegata ad un accesso fisico in queste tecnologie.

`clockrate valore`

Definisce la velocità del link seriale. Il clock rate va abilitato solo nel caso di connessione di router con cavo DCE/DTE, e solo sul router che dispone del lato DCE (ossia lato "centrale telefonica"). Questo comando serve ad un operatore per definire la massima velocità di linea a cui l'utente può trasmettere. In un normale collegamento geografico diretto (CDN, HDSL, etc) il clock viene fornito dal modem e non dall'interfaccia, rendendo quindi inutile questo comando.

`ppp authentication chap | pap`

Abilita l'uso dell'autenticazione su quel particolare link PPP. Per autenticarsi dall'altra estremità del link, il router usa come nome utente il proprio nome contenuto nel comando generale `username`. Entrambi i protocolli di autenticazione possono essere contemporaneamente attivi, e vengono tentati nell'ordine in cui compaiono. Nel caso in cui il protocollo sia CHAP è necessaria impostare non una password, ma la chiave *secret* utilizzata per la sfida da parte di questo protocollo.

`Cisco(config-if)# no fair-queue`

Disattiva algoritmi di scheduling avanzati sull'interfaccia. Questo comando non è peculiare dei link seriali, anche se viene utilizzato maggiormente su questa tipologia di collegamenti in quanto i suoi benefici sono superiori su link a bassa velocità.

1.5.4.1. Esempio di configurazione di interfaccia seriale

Un esempio di configurazione riferito alla rete indicata in figura, è il seguente:

```
Cisco> enable
      Entra in modalità privilegiata.

Cisco# configure terminal
      Entra in modalità di configurazione

Cisco# interface Serial0
      Entra nella modalità di configurazione dell'interfaccia Serial0.
Nota: questa interfaccia è di tipo DCE
e quindi è necessario configurare
anche il clockrate. Per visualizzare se
un'interfaccia è di tipo DTE o DCE è
sufficiente digitare il comando show
controllers serial 0, in modalità
privilegiata.
```

```
Cisco(config-if)# ip address 192.168.89.1
255.255.255.0
```

Assegnazione dell'indirizzo IP (e netmask) all'interfaccia .

```
Cisco(config-if)# encapsulation ppp
      Attiva la tramatura data-link di tipo PPP.
```

```
Cisco(config-if)# no shutdown
      Attiva l'interfaccia, cancellandola dallo stato di shutdown
      (spegnimento amministrativo)
```

```
Cisco(config-if)# clockrate 64000
```

Questo comando imposta la velocità del link, e deve essere digitato solamente sulle interfacce che agiscono come DCE e se le interfacce DTE/DCE sono collegate da un cavo diretto, senza la presenza di modem intermedi.

```
Cisco(config-if)# end
      Esce dal menù di configurazione e ritorna in modalità privilegiata.
```



Esempio di configurazione link seriale

Alcuni comandi peculiari:

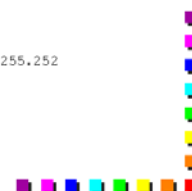
```
Cisco(config-if)# encapsulation ppp | hdlc | x25 | frame-relay
Cisco(config-if)# ppp authentication chap | pap
Cisco(config-if)# no fair-queue
Cisco(config-if)# clockrate valore
```

Esempio di configurazione:

```
Cisco> enable
Cisco# configure terminal
Cisco(config)# interface Serial0
Cisco(config-if)# encapsulation ppp
Cisco(config-if)# ip address 192.168.100.2 255.255.255.252
Cisco(config-if)# no shutdown
Cisco(config-if)# clockrate 64000
Cisco(config-if)# end
Cisco#
```



29



1.5.5. Configurazione di Frame Relay

La configurazione di interfacce frame Relay è più complessa di interfacce tradizionali grazie al maggior numero di possibilità offerte da questa tecnologia. A differenza di altri link layers, non esistono interfacce di tipo "frame relay"; la configurazione passa quindi attraverso l'utilizzo di interfacce seriali collegate ad un'opportuna interfaccia di livello fisico.

Le interfacce possono essere di tipo *multipoint* (la scelta di default) oppure *point-to-point*. Le prime agiscono come una normale rete di tipo NBMA (Non-Broadcast Multiple Access), quindi è possibile definire più hosts con la stessa subnet, risparmiando indirizzi. Tuttavia questa scelta va bene solamente se la topologia fisica è di tipo "a maglia completa". Le interfacce di tipo point-to-point, invece agiscono come dei canali punto-punto dedicati (as. CDN), quindi ogni



Configurazione di Frame Relay

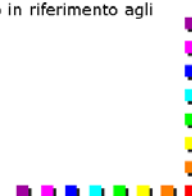
Caratteristiche

- Configurazione su interfacce seriali
- Possibilità di interfacce oppure sub-interface
- Multipoint oppure Point-to-point

Configurazione

- Scelta della seriale in esame (anche subinterface)
- Definizione dell'Encapsulation
- Configurazione del mapping statico o dinamico in riferimento agli indirizzi remoti

30



canale richiede una propria sottorete. Questa soluzione è adatta a topologie fisiche di tipo stellare oppure a maglia non completa.

Siccome non è possibile utilizzare il protocollo ARP su una rete NBMA, è necessario stabilire l'indirizzo IP dell'endpoint remoto. Cisco offre sia la possibilità di definire staticamente l'indirizzo IP dell'endpoint remoto, sia di lasciare al router il compito di scoprirlo da solo attraverso il protocollo di Inverse ARP.

Dal momento che Frame Relay offre la possibilità di configurare più collegamenti diversi (DLCI) sulla stessa interfaccia fisica (Serial), Cisco offre la possibilità di definire, all'interno di un'interfaccia seriale, delle sub-interfacce ognuna con le proprie caratteristiche di encapsulation, topologia, dynamic/static mapping degli indirizzi.

I passi obbligatori per la configurazione sono:

- abilitazione della Frame Relay Encapsulation sull'interfaccia seriale
- configurazione del mapping statico o dinamico degli indirizzi remoti

1.5.5.1. Principali comandi di configurazione

I comandi principali di configurazione sono i seguenti:

`encapsulation frame-relay [ietf]`

Abilita e specifica il tipo di encapsulation relativamente all'interfaccia in esame. Questo è un comando di interfaccia e può operare sia su interfacce seriali, sia su sub-interface.

`frame-relay lmi-type [ansi | cisco | q933i]` **(opzionale; default: cisco)**

Imposta il tipo di protocollo LMI necessario per parlare con la rete Frame Relay

`frame-relay map protocol protocol-address`

`dlci [broadcast] [ietf] [cisco] (opzionale)`

Definisce un mapping statico l'indirizzo (ad esempio IP) dell'endpoint remoto e il PVC (attraverso il suo identificativo DLCI) necessario per raggiungerlo.

`interface type number.subinterface-number {multipoint | point-to-point}`

Definisce se l'interfaccia fisica (oppure la sub-interface) sono di tipo *point-to-point* oppure *multipoint*. La seconda scelta è quella di default. Nel caso in cui non sia ancora stata definita tale sub-interface, questo comando ha come effetto collaterale la sua creazione.

`frame-relay interface-dlci dlci`

Definisce esattamente qual è il DLCI da utilizzare per inviare il traffico a destinazione. Questo comando è obbligatorio per le interfacce di tipo *point-to-point* e per quelle *multipoint* nel quale è stata abilitata la risoluzione dinamica degli endpoints, mentre non è richiesto per le sub-interface *multipoint* configurate con mapping statico.



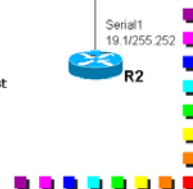
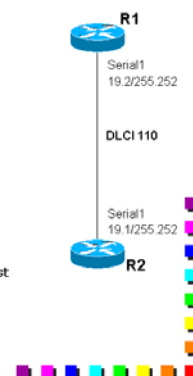
Configurazione FR su interfacce seriali

Configurazione dinamica su interfaccia

- configure terminal #Router R1
 - interface Serial1
 - ip address 192.168.19.2 255.255.255.0
 - encapsulation frame-relay
 - frame-relay interface-dlci 110

Configurazione statica su interfaccia

- configure terminal #Router R1
 - interface Serial1
 - ip address 192.168.19.2 255.255.255.0
 - encapsulation frame-relay
 - frame-relay map ip 192.168.19.1 110 broadcast



1.5.5.2. Gestione del traffico

La tecnologia Frame Relay offre la possibilità di definire alcune soglie di traffico (PIR, EIR, AR) con diversi significati. Il PIR è la massima quantità di dati trasmissibile con certezza dalla rete; l'EIR è la massima quantità di traffico in eccesso che la rete può trasmettere ma di cui non sono date garanzie di recapito (e che viene scartato con priorità maggiore nel momento in cui la rete è congestionata), AR è la velocità di accesso (Access Rate) dell'interfaccia Frame Relay.

