1

Configurazione di dispositivi di rete Cisco

In una rete ben progettata, all'interno della LAN saranno gli switch a occuparsi di dirigere e controllare a livello di accesso il flusso dei dati tra gli *end device*.

Gli switch Cisco (FIGURA **1**) sono generalmente auto configuranti e pronti a funzionare, ma sarà opportuno preoccuparsi di gestire come minimo tutti gli aspetti legati alla sicurezza, essendo i dispositivi più vicini agli utenti e, conseguentemente, maggiormente esposti a ogni tipo di attacco; successivamente sarà comodo, per gli switch più evoluti, configurare quanto serve per gestirli anche da remoto.

I router CISCO (FIGURA **2**), d'altra parte, dovendo interconnettere reti diverse, non potranno certamente essere pronti all'uso: come minimo dovranno essere configurati gli indirizzi IP delle varie interfacce di rete e, anche in questo caso, ci si dovrà preoccupare di configurare quanto necessario per garantire la sicurezza.

Per configurare e gestire sia switch sia router, Cisco mette a disposizione un sistema operativo proprietario: Cisco IOS (*Internetwork Operating System*), basato su un'interfaccia a riga di comando denominata CLI (*Command Line Interface*).

Un altro strumento che Cisco mette a disposizione per la gestione delle infrastrutture di rete è Packet Tracer, un software proprietario che costituisce un simulatore, in cui è possibile:

- definire sia la topologia logica che quella fisica;
- effettuare delle simulazioni con cui è possibile esaminare il percorso di ogni singolo pacchetto;
- utilizzare e configurare alcuni dispositivi Cisco di rete;
- utilizzare e configurare alcuni end device.

Cisco Systems

Cisco Systems nasce nel 1984, fondata da Leonard Bosack e Sandra Lerner. I due, sposati, prima si laureano a Stanford, poi arrivano a capo di due diversi dipartimenti dell'università, e nel frattempo capiscono che la tecnologia dei router poteva avere molto successo anche al di fuori del campo universitario. Iniziano quindi a progettare e costruire a casa loro dei routers, facendo sperimentazione con la rete dell'università e decidono di fondare l'azienda dandole il nome della città (San Francisco) adottando il logo che ricorda le torri del Golden Gate Bridge. Già nel 1990 l'azienda vale più di 200 milioni di dollari. Nel 1997 viene fondata la Cisco Network Academy: un vasto insieme di corsi online su tutti i vari aspetti della gestione delle reti. Oggi Cisco Systems è un colosso da quasi 3 miliardi di dollari che sta spostando la sua attenzione dalla produzione di apparecchiature di rete alla IoT (*Internet of Things*) e al software.

FIGURA **1**

FIGURA **2**

1 Caratteristiche e struttura interna di uno switch

Uno **switch Ethernet** è un dispositivo intermedio per la comunicazione all'interno di una rete LAN, gestisce indirizzi MAC e frame, quindi PDU di livello 2 per l'interconnessione di end device.

Avendo come ruolo quello di dispositivo a cui vengono collegati tutti gli end device di una rete o altri switch, tra le sue principali caratteristiche c'è il numero di porte, che varia tipicamente tra 8 e 48, e la loro banda nominale, che varia invece tra 100 Mbps e 10 Gbps.

La caratteristica più importante di uno switch è denominata *switching bandwidth* e rappresenta le prestazioni del dispositivo espresse in Gigabit/secondo. Solo gli switch di alto livello e con un numero limitato di porte hanno una switching bandwidth complessiva pari alla somma della velocità nominale di tutte le porte Ethernet: questi switch sono capaci di gestire contemporaneamente il massimo livello di traffico dati per ogni porta; dato che questa situazione nella maggior parte dei contesti d'uso non si verifica, la maggior parte degli switch ha una switching bandwidth inferiore.

Un altro aspetto importante è il cosiddetto fattore di forma, ovvero se lo switch:

- ha una configurazione fissa e il numero di porte e i tipi di connessione non possono variare;
- è modulare, ovvero se lo *chassis* permette l'installazione di diversi tipi di moduli contenenti le porte ed è possibile decidere e variare la configurazione cambiando i moduli.

Nelle reti moderne capita di frequente che i dispositivi connessi alle porte degli switch abbiano bisogno di un'alimentazione, un'altra caratteristica da considerare è quindi se lo switch consente o meno il cosiddetto **PoE** (*Power over Ethernet*), con cui la corrente per l'alimentazione dei dispositivi finali passa attraverso il cavo Ethernet di connessione.

Uno switch è costituito da una scheda madre su cui, generalmente, sono presenti:

- processore;
- logica di *switching*;
- buffer per la memorizzazione dei frame;
- memoria FLASH per la memorizzazione del Cisco IOS;
- memoria RAM per contenere l'immagine dell'IOS e il file di configurazione corrente;
- memoria NVRAM (*non-volatile* RAM) per il file di configurazione da caricare all'avvio;
- memoria ROM in cui mantenere un'immagine minima dell'IOS in caso di malfunzionamenti;
- alimentazione;

- *chip* PHY, uno per ogni porta, per la gestione dell'interfaccia a livello fisico.

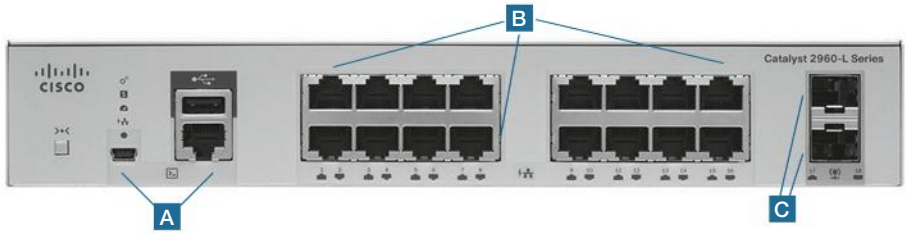

FIGURA **3**

Sul frontale dello switch si trovano le porte di connessione (FIGURA **3**):

A. la porta *console* (con connettore USB mini o RJ45);

B. le porte Ethernet 1Gbps;

C. gli slot per le porte aggiuntive ad alte prestazioni che possono essere Ethernet 1/10 Gbps, o per fibra ottica.

Negli slot per le porte aggiuntive sono inseriti moduli come quello di FIGURA **4**.

FIGURA **4**

Lo switch non è dotato di alcun dispositivo di output né di input, conseguentemente per interagirvi sarà necessario stabilire un qualche tipo di connessione, che potrà essere locale (*console* seriale) o remota (tramite la rete).

- **Console**. Connessione locale tramite un cavo seriale collegato alla porta omonima e un computer dotato di software di emulazione di terminale usando il quale sarà possibile digitare i comandi necessari e vedere sul monitor le risposte ottenute. Questo è il sistema tipico di configurazione iniziale, quando nessun altro sistema di accesso è stato ancora impostato.
- **SSH o Telnet**. Connessione remota che richiede da un lato che l'infrastruttura di rete sia configurata e funzionante e dall'altro che sullo switch sia stato configurato l'indirizzo IP di almeno un'interfaccia virtuale. Tra i due metodi è sicuramente preferibile SSH, che consente un accesso sicuro e la cifratura delle password e dei dati trasmessi. Cisco IOS mette a disposizione un server e un client SSH per stabilire sessioni con altri dispositivi.

Emulazione di terminale

Per stabilire delle sessioni SSH o Telnet esistono numerosi software di emulazione terminale dedicati su tutti i principali sistemi operativi; tra quelli che mettono a disposizione una GUI (ovviamente solo per la configurazione delle impostazioni e per la gestione delle sessioni) ci sono PuTTY e Tera Term in ambiente Windows, SecureCRT o Terminator in ambiente Linux, macOS o Windows.

2 Caratteristiche e struttura interna di un router

Un **router** è un dispositivo intermedio per la comunicazione di rete, ma, a differenza dello switch, gestisce indirizzi IP e pacchetti, quindi PDU di livello 3 per l'interconnessione di LAN e WAN.

