Corso di Reti di Calcolatori
Dipartimento di Informatica
Università degli Studi di Milano

Dispense di Cisco Packet Tracer

Simone Bassis, Giorgio Biacchi, Giulio Casella

Indice

1. Prima di iniziare

Le seguenti dispense non intendono fornire un manuale di utilizzo di Cisco Packet Tracer e sono rivolte a un pubblico che possiede una minima dimestichezza con l'ambiente di simulazione e ne conosce le principali funzionalità e strumenti. Lo scopo di questi appunti consiste piuttosto nello sviscerare alcuni degli aspetti più rilevanti e meno intuitivi che il corso mira ad insegnare, nonché nel permettere agli studenti che non hanno avuto la possibilità di seguire le varie lezioni di affrontare con successo la prova d'esame.

Per chi non avesse familiarità con il software, si consiglia di visionare documentazione, tutorial e esempi di utilizzo che si trovano nella pagina ufficiale `http://www.packettracernetwork.com/`, ovvero scaricando opportuno materiale che trova ampia diffusione nel web (ad esempio le slide reperibili alla pagina `http://laren.di.unimi.it/~simone/labretiinf/slidePT.pdf` e `http://laren.di.unimi.it/~simone/labretiinf/slidePTShort.pdf` costituiscono due validi tutorial introduttivi preparati rispettivamente dal Prof. Marco Listanti e il suo collega Prof. Vincenzo Eramo nei rispettivi corsi di laurea; oppure alla pagina `http://engweb.info/cisco/Packet\%20Tracer\%20Tutorials.html` sono disponibili tutorial organizzati per tematiche), o ancora tramite l'apposita documentazione prevista all'interno del software. Inoltre si faccia riferimento alle slide mostrate a lezione, reperibili al sito `http://network.di.unimi.it/doku.php?id=cisco:start`, di cui si farà riferimento da ora in avanti con il termine homesite.

In queste dispense si daranno dunque per scontati svariati aspetti del software, tra cui:

- modalità fisica/logica, real-time/simulazione con relativi strumenti utili in modalità simulazione (tra cui la scelta dei filtri sui protocolli da visualizzare);
- dispositivi e loro caratteristiche (hub, switch, router, host, server, ...) e funzionalità anesse (aggiunta di componenti quali interfacce di rete, pannelli di configurazione, CLI, altri strumenti messi a disposizione da taluni device, quali terminale, browser, nonché possibili servizi offerti, quali Web, DHCP, etc.);
- cavi di collegamento, suddivisi per tecnologie, dritti (straight) o incrociati (cross);
- visualizzazione del percorso che i singoli pacchetti seguono dalla sorgente a destinazione (in modalità simulazione) con analisi del loro contenuto, della loro elaborazione all'interno dei vari dispositivi di rete per cui transitano e delle informazioni visualizzate livello per livello della pila ISO-OSI;
- rivisitazione dei principali protocolli di rete studiati nella parte di teoria (ICMP, ARP, DHCP) nell'ottica del simulatore, con semplici esempi che ne dimostrano le caratteristiche funzionali e permettono di acquisire più familiarità con i protocolli stessi;
- invio di pacchetti ICMP (ping).

2. In fase di rodaggio

Può rivelarsi estremamente utile, in prima istanza, creare delle semplici topologie di rete per poi verificarne il funzionamento, acquisendo dimestichezza con i vari dispositivi e le funzionalità previste da Packet Tracer nella modalità simulazione, rivisitando al contempo semplici protocolli studiati a teoria (quali ICMP, ARP, DHCP) avvalendosi a tal fine della possibilità di visualizzare il contenuto dei pacchetti in transito.

Tra i vari esempi che si consiglia di implementare riportiamo:

Esempio 2.1. *Due host collegati con cavo cross* (Figura 2.1(a)). Appurato che le interfaccie coinvolte riportino un pallino verde (che sta a significare che la trasmissione dei dati a livello 1 avviene correttamente), si proceda ad assegnare un indirizzo IP agli host (nella scheda Config del dispositivo si aggiunga un indirizzo IP privato (vedi Sezione 3) alla giusta interfaccia (es. FastEthernet0)) così che questi possano comunicare tra loro a livello 3. Si inviino successivamente pacchetti ICMP (ping → echo request – echo reply) e si monitori il transito e il contenuto dei pacchetti in circolazione filtrando il solo protocollo ICMP nella modalità simulazione (i filtri compaiono in basso a destra nel Simulation Panel). △

Esempio 2.2. *Tre host collegati a un hub* – 3 *host* → 1 *hub* (Figura 2.1(b)). Si studino i percorsi seguiti dai pacchetti ICMP: essendo l'hub un dispositivo "stupido", si noti come i pacchetti siano inviati a tutti gli host ad eccezione del mittente (unica decisione che è in grado di prendere). Si osservi inoltre la presenza di un unico dominio di collisione, provando a simulare collisioni tra pacchetti ICMP (generando contemporaneamente due pacchetti ICMP da host differenti). △

Esempio 2.3. 4 *host* → 2 *hub* → 1 *bridge* (Figura 2.1(c)). Anzitutto si osservi come ogni volta che si è chiamati a collegare due apparati di rete o due end device tra loro, sia necessario usare un cavo cross. Si osservi inoltre come, grazie alla sua politica anti-flooding, il bridge apprenda gli indirizzi di livello 2 dagli header dei frame, isolando conseguentemente in due il dominio di collisione. △

Esempio 2.4. 4 *host* → 4 *bridge* → 1 *hub* (Figura 2.1(e)). Scopo di questo esercizio è mostrare come, con una siffatta topologia, non avvengano collisioni (nonostante se ne possano verificare ma solo all'interno dell'hub). È interessante notare come combinando i 4 bridge e l'hub si ottiene uno switch. △

Esempio 2.5. 5 *host (4 pc e* 1 *server)* → 1 *switch* (Figura 2.1(f)). Si segua l'iter dei pacchetti dopo aver abilitato i filtri ICMP e ARP; in particolare, usando lo strumento Lente di ingrandimento sullo switch è possibile visualizzare la ARP Table, le cui entry sono rimosse/scadono dopo alcuni minuti per consentire la dovuta flessibilità nel caso di variazioni degli indirizzi IP degli host (ipotesi probabile quando si utilizzano IP dinamici),

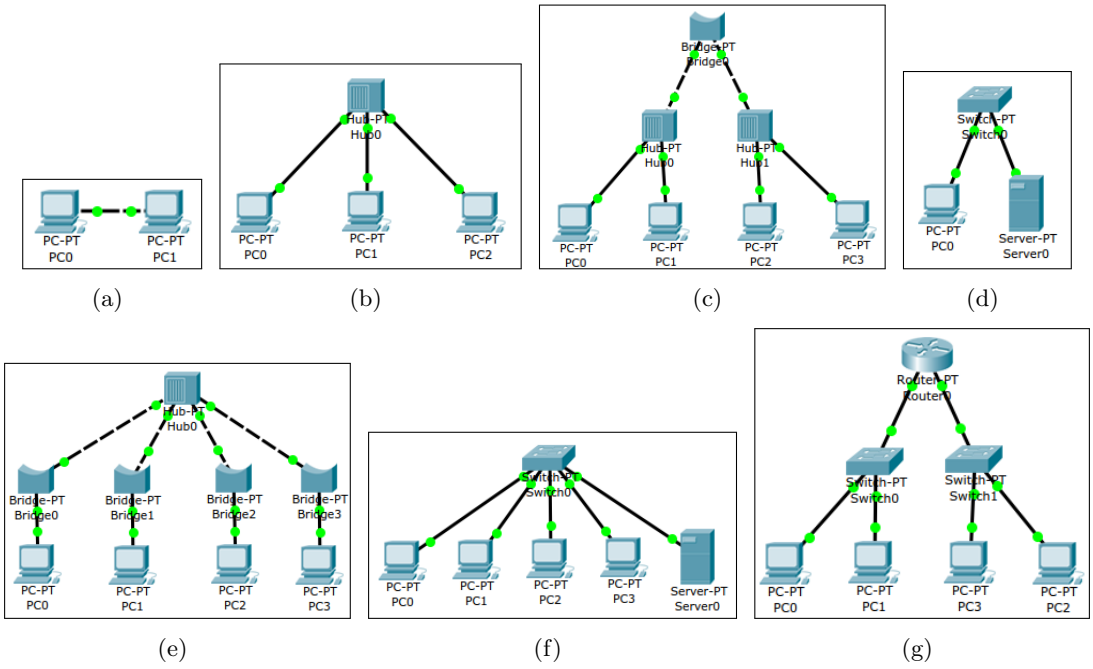

FIGURA 2.1: Topologie di rete utilizzate negli Esempi 2.1-2.7.

oppure della topologia. Si ricorda infine che per poter aggiungere porte o interfacce sui vari dispositivi e, in ogni caso, per modificarne la configurazione hardware, è necessario spegnerli. △

