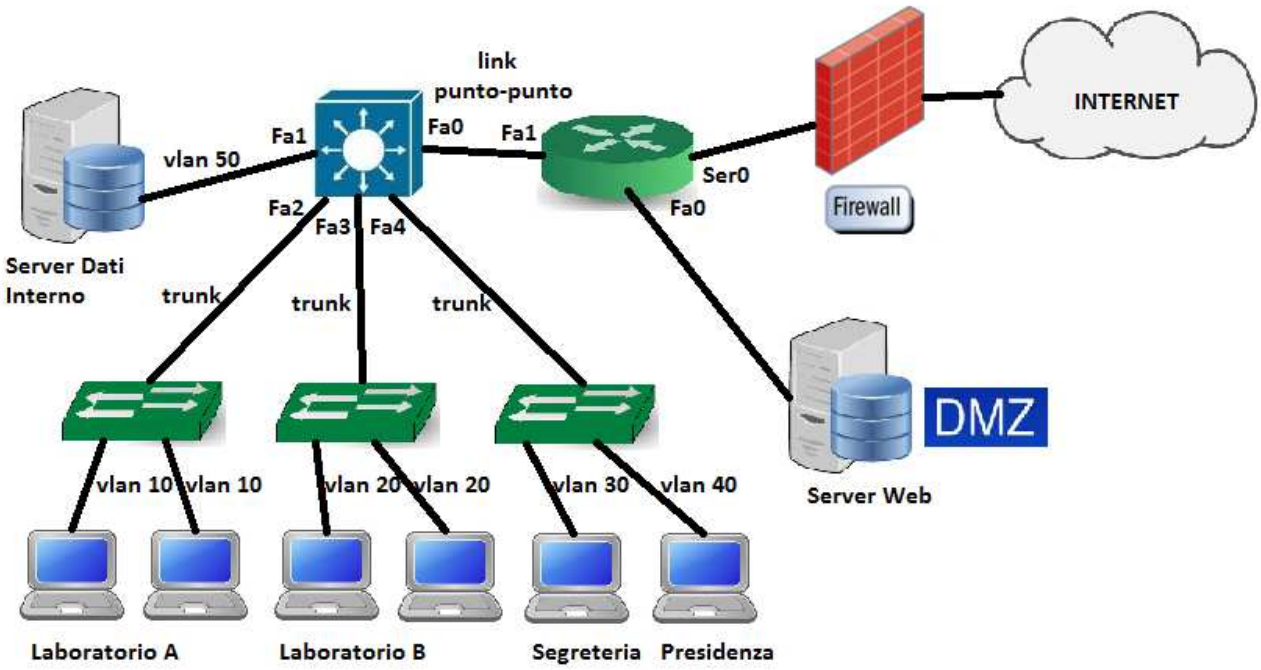
# Esempio di rete aziendale

Autore: Roberto Bandiera – febbraio 2015

Per esemplificare la tipica architettura di una rete aziendale consideriamo la rete di un Istituto scolastico, dove ci sono alcuni laboratori didattici di pc, gli uffici della segreteria e la presidenza, un server per i dati ad uso interno e un server per pubblicare il sito web dell'Istituto e renderlo accessibile in Internet.

Lo schema logico dei componenti attivi della rete è il seguente:




La struttura gerarchica della rete prevede al vertice uno Switch Multilayer Cisco che distribuisce la connettività ai 3 switch che interconnettono i diversi pc dei laboratori e degli uffici.

Per l'accesso a Internet c'è un link punto punto con un Router/Firewall che è connesso ad un Internet Service Provider. E' compito di tale Router/Firewall anche la realizzazione della "rete demilitarizzata" (DMZ) che ospita il server web.

Per strutturare in modo adeguato i diversi ambiti operativi, vengono definite 5 VLAN: una per ciascun laboratorio, una per gli uffici della segreteria, una per la presidenza e una per il server dati interno.

