Predisposizione e installazione di reti Ethernet (wired & wireless)
Introduzione

La larga diffusione di Internet e i vantaggi offerti dagli ambienti di rete distribuiti uniti all'esigenza di collegare un numero crescente di calcolatori hanno aiutato il successo della tecnologia *Ethernet* come standard per le reti locali. Si possono così trovare dispositivi adatti alle esigenze del piccolo ufficio o soluzioni per la grande impresa.

Molti apparati di rete quali *hub* e *switch* che si trovano sul mercato si possono acquistare come *plug and play*, è cioé sufficiente collegarli per poterne sfruttare le funzionalità senza richiedere particolari operazioni.

L'installazione di apparati per piccole reti locali risulta così piuttosto semplice. La scelta di dispositivi, la progettazione dell'infrastruttura e le configurazioni ottimali per un'ambiente di rete con esigenze più consistenti richiedono però conoscenze più approfondite.

Il cablaggio strutturato in UTP Categoria 5 Enhanced

Il cablaggio dell'infrastruttura è richiesto tipicamente con cavi UTP (*Unshielded Twisted Pair*) Categoria 5 *Enhanced*.

Anche se la tecnologia *Ethernet* più diffusa al momento è il *Fast Ethernet* (100Base-T) e per supportarla è sufficiente un cablaggio in UTP Categoria 5, la scelta di realizzare l'infrastruttura in Categoria 5 *Enhanced* è motivata dal fatto che quest'ultima supporta la tecnologia *Gigabit Ethernet* 1000Base-T. È importante quindi predisporre l'infrastruttura in modo scalabile rendendo disponibili cavi compatibili con le tecnologie in via di diffusione e che offrono migliori prestazioni.

Collegamenti dorsali

Negli edifici dove si richieda il cablaggio di collegamenti dorsali è opportuno prendere in considerazione la possibilità di predisporre la posa di due cavi anziché uno. La predisposizione può risultare utile in caso di guasto, oppure può essere utilizzata per incrementare la banda disponibile.

Scegliere gli apparati di rete: *hub* e *switch*

La scelta degli apparati di rete richiede la conoscenza specifica delle loro funzionalità e dell'applicazione per cui andranno installati. Non è sufficiente quindi scegliere tra *hub* o *switch* per realizzare una buona infrastruttura.

Principali caratteristiche di un hub o switch per soluzioni di rete avanzate

- **Funzionalità *stackable***. Per far sì che la soluzione di rete sia scalabile e che quindi sia possibile ampliare il numero di punti rete e di stazioni collegate è importante verificare che tra le caratteristiche degli apparati acquistati sia presente la funzione *stackable*. Questa funzione consente di accorpare in un unico dispositivo due dispositivi; ad esempio è possibile raggruppare uno *switch* a 24 porte con uno a 12 realizzando un dispositivo logico a 36 porte.
- **10/100/1000 *auto-sensing***. I dispositivi che supportano queste funzionalità sono molto semplici da utilizzare. Le porte sono infatti *auto-sensing* e si settano automaticamente la velocità supportata dalla stazione che si collega alla presa di rete. Sarà cosi semplice gestire un ambiente eterogeneo con sistemi a 10, 100 o addirittura i più recenti 1000 Mbps.
- **Auto MDI/MDIX**. La funzione Auto MDI (*Medium Dependent Interface*)/MDIX (*Medium Dependent Interface Crossover*) configura automaticamente la polarità delle porte, sarà indifferente collegare le stazioni con cavi 1:1 (diritti) o crosswire in modo del tutto trasparente.
- **Funzionalità di *management* e SNMP (*Simple Network Management Protocol*)**. Un *hub* o

switch con il supporto per il protocollo SNMP permettono il controllo remoto delle funzionalità del dispositivo, il controllo sul traffico e la generazione di allarmi in caso di guasto di porte o moduli. Queste funzionalità di *management* sono molto utili per monitorare il funzionamento dell'infrastruttura di rete, per scopi di analisi del traffico e manutenzione della rete.

- ***MAC filtering***. Alcuni dispositivi *switch* supportano caratteristiche interessanti come il *MAC (Madium Access Control) filtering* o sistemi per il *MAC Intrusion Dection*. Sono funzioni che sfruttano la conoscenza del *MAC Address* delle interfacce collegate per garantire una maggiore sicurezza in rete.
- **Supporto VLAN**. Il supporto per la gestione delle *Virtual* LAN è una caratteristica importante da tenere in considerazione se si prevede di costruire un ambiente che preveda molto traffico tra gruppi di lavoro che si trovano in posizioni differenti dello stabile. Questa caratteristica può essere sfruttata per ottimizzare la banda disponibile.