Esempio 2.6. 4 *host* → 1 *switch* → 1 *router* ← 1 *switch* ← 4 *host* (Figura 2.1(g)). Ricordandosi di abilitare le porte, di default spente nei router, per permettere il collegamento elettrico (nella scheda Config si abiliti il checkbox Port Status relativo alle interfacce che si vogliono abilitare), si assegni un indirizzo IP diverso alle due interfacce del router collegate ai due switch. Per far questo si aggiungano indirizzo IP e subnet mask (per maggiori informazioni si veda la Sezione 3) nei campi IP Address e Subnet Mask all'interno della interfaccia che si intende configurare (scheda Config). Tale indirizzo IP rappresenta il default gateway per gli host situati nella corrispettiva sottorete. Se la configurazione di questi ultimi è manuale (in altre parole se non è attivo un servizio DHCP) è necessario provvedere a specificare l'indirizzo IP del gateway nell'omonimo campo situato nella scheda Config → Settings dell'host. Si ricordi inoltre che un router separa due reti differenti di livello 3, ottenendo due broadcast domain diversi. Si eseguano prove di connettività interna tra le sottoreti sempre attraverso l'invio di pacchetti ICMP (un solo dispositivo di livello 3 fa "routing", ma non ha bisogno di utilizzare un protocollo di routing); inoltre sugli host si provi a digitare nel terminale (accessibile dalla scheda Desktop dell'host stesso) i comandi `arp -a`, `arp -d`, `ping`. Per finire, si ricordi che, tra router e switch, Packet Tracer prevede l'utilizzo di un cavo dritto (con alcuni tipi di apparati reali andrebbe

usato un cavo cross, mentre molti dei dispositivi moderni sono “auto-crossing”, quindi si possono utilizzare entrambi i tipi di cavo); △

Esempio 2.7. 2 *host (*1 *pc e* 1 *server)* → 1 *switch* (Figura 2.1(d)). Si analizzi il funzionamento del protocollo DHCP (utilizzato per la configurazione automatica dell’indirizzo IP), con particolare riferimento alle 4 fasi principali di cui è composto: discover, offer, request, ack. Si utilizzi a tal fine l’apposito filtro nella modalità Simulazione e si visioni il contenuto dei vari pacchetti in transito. △

3. Subnetting

Per comprendere tutti i dettagli relativi all’indirizzamento si consiglia di consultare la presentazione in PowerPoint Subnetting (Prima parte) disponibile nella homesite. Le definizioni ivi riportate hanno il solo scopo di orientare lo studente introducendo la terminologia necessaria per poter approfondire gli argomenti del corso. Per maggiori dettagli si consiglia di consultare il libro di testo usato nella parte di teoria. Si consiglia inoltre di svolgere tutti gli esercizi proposti nelle slide.

L’esempio seguente mostra come sia possibile configurare le interfacce dei router in Packet Tracer, in modo tale da suddividere la rete in sottoreti (subnet).

Esempio 3.1. Si consideri la semplice topologia mostrata in Figura 3.1, dove i cerchi posti attorno agli switch identificano le due sottoreti. Supponiamo che si richieda di configurare la topologia tramite subnetting della rete 192.168.20.100/25. In particolare, si richiede di ricavare le sottoreti sprecando il minor numero possibile di indirizzi IP, iniziando il subnetting allocando lo spazio per la rete con il maggior numero di interfacce e proseguendo fino alla sottorete più piccola, dando la precedenza, in caso di ambiguità, alle sottoreti i cui apparati hanno nome minore. La stessa politica dovrà poi essere adottata all’interno di ciascuna sottorete, configurando le interfacce in modo tale che all’apparato con nome minore sia associato un indirizzo IP minore (es. IP Router0 $<$ IP Router2).

Per dimensionare la subnet contenente i 5 router, ricordandosi che il primo e l’ultimo indirizzo IP all’interno di una sottorete sono riservati rispettivamente all’indirizzo di rete e a quello di broadcast, si ha bisogno almeno di 7 indirizzi IP. La più piccola sottorete sufficiente a ospitare 5 host è una /29, con subnet mask 255.255.255.248, host address range (range di indirizzi IP riservato agli host) pari a [192.168.20.97 – 192.168.20.102], indirizzo di rete (in gergo subnet ID) 192.168.20.96 e broadcast address 192.168.20.103. Tornerà utile calcolare anche la cosiddetta wildcard mask, ovvero la maschera di bit che indica quale parte dell’indirizzo IP esaminare in taluni contesti quali, in Packet Tracer, per indicare la dimensione della sottorete per alcuni protocolli di routing, come OSPF (trattati più avanti nelle Sezioni 4.1 e 4.2), oppure per indicare a quali indirizzi IP è

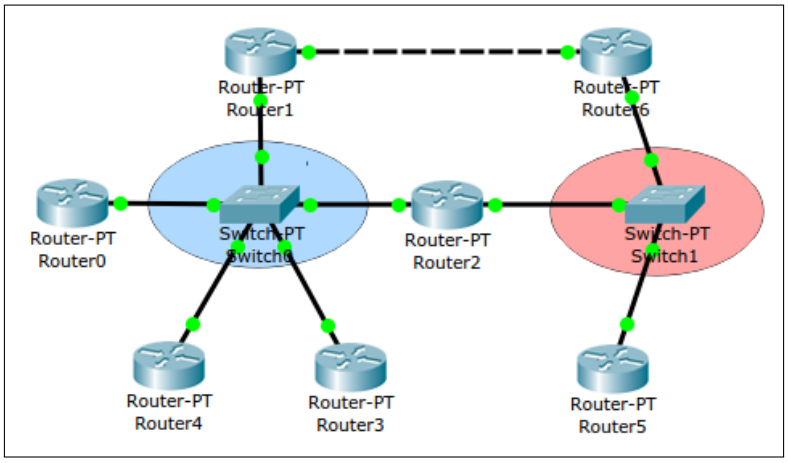

FIGURA 3.1: Un semplice esempio di subnetting (vedi Esempio 3.1).

consentito o meno l'accesso in una access control list (ACL) – vedi Sezione 7. Siccome in termini pratici, in maniera semplicistica, la wildcard mask altro non è se non una subnet mask invertita, nel caso in esame sarà pari a 0.0.0.7. In Packet Tracer è possibile configurare le interfacce direttamente tramite GUI: cliccando sul router che si vuole configurare, nella scheda Config, è sufficiente indicare, all'interno dei campi omonimi, indirizzo IP e subnet mask dell'interfaccia corrispondente. Ad esempio Router0 avrà indirizzo IP 192.168.20.97; Router4 192.168.20.101.

Passando alla seconda sottorete, essendo composta tra 3 router, si ha nuovamente bisogno di una /29, in cui l'host address range risulta pari a [192.168.20.105 – 192.168.20.110] e analogamente per gli altri parametri.

Rimane ora la sottorete che vede un collegamento punto-a-punto tra Router1 e Router6. In tal caso è sufficiente una /30, garantendo la connettività a esattamente 2 host. L'host address range sarà pari a [192.168.20.113 – 192.168.20.114], il network address 192.168.20.112, il broadcast address 192.168.20.115, la subnet mask 255.255.255.252 e la wildcard mask 0.0.0.3. △

Si noti che l'esempio di cui sopra, benchè corretto, non è al momento funzionante, visto che è necessario che ogni router comunichi agli altri router le sottoreti conosciute così da permettere, tramite algoritmi di routing, l'eventuale instradamento dei pacchetti in altre sottoreti.

3.1. Problema dell'allineamento

Un problema di non poco conto è quello dell'*allineamento*. Si consideri il seguente esempio.

Esempio 3.2. Supponiamo che si richieda di configurare una topologia tramite subnetting della rete 192.168.20.100/25 in due sottoreti: la prima (denominata s_1) che contenga 5 host, la seconda (s_2) che ne contenga 14. Supponiamo ora di partire dalla subnet più piccola, di classe /29, con host address range di nuovo pari a [192.168.20.97 – 192.168.20.102]. Per s_2 si ha bisogno di una /28, con subnet mask 255.255.255.240 e wildcard mask 0.0.0.15. Si potrebbe pensare di scegliere il range di indirizzi successivi adiacenti a s_1, che comportano un host address range pari a [192.168.20.104 – 192.168.20.117].

Il problema è che una tale configurazione non è corretta. Per comprenderne il motivo, consideriamo due host h_1 con indirizzo IP 192.168.20.104 e h_2 con indirizzo IP 192.168.20.117, inclusi nel range appena definito. In binario si ha:

IP address h_1:	`11000000 10101000 00010100 01101000`
IP address h_2:	`11000000 10101000 00010100 01110101`
subnet mask s_2:	`11111111 11111111 11111111 11110000`

Ricordando che se due host stanno nella stessa sottorete, allora le due stringhe binarie ottenute applicando l'operatore `AND` logico tra indirizzo IP e subnet mask devono coincidere, si osserva:

IP address h_1 & subnet mask s_2:	`11000000 10101000 00010100 01100000`
IP address h_2& subnet mask s_2:	`11000000 10101000 00010100 01110000`

In altri termini, i due host risultano assegnati a due subnet differenti. △

In termini più rigorosi, tutte le sottoreti devono essere allineate in modo tale che gli estremi siano potenze di 2; questo non solo specifica la dimensione della rete, ma anche l'allineamento dell'indirizzo di rete. In altre parole, una rete di dimensione 2^n (ovvero che contenga 2^n indirizzi) può iniziare solo a intervalli regolari multipli di 2^n; ovvero il primo indirizzo disponibile nell'host address range deve essere composto da tutti 0 negli ultimi n bit per qualsiasi sottorete. Esistono diverse strategie per evitare di incorrere nel problema dell'allineamento. L'euristica più semplice consiste nel gestire dapprima le reti più grandi, via via procedendo fino a trattare le reti più piccole.