La configurazione di questi parametri permette di ottenere performance migliori da parte della rete in quanto permette di attivare i meccanismi di notifica esplicita della congestione da parte del router di bordo (adaptive shaping). Il router sarà quindi in grado di regolare l'ammontare del traffico immesso in base alle notifiche di congestione che gli arriveranno dalla parte interna della rete FR, consentendo lo sfruttamento della massima capacità possibile in ogni condizione di carico della rete. Le applicazioni rimarranno quindi avvantaggiate in quanto, tendenzialmente, non si verificheranno errori nella rete; il TCP ne trarrà particolare giovamento in quanto vengono ad essere eliminati i timeout dovuti ad errori e ritrasmissioni evitando quindi l'andamento di throughput a dente di sega proprio del TCP.

I comandi principali di gestione del traffico sono:

`frame-relay traffic-shaping`

Attivazione della funzionalità di Traffic Shaping sull'interfaccia (o sub-interface) desiderata.

`frame-relay class nome`

Assegnazione di una particolare classe di traffico (chiamata *nome*) all'interfaccia; in questa classe di traffico (specificata a parte) saranno contenuti i parametri contrattualizzati (CIR, PIR ...) ed i criteri per l'adattamento dinamico del traffico offerto.

`map-class frame-relay nome`

Creazione di una nuova map-class (in modalità di configurazione) che conterrà la specifica del traffico.

`frame-relay traffic-rate average peak`

Specifica delle caratteristiche di traffico in termini di CIR (*average*) e CIR+EIR (*peak*).

`frame-relay adaptive-shaping becn`

Attivazione dell'adaptive shaping basato sul BECN; il router sarà in grado di immettere nella rete il maggior numero di dati senza tuttavia provocare perdite.



Gestione del traffico

Parametri

- CIR: Committed Information Rate
- EIR: Excess Information Rate
- PIR: Peak Information Rate
 - CIR + EIR
- Ar: Access Rate

Esempio

- Banda garantita (CIR) 64Kbps, banda in eccesso consentita (EIR) 64Kbps (→ PIR 128Kbps), velocità del canale di accesso (Ar) 2Mbps

Vantaggi

- Regolazione automatica del traffico da parte del router di bordo in base al carico attuale della rete
- Evita problemi di timeout del TCP

33

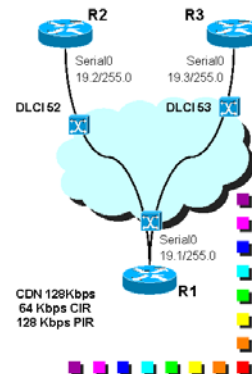


Gestione del traffico FR

configure terminal # Router R2

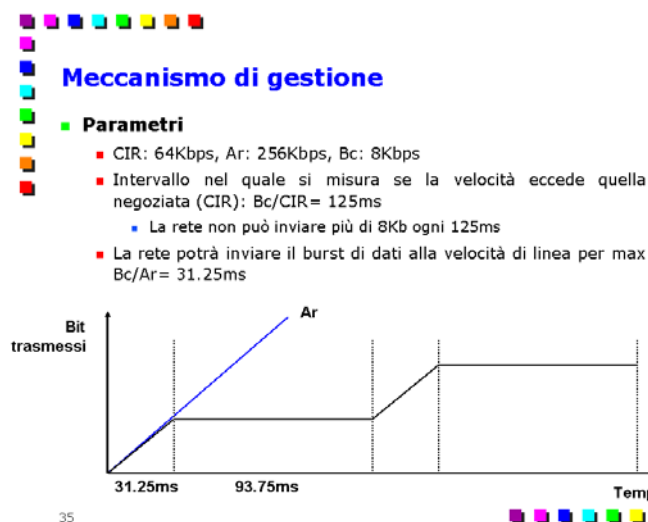
- interface Serial1
 - no ip address
 - encapsulation frame-relay
 - exit
- interface Serial1.1 point-to-point
 - ip address 10.0.19.2 255.255.255.0
 - frame-relay map ip 10.0.19.1 52
 - frame-relay traffic-shaping
 - frame-relay class R2
- map-class frame-relay R2
 - frame-relay traffic-rate 64000 128000
 - frame-relay adaptive-shaping becn
 - end

34



In alcune versioni di IOS esiste un problema legato al comando `frame-relay traffic-rate` per cui i parametri di questo comando non sono interpretati come *average peak* ma *peak peak*. Per impostare invece il vero valore del CIR è necessario utilizzare il comando aggiuntivo `frame-relay mincir out <average>` (ad esempio `frame-relay mincir out 64000` per ottenere un CIR di 64Kbps).

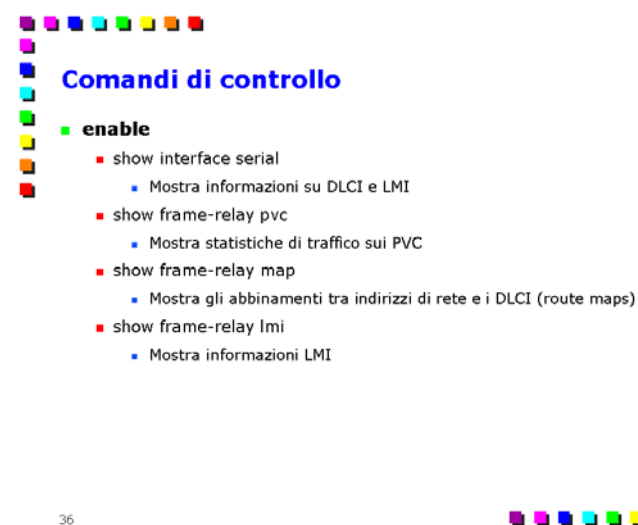
In figura viene mostrato il meccanismo adottato per regolare il traffico, basato principalmente sul Burst Committed (Bc) pari a 8Kbit. In questo esempio il traffico passa alla velocità di linea (256Kbps) fino ad esaurire il valore di Bc, quindi il router inserisce uno stop per poter soddisfare il rate negoziato. Le trasmissioni riprende al tempo 125ms, valore ricavato dividendo Bc per il CIR, quando il rate è ritornato conforme (64Kbps) al CIR negoziato dall'utente.



1.5.5.3. Comandi di controllo

I principali comandi di controllo sono i seguenti:

```
show interface serial
    Mostra informazioni su DLCI e LMI .
show frame-relay pvc
    Mostra statistiche di traffico sui PVC.
show frame-relay map
    Mostra gli abbinamenti tra indirizzi di rete e i DLCI (route maps).
show frame-relay lmi
    Mostra informazioni LMI.
```



1.5.6. IPv6

Ad esempio, per raggruppare tutti gli indirizzi compresi tra 10.0.16.0 e 10.31.255.255 con un'unica entry è possibile scrivere la coppia indirizzo-netmask 10.0.16.0 255.255.16.255, oppure la coppia indirizzo-wildcard 10.0.16.0 0.0.15.255.



Wildcard: esempio

Esempio

- Raggruppare in un'unica entry tutte le sottoreti comprese tra 10.0.16.0 e 10.0.31.0 (netmask 255.255.255.0)

network.host

Da 10.0.16.0

A 10.0.31.0

network.host (binario)

Da ...00010000.00000000

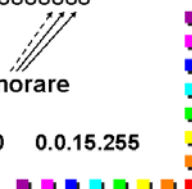
A ...00011111.00000000

Controllare

Ignorare

→ Indirizzo e Wildcard risultante: 10.0.16.0 0.0.15.255

39



1.7. Esercizi

1.7.1. Interfacce Unnumbered

Scrivere i comandi necessari alla configurazione dei router Cisco in relazione alla topologia indicata in figura.

Si scriva la configurazione sia nel caso in cui non si assegni un indirizzo IP all'interfaccia di loopback, sia nel caso in cui gli si assegni un indirizzo.

Soluzione

L'esercizio consiste nella configurazione delle interfacce e la configurazione dell'opportuna static route. La configurazione del router R2 è speculare ad R1.

Nel caso in cui non si assegni un indirizzo all'interfaccia di loopback la configurazione è la seguente:

```
configure terminal
interface serial0
  ip unnumbered loopback0
  exit
interface ethernet0
  ip address 192.168.14.1 255.255.255.0
  exit
ip route 192.168.10.0 255.255.255.0 serial0
end
```

Nel caso in cui si assegni un indirizzo all'interfaccia di loopback diventa:

```
configure terminal
interface serial0
  ip unnumbered loopback0
  exit
```



Interfacce Unnumbered

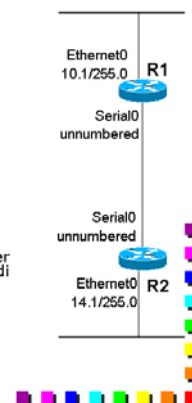
configure terminal #router R1

- interface serial0
 - ip unnumbered loopback0
 - exit
- interface loopback0
 - ip address 192.168.20.1 255.255.255.255
 - exit
- interface ethernet0
 - ip address 192.168.10.1 255.255.255.0
 - exit
- ip route 192.168.14.0 255.255.255.0 serial0
- ip route 192.168.24.1 255.255.255.255 serial0
- end

NOTA

- In corsivo vi sono le righe aggiuntive per l'assegnazione di un indirizzo IP all'interfaccia di loopback

41



```

interface loopback0
  ip address 192.168.24.1 255.255.255.255
exit
interface ethernet0
  ip address 192.168.14.1 255.255.255.0
exit
ip route 192.168.10.0 255.255.255.0 serial0
ip route 192.168.20.1 255.255.255.255 serial0
end

```

In questo caso non è possibile assegnare l'indirizzo 127.x.x.x all'interfaccia di loopback; in alcuni casi è invece possibile assegnare un indirizzo che è in sovrapposizione con un'altra interfaccia (es Ethernet0) evitando la seconda route statica e l'occupazione di un indirizzo (e una rete) aggiuntivi.