Il suo compito è quello di memorizzare informazioni specifiche, dipendenti dalle tecniche e dai protocolli utilizzati, per determinare il percorso ottimale di un pacchetto dal router stesso alla sua destinazione (definita dall'indirizzo IP di destinazione del pacchetto) e, di conseguenza, l'interfaccia di uscita del router su cui propagarlo.

Un router Cisco è un computer e, in quanto tale, è costituito da una scheda madre su cui tipicamente sono presenti:

- alimentatore;
- CPU per l'esecuzione del sistema operativo IOS;
- moduli DDR RAM;
- modulo NVRAM (*non-volatile* RAM);
- *slot* per WAN *Interface Cards* (WIC);
- modulo ROM;
- coprocessore crittografico;
- RTC (*RealTime Clock*).

Le unità di memoria utilizzate all'interno del router sono di diverso tipo:

- **ROM**. In questa memoria non volatile vengono memorizzati: un sistema operativo ridotto, in modo da permettere un eventuale ripristino di un'immagine corrotta; le informazioni di *boot* e il software POST (*Power-On Self-Test*) per il *check* iniziale dei componenti hardware.
- **RAM**. In questa memoria abbastanza veloce vengono memorizzate:
  - immagine del sistema operativo e il file di configurazione corrente;
  - *cache* ARP degli indirizzi MAC delle porte Ethernet;
  - tabella di *routing*, necessaria per la determinazione dei percorsi di instradamento dei pacchetti;
  - buffer in cui memorizzare i pacchetti durante il tempo in cui vengono elaborati prima del loro instradamento.
- **NVRAM**. Memoria non volatile in cui salvare il file di configurazione da caricare in fase di boot.
- **FLASH**. Memoria non volatile che contiene il sistema operativo, così come altri file a esso collegati, quali file di configurazione di *backup* o file di *log*. Sarà da questa memoria che il sistema operativo verrà copiato nella RAM durante il processo di boot.

La parte fondamentale del router, in quanto dispositivo di collegamento con altre reti e altri dispositivi, risiede nel pannello posteriore, qui si trova-

no infatti tutti gli slot per le connessioni; solo a titolo di esempio ecco quelli del router Cisco 1941 (FIGURA **5**):

A. **slot WIC** in cui possono essere inseriti diversi moduli, come quello per la gestione di due porte seriali (FIGURA **6**), o le connessioni wireless e DSL. La possibilità di intercambiare i diversi moduli aumenta notevolmente la flessibilità d'uso del dispositivo;

B. **porte console** per la configurazione iniziale e la manutenzione di emergenza; generalmente, come in questo caso, sono presenti nelle due versioni RJ45 e USB mini;

C. **porte Gigabit Ethernet**, vengono di solito utilizzate per la connessione a switch per fornire accesso a una LAN;

D. **porte USB**, in modo da poter estendere la capacità di memorizzazione del dispositivo mediante memorie FLASH esterne.

Analogamente a quanto visto per lo switch, anche per accedere al router si devono utilizzare la porta console o una connessione da remoto mediante Telnet o SSH.

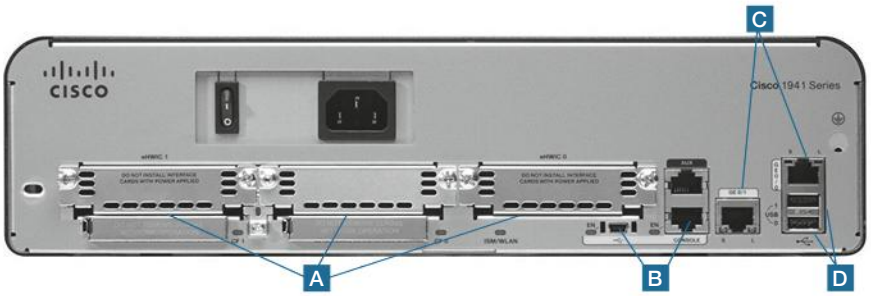

FIGURA **5**

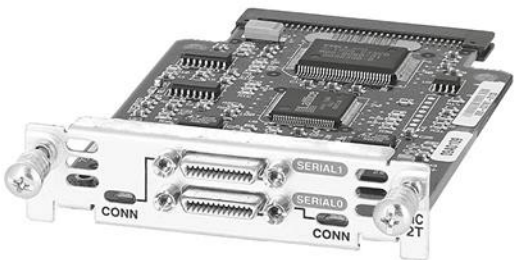

FIGURA **6**

3 Sistema operativo Cisco IOS e linguaggio Cisco CLI

Cisco IOS è un sistema operativo proprietario con interfaccia a riga di comando (CLI) e con funzionalità di *routing*, *switching* e *internetworking*.

Anche se è stato sviluppato inizialmente per i router Cisco, è stato adottato poi anche su molti switch, tra cui la serie Catalyst, e fornisce le seguenti funzionalità:

- gestire protocolli di rete;
- connettere dispositivi anche utilizzando diverse tecnologie di livello *data-link*;
- rendere sicure le risorse.

OSSERVAZIONE Le interfacce per l'uso dei sistemi operativi sono interfacce grafiche a finestre, dette GUI (*Graphical User Interface*), ma in Cisco IOS ci troviamo invece di fronte a una CLI, ovvero un'interfaccia testuale in cui si devono digitare i comandi desiderati comprensivi dei necessari parametri. I dispositivi Cisco più recenti comunque mettono a disposizione anche una GUI di monitoraggio e configurazione, spesso nella forma di un'applicazione web accessibile via rete.

L'interfaccia di tipo CLI richiede la digitazione di ogni comando che si desidera impartire, nella forma:

```
Prompt>comando parametro1 parametro2 ... parametroN
```

Un comando, in Cisco IOS, è costituito da una sequenza di caratteri che termina con uno spazio se seguono dei parametri o con la fine della riga, che dà il via all'esecuzione del comando. Un parametro è una sequenza di caratteri alfanumerici terminata da uno spazio; i parametri rappresentano i dati necessari al comando per eseguire il suo compito.

Anche se l'interfaccia CLI non è *user friendly* come le GUI dei principali sistemi operativi, nell'interprete Cisco CLI sono presenti diverse caratteristiche per facilitare il lavoro.

- **Autocompletamento**. Dovendo digitare ogni carattere di un comando e i relativi parametri, si corre il rischio di effettuare errori materiali di digitazione o di non ricordare la denominazione esatta del comando, quindi in ogni momento è possibile premere il tasto di tabulazione per completare automaticamente il comando stesso.
  Chiaramente nel caso in cui quanto digitato sia ambiguo, ovvero possa corrispondere a più di un comando valido per il contesto corrente, l'interprete CLI si limiterà a riproporre quanto scritto nell'attesa di una disambiguazione.
- **Versione breve**. È possibile scrivere la versione non ambigua più corta possibile di ogni comando. In altre parole, laddove l'interprete CLI è in grado di applicare l'autocompletamento, è inutile continuare a scrivere: il comando (o il parametro) verrà interpretato correttamente come se scritto per intero o autocompletato con il tasto di tabulazione.
- ***History***. Ogni comando inviato viene salvato in un file history, visualizzabile con il comando `show history`, ma soprattutto che si può utilizzare in qualsiasi contesto per ripetere un comando senza digitarlo premendo il tasto «⌧»; è possibile scorrere in questo modo tutti i comandi già utilizzati secondo una politica LIFO (*Last-In First-Out*). L'history è relativa solo all'ultima sessione di connessione, all'uscita viene cancellata.
- ***Help* contestuale**. In ogni momento durante la digitazione è possibile premere il tasto «?» per ottenere un aiuto contestuale, il risultato varia a seconda della posizione in cui è stato inserito il carattere «?».
  Se si sta ancora inserendo il comando infatti, digitare il «?» presenterà una lista di tutti i comandi validi nel contesto corrente che iniziano con i caratteri che sono già stati digitati. Se, per esempio, si digita la sequen-

Autocompletamento

Più o meno da sempre l'autocompletamento dei comandi all'interno delle interfacce di comando testuali è stata un'esigenza sentita; tra i primi esempi che possiamo citare c'è il Berkeley Time Sharing System per SDS 940, a metà degli anni Sessanta. Unix, il primo sistema operativo che viene in mente pensando a questa funzionalità, la introduceva già nelle prime versioni e tutti i principali sistemi operativi con un'interfaccia di comando testuale (DOS, Windows, Linux, macOS) l'hanno mantenuta e/o evoluta.

za di caratteri «e?» verrà mostrata la lista dei comandi validi che iniziano con il carattere «e», ovvero **enable** ed **exit**.
Se, al contrario, il comando è già stato completato ed è quindi stato inserito lo spazio, la digitazione del carattere «?» fornirà dei suggerimenti accurati su tutti i possibili parametri che possono essere forniti al comando digitato. Scrivendo per esempio «**show** ?» verrà mostrata la lunga lista dei parametri che si possono fornire al comando **show**.