Esercizio 3.1. Si configuri la topologia proposta nell'Esempio 3.2 adottando la strategia proposta, ovvero gestendo dapprima la rete più grande. Si ripetano tutti i passaggi mostrati nell'esempio, e ci si assicuri che il primo e l'ultimo indirizzo nell'host address range di entrambe le sottoreti non soffrano del problema dell'allineamento. △

Esercizio 3.2. Si implementino in Packet Tracer le soluzioni agli esercizi proposti nelle slide Subnetting (Prima parte) disponibili nella homesite. △

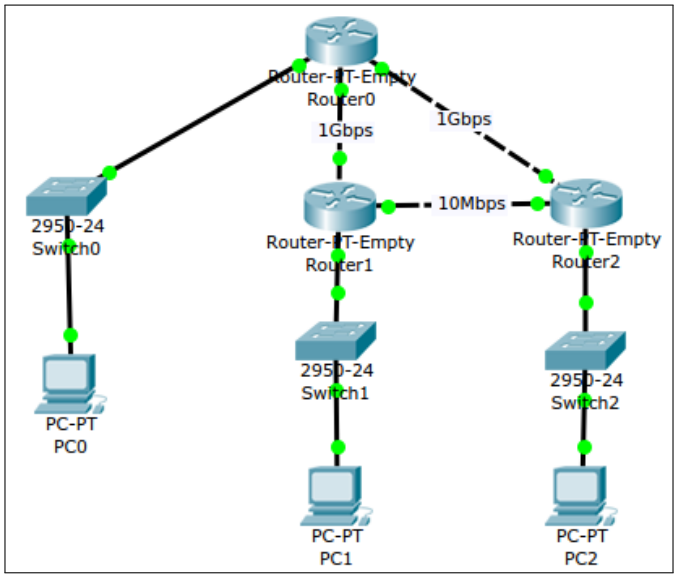

FIGURA 4.1: Algoritmi di routing (vedi Esempio 4.1).

4. ROUTING

In questa sezione ci si prefigge di configurare correttamente i router in modo tale da permettere a host appartenenti a sottoreti differenti di poter comunicare tra loro. Si parta da questo semplice esempio.

Esempio 4.1. Si consideri la topologia illustrata in Figura 4.1 (si faccia riferimento, a tal proposito, alla activity di Packet Tracer Topologia senza routing disponibile nella homesite). Si configurino i router in modo che le interfacce tra ogni coppia di router abbiano indirizzi appartenenti alla stessa sottorete. Nel caso di configurazione corretta, il ping tra router avrà esito positivo. Si operi ad esempio seguendo le indicazioni riportate in Tabella 4.1. Si configurino inoltre le interfacce che connettono i PC ai router, ad esempio fornendo indirizzo IP 192.168.1.2, 192.168.10.100 e 192.168.20.100 rispettivamente a PC0, PC1 e PC2, ricordandosi di configurare correttamente subnet mask e gateway, in modo tale che tutte le coppie di dispositivi adiacenti possano comunicare tra loro. Si noti come le tabelle di routing sui router siano vuote: in altre parole è necessario configurare i protocolli di routing su tali apparati affinchè sia possibile far comunicare tra loro anche host appartenenti a sottoreti differenti. △

Esistono due principali famiglie di algoritmi di routing:

– distance-vector (es. RIP): ogni router non ha conoscenza completa della topologia di rete, ma solo del proprio vicinato. Come metrica per valutare il percorso

Tabella 4.1: Configurazione delle interfacce dei router presenti in Figura 4.1.

apparato	interfaccia	indirizzo IP	subnet mask
Router0	GigabitEthernet0/0	192.168.1.1	255.255.255.252
	GigabitEthernet1/0	192.168.1.5	255.255.255.252
	GigabitEthernet2/0	192.168.1.9	255.255.255.252
Router1	GigabitEthernet0/0	192.168.1.6	255.255.255.252
	GigabitEthernet1/0	192.168.10.1	255.255.255.0
	Ethernet2/0	192.168.1.13	255.255.255.252
Router2	GigabitEthernet0/0	192.168.1.10	255.255.255.252
	GigabitEthernet1/0	192.168.20.1	255.255.255.0
	Ethernet2/0	192.168.1.14	255.255.255.252

migliore utilizza l'hop count, ovvero il numero di passi necessari per raggiungere la destinazione;

- Link-state (es. OSPF): richiede una conoscenza completa della rete. Utilizza altre metriche per valutare il percorso migliore, legate al costo della singola tratta, tipicamente inversamente proporzionale alla velocità della stessa.

4.1. RIP

Vediamo ora come sia possibile istruire i router per far sì che si scambino le informazioni sulle sottoreti conosciute, partendo dal protocollo RIP (si faccia riferimento, a tal proposito, alla activity di Packet Tracer Topologia RIP disponibile nella homesite). In modalità configurazione globale si digiti il comando `router rip` così che il prompt diventi `config-router#`. Utilizzando il tasto `?` otteniamo al solito un elenco dei possibili comandi disponibili in questa modalità: tra questi citiamo:

- `distance`: definisce la distanza amministrativa. Come già anticipato, se RIP usa il concetto di distanza, OSPF usa quello di peso: si tratta di due metriche differenti che non sono confrontabili. La distanza amministrativa serve appunto per confrontare due rotte che usano metriche differenti, ovvero in topologie che fanno uso di un mix di protocolli di routing differenti.
- `network`: premesso che il router deve rendere pubbliche le reti che conosce, il comando `network 192.168.1.0` permette di comunicare che il router conosce la rete 192.168.1.0. Si ottiene una configurazione completa di RIP ripetendo tale comando su ogni router per tutte le reti note. Da notare che per configurare RIP è sufficiente indicare il subnet address; manca in altre parole la subnet mask.

Tabella 4.2: Configurazione del protocollo RIP sui router presenti in Figura 4.1.

apparato	comando
Router0	`network 192.168.1.0`
	`network 192.168.1.4`
	`network 192.168.1.8`
Router1	`network 192.168.1.4`
	`network 192.168.10.0`
	`network 192.168.1.12`
Router2	`network 192.168.1.8`
	`network 192.168.20.0`
	`network 192.168.1.12`

Tale scelta deriva dal fatto che la versione 1 di RIP (default in Packet Tracer) è *classful*, ovvero non permette la suddivisione della rete in sottoreti, al contrario della versione 2 che dà la possibilità di suddividere la rete in sottoreti più piccole.

- `version`: permette di configurare quale versione di RIP si desidera utilizzare: la 1 (classful) o la 2 (classless inter-domain routing).
- `passive interface`: permette di indicare su quali interfacce non si vogliono inviare le varie notifiche. Ad esempio il comando

  ```
  passive interface GigabitEthernet0/0
  ```

  evita che le notifiche sulle reti conosciute siano inviate sull'interfaccia passata come argomento. Il vantaggio è la riduzione del traffico generato dagli algoritmi di routing in sottoreti che contengono solo host, per i quali tali notifiche non hanno alcun significato e vengono ignorate.

Esempio 4.2. Riprendendo la topologia configurata nell'Esempio 4.1, si configurino le reti note ai router presenti nella topologia, utilizzando i comandi presenti in Tabella 4.2. In Tabella 4.3 si riporta la routing table presente in Router1 e accessibile, in Packet Tracer, attraverso lo strumento lente di ingrandimento. Se inizialmente la tabella di routing non mostra alcuna nuova informazione, ad eccezione delle reti che sono state configurate con il comando `network`, una volta terminata la dichiarazione delle rotte che ogni router conosce, si può osservare come questa venga aggiornata con tutte le informazioni disponibili congiuntamente. In particolare, nella tabella: C → directly connected, R → RIP, O → OSPF. Nelle tabelle di routing viene indicata l'interfaccia per raggiungere una certa rete, il next hop IP, ovvero il gateway da percorrere per andare verso la rete indicata, e per finire la metrica (es. 110/11 è più distante di 110/2).