1.7.2. Configurazione di interfacce Frame-Relay

Scrivere i comandi necessari alla configurazione dei router Cisco in relazione alla topologia indicata in figura, supponendo che la linea seriale sia gestita attraverso la tecnologia Frame-Relay e che sia presente, ad ambedue le estremità, un solo canale logico con DLCI pari a 50. Si supponga che la configurazione sia di tipo point-to-point.

Soluzione

La soluzione migliore consiste nel creare delle sub-interfacce per la gestione di vari DLCI diversi (anche se a rigore non sarebbe obbligatorio in quanto è presente un solo canale virtuale). La configurazione è molto semplice e consiste nella creazione di opportune sub-interfacce per la gestione di eventuali canali logici diversi; l'unico comando degno di nota è appunto l'impostazione del canale logico (DLCI) opportuno all'interno della sub-interfaccia.

La configurazione del router R1 è indicata in figura; quella di R2 è speculare:

```

configure terminal
interface serial0
  no ip address
  encapsulation frame-relay
  exit
interface serial0.50 point-to-point
  ip address 192.168.19.2 255.255.255.252
  frame-relay interface-dlci 50
end

```

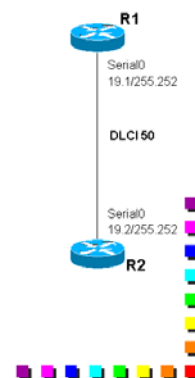


Frame-Relay point-to-point

■ configure terminal

- interface serial0
 - no ip address
 - encapsulation frame-relay
 - exit
- interface serial0.50 point-to-point
 - ip address 192.168.19.1 255.255.255.252
 - frame-relay interface-dlci 50
 - end

42



1.7.3. Configurazione di interfacce Frame-Relay

Scrivere i comandi necessari alla configurazione dei router Cisco in relazione alla topologia indicata in figura, supponendo che la linea seriale sia gestita attraverso la tecnologia Frame-Relay e che siano presenti due canali logici, di cui il primo (DLCI 104) *point-to-point*, mentre il secondo (DLCI 103) di tipo *multipoint*.

Soluzione

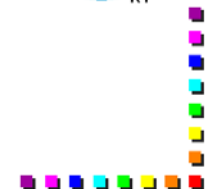
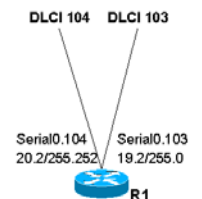
La soluzione è indicata in figura: vengono semplicemente definite due sub-interfaces.



Configurazione di FR

■ configure terminal

- interface serial0
 - no ip address
 - encapsulation frame-relay
 - frame-relay lmi-type ansi
 - exit
- interface serial0.103 multipoint
 - ip address 10.0.19.2 255.255.255.0
 - frame-relay interface-dlci 103
 - exit
- interface serial0.104 point-to-point
 - ip address 10.0.20.2 255.255.255.252
 - frame-relay map ip 10.0.20.2 104 broadcast



43

Capitolo 2. Routing IP su router Cisco

2.1. Per iniziare

2.1.1. Pre-requisiti

La fruizione ottimale di questo modulo richiede le seguenti conoscenze di base:

- Il protocollo IPv4
- conoscenza delle problematiche e delle tecnologie di trasporto di livello 1-2 della pila OSI
- Generalità e configurazione di router Cisco

E' inoltre richiesta la presenza di una certa dimestichezza con le esigenze di configurazione di una rete reale.

2.1.2. Obiettivi

Al termine di questo modulo il partecipante sarà in grado di padroneggiare i comandi fondamentali per la configurazione del routing su un router Cisco. In particolare, questo modulo comprende i comandi fondamentali per il routing statico, ai principali protocolli di routing dinamico (RIP, IGRP/EIGRP, OSPF, BPF); verranno quindi accennate le problematiche di redistribuzione e di access-list applicate ai protocolli di routing. L'elenco dei comandi presentati è normalmente integrato da esempi che dimostrano come questi possano essere impiegati in campo.

Questo modulo intende porsi come guida rapida alla configurazione di apparati Cisco senza porsi in alternativa ai manuali ufficiali; l'obiettivo consiste nell'offrire al lettore uno spunto di partenza strutturato per poter cominciare l'interazione in maniera più familiare con gli apparati.

Sono inoltre previsti esercizi di vari gradi di difficoltà relativi agli argomenti trattati.

2.1.3. Struttura

Questo modulo è strutturato secondo i seguenti punti:

- comandi di routing di carattere generale, e comandi di controllo
- gestione del routing statico
- gestione del routing dinamico (RIP, IGRP/EIGRP, OSPF, BGP)
- redistribuzione

Terminerà il modulo una sezione di esercizi.

2.1.4. Sommario

Essendo questo modulo un "manuale di laboratorio", non è disponibile il sommario.

2.2. Comandi di configurazione

Questa sezione descrive i comandi fondamentali per quanti riguarda l'aspetto del routing, ossia, la capacità della macchina di capire dove e come inoltrare i pacchetti che non sono destinati ad host presenti localmente.

Comandi generali

I principali comandi generali riferiti al routing sono i seguenti:

Cisco(config)# ip routing

Abilita il router ad instradare pacchetti IP (processo di forwarding). Questo comando: è utile anche in forma negata (*no ip routing*) per cancellare completamente la precedente configurazione di routing e lasciare il router spoglio. A questo punto è possibile riabilitare il routing e procedere alla nuova configurazione.

Cisco(config)# ipv6 unicast-routing

Abilita il router ad instradare pacchetti IPv6. E' l'omologo del precedente, ma riferito al protocollo IPv6.

Cisco(config)# ip classless

Nel momento in cui il router riceve un pacchetto per cui non ha una route specifica (e nemmeno la default route), usa la migliore supernet route possibile. Questo comando è utilizzato per favorire l'aggregabilità delle route mediante l'impiego del CIDR.

Comandi generali

■ configure terminal

- ip routing
 - Spesso utile nella forma negata "no ip routing"
- ipv6 unicast-routing
- ip classless

2.2.1. Route statiche e di default

E' il modo più semplice per abilitare il routing; non è tuttavia molto robusto in quanto tutto deve essere fatto manualmente e quindi sono estremamente frequenti gli errori (oltre alla mancanza di aggiornamento automatico da parte della rete).

```
Cisco(config)# ip route indirizzo
maschera next_hop [distanza]
```

I pacchetti destinati alle reti comprese nel range (indirizzo, maschera) devono essere instradati verso router, che deve essere (1) in una sottorete direttamente collegata a una delle interfacce, oppure (2) una porta del router corrente nel caso in cui l'interfaccia sia unnumbered.

La route può essere sostituita da una appresa dinamicamente e avente distanza inferiore

```
Cisco(config)# ip default-network indirizzo
```

Configura una route di default. E' immessa da uno smart router il quale normalmente conosce le route per qualsiasi destinazione e diffonde la route di default tramite i protocolli di routing. La modalità con cui questa è propagata dipende dal protocollo di routing: RIP annuncia 0.0.0.0 0.0.0.0, IGRP annuncia *indirizzo* indicandola come route esterna e candidata per la route di default.

```
Cisco(config)# ipv6 route indirizzo/prefixlength next_hop
```

E' analogo al comando relativo al protocollo IPv4.

Le route statiche non vengono visualizzate dal comando `show ip route` se il percorso non è attivo, ossia se il next hop indicato nel comando stesso non è raggiungibile.



Route statiche

configure terminal

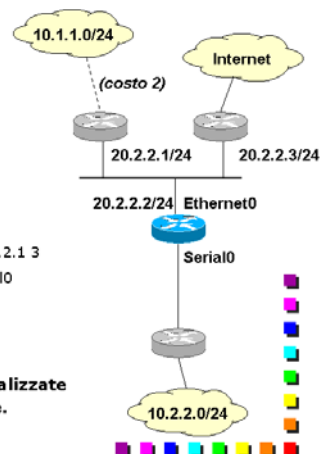
```
interface ethernet0
ip address 20.2.2.2 255.255.255.0
exit
```

interface serial0

```
ip unnumbered loopback0
encapsulation ppp
exit
ip route 10.1.1.0 255.255.255.0 20.2.2.1 3
ip route 10.2.2.0 255.255.255.0 serial0
ip default-network 20.2.2.3
exit
```

show ip route

NOTA: le route non vengono visualizzate se il next hop non è raggiungibile.