Lo schema di indirizzamento dei dispositivi di rete è riassunto nella seguente tabella:

| Rete | VLAN | Indirizzo IP della rete | Default gateway |
|---|---|---|---|
| Laboratorio A | 10 | 192.168.10.0/24 | 192.168.10.1 |
| Laboratorio B | 20 | 192.168.20.0/24 | 192.168.20.1 |
| Segreteria | 30 | 192.168.30.0/24 | 192.168.30.1 |
| Presidenza | 40 | 192.168.40.0/24 | 192.168.40.1 |
| Server Dati | 50 | 192.168.50.0/24 | 192.168.50.1 |
| Link punto-punto | -- | 192.168.60.0/24 | -- |
| DMZ | -- | 192.168.70.0/24 | 192.168.70.1 |

L'Internet Service Provider fornisce alla scuola un pacchetto 6 di indirizzi IP pubblici: 212.120.80.80/29.

In questo modo all'interfaccia Ser0 del Router si assegna l'indirizzo 212.120.80.82 e al server web l'indirizzo 212.120.80.83 grazie alla funzione di NAT STATICO realizzata dal Router/Firewall stesso.

Restano a disposizione per eventuali ulteriori macchine gli indirizzi 212.120.80.84, …85, …86 (l'indirizzo 212.120.80.81 è associato all'interfaccia del Router del Provider).

## Configurazione degli switch

Gli switch di livello 2 sono configurati dichiarando l'esistenza delle VLAN ad esso collegate e associando alle stesse le porte a cui si connettono i pc. Invece il link verso lo Switch Multilayer si configura come "trunk".

A titolo esemplificativo si riportano i comandi per la configurazione dello Switch del Laboratorio A, nell'ipotesi che si usi la porta Fa0 per il trunk:

```
S(config)# vlan 10
S(config-vlan)# exit
S(config)# interface range Fa1-20
S(config-if)# switchport mode access
S(config-if)# switchport access vlan 10
S(config-if)# exit
S(config)# interface Fa0
S(config-if)# switchport mode trunk
S(config-if)# exit
```

Per quanto riguarda, invece, lo Switch Multilayer, dopo averne abilitato le funzionalità di routing (con il comando *ip routing*), si dichiarano tutte le VLAN della rete, si configurano come porta di accesso quella della VLAN 50 a cui appartiene il server dati interno e come trunk i collegamenti verso gli altri 3 switch:

```
S# configure terminal
S(config)# ip routing
S(config)# vlan 10
S(config-vlan)# vlan 20
S(config-vlan)# vlan 30
S(config-vlan)# vlan 40
S(config-vlan)# vlan 50
S(config-vlan)# exit

S(config)# interface Fa1
S(config-if)# switchport mode access
S(config-if)# switchport access vlan 50
S(config-if)# exit

S(config-if)# interface Fa2
S(config-if)# switchport trunk encapsulation dot1q
S(config-if)# switchport mode trunk
```

```
S(config-if)# exit

S(config)# interface Fa3
S(config-if)# switchport trunk encapsulation dot1q
S(config-if)# switchport mode trunk
S(config-if)# exit

S(config)# interface Fa4
S(config-if)# switchport trunk encapsulation dot1q
S(config-if)# switchport mode trunk
S(config-if)# exit
```