Differenziazione dei contesti (*mode*). In Cisco IOS non tutti i comandi sono disponibili contemporaneamente, ma sono divisi in diversi contesti; in questo modo è possibile da un lato limitare l'accesso ad alcuni comandi tramite delle password per concedere privilegi differenziati agli utenti, dall'altro restringere il numero di comandi mostrati nel caso di accesso all'help contestuale.

Muoversi in questi contesti può essere all'inizio disorientante, ma con un po' di pratica si apprezza la distinzione; esistono 4 contesti principali:

1. *User EXEC mode*;
2. *Privileged EXEC mode*;
3. *Global configuration mode*;
4. *Interface configuration mode*.

I primi tre servono per visualizzare, modificare e configurare il sistema, l'ultimo è specifico per la configurazione delle interfacce. Esistono poi contesti più specifici come:

- *Routing protocol configuration mode*, per configurare i protocolli di routing necessari;
- *Line configuration mode*, per la configurazione di *line*;
- *ROMMON mode*, per il recupero del sistema operativo se al boot non ne viene trovato uno installato e funzionante;
- *Setup mode*, se al boot non viene trovato un file di configurazione;
- *Access List configuration mode*, per la configurazione delle ACL (*Access Control List*).

L'approccio è gerarchico, per cui si accede a contesti più interni esclusivamente attraverso quelli più esterni, eventualmente previa autorizzazione, come illustrato nel diagramma di FIGURA 7, a pagina seguente, e nella seguente descrizione.

User EXEC mode. Indipendentemente dalle modalità di connessione al sistema, a prescindere se è stato configurato in modo da richiedere o meno una password per accedere, il primo contesto in cui si opera è *User EXEC mode*.

L'insieme dei comandi a disposizione è estremamente limitato e serve essenzialmente per visualizzare alcune statistiche ed effettuare la gestione dei problemi di base, ma non permette di modificare alcuna delle impostazioni. Da qui si accede al contesto successivo impiegando il comando **enable**.

Privileged EXEC mode. L'insieme dei comandi a disposizione in questo contesto permette di:

- analizzare, salvare e cancellare la configurazione del dispositivo;
- effettuare il backup o il *restore* di IOS;
- installare una nuova immagine di IOS;
- effettuare analisi dei problemi del dispositivo;
- far ripartire il dispositivo.

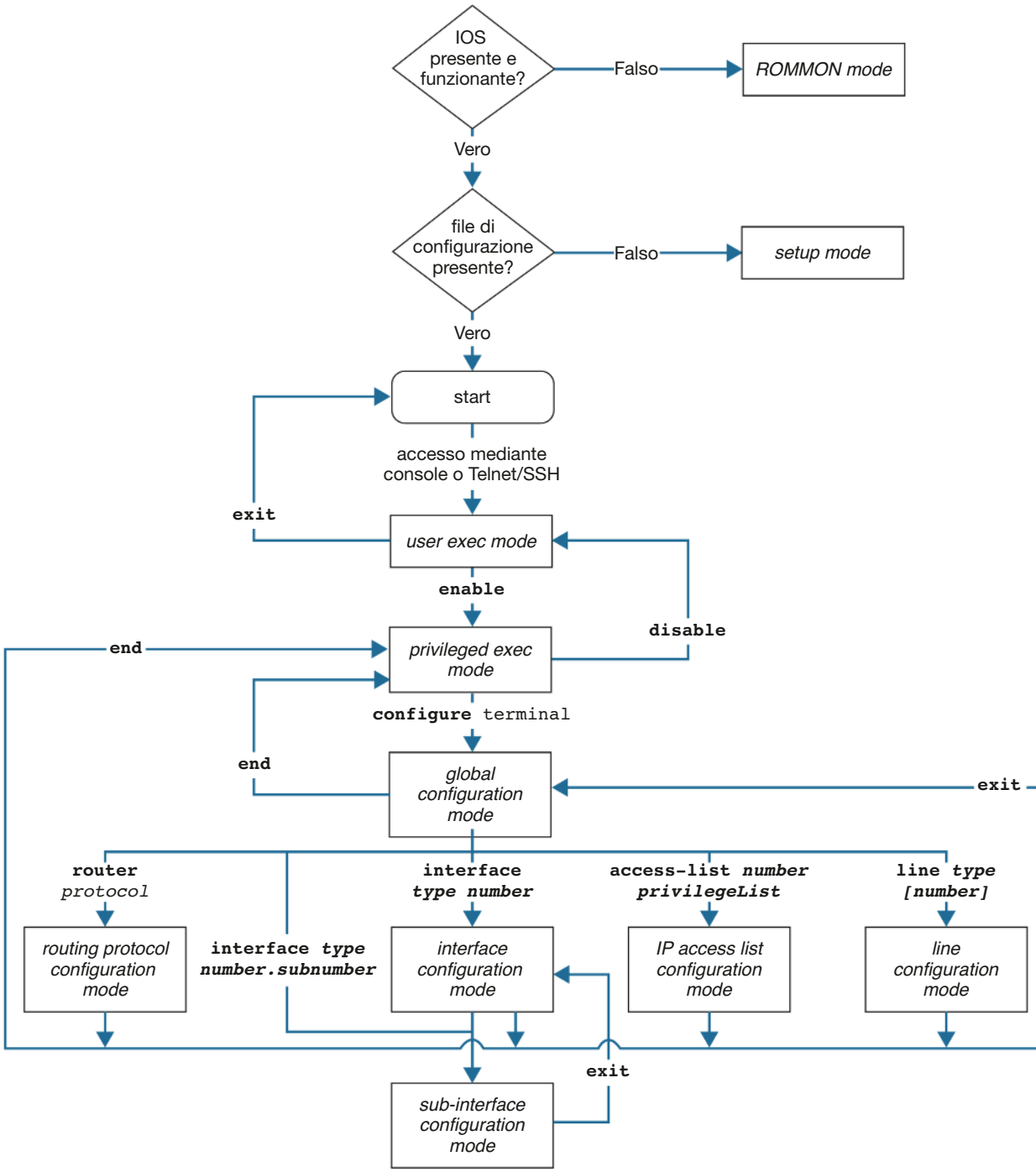

FIGURA 7

Per modificare la configurazione del dispositivo è necessario passare al contesto successivo.

Per ritornare al contesto precedente si usa il comando **`disable`**.

Global configuration mode. Questo è il contesto in cui è presente il maggior numero di comandi, quasi tutti per la configurazione del dispositivo in ogni sua componente attraverso la creazione di nuove impostazioni e la modifica, l'aggiornamento o anche la cancellazione di impostazioni esistenti.

Il comando necessario per raggiungere questo contesto è **`configure`** `terminal` ovviamente a partire dal contesto *Privileged EXEC mode*. Per tornare al contesto precedente si usano i comandi **`exit`** o **`end`**.

Sub-configuration mode. Visto il gran numero di comandi, per organizzarli nel modo più efficace, sono stati ulteriormente suddivisi, dove necessario, in sotto-contesti di configurazione; il principale di essi è *Interface configuration mode*, a cui si accede con il comando **`interface`** seguito dal nome dell'interfaccia che si intende configurare.