2.2.2. Routing dinamico: comandi comuni ai vari protocolli di routing

I protocolli di routing definiscono alcuni comandi che sono comuni tra i vari protocolli. I principali sono i seguenti:

router proto [ID]

Abilita il protocollo di routing specificato; entra in modalità di configurazione di tale protocollo; ha modalità leggermente diverse per ogni protocollo in quanto, ad esempio, il valore *ID* è richiesto da alcuni protocolli e non da altri, e nei protocolli in cui è richiesto può avere un significato differente. Questo comando verrà specificato meglio da ogni protocollo di routing.

network indirizzo_di_rete

Specifica contemporaneamente due informazioni:

- le reti (direttamente connesse al router) che sono nel dominio di routing in esame (e che verranno annunciate dal protocollo);



Routing dinamico: comandi generali (1)

configure terminal

```
interface ethernet0
ip address 10.1.1.1 255.255.255.0
exit
```

```
interface ethernet1
ip address 20.2.2.2 255.255.255.0
exit
```

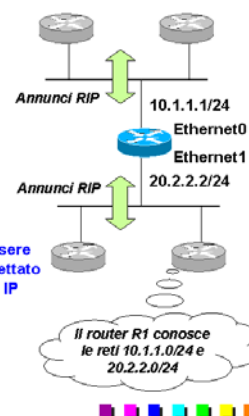
router rip

```
network 10.1.1.1
network 20.2.2.2
end
```

Indica:

- le reti da annunciare
- da quali interfacce vanno inviati e ricevuti gli annunci di routing

Formalmente dovrebbe essere una rete, ma è spesso accettato anche un singolo indirizzo IP



- le interfacce che dovranno partecipare a quel dominio di routing (il router automaticamente capisce quali sono le sue interfacce interessate dal dominio, ed abilita l'invio e la ricezione di messaggi di updates attraverso quelle interfacce)

Il valore *indirizzo_di_rete* dovrebbe essere formalmente un indirizzo di una rete direttamente connessa al router; in pratica i Cisco accettano anche degli indirizzi IP singoli (ad esempio quelli delle singole interfacce) e li traducono in indirizzi di rete automaticamente. Così, nella rete in esempio, i comandi *network 10.1.1.1* e *network 10.1.1.0* sono equivalenti.

I router Cisco tendono tuttavia a "summarizzare" le informazioni specificate da questo comando. Così, ad esempio, una *network 10.1.1.1* viene automaticamente trasformata in *10.0.0.0/8* (secondo la netmask "naturale"), e gli annunci vengono inviati e ricevuti su tutte le interfacce i cui indirizzi sono compresi in quel range. Per selezionare attivare solo alcune tra le interfacce in esame è necessario l'utilizzo del comando *passive-interface*.

La sintassi di questo comando è leggermente diversa in OSPF e in BGP.

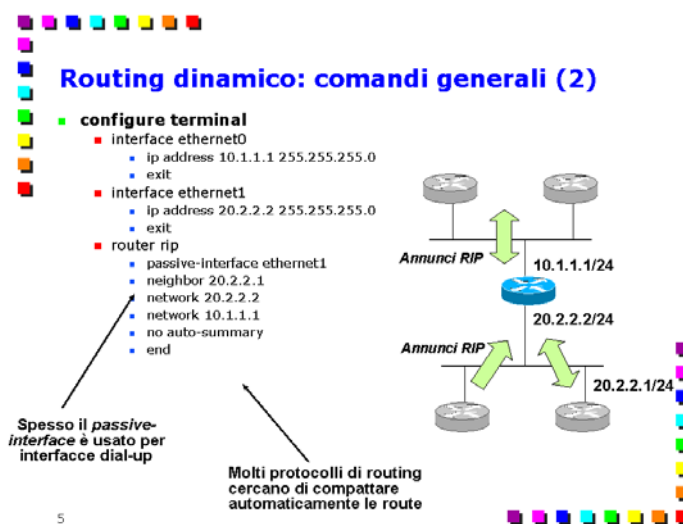
passive-interface interfaccia

Inibisce l'invio di messaggi di update sull'interfaccia (che, ad esempio, è al bordo del dominio di routing). Può essere una ragione amministrativa (evitare di propagare messaggi in una specifica direzione) oppure economica (impedire la generazione di messaggi di routing su linee commutate quali ISDN). Questa interfaccia è comunque in grado di accettare e processare routing updates che arrivano ad essa (inibisce l'*invio* ma non la *ricezione*): per la disabilitazione della ricezione è necessario utilizzare altri strumenti quali le access-list.

Questo comando ha significati leggermente diversi per ogni protocollo di routing; ad esempio in EIGRP l'interfaccia "passiva" viene totalmente disabilitata dal punto di vista delle route (viene pertanto bloccata sia la ricezione che la trasmissione).

neighbor indirizzo

Indica al router di inviare i messaggi all'indirizzo *indirizzo* specificato; è usato su reti senza capacità broadcast oppure per prevenire l'invio dei messaggi di aggiornamento a specifici router (ad esempio su LAN in congiunzione al comando *passive-interface*, per abilitare solo specifici neighbors per ragioni di policy).



2.2.3. Comandi specifici per RIP

I comandi specifici per il protocollo RIP sono i seguenti:

router rip

Abilita il protocollo di routing RIP. Dal momento che questo comando non ha il parametro *ID*, non possono coesistere più istanze di RIP sulla stessa macchina.

version 1 / 2

Abilita l'invio di messaggi secondo la versione 1 o 2 (default 1); nella ricezione capisce ambedue le versioni.

ip split horizon (comando di interfaccia)

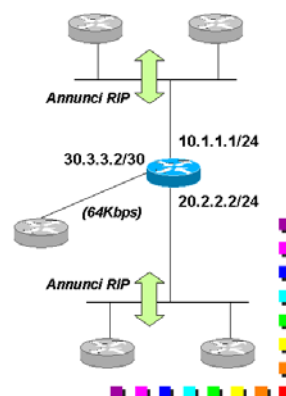
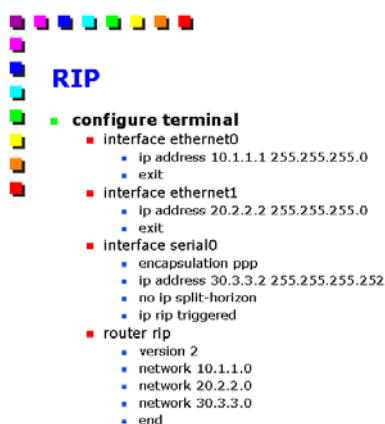
Abilita l'utilizzo dello *split horizon* per il protocollo RIP. Il comando è normalmente abilitato sulle interfacce su reti broadcast (ad esempio Ethernet), mentre è normalmente disabilitato sulle interfacce su reti non broadcast (ad esempio FrameRelay). Questo comando deve essere dato sulla particolare interfaccia (ad esempio Serial 0) sulla quale si vuole disabilitare questa caratteristica.

Questo comando può essere applicato a tutti gli algoritmi di tipo Distance Vector (quindi IGRP ed EIGRP).

ip rip triggered (comando di interfaccia)

E' utilizzato su link molto lenti per disabilitare l'invio periodico di annunci RIP. Su tali link, l'invio del pacchetto di routing update potrebbe impiegare parecchio tempo, consumando inutilmente la banda già scarsa. Il comando in esame forza il router ad inviare annunci RIP su quell'interfaccia solo se il database è cambiato.

Come il comando precedente, è un comando disponibile all'interno della configurazione dell'interfaccia.



2.2.4. Comandi specifici per IGRP-EIGRP

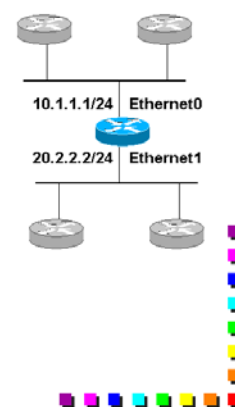
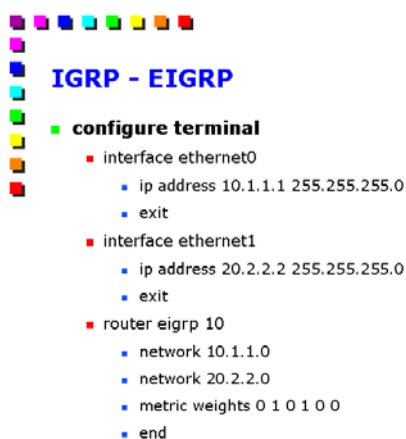
I comandi specifici per i protocolli IGRP/EIGRP sono i seguenti:

router igrp process_id - router eigrp process_id

Attiva il processo di routing. Il *process_id* identifica il particolare processo di routing in esecuzione, che deve essere uguale in tutti i router del dominio IGRP/EIGRP in quanto l'informazione viene inclusa negli annunci. Se si è in un AS registrato è buona norma porre questo identificativo pari al numero dell'AS; nel caso si voglia impiegare contemporaneamente IGRP e EIGRP (per esempio per necessità di transizione), IGRP e EIGRP possono scambiarsi informazioni solo se *process_id* = AS.

metric weights tos k1 k2 k3 k4 k5

Cambia il valore dei parametri utilizzati per il calcolo del costo per uno specifico codice *Type Of Service* (anche se è fortemente sconsigliato cambiarli); il significato dei termini è analogo al comando



default-metric. I valori di default sono *tos*: 0, $k1=k3=1$, $k2=k4=k5=0$.

no metric holddown (solo IGRP)

Disabilita l'algoritmo di hold down di IGRP, migliorando il tempo di convergenza a scapito di possibilità di loop.