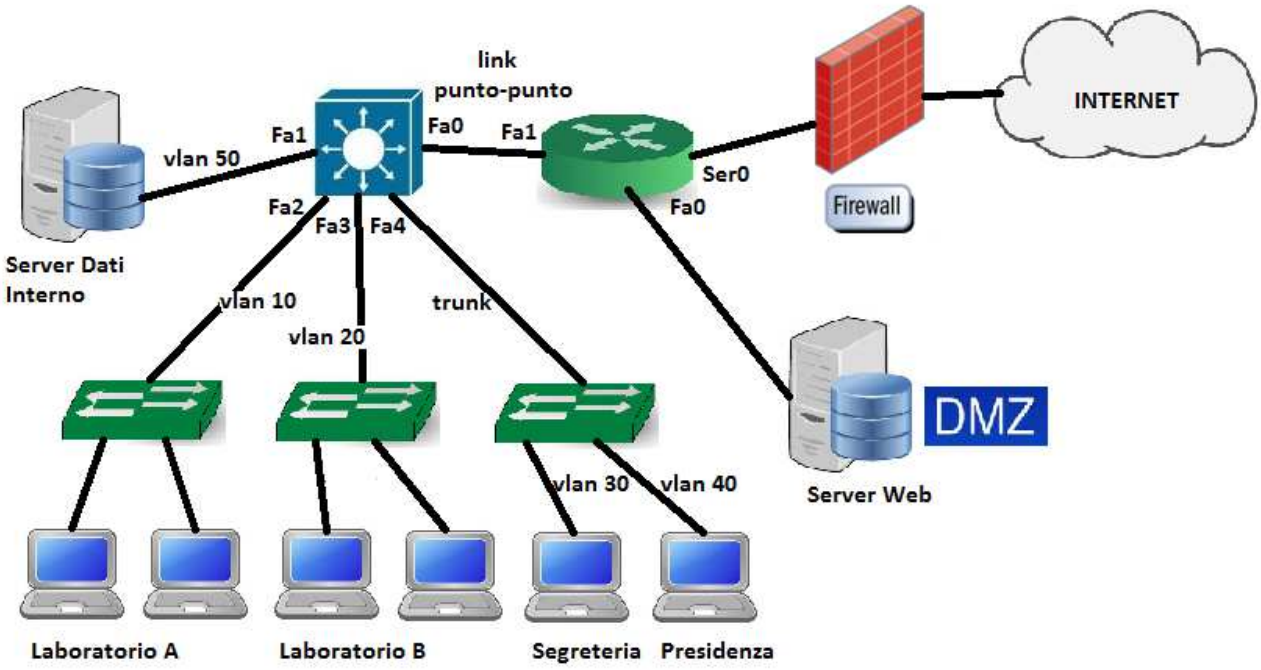
Per consentire il routing tra le diverse VLAN si devono configurare le cosiddette Switch Virtual Interface (SVI), assegnandovi gli opportuni indirizzi IP. Le SVI sono semplicemente le interfacce virtuali associate alle singole VLAN. Si ricorda che queste interfacce virtuali costituiscono il default gateway per i pc delle diverse VLAN.

```
S(config)# interface vlan 10
S(config-if)# ip address 192.168.10.1 255.255.255.0
S(config-if)# no shutdown

S(config)# interface vlan 20
S(config-if)# ip address 192.168.20.1 255.255.255.0
S(config-if)# no shutdown

S(config)# interface vlan 30
S(config-if)# ip address 192.168.30.1 255.255.255.0
S(config-if)# no shutdown

S(config)# interface vlan 40
S(config-if)# ip address 192.168.40.1 255.255.255.0
S(config-if)# no shutdown

S(config)# interface vlan 50
S(config-if)# ip address 192.168.50.1 255.255.255.0
S(config-if)# no shutdown
```

## Configurazione semplificata degli switch

La suddetta configurazione della rete può essere semplificata osservando che ciascuno degli Switch dei laboratori deve gestire una singola VLAN e quindi si possono utilizzare anche Switch semplici, senza bisogno di configurare negli stessi alcuna VLAN.

Le porte dello Switch Multilayer a cui vengono connessi gli switch dei laboratori vengono pertanto configurate in modalità “mode access” specificando il numero della VLAN corrispondente.




Soltanto lo Switch degli uffici amministrativi necessità di essere configurato per gestire le due diverse VLAN per la Segreteria e la Presidenza.

La configurazione dello Switch Multilayer è la seguente:

```
S# configure terminal
S(config)# ip routing
S(config)# vlan 10
S(config-vlan)# vlan 20
S(config-vlan)# vlan 30
S(config-vlan)# vlan 40
S(config-vlan)# vlan 50
S(config-vlan)# exit


S(config)# interface Fa1
S(config-if)# switchport mode access
S(config-if)# switchport access vlan 50
S(config-if)# exit
```

```
S(config-if)# interface Fa2
S(config-if)# switchport mode access
S(config-if)# switchport access vlan 10
S(config-if)# exit

S(config-if)# interface Fa3
S(config-if)# switchport mode access
S(config-if)# switchport access vlan 20
S(config-if)# exit

S(config)# interface Fa4
S(config-if)#  switchport trunk encapsulation dot1q
S(config-if)# switchport mode trunk
S(config-if)# exit
```

La configurazione delle SVI è la stessa del caso precedente e consente il routing dei pacchetti da una VLAN all'altra.

## Il link con il Router

Il link punto-punto tra Switch Multilayer e Router/Firewall costituisce una rete a tutti gli effetti.