Differenziazione del *prompt* al variare del contesto. Per riconoscere più rapidamente il contesto corrente, il prompt cambia al variare del contesto, nel seguente modo (nell'ipotesi che il nome assegnato al dispositivo sia `dispositivo1`, TABELLA **1**):

TABELLA **1**

Mode	Prompt
User EXEC	`dispositivo1>`
Privileged EXEC	`dispositivo1#`
Global configuration	`dispositivo1(config)`
Interface configuration	`dispositivo1(config-if)`

***Shortcut* da tastiera**. Per velocizzare il lavoro, all'interno dell'interprete CLI è possibile utilizzare un discreto numero di scorciatoie da tastiera, tra le principali (TABELLA **2**):

TABELLA **2**

Comando	Effetto
`Ctrl + K`	Cancella tutti i caratteri dal cursore a fine riga.
`Esc + D`	Cancella tutti i caratteri dal cursore a fine parola.
`Ctrl + A`	Sposta il cursore a inizio riga.
`Esc + B`	Sposta il cursore indietro di una parola.
`Ctrl + D`	Cancella il carattere a destra del cursore (il tasto di cancellazione non viene riconosciuto).
`Ctrl + Shift + 6`	Sequenza di *break* generale: importante nei tentativi di connessione per non dover attendere i *timeout*.

OSSERVAZIONE I comandi di impostazione modificano la configurazione corrente di funzionamento del dispositivo memorizzata nella memoria RAM volatile (*running-config*). Al momento dell'accensione o di un riavvio il dispositivo si autoconfigura a partire dalla configurazione iniziale memorizzata nella memoria NVRAM permanente (*startup-config*). Il comando che permette di salvare la configurazione corrente come nuova configurazione permanente di avvio è il seguente:

```
copy running-config startup-config
```

ESEMPIO

Configurazione di base di uno switch

La configurazione di base di uno switch prevede l'impostazione di un nome per il dispositivo, in modo da rendere più agevole la gestione della rete e di un *banner* da presentare a ogni accesso al dispositivo; per ragioni di sicurezza devono essere impostate le password di accesso alla modalità *Privileged EXEC mode* e al dispositivo mediante console o mediante Telnet/SSH. La configurazione dell'indirizzo IP con relativa *subnet mask* e dell'indirizzo IP del *default gateway* non è necessaria per il funzionamento di uno switch, ma consente di accedere al dispositivo via rete mediante il protocollo Telnet o SSH (TABELLE **3** e **4**).

TABELLA **3**

Parametro da configurare	Valore
Nome dispositivo	`Sw-LabInf`
Banner	`Sw-LabInf: l'accesso è consentito solo agli utenti autorizzati`
Password di accesso via console	`Password1`
Password di accesso a *Privileged EXEC mode*	`Password2`
Password di accesso via Telnet/SSH	`Password3`
Indirizzo IP	`192.168.1.253`
Subnet mask	`255.255.255.0`
Default gateway	`192.168.1.254`

TABELLA **4**

Scopo	Comando
Entrare in *Privileged EXEC mode*	`Switch>`**`enable`**
Entrare in *Global configuration mode*	`Switch#`**`configure`**` terminal` `Enter configuration commands, one per line. End with CNTL/Z.`
Notare il cambio di prompt Cambiare il nome al dispositivo	`Switch(config)`**`#hostname`**` Sw-LabInf`
Notare di nuovo il cambio di prompt Impostare il banner per tutte le implicazioni legali	`Sw-LabInf(config)`**`#banner`**` motd @Sw-LabInf: l'accesso è consentito solo agli utenti autorizzati@`
Impostare la password di accesso a *Privileged EXEC mode*	`Sw-LabInf(config)`**`#enable`**` secret Password1`
Criptare le password di line	`Sw-LabInf(config)`**`#service password-encryption`**
Impostare la password di accesso al dispositivo via console	`Sw-LabInf(config)`**`#line`**` console 0`
Notare il prompt di *Sub-configuration mode* Può essere impostata la password relativa	`Sw-LabInf(config-line)`**`#password`**` Password2`
Richiedere che per accedere debba essere eseguito un login in cui si chiede la password	`Sw-LabInf(config-line)`**`#login`**
Tornare in *Global configuration mode*	`Sw-LabInf(config-line)`**`#exit`**
Impostare la password di accesso al dispositivo via Telnet	`Sw-LabInf(config)#line vty 0 3`
Impostare la password relativa	`Sw-LabInf(config-line)`**`#password`**` Password3`
Richiedere che per accedere debba essere eseguito un login in cui si chiede la password	`Sw-LabInf(config-line)`**`#login`**
Tornare in *Global configuration mode*	`Sw-LabInf(config-line)`**`#exit`**
Per configurare l'indirizzo IP, si deve usare la VLAN 1	`Sw-LabInf(config)`**`#interface`**` vlan 1`

Scopo	Comando
Assegnare l'indirizzo IP e la subnet mask	`Sw-LabInf(config-if)#ip address 192.168.1.253 255.255.255.0`
Attivare l'interfaccia	`Sw-LabInf(config-if)#no shutdown`
Tornare in *Global configuration mode*	`Sw-LabInf(config-if)#exit`
Assegnare il default gateway	`Sw-LabInf(config)#ip default-gateway 192.168.1.254`
Per SSH serve anche il dominio	`Sw-LabInf(config)#ip domain name dominioIP`

Generare le chiavi crittografate (verranno usati il nome *host* e il nome di dominio)	`Sw-LabInf(config)#crypto key generate rsa`
	
	`The name for the keys will be: Sw-LabInf.dominioIP`
	`Choose the size of the key modulus in the range of 360 to 2048 for your General Purpose Keys. Choosing a key modulus greater than 512 may take a few minutes.`
	
	`How many bits in the modulus [512]: 1024`
	`% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]`

Impostare login e password per la connessione SSH	`Sw-LabInf(config)#username admin password Password3`
Specificare la versione	`Sw-LabInf(config)#ip ssh version 2`
Impedire la connessione non SSH	`Sw-LabInf(config)#line vty 0 3`
	`Sw-LabInf(config-line)#transport input ssh`
	`Sw-LabInf(config-line)#login local`
Tornare in *Global configuration mode*	`Sw-LabInf(config-line)#exit`
Tornare in *Privileged EXEC mode*	`Sw-LabInf(config)#exit`
Salvare il file nella memoria NVRAM (attenzione a non invertire i nomi)	`Sw-LabInf#copy running-config startup-config`

OSSERVAZIONE A riguardo della sicurezza: il comando

```
enable password Password1
```

imposta la password tanto quanto il comando che è stato usato

```
enable secret Password1
```

ma il primo scrive in chiaro la password nel file di configurazione, mentre il secondo la cripta usando una funzione *hash* SHA-256.
Anche il comando

```
service password-encryption
```

cripta le password di accesso che altrimenti verrebbero scritte in chiaro nel file di configurazione. L'algoritmo usato in questo caso però è considerato debole e facilmente reversibile (esistono strumenti che lo decifrano).

ESEMPIO

Configurazione di base di un router

La configurazione di base di un router prevede l'impostazione di un nome per il dispositivo, in modo da rendere più agevole la gestione della rete e di un banner da presentare a ogni accesso al dispositivo; per ragioni di sicurezza devono essere impostate le password di accesso alla modalità *Privileged EXEC mode* e al dispositivo mediante console o mediante Telnet/SSH. Dovranno essere configurate poi tutte le interfacce di rete che si devono utilizzare almeno per quanto riguarda indirizzo IP e subnet mask (TABELLE **5** e **6**).