2.2.5. Comandi specifici per OSPF

I comandi specifici per il protocollo OSPF sono i seguenti:

router ospf process_id

Abilita un processo di routing OSPF. Il *process_id* identifica il processo di routing OSPF all'interno del router ed ha significato locale (contrariamente a IGRP/EIGRP non viene trasmesso all'esterno del router). E' quindi possibile avere valori di *process_id* diversi sui vari router che compongono la nuvola OSPF.

network indirizzo wildcard area id_area

Il protocollo OSPF prevede che le reti da annunciare vengano indicate esplicitamente con la coppia <indirizzo, wildcard>. Queste informazioni individuano una o più interfacce che si trovano nell'area *id_area* sulle quali vengono inviati e ricevuti i messaggi OSPF. La maschera è di tipo *wildcard* (come le access list), mentre *id_area* è codificato su 4 byte, ed è possibile utilizzare sia la notazione decimale che quella decimale puntata. Spesso viene assegnato un indirizzo IP (ad esempio l'indirizzo IP dell'area border router) all'*id_area*.

area id_area stub

Dichiara l'area *id_area* una stub area.

area id_area range indirizzo maschera

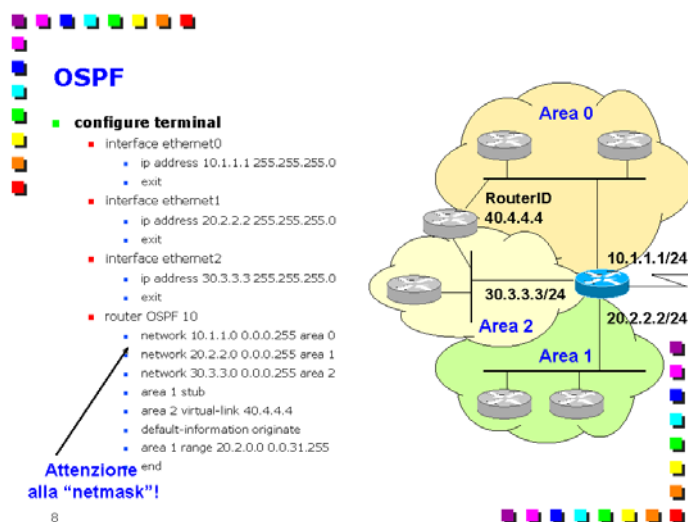
Specifica un address range da annunciare all'esterno dell'area *id_area*, consentendo l'aggregazione di informazioni per la propagazione all'esterno dell'area *id_area* (se all'interno dell'area c'è almeno un'interfaccia con l'indirizzo che cade all'interno dell'address range, all'esterno è annunciato l'address range invece dei singoli indirizzi).

area id_area virtual-link ID_router

Crea un link virtuale con il router che ha *ID_router*, dove questo valore è individuabile visualizzando i database di OSPF; l'area *id_area* è comune ai due router.

default-information originate [always]

Abilita il router di annunciare una route di default all'interno del suo dominio OSPF, comportandosi da AS Boundary Router (lo stesso scopo può essere ottenuto con il redistribute). Un AS boundary router non annuncia necessariamente la route di default, in quanto potrebbe annunciare più route esterne imparate da altri protocolli. Se il router non ha alcuna route di default, questo comando è influente, a meno che si specifichi la keyword *always*, nel qual caso viene comunque sempre immessa una route di default in quel dominio anche se il router non ne ha una propria.



2.2.6. Comandi specifici per BGP

La configurazione di BGP è più complessa degli altri protocolli di routing e comprende i seguenti passi fondamentali:

- abilitazione del routing BGP
- configurazione dei BGP peers

I comandi specifici per il protocollo BGP sono i seguenti:

router bgp AS

Attiva il processo di routing BGP nell'Autonomous System AS.

network *indirizzo* [mask *netmask*]

Identifica questa rete come appartenente al dominio BGP locale e la inserisce nella propria routing table.

Il significato è diverso dai protocolli IGP in quanto il comando **network** non definisce le interfacce sulle quali bisogna inviare gli annunci. Contrariamente ad OSPF, la netmask è nella forma classica.

neighbor *indirizzo* remote-as AS

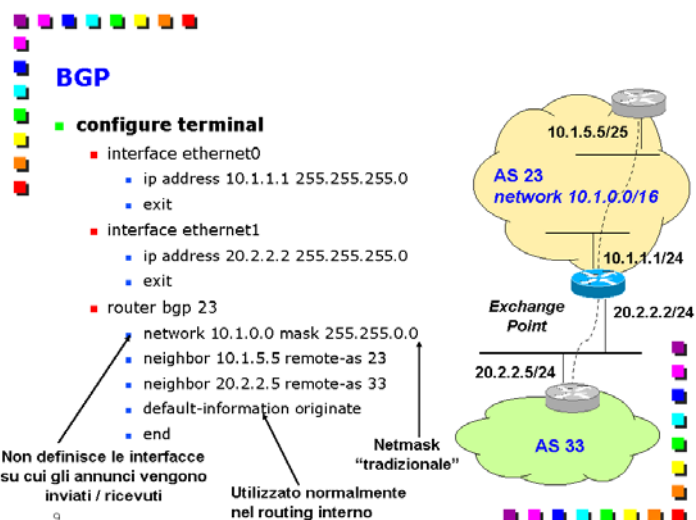
Dichiara come peer (neighbor) il router *indirizzo* dell'Autonomous System AS. I neighbor possono essere Internal o External. I peer di tipo *external* sono spesso contraddistinti da un link fisico in comune, mentre quelli di tipo *internal* possono essere posizionati in un qualunque locazione dell'AS.

aggregate-address *indirizzo* *maschera*

Se esiste almeno una route per una rete che rientra nel range di indirizzi (*indirizzo*, *maschera*) BGP annuncia questo range.

default-information originate

Abilita la propagazione della route di default (0.0.0.0) all'interno del dominio BGP. La generazione di questa route non è fatta in automatico dal BGP, ma deve essere appresa da altre parti (ad esempio mediante redistribuzione). Questo comando non viene normalmente utilizzato nel routing tra Autonomous Systems; piuttosto, può essere utilizzato qualora il protocollo BGP sia abilitato all'interno di un AS come protocollo di routing interno (ad esempio in congiunzione di MPLS).



2.2.7. Redistribuzione

E' quel processo che permette di collegare due domini di routing diversi scambiandosi vicendevolmente le route apprese in ognuno di essi. A differenza di avere un dominio unico, il processo di redistribuzione provoca un compattamento delle informazioni di routing in modo da rendere il processo più scalabile. In altre parole un dominio di routing non conoscerà completamente la topologia dell'altro dominio, ma solo delle informazioni tendenti a dire **quali reti** sono presenti, ma non **qual è il percorso** esatto che i pacchetti faranno per raggiungerle.

Per evitare il caso in cui ci siano percorsi diversi transitanti in domini diversi verso una stessa destinazione, i router Cisco definiscono dei costi standard per ogni protocollo di routing in modo che il confronto di costo possa essere fatto sul protocollo anziché sul percorso vero e proprio. Così, ad esempio, le route statiche avrà costo 1, il protocollo di routing EIGRP avrà costo 90, OSPF 110, RIP 120, e così via. Se ne deduce che, indipendentemente dal percorso, una route statica per una certa destinazione sarà sempre preferita rispetto a qualunque protocollo di routing.

La redistribuzione può essere uni o bi-direzionale. La prima può essere utilizzata per redistribuire, all'occorrenza, solo le route di un dominio in un altro.

Uno dei problemi di questo meccanismo è che ogni protocollo di routing ha una modalità di computo della metrica diverso dagli altri. E' allora necessario dire esplicitamente al router la metrica con la quale gli annunci dell'altro dominio dovranno essere propagati, con il comando *default-metric*.

I principali comandi connessi alla redistribuzione sono:

redistribute *protocollo* [*id*]

Distribuisce nel dominio del router in questione le informazioni raccolte tramite il protocollo *protocollo*; è un sottocomando della modalità router. Il valore *id* è necessario per discriminare tra più processi dello stesso protocollo (es. EIGRP, OSPF, etc).

default-metric *metrics*

Indica che tutte le route apprese dall'esterno sono da ridistribuire con metrica *metrics*; ha modalità leggermente diverse per ogni protocollo in quanto la metrica è diversa. Ad esempio il comando *default-metric 10000 100 255 1 1500*

(utilizzato all'interno di un router IGRP/EIGRP) corrisponde alla specifica dei termini *banda*, *ritardo*, *affidabilità*, *carico*, *MTU*

Questo comando non è necessario nel caso in cui si vogliano redistribuire le informazioni tra due istanze diverse dello stesso protocollo (ad esempio tra un dominio OSPF e un altro dominio OSPF).

Redistribuzione: concetti fondamentali

Caratteristiche

- Compattamento dell'informazione (scalabilità)
- Problematiche di metrica
- Uni- o bi-direzionale
- Costi standard (1 = statiche, 90 = EIGRP, 110 = OSPF, ...)