Nello Switch Multilayer la corrispondente porta verrà configurata come "routed port" mediante il comando *no switchport*: come se fosse a tutti gli effetti l'interfaccia di un router.

```
S(config)# interface Fa0
S(config-if)# no switchport
S(config-if)# ip address 192.168.60.2 255.255.255.0
S(config-if)# no shutdown
```

Si deve anche configurare la route di default verso il Router/Firewall, la cui interfaccia avrà indirizzo IP 192.168.60.1:

```
S(config)# ip route 0.0.0.0 0.0.0.0 192.168.60.1
```

## La configurazione del Router/Firewall

Le interfacce del Router/Firewall vengono configurate con gli indirizzi IP previsti:

```
R# configure terminal
R(config)# interface Fa1
R(config-if)# ip address 192.168.60.1 255.255.255.0
R(config-if)# no shutdown

R(config)# interface Fa0
R(config-if)# ip address 192.168.70.1.255.255.255.0
R(config-if)# no shutdown

R(config)# interface Ser0
R(config-if)# ip address 212.120.80.82 255.255.255.248
R(config-if)# no shutdown
```

Per quanto riguarda il routing statico, si deve impostare la route di default verso il Provider e una route verso le diverse reti interne opportunamente riassunte ("summarized") con 192.168.0.0/16:

```
R(config)# ip route 0.0.0.0 0.0.0.0 212.120.70.1
R(config)# ip route 192.168.0.0 255.255.0.0 192.168.60.2
```

## Impostazione del NAT statico per il server web

Avendo a disposizione un insieme di indirizzi IP pubblici da assegnare ai server della rete DMZ, si deve configurare il Router/Firewall in modo che associ in modo statico uno di questi indirizzi al server web esposto al pubblico di Internet.

In questo modo i pacchetti che hanno come mittente il server web (192.168.70.2) verranno spediti in Internet facendo figurare come mittente l'indirizzo IP 212.120.80.83 (deciso in precedenza). Questa operazione di "traduzione dell'indirizzo" viene effettuata dal Router/Firewall.

Allo stesso modo, i pacchetti che il Router/Firewall riceve e che sono destinati a 212.120.80.83 verranno inoltrati nella rete interna con destinatario 192.168.70.2.

Per configuare tale funzione di NAT (Network Address Translation) si danno i seguenti comandi al Router/Firewall: innanzitutto si associa in modo statico un indirizzo interno (192.168.70.2) ad un indirizzo pubblico (212.120.80.83) e poi si indica quali interfacce sono verso l'interno (inside) e verso l'esterno (outside) della rete aziendale.

```
R(config)# ip nat inside source static 192.168.70.2 212.120.80.83

R(config)# interface Fa0
R(config-if)# ip nat inside
R(config-if)# exit
```

```
R(config)# interface Ser0
R(config-if)# ip nat outside
R(config-if)# exit
```

## Impostazione del NAT per i pc della rete

Per consentire ai pc della rete aziendale di uscire in Internet, si deve impostare anche la traduzione dei loro indirizzi privati con un indirizzo pubblico.

A tal fine, la soluzione più conveniente è quella di impostare il cosiddetto NAT Overload, che sostituisce a tutti gli indirizzi privati dei pacchetti spediti dai pc della rete aziendale l'indirizzo IP pubblico dell'interfaccia Ser0 del Router/Firewall a cui viene aggiunto un conveniente numero di porta in modo da riuscire a distinguere i diversi traffici di pacchetti.

Innanzitutto si definisce la lista degli indirizzi IP autorizzati ad uscire (list 1) e poi si associa tale lista all'interfaccia di uscita Ser0 specificando la modalità overload:

```
R(config)# access-list 1 permit 192.168.0.0 0.0.255.255
R(config)# ip nat inside source list 1 interface Ser0 overload
```

La suddetta lista comprende tutti i pc della rete interna (si noti l'uso della "wild card mask" 0.0.255.255 per specificare che i primi 2 otteti dell'indirizzo sono fissati mentre i restanti 2 no).

Si completa la configurazione con i comandi che specificano quali sono le interfacce interne (inside) e quella esterna (outside):

```
R(config)# interface Fa1
R(config-if)# ip nat inside
R(config-if)# exit

R(config)# interface Ser0
R(config-if) ip nat outside
R(config-if)# exit
```