TABELLA **5**

Parametro da configurare	Valore
Nome dispositivo	`Router-Li`
Banner	`Router-Li: l'accesso è consentito solo agli utenti autorizzati`
Password di accesso via console	`Password1`
Password di accesso a *Privileged EXEC mode*	`Password2`
Password di accesso via Telnet/SSH	`Password3`
GigabitEthernet 0/0: indirizzo IPv6	`FC00:1234:1:0::1/64` `FE80:ABCD::1/64 (link-local)`
GigabitEthernet 0/1: indirizzo IPv4 e subnet mask	`192.168.1.254` `255.255.255.0`
Serial 0/1/0: indirizzo IPv6	`FC00:1234:2:0::1/64` `FE80:ABCD::1/64 (link-local)`
Serial 0/1/0: indirizzo IPv4 e subnet mask	`10.0.1.1` `255.255.255.252`

TABELLA **6**

Scopo	Comando
Entrare in *Privileged EXEC mode*	`Router>`**`enable`**
Entrare in *Global configuration mode*	`Router`**`#configure`**` terminal`
Cambiare il nome al dispositivo	`Router(config)`**`#hostname`**` Router-Li`
Impostare il banner	`Router-Li(config)`**`#banner`**` motd @Router-Li: l'accesso è consentito solo agli utenti autorizzati@`
Impostare la password di accesso a *Privileged EXEC mode*	`Router-Li(config)`**`#enable secret`**` Password1`
Criptare le password di line	`Sw-LabInf(config)`**`#service password-encryption`**
Impostare la password di accesso al dispositivo via console, si deve configurare line console	`Router-Li(config)`**`#line`**` console 0`
Impostare la password relativa	`Router-Li(config-line)`**`#password`**` Password2`
Richiedere che al login venga chiesta la password	`Router-Li(config-line)`**`#login`**
Tornare in *Global configuration mode*	`Router-Li(config-line)`**`#exit`**
Impostare la password di accesso al dispositivo via Telnet; si devono configurare le *line vty*	`Router-Li(config)`**`#line`**` vty 0 3`
Impostare la password relativa	`Router-Li(config-line)`**`#password`**` Password3`
Richiedere che al login venga chiesta la password	`Router-Li(config-line)`**`#login`**
Tornare in *Global configuration mode*	`Router-Li(config-line)`**`#exit`**
Abilitare il meccanismo di inoltro con IPv6	`Router-Li(config)`**`#ipv6 unicast-routing`**
Selezionare la prima interfaccia Ethernet (solo IPv4)	`Router-Li(config)`**`#interface`**` gigabitEthernet 0/0`

Scopo	Comando
Impostare l'indirizzo IPv4 e la subnet mask	`Router-Li(config-if)#ip address 192.168.1.254 255.255.255.0`
Attivare l'interfaccia	`Router-Li(config-if)#no shutdown`
Tornare in *Global configuration mode*	`Router-Li(config-if)#exit`
Selezionare la seconda e procedere analogamente (solo IPv6)	`Router-Li(config)#interface gigabitEthernet 0/1`
Impostare l'indirizzo IPv6 *Unique-local* con il prefisso	`Router-Li(config-if)#ipv6 address FC00:1234:1:0::1/64`
Impostare l'indirizzo IPv6 *Link-local*	`Router-Li(config-if)#ipv6 address FE80:ABCD::1 link-local`
Attivare IPv6	`Router-Li(config-if)#ipv6 enable`
Attivare l'interfaccia	`Router-Li(config-if)#no shutdown`
Tornare in *Global configuration mode*	`Router-Li(config-if)#exit`
Selezionare l'interfaccia seriale e procedere analogamente con indirizzi sia IPv4 sia IPv6	`Router-Li(config)#interface Serial 0/1/0`
Impostare l'indirizzo IPv4 e la subnet mask	`Router-Li(config-if)#ip address 10.0.1.1 255.255.255.252`
Impostare l'indirizzo IPv6 *Unique-local* con il prefisso	`Router-Li(config-if)#ipv6 address FC00:1234:2:0::1/64`
Impostare l'indirizzo IPv6 *Link-local*	`Router-Li(config-if)#ipv6 address FE80:ABCD::1 link-local`
Attivare IPv6	`Router-Li(config-if)#ipv6 enable`
Attivare l'interfaccia	`Router-Li(config-if)#no shutdown`
Tornare in *Global configuration mode*	`Router-Li(config-if)#exit`
Tornare in *Privileged EXEC mode*	`Router-Li(config)#exit`
Salvare il file in memoria nella NVRAM (attenzione a non invertire i nomi)	`Router-Li#copy running-config startup-config`

4 Il software di simulazione Packet Tracer

Packet Tracer è un programma di simulazione multipiattaforma sviluppato da Cisco: può essere eseguito su Linux, Windows, macOS Android e iOS per realizzare infrastrutture di rete anche molto complesse utilizzando dispositivi Cisco, verificandone la configurazione e, eventualmente, simulandone il comportamento.

L'applicazione si presenta con una GUI standard (FIGURA **8**, a pagina seguente):

A. la barra dei menu;

B. la barra dei comandi principale;

C. la barra dei comandi secondaria;

D. la barra in basso per la selezione delle categorie di componenti;

E. la barra per la selezione dei componenti;

F. l'elenco dei componenti selezionati;

G. i pulsanti di selezione tra la topologia logica e quella fisica;

H. i pulsanti di selezione tra la modalità *realtime* e quella di simulazione;

I. i pulsanti per la navigazione nella gerarchia logica o fisica, a seconda della topologia;

J. l'ambiente di lavoro.

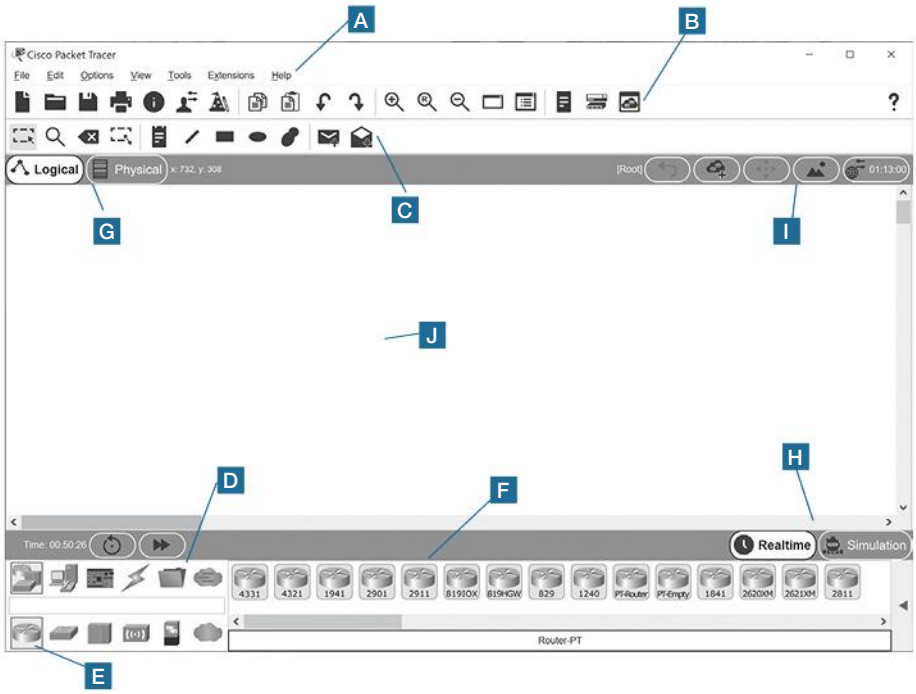

FIGURA **8**

Permette di gestire un unico progetto alla volta, anche se della rete in esame è possibile definire contemporaneamente sia la topologia logica sia quella fisica.

La vista principale di Packet Tracer consente di definire l'infrastruttura di rete secondo il modello logico desiderato, a prescindere dalla collocazione fisica dei dispositivi.

La definizione della rete avviene effettuando il trascinamento del componente desiderato dalla barra in basso verso l'area di lavoro al centro.

La selezione dell'oggetto desiderato avviene in due passi: prima si seleziona la categoria di dispositivi tra quelle disponibili tra le icone della barra **D** e poi, conseguentemente, la sottocategoria tra quelle presenti tra le icone della barra **E**; ovviamente le sottocategorie presenti varieranno in base alla scelta precedente.

A questo punto dall'elenco grafico **F** sarà possibile selezionare il dispositivo desiderato e trascinarlo nell'ambiente di lavoro.