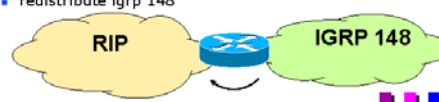
Esempio

- distribuisce nel dominio di routing RIP le informazioni apprese nel dominio IGRP 148

configure terminal

- router rip
 - redistribute igrp 148

10



Redistribuzione: esempio

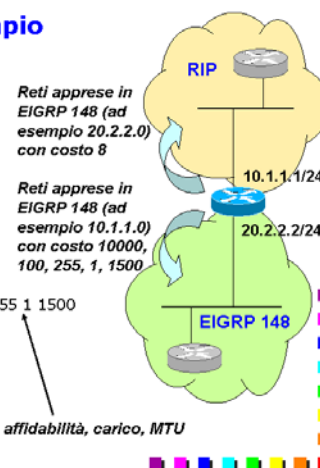
configure terminal

- router rip
 - network 10.1.1.0
 - redistribute eigrp 148
 - default-metric 8
 - exit
- router eigrp 148
 - network 20.2.2.2
 - redistribute rip
 - default-metric 10000 100 255 1 1500
 - redistribute static
 - redistribute connected
 - end

Non indicate in figura

Banda, ritardo, affidabilità, carico, MTU

11



redistribute static

Redistribuisce all'interno del protocollo di routing in esame tutte le sue route statiche.

redistribute connected

Redistribuisce le informazioni sulle reti connesse, ossia le route che vengono create automaticamente per il fatto di avere una interfaccia in esse. Il processo di routing in esame acquisirà pertanto le route di tutte le interfacce del router, indipendentemente dal protocollo di routing attivato su ognuna di esse. Le route interessate da questo comando sono quelle non specificate da un esplicito comando network; per OSPF e IS-IS queste route sono redistribute come appartenenti all'esterno dell'AS.

2.3. Comandi di controllo

Questi comandi, contrariamente a quelli precedenti, sono attivabili dalla modalità privilegiata.

show ip route

Mostra la routing table del protocollo IP. Le informazioni più importanti comprendono il protocollo di routing con il quale se è appresa la route (ad esempio C per le route connesse, S per quelle statiche, R per quelle RIP), il nome della rete di destinazione, il costo (che comprende sia il costo della route, sia il costo proprio del protocollo di routing, necessario per scegliere due route verso la stessa destinazione ma provenienti da due protocolli di routing distinti), il next hop.

show ipv6 route

Analogo al comando precedente, ma riferito al protocollo IPv6.

clear ip route {network [mask] | *} }

[Modalità privilegiata] Permette la cancellazione di una o più route che si suppongono non più valide. Questo comando non permette la cancellazione delle route statiche.

show ip protocols

Visualizza lo stato di ogni protocollo di routing attivo (tempistiche, parametri (es per EIGRP), redistribuzioni, ...).

show ip eigrp interfaces | neighbors | topology | traffic

Comandi di controllo del funzionamento del processo EIGRP.

show ip ospf | bgp

Visualizza le informazioni generali sul processo in esame.

show ip ospf database

Mostra il database dei link state advertisement ricevuti.

show ip ospf neighbor

Visualizza tutti i router OSPF adiacenti, indipendentemente dall'area a cui appartengono; il campo *neighbor_ID* mostra l'identificativo (*router_ID*) del router remoto. Nel caso in cui il router sia su una Ethernet, mostra anche chi è il Designated Router e il Backup DR, il loro indirizzo su quella rete e l'indirizzo attraverso il quale sono raggiungibili.

show ip ospf border-routers | interface | virtual-links

Comandi di controllo del routing

Comandi generali:

- show ip route
- Show ipv6 route
- clear ip route *
- show ip protocols

EIGRP

- show ip eigrp interfaces | neighbors | topology | traffic

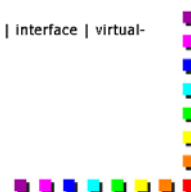
OSPF

- show ip ospf
- show ip ospf database | border-routers | neighbors | interface | virtual-links

BGP

- show ip bgp
- show ip bgp summary

12



Altri comandi per la visualizzazione di aspetti specifici di OSPF.

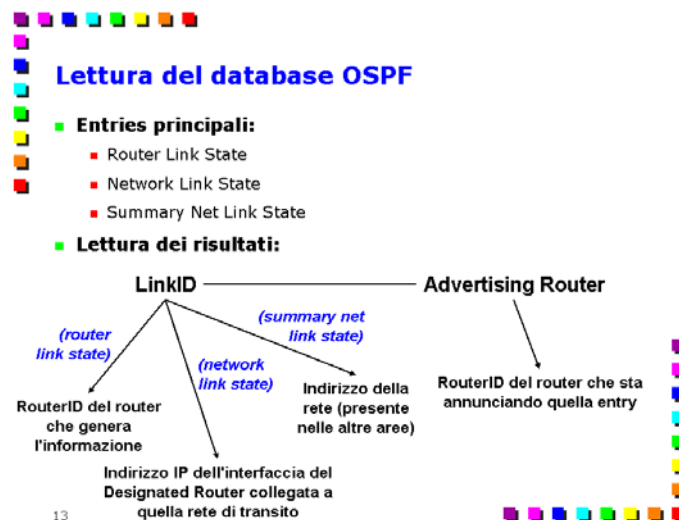
show ip bgp summary

Visualizza l'elenco dei peer BGP.

2.3.1. Lettura del database OSPF

OSPF offre il grande vantaggio di visualizzare un'ottima descrizione della rete. Il comando `show ip ospf database` può però essere ostico nella sua interpretazione. Per la lettura dei risultati è allora necessario ricordare che:

- Router Link State: rappresenta l'elenco dei router presenti sull'area in esame
- Network Link State: rappresenta l'elenco delle reti broadcast contenute nell'area in esame
- Summary Net Link State: rappresenta l'elenco delle reti presenti nelle altre aree; sparisce qui la distinzione tra reti di transit (broadcast) e reti tradizionali (punto-punto)



Ogni entry (del tipo specificato sopra) è composta da due informazioni, il *LinkID* e l'*Advertising Router*. Il significato di questi campi è variabile a seconda del tipo di entry ed è schematizzato in figura. Nel caso di un Router Link, il LinkID e l'ADVRouter coincidono (perché è il router che annuncia sé stesso).

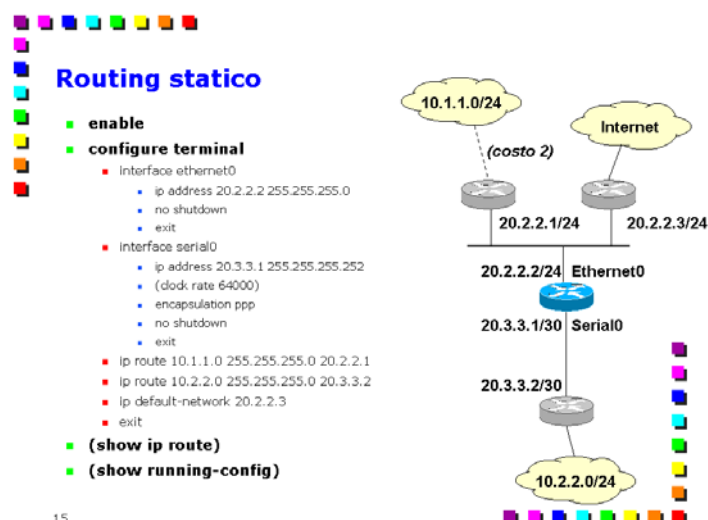
Il RouterID è solitamente dato dal più alto indirizzo configurato sulle interfacce del router in esame, tranne nel caso in cui sia stato configurato l'indirizzo di Loopback che diventa automaticamente il RouterID.

Il database è ovviamente uguale all'interno dei vari router appartenenti alla stessa area (a meno che la rete sia in fase di riconfigurazione). Ogni router può comunque avere uno o più database, a seconda che sia un semplice internal router (e quindi è immerso in una sola area) oppure un router di bordo tra più aree.

2.4. Esercizi

2.4.1. Routing statico

Scrivere i comandi necessari alla configurazione dei router Cisco in relazione alla topologia indicata in figura, attraverso l'impiego di routing statico.



15

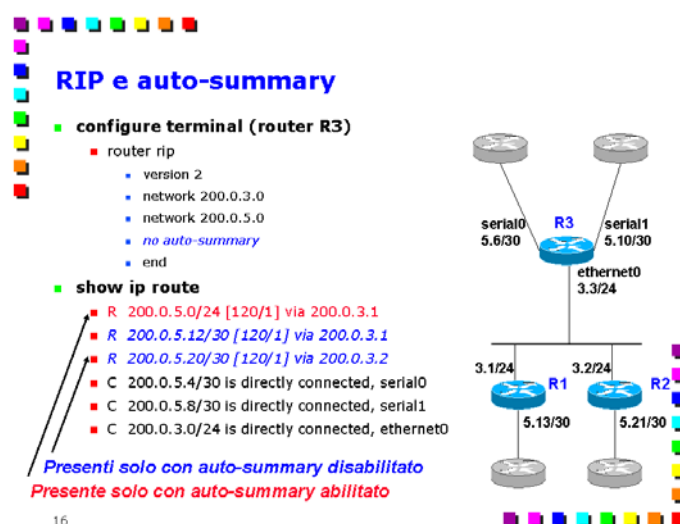
2.4.1.1. Soluzione

La soluzione comprende la configurazione delle interfacce, quindi la scrittura delle tre route. Le prime due sono relative alle due reti /24, mentre la terza (attraverso il comando `ip default-network`) definisce una route di default per il resto del mondo Internet.