Si noti infine la possibile ridondanza nelle entry presenti in tabella (vedi 192.168.1.8/30): possono infatti essere presenti due reti ripetute che non sono però uguali, differendo nel percorso. In particolare, vengono ripetute solo le reti che condividono uno stesso numero di hop nella colonna Metric; in caso contrario viene scelta la rotta con il minor numero di hop. Si ricordi infine di configurare correttamente le passive interface. △

4.2. OSPF

Mostriamo ora come sia possibile configurare il protocollo OSPF (si faccia riferimento, a tal proposito, alla activity di Packet Tracer Topologia OSPF disponibile nella homesite). OSPF divide l'indirizzamento in aree, identificate come interi a 32 bit che per comodità possono essere espressi in dot notation. Il motivo di tale suddivisione è che all'interno di un dispositivo di rete possono girare più istanze di OSPF: una per ogni area. I comandi da seguire sono, nell'ordine, i seguenti:

1. `router ospf process_id`, dove `process_id` è l'identificativo numerico dell'istanza di OSPF (ad esempio 1). Il prompt passa in modalità config-router#.

2. `area area_id stub`, dove `area_id` è l'identificativo numerico dell'area (ad esempio 1), mentre `stub` è un tipo di area che non riceve notifiche/annunci da reti al di fuori dell'organizzazione.

3. `network IP_address wildcard_mask area area_id`. Come in RIP, il comando `network` permette di configurare le reti conosciute. Siccome però OSPF è classless, oltre a specificare il subnet address (`IP_address`) è necessario specificare la subnet fornendo la rispettiva wildcard mask (la negazione della subnet mask: ad esempio una /30 ha wildcard mask 0.0.0.3; una /24 0.0.0.255). Per finire, è necessario specificare l'area in cui l'istanza corrente di OSPF andrà ad operare, fornendone l'identificativo (`area_id`). Ad esempio, in riferimento alla Tabella 4.2, il comando

Tabella 4.3: Routing Table per Router1.

Type	Network	Port	Next Hop IP	Metric
R	192.168.1.0/30	GigabitEthernet0/0	192.168.1.5	120/1
C	192.168.1.4/30	GigabitEthernet0/0	– – –	0/0
R	192.168.1.8/30	GigabitEthernet0/0	192.168.1.5	120/1
R	192.168.1.8/30	Ethernet2/0	192.168.1.14	120/1
C	192.168.1.12/30	Ethernet2/0	– – –	0/0
C	192.168.10.0/24	GigabitEthernet1/0	– – –	0/0
R	192.168.20.0/24	Ethernet2/0	192.168.1.14	120/1

`network 192.168.1.0 0.0.0.3 area 1` permette di configurare una delle reti note per Router0.

Valgono le stesse regole viste in RIP per selezionare su quali interfacce non si vogliono inviare notifiche nell'istanza corrente del protocollo di routing (settando opportunamente le passive-interface).

Si ricordi infine che uno dei valori aggiunti nell'utilizzo di OSPF è che tiene traccia della capacità del link che connette due router e non si limita a considerare il numero di hop, come invece accade in RIP.

5. VLAN e Trunking802.1Q

Delle VLAN (Virtual LAN) si è ampiamente discusso durante le lezioni di teoria. Ci limitiamo qui a riproporne la definizione e alcuni fatti ovvi, così come descritti in Wikipedia e altre fonti sul web (`http://www.andreabeggi.net/2007/10/02/vlan-cosa-sono-e-perche-si-usano/`).

> In telecomunicazioni e informatica il termine VLAN (Virtual LAN) indica un insieme di tecnologie che permettono di segmentare il dominio di broadcast, che si crea in una rete locale (tipicamente IEEE 802.3) basata su switch, in più reti locali logicamente non comunicanti tra loro, ma che condividono globalmente la stessa infrastruttura fisica di rete locale.
>
> Le applicazioni di questa tecnologia sono tipicamente legate ad esigenze di separare il traffico di gruppi di lavoro o dipartimenti di una azienda, per applicare diverse politiche di sicurezza informatica.
>
> ...
>
> Una LAN virtuale, comunemente detta VLAN, è un gruppo di host che comunicano tra di loro come se fossero collegati allo stesso cablaggio, a prescindere dalla loro posizione fisica. una VLAN ha le stesse caratteristiche di una LAN fisica, ma consente di raggruppare le workstation come se fossero attestate sullo stesso segmento di rete. Invece di spostare gli host, la configurazione della rete si fa tramite strumenti software.
>
> ...
>
> Uno dei termini impiegati per definire una LAN, è "dominio di broadcast": un segmento della rete all'interno del quale diversi host di uno stesso subnet comunicano tra di loro senza dover "passare" da un router, appartenendo alla stessa VLAN.
>
> L'utilizzo delle VLAN porta diversi benefici, tra i quali:

- *Facilità di gestione delle infrastrutture di rete*: invece di spostare cavi, riposizionare uplink, aggiungere dispositivi e ricablare intere zone, si gestiscono le VLAN tramite strumenti software.
- *Ottimizzazione dell'uso delle infrastrutture*: se desidero isolare una subnet non devo aggiungere uno switch e/o un router, ma mi sarà sufficiente riassegnare alcune porte.
- *Forte scalabilità*: in pochi minuti si riassegna una porta e si sposta una patch, e le VLAN si possono estendere su diversi switch, rendendo semplice e relativamente economica l'espansione della rete.
- *Possibilità di estensione oltre i limiti fisici di un singolo switch*: oltre alla scalabilità, c'è il vantaggio di poter estendere una LAN su (ad esempio) piani diversi, utilizzando una unica dorsale di collegamento.
- *Economicità*: con un apparato di livello 3, si può fare routing tra le VLAN.
- *Diminuzione del traffico di rete*: tramite VLAN si confina facilmente il broadcast.

L'assegnazione di un host ad una VLAN può seguire diversi criteri, tra cui: MAC address, indirizzo IP e porta dello switch; la maggior parte degli switch moderni con un adeguato numero di porte sono in grado di gestire le VLAN.

Le VLAN riguardano il livello 2, mentre le subnet interessano il livello 3, ma molto spesso ad una VLAN corrisponde una sola sottorete, completando il metodo di assegnazione basato sulla porta dello switch, che è il modello sicuramente più diffuso.

Se lo switch gestisce il livello 3, le VLAN possono comunicare tra di loro tramite routing, senza dover introdurre un elevato numero di router sulla rete.

Facciamo un esempio pratico: su uno switch a 48 porte, si potrebbero assegnare le porte da 1 a 30 per la VLAN principale, con i client ed i server di dominio, da 31 a 35 una VLAN per le stampanti, su una subnet diversa e routing da e verso la LAN, sulle porte restanti si potrebbe attestare una VLAN completamente separata per ospitare una rete di test che non si vuole condividere con il resto delle attività. A questo punto è semplicissimo riassegnare le porte e/o gli host, semplicemente riconfigurando lo switch e spostando un cavo. Alcune porte potrebbero essere usate per isolare (con una blanda sicurezza) il traffico WiFi da quello cablato.

Le VLAN possono estendersi al di là dei limiti fisici dei singoli switch, tramite il VLAN tagging. Il protocollo 802.1Q, che regola le VLAN, prevede che ciascun frame ethernet venga "etichettato" con le informazioni relative alla VLAN di appartenenza. In questo modo, host lontani fisicamente possono appartenere alla stessa VLAN: è sufficiente che gli switch interessati al trasporto dei frame siano collegati tra di loro (tramite "trunk", un collegamento in grado di trasportare diverse VLAN) con porte opportunamente "taggate".

La gestione della VLAN, nei casi più semplici si effettua collegandosi con un browser all'indirizzo IP dello switch, oppure via seriale direttamente connessi alla porta console del dispositivo. △

Per una panoramica introduttiva al concetto di VLAN in Packet Tracer, si consideri la activity di Packet Tracer Simple VLAN disponibile nella homesite (vedi Figura 5.1). Gli step da seguire per poter definire più VLAN all'interno di una topologia di rete sono molto semplici. Si tratta di configurare gli switch in modo tale da aggiungere al database interno delle VLAN le reti virtuali di cui si vuole disporre. In sostanza, cliccando sulla scheda Config e successivamente VLAN Database, è possibile aggiungere, modificare o cancellare VLAN. Ognuna di queste prevede sia un identificativo simbolico (VLAN Name, ovvero un nome user-friendly) sia un identificativo numerico (VLAN Number, che sarà poi utilizzato per riferirsi alla VLAN all'interno dei dispositivi di rete). Nell'esempio in questione sono state aggiunte due VLAN: VLAN0002 con id 2 e VLAN0003 con id 3. Gli host connessi alla prima sono colorati in verde, alla seconda in blu. In effetti può essere utile considerare i pacchetti che transitano in una VLAN come se fossero opportunamente colorati del colore identificato dalla VLAN stessa.