Selezionando per esempio prima `Network devices` (la scelta viene evidenziata colorando lo sfondo dell'icona corrispondente) e poi `Switches` si presenta la situazione riportata in FIGURA **9**

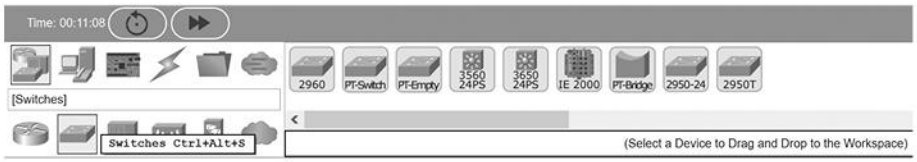

FIGURA **9**

da cui può essere selezionato lo switch desiderato.

Dopo aver posizionato nell'ambiente di lavoro tutti i dispositivi necessari, si può procedere al loro collegamento; per farlo si utilizza la categoria `Connections` che ha come sottocategorie solo l'omonima `Connections` e `Structured Cabling` (utilizzabile solo nella topologia fisica) per il cablaggio strutturato (FIGURA **10**).

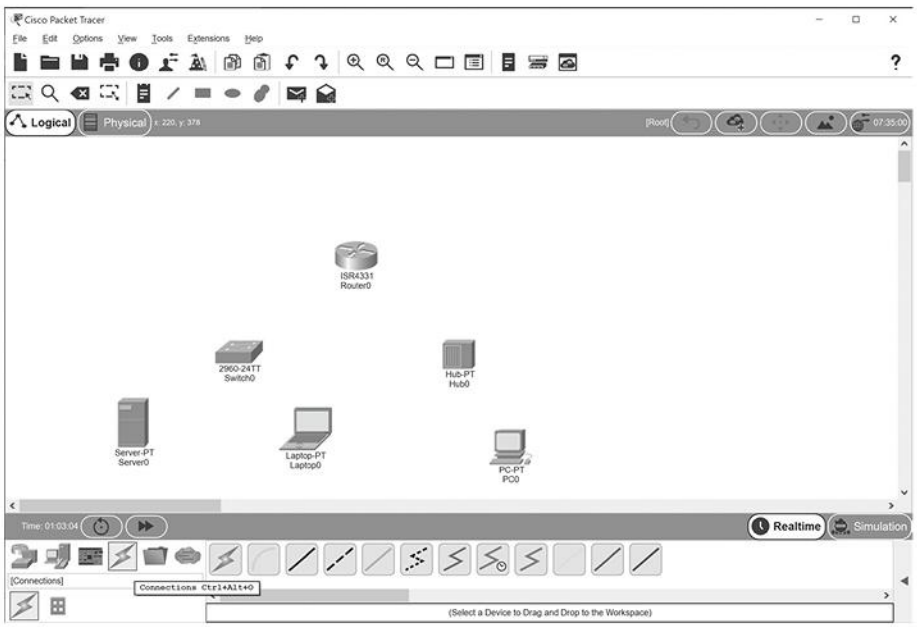

FIGURA **10**

Il primo elemento di connessione da sinistra è la connessione automatica, da utilizzarsi ovviamente solo quando la scelta è univoca.

Se si vuole effettuare la connessione tra un end device e uno switch (o router) attraverso la porta console, si deve utilizzare il cavo omonimo. Quando è stato selezionato un tipo di connessione e si clicca sopra un dispositivo, viene presentata la lista delle porte a cui è possibile connettere il collegamento; se per esempio è già stato collegato il cavo console sulla porta omonima dello switch e si clicca su un dispositivo di tipo *laptop*, viene visualizzato quanto rappresentato in FIGURA **11**, a pagina seguente: la porta da selezionare è la seriale (RS 232).

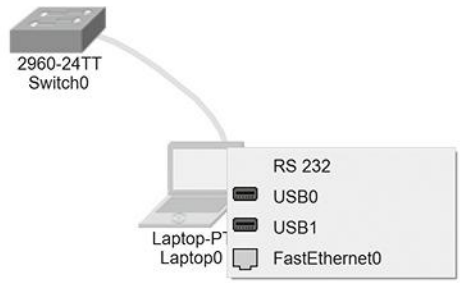

FIGURA **11**

FIGURA **12**

Per connettere degli end device a dispositivi di rete come switch, router o hub utilizzando le porte Ethernet deve essere utilizzato il cavo *straight-through* (FIGURA **12**). Per connettere dispositivi dello stesso tipo (switch con switch o PC con PC) veniva utilizzato un cavo *crossover*, eventualmente rappresentato in nero tratteggiato, ma i dispositivi moderni sono capaci di auto negoziare il tipo di collegamento.

Due router sono normalmente connessi mediante un cavo seriale: scegliendo il cavo DCE il primo dei router su cui si clicca sarà il dispositivo DCE che genera il segnale di clock e l'altro DTE, scegliendo l'altro cavo accadrà il contrario.

Dopo aver effettuato il collegamento, Packet Tracer mostra in ogni istante lo stato di funzionamento di quanto definito: sono presenti due frecce verdi rivolte verso l'alto nel caso in cui il collegamento sia attivo, o due frecce rosse rivolte verso il basso nel caso in cui non lo sia (FIGURA **13**).

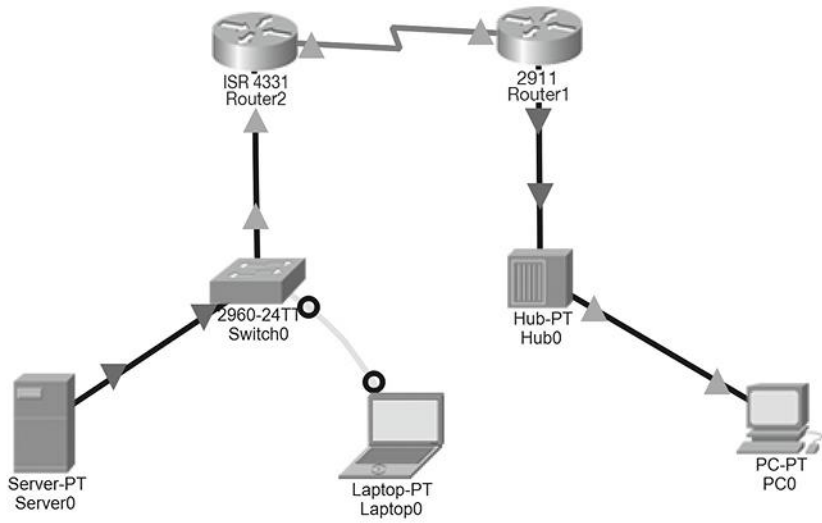

FIGURA **13**

Per mostrare o meno i modelli dei dispositivi, i nomi delle porte e altri elementi di configurazione, si devono selezionare opzioni nella scheda `Interface` della finestra `Preferences`, accessibile dal menu principale `Options`.

Per configurare i dispositivi utilizzati è sufficiente cliccare sopra quello da modificare: comparirà una nuova finestra contenente un numero di schede che varia in base al dispositivo (FIGURA **14**).