In figura sono anche riportati alcuni comandi (`show ip route` e `show running-config`) che possono essere utilizzate per visualizzare il risultato della configurazione. Il comando `clock rate 64000` è necessario solamente qualora le due interfacce seriali dei router siano collegate direttamente, senza alcun modem intermedio. La prima configurazione è tipica di un laboratorio, la seconda è tipica di una rete reale.

2.4.2. RIP e Auto-Summary

Verificare le necessità di abilitare il comando `auto-summary` all'interno della configurazione dei router in figura.



16

2.4.2.1. Soluzione

La configurazione dei tre router è assolutamente identica, e quindi viene riportata (in figura) solo quella di R3. Tuttavia il protocollo RIP ha, come opzione di default, la summarizzazione abilitata. Questo significa che ogni router tende ad annunciare la rete naturale (ad esempio una classe C) anziché la vera rete configurata sulle proprie interfacce, indipendentemente dal fatto che la versione 2 di RIP permette il trasporto di maschere (e quindi di reti a lunghezza variabile). Nel caso in esame, ogni router annuncerà la conoscenza delle reti 200.0.3.0/24 e 200.0.5.0/24 come reti proprie.

Si analizzi ora il comportamento del router R3 (il comportamento di R1 e R2 è speculare): egli riceverà dagli altri router un annuncio relativo all'intera rete 200.0.5.0/24. Siccome R3 è direttamente connesso alla rete 200.0.5.8/30, raggiungerà questi indirizzi attraverso l'interfaccia direttamente connessa, e raggiungerà tutti gli altri indirizzi della rete 200.0.5.0/24 attraverso, ad esempio, R1. Infatti, ricevendo due annunci identici da R1 e da R2, sceglierà uno dei due router come il proprio next hop, a caso.

Con questa configurazione il R3 non sarà pertanto in grado di raggiungere gli indirizzi della rete 200.0.5.20/30, dal momento che tutti i pacchetti verso quella direzione verranno comunque mandati a R1.

La soluzione a questo problema consiste nell'abilitazione del comando *no auto-summary* all'interno della configurazione del router *rip*. In questo modo la summarizzazione non viene fatta automaticamente e il router R3 riceverà correttamente gli annunci 200.0.5.12/30 da R1, e 200.0.5.20/30 da R2.

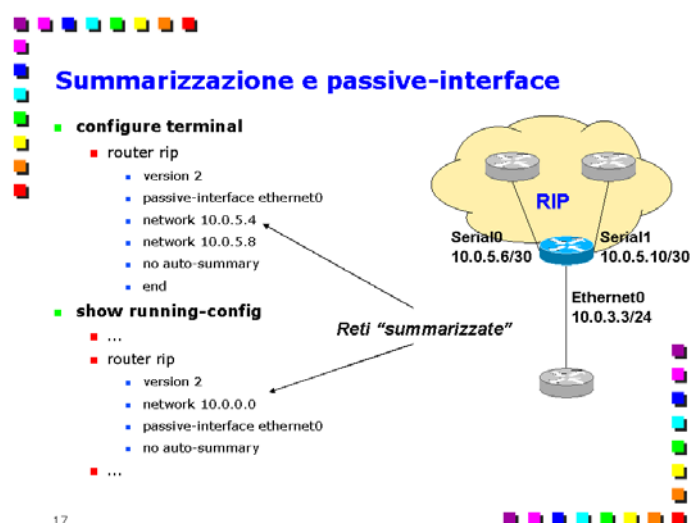
L'auto-summarizzazione ha modalità leggermente diverse per ogni protocollo di routing. Ad esempio il protocollo EIGRP automaticamente inserirebbe in R3 una riga nella tabella di routing del tipo

```
D 200.0.5.0/24 is a summary, Null0
```

Il router R3 non sarà pertanto in grado di raggiungere nessun indirizzo 200.0.5.0/24 (tranne quelli direttamente connessi) a causa di questa riga-extra, che dice al router che tutte le destinazioni 200.0.5.0/24 sono raggiungibili localmente.

2.4.3. Summarizzazione e Passive Interface

Data la rete in figura, verificare come il router Cisco compatti le informazioni del comando *network* secondo la netmask naturale.



17

2.4.3.1. Soluzione

La soluzione è indicata in figura. Nonostante il comando `no auto-summary` e nonostante il comando `network` per le varie interfacce sia stato specificato separatamente, il router inserisce nella sua configurazione una sola rete che è un sovrinsieme delle reti specificate, come è possibile vedere dall'output del comando `show running-config`. Questa configurazione farà sì che il router consideri tutte le proprie interfacce come appartenenti alla nuvola RIP.

La soluzione a questo problema consiste nel dichiarare l'interfaccia `ethernet0` come interfaccia passiva, disabilitando pertanto l'invio di annunci in quella direzione, a cui sarebbe necessario aggiungere anche una access-list in ingresso per impedire anche la ricezione di route.

Si noti tuttavia come gli annunci generati dal router tengano in conto del comando `no auto-summary`, ossia il router propagherà gli annunci per le proprie reti secondo la netmask corretta (/30); solo il comando `network` non è affetto dal `no auto-summary`.

2.4.4. RIP e Passive Interface

Data la rete in figura, si configurino i router in modo che i router R2 ed R3 si scambino gli annunci RIP in modalità diretta, senza inviarli al router R1 e senza accettare da esso alcuna informazione..

RIP e passive-interface (1)

```

■ configure terminal (router R3)
  ■ router rip
    ■ version 2
    ■ network 200.0.3.0
    ■ network 200.0.5.0
    ■ passive-interface ethernet0
    ■ neighbor 200.0.3.2
    ■ no auto-summary
    ■ end

■ show ip route
  ■ R: 200.0.5.12/30 [120/1] via 200.0.3.1
  ■ R: 200.0.5.20/30 [120/1] via 200.0.3.2
  ■ C 200.0.5.4/30 [120/1] is directly connected
  ■ C 200.0.5.8/30 [120/1] is directly connected
  ■ C 200.0.3.0/24 [120/1] is directly connected
  
```

2.4.4.1. Soluzione

La soluzione è mostrata in figura: sui router R2 ed R3 è necessario attivare i comandi `passive-interface`, in modo da disabilitare l'invio di pacchetti di routing update su quell'interfaccia, `neighbor`, in modo da indicare che l'host in esame deve in realtà ricevere annunci RIP (e che vengono quindi inviati in unicast). Il secondo comando è speculare sui router R2 ed R3: R2 indicherà l'indirizzo 200.0.3.3 come proprio neighbor, mentre R3 indicherà l'indirizzo 200.0.3.2.

Con questa configurazione, il router R1 non riceverà nessun annuncio di routing, mentre i suoi annunci si propagheranno al resto della rete: in altre parole R1 non sarà in grado di raggiungere le reti gestite da R2 ed R3, mentre questi ultimi saranno in grado di raggiungere le reti gestite da R1. Per far sì che gli annunci di R1 vengano rifiutati da R2 ed R3 è necessario

utilizzare una ulteriore configurazione ad esempio mediante l'abilitazione di filtri sulle routing update in ingresso mediante access list.

E' interessante verificare invece il comportamento della rete nel caso in cui venga omesso il comando `passive-interface` sul solo router R3 (oppure solo su R2): gli annunci RIP vengono mandati sul canale sia in broadcast che in unicast (dal momento che è attivo il comando `neighbor`). In altre parole, il comando `neighbor` non forza automaticamente la generazione esclusivamente di messaggi unicast e la presente configurazione ne è una prova.

Come visualizzato in figura, pertanto, il router R1 sarà in grado di raggiungere completamente tutta la rete in esame dal momento che riceverà i messaggi di routing update inviati in broadcast da R1.

La gestione del comando `passive-interface` è leggermente diversa per il protocollo EIGRP: un router EIGRP disabilita completamente il protocollo di routing su quell'interfaccia, ossia non invierà né riceverà alcun messaggio di routing da essa.

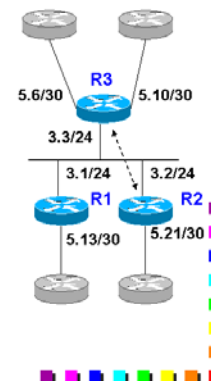


RIP e passive-interface (2)

```

■ configure terminal (router R3)
■ router rip
  ■ version 2
  ■ network 200.0.3.0
  ■ network 200.0.5.0
  ■ neighbor 200.0.3.2
  ■ no auto-summary
  ■ end

■ show ip route (router R1)
  ■ R 200.0.5.4/30 [120/1] via 200.0.3.3
  ■ R 200.0.5.8/30 [120/1] via 200.0.3.3
  ■ R 200.0.5.20/30 [120/1] via 200.0.3.2
  ■ C 200.0.5.12/30 [120/1] is directly connected
  ■ C 200.0.3.0/24 [120/1] is directly connected
  
```



19

2.4.5. OSPF con 2 aree e 2 reti

Scrivere i comandi necessari alla configurazione dei router Cisco in relazione alla topologia indicata in figura, supponendo attivo il protocollo OSPF.