Quello che ci chiediamo ora è come si possano far dialogare tra di loro gli host all'interno della stessa VLAN ma collegati a switch differenti. Una soluzione, improponibile nel

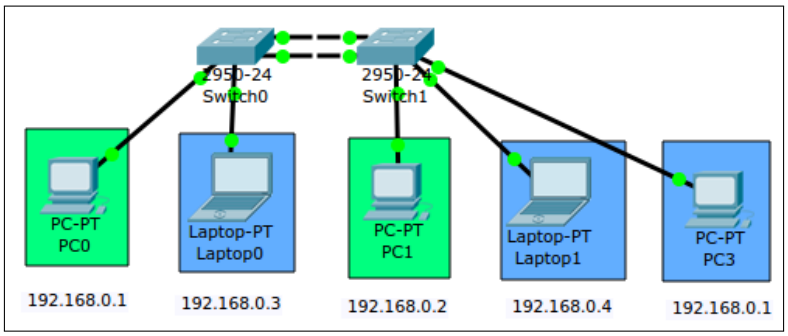

FIGURA 5.1: Topologia con 2 VLAN. Su entrambi gli switch le prime 12 porte sono assegnate alla VLAN 2, le ultime 12 alla VLAN 3. Il trasporto delle VLAN avviene tramite due cavi cross collegando porte Access nella stessa VLAN su entrambi gli switch. Le VLAN 2 e 3 non parlano tra di loro; per questo è possibile assegnare lo stesso indirizzo a PC0 e a PC3.

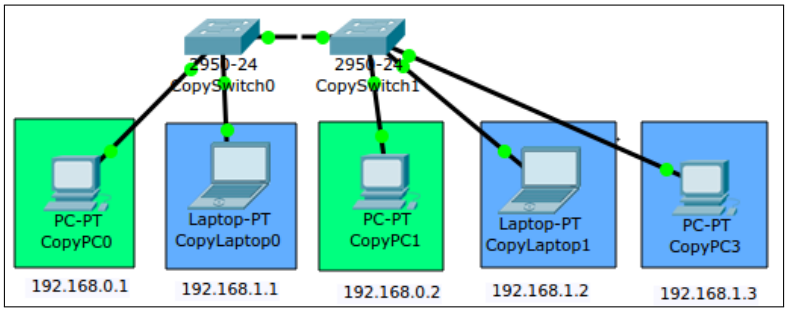

FIGURA 5.2: Topologia con 2 VLAN (stessa configurazione di Figura 5.1). Il trasporto delle VLAN avviene tramite porta Trunk configurata sulla porta 24 di entrambi gli switch.

caso si sia in presenza di un numero elevato di VLAN, è quella di aggiungere tanti cavi cross tra gli switch quante sono le VLAN attive, configurando all'interno dello switch ognuna delle interfacce a cui tali cavi sono collegate in modo che trasportino i pacchetti di una precisa VLAN (vedi Figura 5.1). In alternativa, è possibile utilizzare una piccola estensione di Ethernet, il protocollo 802-1Q (trunk VLAN), che permette con un solo cavo di risolvere il problema. Si usa dunque la modalità Trunk e si seleziona quel sottoinsieme di VLAN che si vuole trasportare sul cavo (vedi Figura 5.2). In sostanza l'interfaccia che collega gli switch deve essere configurata non più in modalità Access specificando a quale VLAN è consentito il transito dei pacchetti (vedi scheda Config nella sezione Interface), bensì in modalità Trunk, specificando il sottoinsieme di VLAN su cui i pacchetti possono transitare (vedi configurazione sulla parte destra nella activity di Packet Tracer).

Nella maggior parte delle situazioni reali, è però opportuno che host appartenenti a VLAN differenti possano dialogare tra loro. Affinchè ciò sia possibile è necessario introdurre un apparato di livello 3, ovvero un router, che fungerà da gateway per gli host appartenenti alle VLAN. Siccome host appartenenti a VLAN diverse necessitano di un gateway differente, tale router dovrebbe, in linea di principio, disporre almeno di tante interfacce quante sono le VLAN, comportando lo stesso problema di scalabilità osservato in precedenza. La soluzione consiste nel configurare il router così che possa trasportare 802-1Q: in tal caso sarà sufficiente una sola interfaccia per poter permettere a host appartenenti a VLAN differenti di poter comunicare tra loro, ognuno con un proprio gateway (diverso nelle varie VLAN).

Si consideri la topologia riportata in Figura 5.3 (si faccia riferimento, a tal proposito, alle activity di Packet Tracer Simple VLAN 2 e Sottointerfacce 802.1q e access list disponibili nella homesite). Si assegnino ai PC da 0 a 4 gli indirizzi IP da 192.168.0.1 a 192.168.0.4, con gateway 192.168.0.254 (in sostanza l'ultimo indirizzo IP disponibile è riservato al gateway, mentre i primi sono assegnati agli host). Analogamente si assegnino ai PC da 5 a 8 gli indirizzi IP da 192.168.1.1 a 192.168.1.4, con gateway 192.168.1.254. Per poter avvalersi del protocollo 802.1Q, gli switch devono essere configurati in modo tale

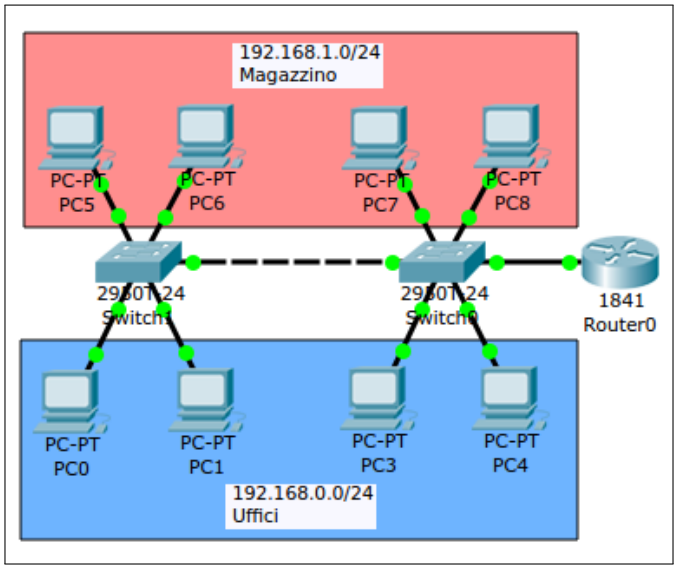

FIGURA 5.3: Topologia con 2 VLAN in cui tutti gli host possono comunicare tra loro.

da aggiungere due VLAN all'interno del proprio database (Uffici con id 20 e Magazzino con id 30). Le stesse interfacce che collegano host sulla VLAN Magazzino (risp. Uffici) devono essere configurate in modalità Access sulla VLAN 30 (risp. 20). L'interfaccia su cui è inserito il cavo cross che collega i due switch deve invece essere configurata in modalità Trunk, eventualmente specificando l'id delle due VLAN di cui si vuole permettere il transito dei pacchetti (di default il traffico è consentito a tutte le VLAN, sia quelle predefinite sia quelle user-defined). Rimane solo da configurare il router. A tal fine, si usa il concetto di sottointerfaccia (subinterface), una suddivisione logica e non fisica di una interfaccia. In modalità configurazione (enable → configure terminal), si digitano i comandi:

```
interface FastEthernet 0/0.20
encapsulation dot1Q 20
ip address 192.168.0.254 255.255.255.0
no shutdown

interface fastEthernet 0/0.30
encapsulation dot1Q 30
ip address 192.168.1.254 255.255.255.0
no shutdown
```

dove in sostanza nella prima riga viene creata la sottointerfaccia responsabile dei pacchetti delle singole VLAN (aggiungendo un punto ed un numero identificativo come suffisso al nome standard dell'interfaccia); nella seconda viene specificato l'uso del protocollo Trunking 802.1Q; nella terza viene indicato l'indirizzo IP e subnet mask dell'interfaccia (alias il gateway configurato sugli host appartenenti alla VLAN in questione); questa

operazione identifica la VLAN di cui la sottointerfaccia appartiene; si noti che si è utilizzato lo stesso ID numerico anche nel suffisso del nome della sottointerfaccia; non è un obbligo ma una *bestpractice*; per finire, nell'ultima riga viene abilitata a livello fisico l'interfaccia. Di tali istruzioni, l'unica che può essere compiuta direttamente tramite GUI è quest'ultima, cliccando sull'apposito checkbox Port Status nella scheda Config → FastEthernet0/0.

6. DHCP

Il servizio DHCP serve per configurare in maniera automatica indirizzo IP, subnet mask e gateway negli host appartenenti a una certa sottorete. Ovviamente non è necessario avere un server DHCP per ogni sottorete, purchè si specifichino correttamente i serverPool, ovvero strutture dati definite all'interno del server DHCP che specificano come gestire gli host appartenenti a una certa sottorete.