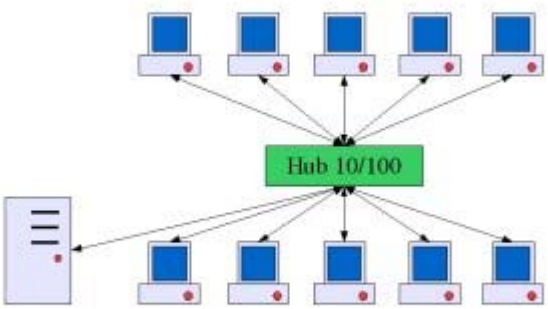
Accorgimenti per la predisposizione e installazione di hub o switch

Per la predisposizione e l'installazione di *hub* e *switch* è necessario conoscere il tipo di applicazione che l'infrastruttura di rete dati realizza. In particolare è opportuno adottare alcuni accorgimenti utili nel casi sia prevista la **centralizzazione delle risorse di calcolo** con un sistema *server*.

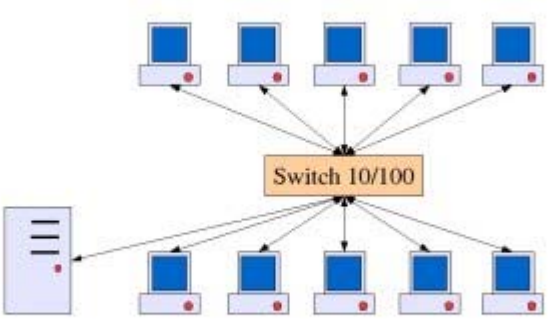
Il parametro fondamentale da prendere in considerazione in questo caso è l'aggregato della banda.

Un esempio pratico può aiutare la comprensione del problema:

Supponiamo di collegare 10 stazioni ad un sistema *server* e, che le stazioni accedano contemporaneamente al *server* generando traffico fino ad occupare tutta la banda disponibile sul loro singolo canale in una rete 10/100Mbps. L'effetto previsto è quello di un sensibile aumento delle collisioni delle trame dati in transito.



Adottando uno *switch* al posto di un *hub* le prestazioni migliorano poiché il numero di collisioni diminuisce sensibilmente. Le trame infatti non vengono replicate su tutte le porte del dispositivo, ma trasmesse solo sulle porte dove si trovano le interfacce di rete a cui sono destinate.

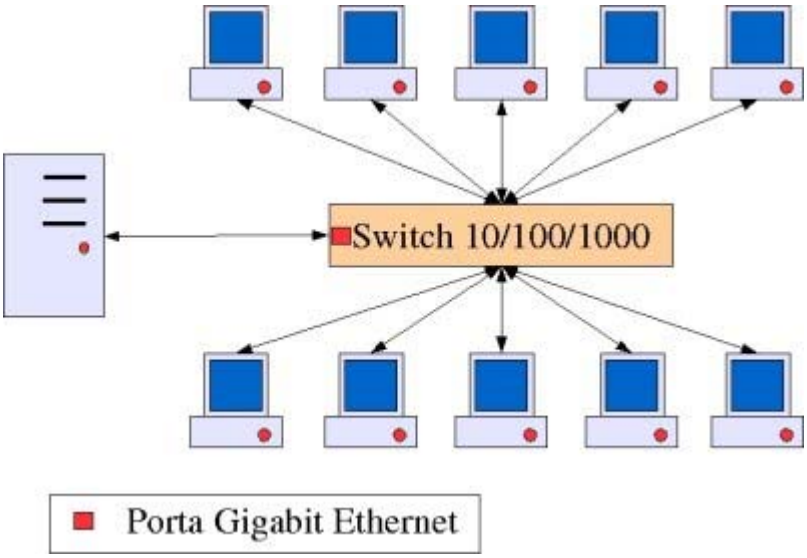


Progressivamente, in funzione anche del protocollo di rete utilizzato, la banda disponibile per il collegamento con il *server* si riduce al totale della banda disponibile diviso il numero delle stazioni attive e collegate.

100Mbps/11stazioni = circa 9Mbps per ogni collegamento (in realtà sono molto meno a causa dell'*overhead* di protocollo dei vari strati di rete e delle numerose collisioni).

L'accorgimento è di predisporre il *server* con un collegamento di rete che corrisponda all'aggregato della banda prodotto dai singoli collegamenti *client*. Sarà allora opportuno predisporre uno *switch* 10/100/1000Mbps, equipaggiare le stazioni di lavoro con schede di rete 10/100Mbps e il *server* con una scheda 1000Mbps.

In questo modo ogni stazione *client* avrà a disposizione:
1000Mbps/ 10stazioni = 100Mbps
cioè la massima banda teorica disponibile per ogni collegamento.



Lo stesso ragionamento può essere facilmente applicato al collegamento in cascata di apparati *hub* e *switch* al fine di ottimizzare il flusso di dati sulla rete.