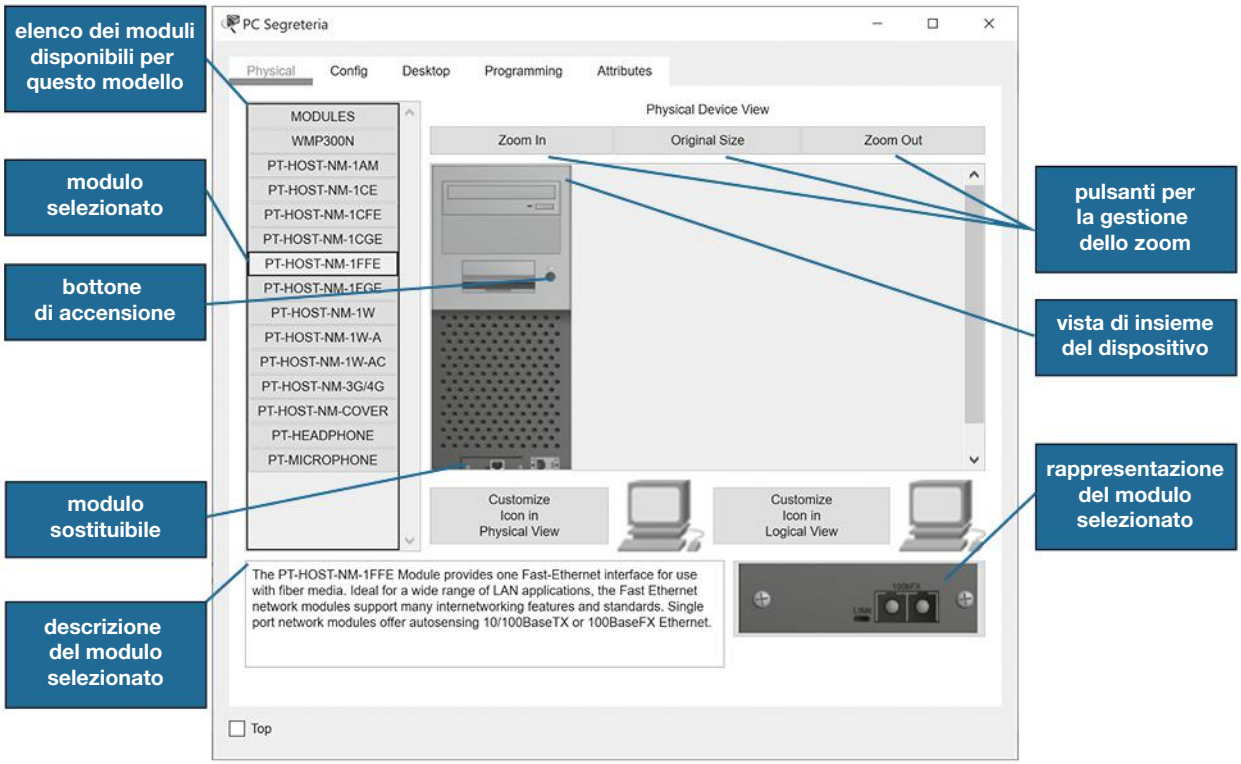

FIGURA **14**

Praticamente tutti i dispositivi hanno la scheda `Physical`, tramite la quale è possibile accendere/spegnere il dispositivo e modificarne la configurazione fisica utilizzando i moduli elencati a sinistra nella colonna `Modules`; non è possibile modificare la configurazione fisica se il dispositivo è acceso. Per inserire un modulo si deve trascinare dalla lista di sinistra fino a uno slot vuoto. Nel caso uno slot sia pieno si deve prima svuotare trascinandolo da dove si trova fino alla lista dei moduli.

Dalla scheda `Config` è possibile effettuare la configurazione dei parametri principali per un end device selezionando `Settings` nella lista `Global` di sinistra, come il *display name* (ovvero quello che si vede nell'interfaccia), default gateway e DNS; è possibile altresì impostare i parametri per ogni interfaccia elencata sotto `Interface` sempre nella lista di sinistra, come gli indirizzi IPv4 e IPv6 o il MAC *address* (FIGURA **15**, a pagina seguente).

Dalla scheda `Desktop` è possibile accedere alle varie applicazioni dell'end device, quali il browser per la navigazione della rete Internet, o il prompt dei comandi per verificare la connessione tra dispositivi utilizzando i comandi **`ping`** o **`traceroute`** (FIGURA **16**, a pagina seguente).

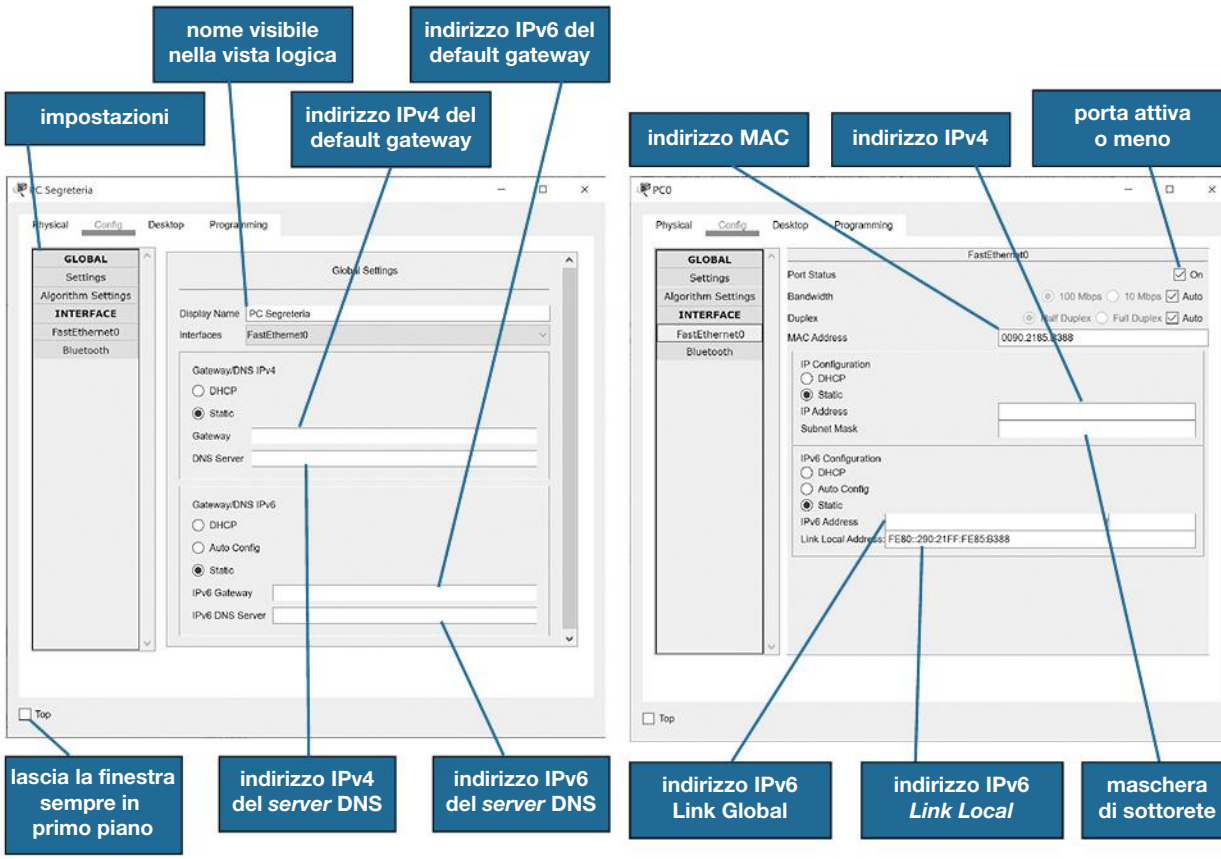

FIGURA **15**

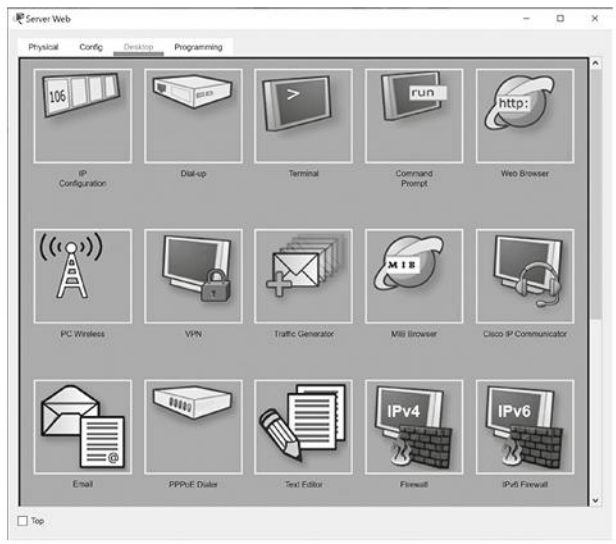

FIGURA **16**

Nel caso in cui l'end device sia un server, sarà presente anche una scheda `Services` con cui configurare i servizi che si desiderano attivare: selezionare il servizio dalla lista `Services` sulla sinistra e impostare i parametri sulla destra (FIGURA **17**).