Esempio 6.1. Si consideri la topologia riportata in Figura 6.1. In particolare sono definite due VLAN: First (abbreviazione di First Floor) con id 200 e Second (abbreviazione di Second Floor) con id 400; l'interfaccia GigabitEthernet0/0 di Router0 è inoltre configurata in modo tale da permettere agli host appartenenti alle due VLAN di poter comunicare tra loro in modalità trunk (si faccia riferimento alla Sezione 5). Se 192.168.1.30 è l'indirizzo del gateway nella subnet First Floor e 192.168.1.14 quello del gateway nella subnet Second Floor, Router0 viene dunque configurato con i seguenti comandi:

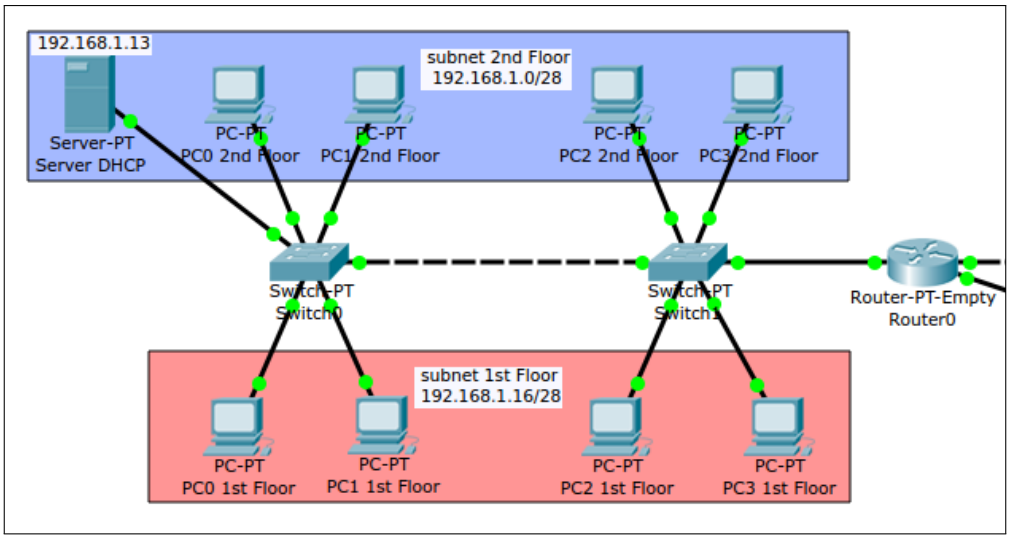

FIGURA 6.1: Topologia con 2 VLAN e servizio DHCP.

```
interface GigabitEthernet0/0.400
encapsulation dot1Q 400
ip address 192.168.1.14 255.255.255.240

interface GigabitEthernet0/0.200
encapsulation dot1Q 200
ip address 192.168.1.30 255.255.255.240
ip helper-address 192.168.1.13
```

Si noti che in una delle due sottoreti non è presente un server DHCP; conseguentemente una richiesta DHCP inviata in broadcast sarà confinata all'interno del broadcast domain; l'ultima istruzione è necessaria per specificare l'indirizzo IP del server DHCP che configurerà gli host della sottorete. In sostanza viene istruito il router per inoltrare una richiesta DHCP in broadcast all'indirizzo IP specificato. In generale, tale istruzione va specificata per ogni interfaccia la cui subnet non contiene il server DHCP ma in cui gli host si avvalgono di tale servizio di configurazione automatica.

Per poter attivare il servizio DHCP, nella scheda Services → DHCP del server deputato a erogare detto servizio è necessario attivare il checkbox Service. Inoltre, per ogni subnet che contiene host gestiti dal server DHCP, ad eccezione di quella in cui il server è inserito (per cui esiste già un serverPool di default), si dovrà creare un nuovo serverPool specificando il nome del pool (Pool Name), il gateway di default (Default Gateway, il primo indirizzo IP disponibile che può essere assegnato agli host (Start IP Address), la subnet mask (Subnet Mask) e per finire il numero massimo di host che possono avvalersi del servizio (Maximum number of Users). La Figura 6.2 mostra un esempio di configurazione compatibile con lo scenario in esame (si noti che alcuni parametri, quali Start IP Address e Maximum number of Users sono settati in modo da rispettare specifiche di progetto non riportate nell'esempio). Per finire, in talune situazioni (come nel caso corrente), si ricorda che può essere necessario modificare la configurazione del serverPool di default.

Si ricorda infine che per tutti gli host che si avvalgono del servizio DHCP si dovrà attivare il checkbox DHCP nella scheda Config. △

7. Access Control List (ACL)

Le Access Control List (ACL) sono usate per filtrare (permettere o negare selettivamente) traffico di rete su apparati di livello 3 (router), controllando se i pacchetti possono essere inoltrati o se devono essere bloccati in ingresso a o in uscita da una determinata interfaccia. Il router esamina dunque ogni pacchetto per determinare se inoltrarlo o bloccarlo sulla base dei criteri specificati nella ACL applicata all'interfaccia per qui questi transitano. Nel seguito si fornirà solo una breve panoramica delle ACL; si consiglia al lettore di riferirsi a materiale disponibile sul web per ulteriori approfondimenti.

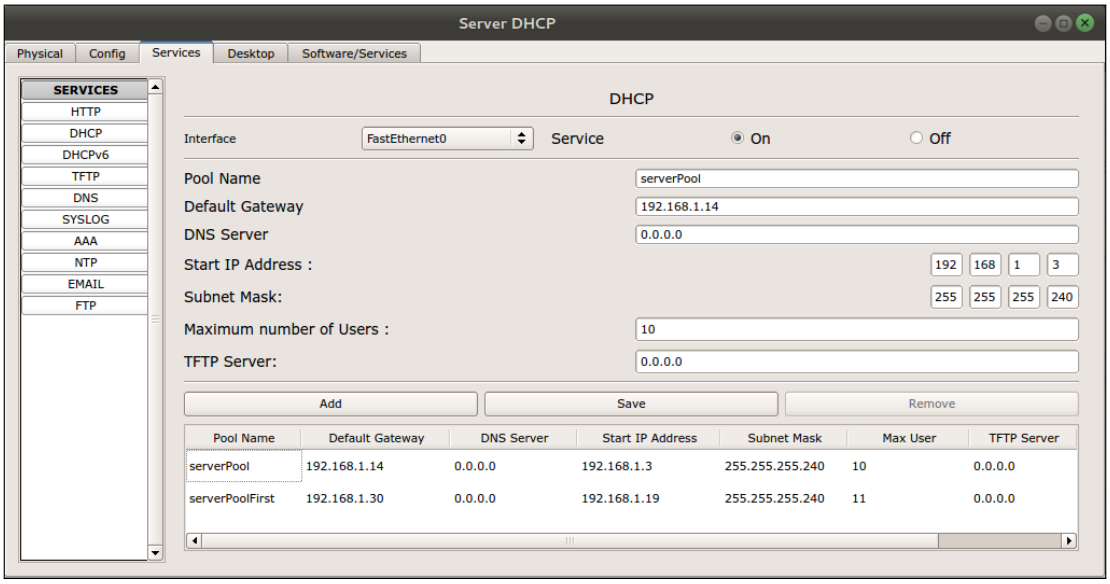

FIGURA 6.2: Esempio di configurazione dei serverPool.

Esistono due tipi differenti di ACL:

1. *ACL standard*. Si tratta del primo tipo di ACL definito in Packet Tracer (attualmente deprecato). Il traffico può essere filtrato solo sulla base dell'indirizzo IP sorgente dei pacchetti IP. Il numero identificativo di tali ACL deve essere compreso tra 1 e 99 o tra 1300 e 1999.

2. *ACL extended*. Si tratta di ACL più complesse che permettono il filtraggio del traffico IP sulla base di una combinazione di diversi criteri: indirizzo IP sorgente, indirizzo IP destinazione, porte TCP o UDP, protocollo, ... Il numero identificativo di tali ACL deve essere compreso tra 100 e 199 o tra 2000 e 2699.

Essendo più flessibili e potenti, nel seguito si farà riferimento esplicito alle sole ACL extended[1]. I passi di base per configurare una ACL sono due:

1. tramite il comando `access-list` (accessibile in modalità configurazione globale) viene creata una nuova entry in una ACL e ne vengono definite le politiche (criteri di selezione dei pacchetti e decisione da intraprendere: permettere o negare);

2. tramite il comando `ip access-group` (accessibile in modalità configurazione interfaccia) viene applicata una ACL esistente sulla relativa interfaccia.

Per quanto riguarda la prima fase, si riporta di seguito la sintassi del comando `access-list`:

[1]Nel seguito per riferirsi alle ACL extended si utilizzerà semplicemente l'acronimo ACL.

```
access-list access-list-number permit | deny protocol source
source-wildcard [operator port] destination destination-wildcard
[operator port] [established] [log]
```

una cui sommaria descrizione dei parametri è fornita in Tabella 7.1.