Si scriva inoltre l'output di massima del comando `show ip ospf database`, ossia l'elenco (e il tipo) dei vari LSA presenti in ciascun router.



OSPF con 2 aree e 2 reti

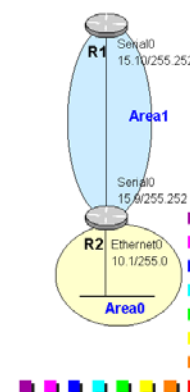
```

■ enable

■ configure terminal #router R1
  ■ interface serial0
    ■ ip address 192.168.15.10 255.255.255.252
    ■ encapsulation ppp
    ■ exit
  ■ router ospf 20
    ■ network 192.168.15.8 0.0.0.3 area 1
    ■ end

■ show ip ospf database

Router Link State (area 1)
  192.168.15.9 192.168.15.9
  192.168.15.10 192.168.15.10
Summary Net Link State (area 1)
  192.168.10.0 192.168.15.9
  
```



20

2.4.5.1. Soluzione

La configurazione della rete con OSPF è semplice, in quanto esistono semplicemente 2 aree, due soli router e non sono richieste configurazioni avanzate (virtual links, magliature sul backbone).

La configurazione di R1 è indicata in figura; quella di R2 è leggermente più complessa in quanto il router appartiene a due aree:

```

configure terminal
interface serial0
  ip address 192.168.15.9 255.255.255.252
  
```

```

encapsulation ppp
exit
interface ethernet0
ip address 192.168.10.1 255.255.255.0
exit
router ospf 30
network 192.168.10.0 0.0.0.255 area 0
network 192.168.15.8 0.0.0.3 area 1
end

```

Si noti che l'identificativo del router OSPF è puramente locale; infatti il router R1 ha identificativo del processo OSPF pari a 20 mentre R2 ha ID pari a 30.

Il database di R2 è un superset rispetto a quello di R1 (mostrato in figura):

```
show ip ospf database
```

```

Router Link State (area 0)
  192.168.15.9 192.168.15.9
Summary Net Link State (area 0)
  192.168.15.8 192.168.15.9
Router Link State (area 1)
  192.168.15.9 192.168.15.9
  192.168.15.10 192.168.15.10
Summary Net Link State (area 1)
  192.168.10.0 192.168.15.9

```

Una possibile osservazione è relativa all'area 0, nella quale è presente un solo router (il cui LinkID è 192.168.15.9): siccome l'annuncio è fatto dal router stesso (192.168.15.9) i due valori di LinkID e AdvRouter coincidono (il router annuncia sé stesso).

2.4.6. OSPF con 2 aree e 3 reti

Scrivere i comandi necessari alla configurazione dei router Cisco in relazione alla topologia indicata in figura, supponendo attivo il protocollo OSPF.

Si scriva inoltre l'output di massima del comando `show ip ospf database`, ossia l'elenco (e il tipo) dei vari LSA presenti in ciascun router.

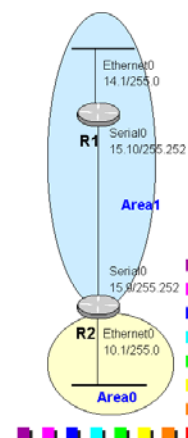
enable

```

configure terminal #router R1
interface serial0
  ip address 192.168.15.10 255.255.255.252
  encapsulation ppp
  exit
interface ethernet0
  ip address 192.168.14.1 255.255.255.0
  exit
router ospf 20
  network 192.168.15.8 0.0.0.3 area 1
  network 192.168.14.0 0.0.0.255 area 1
  end

show ip ospf database
Router Link State (area 1)
  192.168.15.9 192.168.15.9
  192.168.15.10 192.168.15.10
Summary Net Link State (area 1)
  192.168.10.0 192.168.15.9

```



21

2.4.6.1. Soluzione

La configurazione della rete con OSPF è molto simile a quella dell'esercizio precedente, in quanto l'unica aggiunta è una seconda rete

Ethernet nell'Area1. La configurazione di R1 è riportata in figura; quella di R2 è invece identica all'esercizio precedente:

```
configure terminal
interface serial0
  ip address 192.168.15.9 255.255.255.252
  encapsulation ppp
  exit
interface ethernet0
  ip address 192.168.10.1 255.255.255.0
  exit
router ospf 30
  network 192.168.10.0 0.0.0.255 area 0
  network 192.168.15.8 0.0.0.3 area 1
end
```

Per quanto riguarda i risultati del comando `show ip ospf database` vi saranno le seguenti caratteristiche:

- il database rimane invariato nell'area1 (non è stato aggiunto alcun router)
- si aggiunge un Summary Net Link State nell'area0 (quello relativo alla rete aggiunta nell'area 1)
- non ci sono altri tipi di LSA in quanto, pur con l'aggiunta di una nuova Ethernet, su questa rete non viene forzato un processo di elezione dal momento che un solo router è presente nella rete broadcast

Il risultato di R1 è riportato in figura; quello di R2 sarà il seguente:

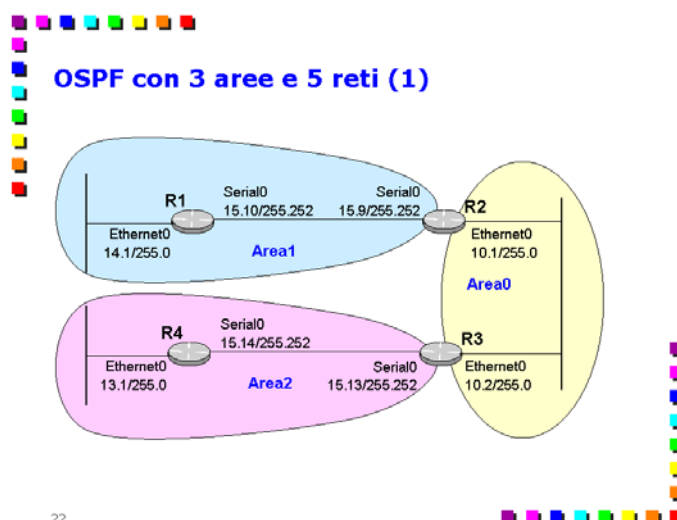
```
show ip ospf database
```

```
Router Link State (area 0)
  192.168.15.9 192.168.15.9
Summary Net Link State (area 0)
  192.168.15.8 192.168.15.9
  192.168.14.0 192.168.15.9
Router Link State (area 1)
  192.168.15.9 192.168.15.9
  192.168.15.10 192.168.15.10
Summary Net Link State (area 1)
  192.168.10.0 192.168.15.9
```

2.4.7. OSPF con 3 aree e 5 reti

Scrivere i comandi necessari alla configurazione dei router Cisco in relazione alla topologia indicata in figura, supponendo attivo il protocollo OSPF.

Si scriva inoltre l'output di massima del comando `show ip ospf database`, ossia l'elenco (e il tipo) dei vari LSA presenti in ciascun router.



22

2.4.7.1. Soluzione

La configurazione della rete con OSPF è simile a quella degli esercizi precedenti (R2 è indicato in figura); non si riporta il router R4 che comunque può essere facilmente ricavato per analogia da R3:

Router R1

```
configure terminal
interface serial0
ip address 192.168.15.10 255.255.255.252
encapsulation ppp
exit
interface ethernet0
ip address 192.168.14.1 255.255.255.0
exit
router ospf 20
network 192.168.15.8 0.0.0.3 area 1
network 192.168.14.0 0.0.0.255 area 1
end
```

Router R3

```
configure terminal
interface serial0
ip address 192.168.15.13 255.255.255.252
encapsulation ppp
exit
interface ethernet0
ip address 192.168.10.2 255.255.255.0
exit
router ospf 30
network 192.168.10.0 0.0.0.255 area 0
network 192.168.15.12 0.0.0.3 area 2
end
```

Per quanto riguarda i risultati del comando `show ip ospf database` vi saranno le seguenti variazioni:



23

- comparirà un Network Link State (Ethernet1 10.x nell'area 0), ossia un link state relativo a una rete di transito (Ethernet). Questo è dovuto alla presenza di più di un router sulla rete, che forza un processo di elezione del Designated Router
- aumenterà il numero del Summary Net Link State, dal momento che sono state aggiunte parecchie nuove reti
- non cambieranno invece i Router Link State dell'area 1, in quanto in quest'area non sono state fatte variazioni.

Per una compattezza dei risultati viene riportato solo l'output relativo al router R3 (R2 è in figura); dal momento che il database della stessa area è identico sui vari router, i database di R1 e R4 si ricavano di conseguenza.

```
show ip ospf database
```

```
Router Link State (area 0)
  192.168.15.9 192.168.15.9
  192.168.15.13 192.168.15.13
Network Link State (area 0)
  192.168.10.2 192.168.15.13
Summary Net Link State (area 0)
  192.168.15.8 192.168.15.9
  192.168.14.0 192.168.15.9
  192.168.15.12 192.168.15.13
  192.168.13.0 192.168.15.13
Router Link State (area 2)
  192.168.15.13 192.168.15.13
  192.168.15.14 192.168.15.14
Summary Net Link State (area 2)
  192.168.10.0 192.168.15.13
  192.168.14.0 192.168.15.13
  192.168.15.8 192.168.15.13
```