Quando si clicca su un router o uno switch, o comunque un *manageable network device*, accanto alla scheda `Config` è presente la scheda `CLI`, da cui si accede all'interfaccia a riga di comando di Cisco IOS e da cui possono essere effettuate le configurazioni più dettagliate (FIGURA **18**).

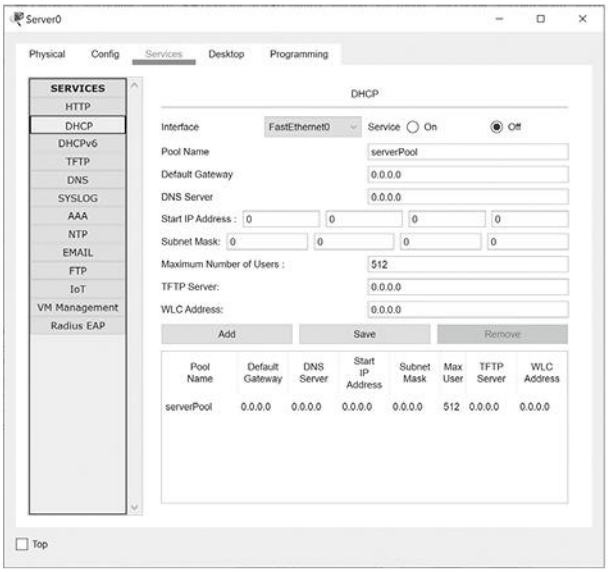

FIGURA **17**

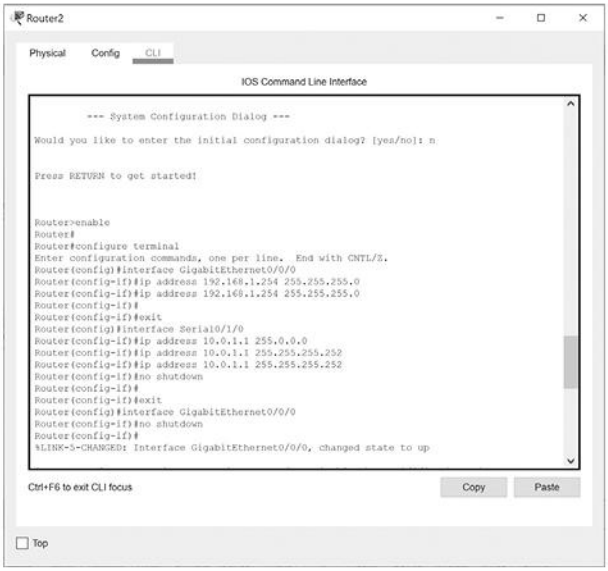

FIGURA **18**

Spesso è utile definire delle annotazioni nella vista logica, per indicare per esempio degli indirizzi IP, per racchiudere all'interno di un elemento grafico i dispositivi di una LAN o, semplicemente, per aggiungere dei commenti alla documentazione. Per quanto limitati, gli strumenti per farlo sono presenti nella barra dei comandi secondaria.

Per definire la topologia fisica, è sufficiente cliccare sul pulsante `Physical` posto a sinistra sopra l'area di lavoro; la struttura fisica è organizzata in modo gerarchico tramite contenitori: *intercity*, *city*, *building*, *closet*, *rack/table*.

Ogni livello ha una vista a sé in cui si vedono solo eventuali dispositivi e i contenitori di livello successivo in esso contenuti (per esempio nella vista *building* si vedranno solo i *closet* al suo interno). Per scendere di livello nella gerarchia si deve cliccare sull'oggetto desiderato, mentre per tornare indietro serve il pulsante `Back` posizionato sopra l'area di lavoro a destra.

Quando si inseriscono i dispositivi nella vista logica, sono creati automaticamente una nuova *city* in cui è presente un nuovo building che contiene gli end device e un nuovo *closet* al suo interno con un nuovo *rack* per contenere i *network device* (FIGURA **19**).

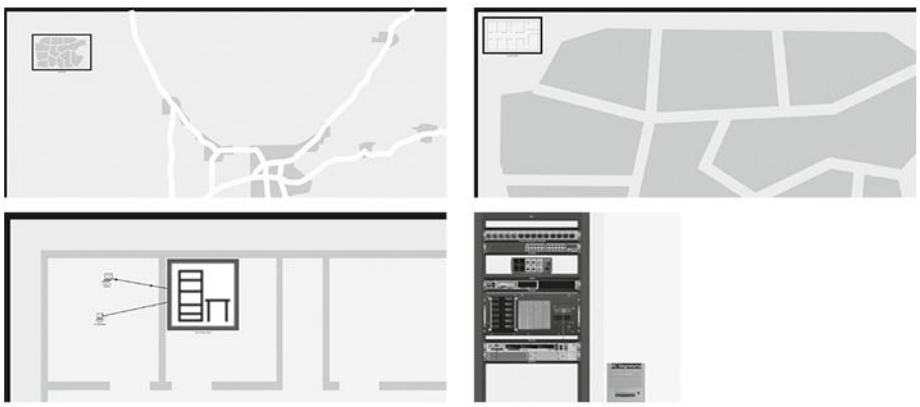

FIGURA **19**

Tramite i pulsanti posizionati a destra sopra l'area di lavoro è possibile definire nuovi oggetti e/o spostare quanto necessario in altri contenitori.

In generale la gestione sia della navigazione sia degli spostamenti è molto facilitata dalla finestra `Navigation panel` che presenta una lista ad albero di tutto quanto presente nella topologia fisica; cliccando su un elemento dell'albero e poi sul pulsante `Jump to Selected Location` è possibile navigare la gerarchia e, utilizzando il trascinamento, spostare i dispositivi da un contenitore all'altro (FIGURA **20**).

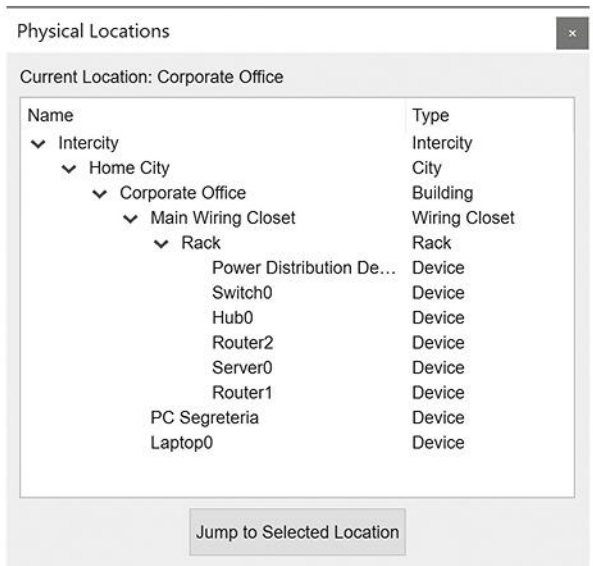

FIGURA **20**

Per analizzare e risolvere eventuali problemi sull'infrastruttura di rete definita, è possibile passare dal modo **Realtime** alla modalità **Simulation** utilizzando il pulsante omonimo posizionato a destra sotto l'area di lavoro.

Nella zona a destra dell'area di lavoro comparirà una finestra dal titolo `Simulation Panel`: alcune finestre come questa possono essere bloccate nella zona destra (*docked*) con un doppio click sulla barra del titolo, o sbloccate trascinandole nell'area di lavoro.

Il pannello di simulazione è costituito da tre zone principali:

- **lista degli eventi** (*Event list*) visualizza i passi effettuati da ciascuno dei pacchetti generati da ciascuno dei dispositivi ordinati cronologicamente; il significato di ogni valore è riportato nel titolo della colonna;
- **controlli di simulazione** (*Play controls*) sono controlli per andare indietro di un passo, far procedere in continuo la simulazione e andare avanti di un passo, rispettivamente. Subito sotto è presente anche uno *slider* per la regolazione della velocità della simulazione;
- **filtri sugli eventi** (*Event list filters*) elenco di tutti i protocolli che devono essere mostrati nella lista degli eventi in quel momento.