Comando / Parametri	Descrizione
`access-list`	Comando principale
`access-list-number`	Identifica la lista usando un numero compreso tra 100 e 199 o tra 2000 e 2699
`permit | deny`	Indica se questa entry permette o blocca l'indirizzo specificato; essendo le ACL first match, è sempre più opportuno premettere i `permit` ai vari `deny`
`protocol`	IP, TCP, UDP, ICMP, GRE o IGRP
`source and destination`	Identifica indirizzi IP sorgente e destinazione
`source-wildcard and destination-wildcard`	L'operatore può essere `lt` (less than), `gt` (greater than), `eq` (equal to) o `neq` (not equal to). Il numero di porta può riferirsi o alla porta sorgente o alla porta destinazione, in funzione del punto in cui il parametro `port number` è configurato nella ACL. In alternativa al numero di porta, è possibile utilizzare il nome del protocollo di riferimento, come Telnet, FTP, SMTP, ...
`established`	Solo per inbound TCP connection. Permette al traffico TCP di passare se il pacchetto è una risposta alla outbound-initiated TCP session. Questo tipo di traffico ha il bit ACK settato
`log`	Invia un messaggio di log alla console

TABELLA 7.1: Comando `access-list` usato per definire una ACL e descrizione sommaria dei suoi argomenti.

In sostanza dopo essere entrati in modalità configurazione (config router → config terminal), digitando il comando `access-list id`, con `id` numero compreso tra 100 e 199, è possibile: aggiungere commenti (`remark`), permettere (`permit`) o negare (`deny`) il transito di pacchetti. Fa seguito l'identificativo del protocollo che deve essere filtrato (TCP, UDP, ICMP, ..., oppure IP per riferirsi ad ogni protocollo Internet). Segue un descrittore degli host sorgenti da monitorare: any (qualsiasi host sorgente), oppure host (un singolo host), o ancora fornendo direttamente l'indirizzo di rete e wild-card mask di una intera sottorete.

Esempio 7.1. Consideriamo la topologia in Figura 7.1 (si faccia riferimento, a tal proposito, alla activity di Packet Tracer Sottointerfacce 802.1q e access list disponibile nella homesite). Supponiamo che a Server-PT sia assegnato l'indirizzo IP 192.168.200.200 e supponiamo di voler permettere l'accesso al server web ma non ICMP. I comandi da digitare sono:

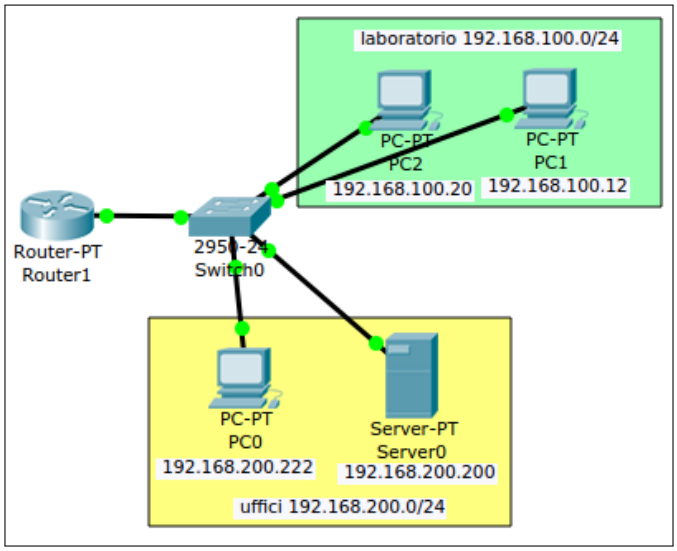

FIGURA 7.1: Topologia con 2 VLAN per introdurre il concetto di ACL.

```
access-list 110 permit TCP any host 192.168.200.200 eq 80
access-list 110 deny ICMP any any
```

dove il primo consente di far passare traffico TCP proveniente da any diretto all'host 192.168.200.200 sulla porta 80; il secondo vieta ICMP (ping) da qualunque sorgente a qualunque destinazione.

Per quanto riguarda invece la seconda fase, ovvero l'attivazione di una ACL su una specifica interfaccia, è necessario specificare a quale interfaccia si vuole che venga applicata. Nel caso in esame o la si applica all'interfaccia che contiene l'host 192.168.200.200 o all'altra. Sebbene per quanto concerne la configurazione del router i due approcci sono interscambiabili, a livello operativo bisogna prestare attenzione ad aspetti funzionali. In altre parole, se si applicasse la ACL all'altra interfaccia e in futuro dovessero essere aggiunte nuove VLAN, queste non si troverebbero applicata la regola; è di indubbio vantaggio dunque l'applicazione della ACL alla interfaccia che contiene l'host 192.168.200.200. I comandi per ottenere questo risultato sono:

```
interface fastEthernet 0/0.100
ip access-group 110 out
```

Una possibile fonte di confusione è la scelta del parametro `in` o `out` nell'ultima istruzione, ovvero nell'applicazione del filtro ai pacchetti che entrano o che escono dall'interfaccia. In sostanza cambia la direzione in cui il traffico viene filtrato: siccome nel caso in esame si sta filtrando il traffico diretto verso la rete che contiene l'host 192.168.200.200, la scelta corretta è `out`, visto che si vuole filtrare il traffico che esce dall'interfaccia e va verso

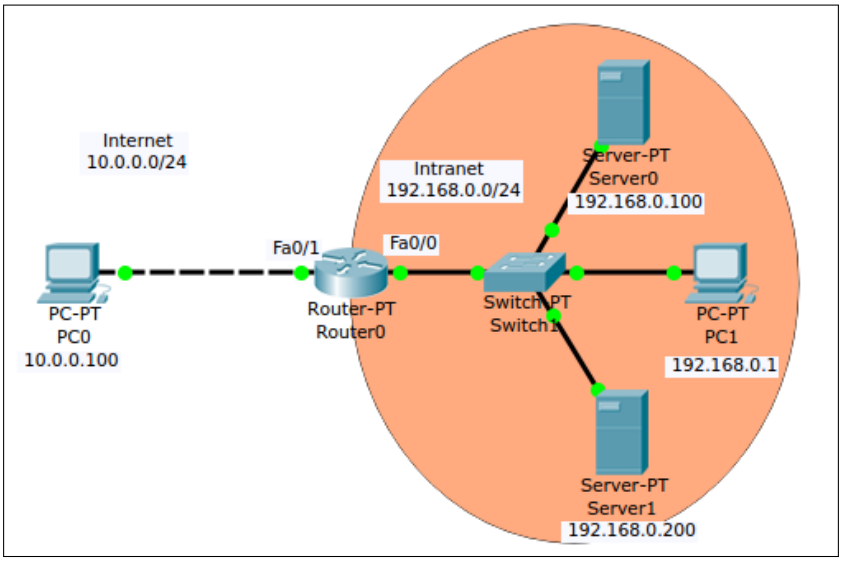

FIGURA 7.2: Topologia con accesso limitato alla Intranet (vedi Esempio 7.2). Si noti il cavo cross tra PC0 e Router0, obbligatorio nei vecchi router in mancanza di uno switch intermedio.

la rete che contiene l'host. Attenzione, dunque, alla prospettiva con cui considerare la direzione in entrata o in uscita del traffico: prospettiva che è quella del router su cui il filtro viene attivato. In altre parole, è necessario mettersi nei panni del router: il traffico da filtrare è sì in ingresso alla rete che contiene l'host, ma per il router è diretto alla rete che contiene l'host e dunque è in uscita. △

Esempio 7.2. Si consideri ora la topologia illustrata in Figura 7.2. Si supponga che la Intranet aziendale disponga di due siti web: uno accessibile a tutto il mondo (Server1), l'altro riservato ad uso interno privato (Server0). Si supponga inoltre che nessun host esterno all'azienda abbia accesso alla Intranet. Il router dispone di due interfacce: FastEthernet 0/0 (interna) con indirizzo IP 192.168.0.254 e FastEthernet 0/1 (esterna) con indirizzo IP 10.0.0.254.

La prima fase consta nella definizione del filtro. Anzitutto la scelta ricade in una ACL extended, dovendo filtrare solo il traffico web e non solo sull'indirizzo IP sorgente.

```
ip access-list extended 100
permit TCP any host 192.168.0.200 eq www
deny IP any any
```

In sostanza, nella ACL nr. 100 si permette il traffico TCP diretto da qualunque sorgente all'host 192.168.0.200 sulla porta 80. L'ultima istruzione serve per vietare l'accesso di tutto il traffico Internet: adottando le ACL una politica first match, lasciando in ultima posizione il comando `deny` non si rischia di bloccare il traffico TCP diretto a Server1.

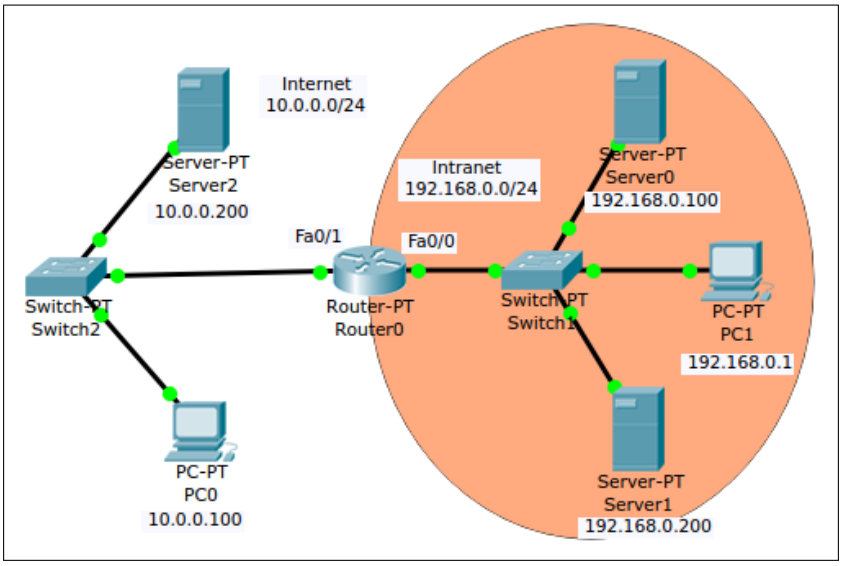

FIGURA 7.3: Topologia con accesso limitato alla Intranet (vedi Esempio 7.2). Si noti il cavo cross tra PC0 e Router0, obbligatorio nei vecchi router in mancanza di uno switch intermedio.

La seconda fase consiste nell'applicazione della ACL alla giusta interfaccia. È necessario anzitutto entrare in modalità configure interface per poi attivare l'ACL:

```
interface FastEthernet 0/1
ip access-group 100 in
```

Si noti come sia possibile impartire questi comandi anche all'interfaccia interna. In tal caso la modalità di accesso non sarebbe `in`, ma `out`, per i motivi spiegati in precedenza. △

Esempio 7.3. Si consideri infine la topologia rappresentata in Figura 7.3 che rappresenta una variante dello scenario adottato nell'esempio precedente. Si noti anzitutto come Server2 non sia in grado di pingare Router0, visto che la ACL definita nell'Esempio 7.2 è applicata alla interfaccia esterna. Se Server2 si connettesse a Server1 (il server aziendale pubblico), non sarebbe in grado di visionare la pagina web, visto che i pacchetti di ritorno non riescono a uscire da Router0 quando la porta sorgente è la 80, come quella su cui è in ascolto Server2. Per risolvere il problema entra in gioco TCP e, in particolare, il three-way-handshake. In sostanza, volendo permettere a tutto il traffico generato nella Intranet di uscire, senza specificare nel dettaglio tutte le porte, è sufficiente osservare che questo genere di pacchetti ha il campo ack del three-way-handshake settato a 1. Operativamente, in aggiunta al filtro già applicato, va inserito il comando:

```
access-list 100 permit TCP any any established
```

dove `established` significa appunto "pacchetti con ack pari a 1" ovvero a connessione TCP stabilita. △

8. Network Address Translation (NAT)

Sebbene svariati siano i compiti del NAT (si faccia riferimento alle lezioni di teoria), in queste dispense ci si limiterà a nascondere gli indirizzi interni quando alcuni pacchetti escono dalla Intranet. Si usi a tal fine la stessa topologia illustrata in Figura 7.3, togliendo le ACL correntemente attive (è sufficiente a tal fine togliere ip access-group nell'interfaccia, con il comando `no IP access-group`).

Nella configurazione dell'interfaccia interna (FastEthernet 0/0) si digita:

```
ip nat inside
```

mentre in quella esterna (FastEthernet 0/1):

```
ip nat outside
```

A questo punto, tornando in modalità configurazione, digitando il comando `ip nat inside source ?` si osservano due possibili argomenti:

- `static`: richiede una corrispondenza (indirizzo interno – indirizzo esterno);
- `list`: richiede una ACL che specifichi quali indirizzi siano idonei ad essere tradotti.

Si dovrà dunque creare una ACL che permetta a tutti gli indirizzi coinvolti di essere tradotti (la ACL non deve essere applicata):

```
access-list 110 permit IP any any
```

Tornando al NAT:

```
ip nat inside source list 110 ?
```

si passa alla politica di traduzione, che può essere:

- `pool`: un pool di indirizzi tra cui scegliere un indirizzo pubblico per la traduzione dell'indirizzo privato;
- `interface`: l'indirizzo IP dell'interfaccia in questione.

Il comando completo:

```
ip nat inside source list 110 interface fastEthernet 0/1
```

si legge: "quando si fa NAT degli indirizzi interni si usi come criterio degli indirizzi da tradurre quello indicato nella ACL 110 e si traducano gli indirizzi usando l'indirizzo IP dell'interfaccia FastEthernet 0/1".

Esistono altre modalità di utilizzo del NAT; ad esempio si potrebbero avere nella Intranet diversi server web con indirizzi privati che si vuole rendere pubblici. Sul router si dovrebbe definire un mapping statico tra porta e indirizzo privato. Tali argomentazioni esulano dagli obiettivi del corso.

Appendice A. Breve introduzione alla CLI

Così come per il resto di questa dispensa, le informazioni riportate in questa appendice hanno carattere parziale e servono esclusivamente ad introdurre lo studente nell'uso della Command Line Interface (CLI) dei router. Le stesse slide consigliate nella parte introduttiva coprono parte degli argomenti trattati e forniscono le informazioni essenziali per poter interagire con la CLI.

Se la CLI (accessibile dall'omonima scheda del dispositivo) copre tutte le funzionalità fornite dalla GUI, non è vero l'opposto; in altre parole alcune funzioni e strumenti del dispositivo sono configurabili solo tramite CLI. Nondimento è utile visionare come i comandi effettuati tramite GUI siano tradotti automaticamente nel linguaggio della CLI.

Nonostante sia opportuno conoscere alcuni comandi basilari, due funzionalità della CLI permettono anche a utenti meno esperti di interagire con lo strumento senza eccessiva difficoltà:

- tasto `?`: mostra una lista dei possibili comandi disponibili (e annessa descrizione) in un certo contesto operativo; inoltre, all'interno di un comando, mostra un elenco dei parametri disponibili per poterlo correttamente completare;
- tasto `tab`: permette di completare un comando immettendone i primi caratteri che lo compongono, purchè questi lo specifichino univocamente;
- uso di forme abbreviate: è possibile utilizzare un comando immettendone solo i primi caratteri; se la stringa immessa è lunga a sufficienza da evitare confusione con altri comandi, allora questo viene eseguito come fosse stato digitato nella sua interezza. Ad esempio `en` può sostituire `enable`, così come `config t` il comando `configure terminal`;
- stringa `no` *command*: serve per negare il comando attivo *command*.

Diverse sono le modalità di accesso ai comandi della CLI. Nel caso si digiti un comando non ammesso all'interno di una certa modalità, è possibile che venga sollevato un messaggio di errore. Le principali modalità sono elencate in Tabella A.1. Sebbene la modalità utente sia quella a cui si accede di default, i comandi utili agli scopi del corso in questa modalità sono limitati. È possibile accedere alla modalità privilegiata attraverso il comando `enable`. Da qui con il comando `show running-config` (risp. `show startup-config`) è possibile visualizzare la configurazione attuale (risp. iniziale, di default vuota) del router; con il comando `write` (abbreviazione di `write memory`) si provvede al salvataggio della configurazione attuale del router, cosicchè alla riaccensione del dispositivo ne venga ripristinato lo stato corretto (di default una volta che il router viene spento, perde tutte le configurazioni); per finire, con il comando `configure terminal` si passa nella modalità di configurazione globale.

Tra i comandi più semplici in modalità configurazione globale, ricordiamo:

Tabella Appendice A.1: Elenco delle principali modalità di accesso alla CLI.

Prompt	Descrizione
`Router>`	User mode
`Router#`	Privileged mode (o EXEC-level mode)
`Router(config)#`	Global configuration mode
`Router(config-if)#`	Interface mode
`Router(config-subif)#`	Subinterface mode
`Router(config-line)#`	Line mode
`Router(config-router)#`	Router configuration mode

- `hostname RouterCisco`: assegna al Router il nome passato come argomento (RouterCisco nel caso in esame);
- `enable password cisco`: assegna una password per accedere alla modalità di configurazione;
- `exit`: esce dalla modalità di configurazione attuale, ritornando alla precedente.

È possibile mostrare un elenco delle interfacce presenti sull'apparato e dei relativi parametri di funzionamento attraverso il comando `show interfaces`. Si ricorda che una interfaccia viene identificata da 3 parti: i) parte alfabetica → tecnologia (es. fastEthernet); ii) primo numero → slot in cui è inserita; e iii) secondo numero → posizione all'interno dello slot; questi ultimi sono separati dal carattere / (es. fastEthernet 0/0). Per configurare una interfaccia, ad esempio fastEthernet 0/0, è sufficiente digitare il comando `interface fastEthernet 0/0`: il prompt mostrerà la nuova modalità a cui si è acceduti (modalità interfaccia). In questa modalità è possibile, ad esempio:

- `ip address`: assegnare all'interfaccia l'indirizzo IP via DHCP o direttamente fornendone l'ottetto (es. `ip address 192.168.1.0 255.255.255.252`);
- `no shutdown`: cambiare stato alla scheda ponendolo su up;
- `exit`: uscire dalla modalità di configurazione attuale, ritornando alla precedente.

Esistono tantissimi altri comandi: i più importanti saranno discussi nelle sezioni di competenza.