Scegliere apparati di rete wireless: Access Point (AP)

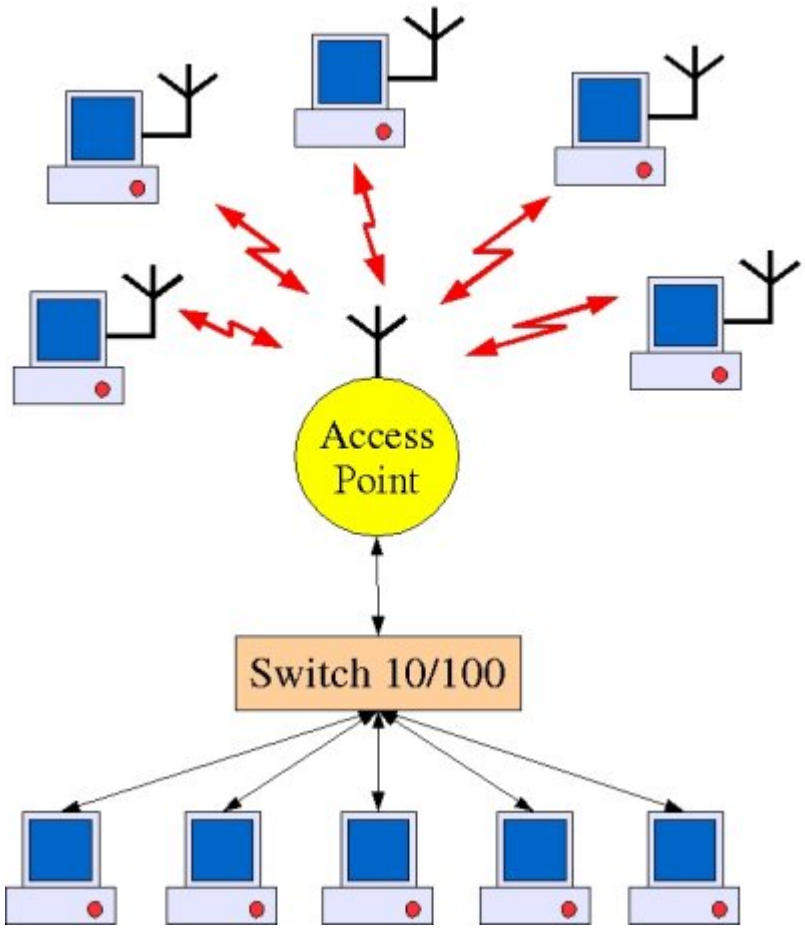
Per la scelta di apparati di rete *wireless* è necessario conoscere le principali caratteristiche degli standard 802.11a, 802.11b e 802.11g (in arrivo).

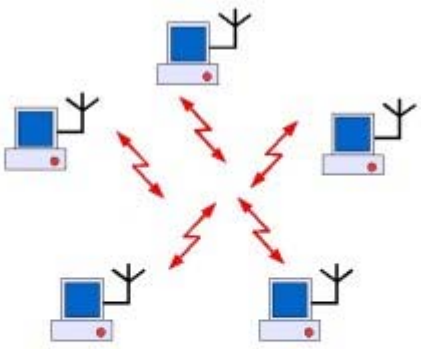
Access Point

Un *Access Point* (AP) è un dispositivo con funzionalità di *bridging* tra una rete cablata su cavo e una rete *wireless*. Attraverso gli standard per il *wireless Ethernet* è possibile realizzare dei collegamenti di tipo *Infrastructure*, cioè predisposti con un infrastruttura centrale. La comunicazione tra le stazioni collegate è di tipo punto-multipunto e sfrutta il protocollo di accesso al mezzo CSMA/CA con ACK.

Eventualmente è anche possibile il collegamento ad-hoc dove le stazioni sono collegate tra loro, senza l'ausilio di un *Access Point* in tipologia *peer-to-peer*.

In entrambi i casi i dispositivi impiegati effettuano la trasmissione dei dati mezzo onde-radio, il *bus* logico che realizza la rete è quindi facilmente intercettabile rendendo meno sicuro il sistema.





WEP Encryption

Per ovviare a questo possibile inconveniente gli standard 802.11 prevedono la possibilità di crittografare i dati con il sistema *WEP* (*Wired Equivalent Privacy*, ossia con grado di sicurezza equivalente alla rete cablata). In realtà sono ancora molte le discussioni sulla reale sicurezza del sistema, resta comunque il fatto che la possibilità di crittografare con tecnologia *WEP* sia una caratteristica fondamentale da ricercare in prodotto acquistato come *Access Point*.

***MAC Address* filtering**

Un'altra caratteristica importante consiste nella possibilità di filtrare i *MAC Address* delle interfacce di rete che cercano di collegare l'infrastruttura. È un'altra caratteristica importante a garantire la sicurezza del proprio punto di accesso *wireless*.

Sistemi di autentica quali RADIUS (*Remote Authentication Dial-In User Service*) o 802.1x

Nel predisporre un'infrastruttura *wireless* di ampie dimensioni e con un vasto numero di utenti previsti è inoltre opportuno prevedere un sistema di autentica centralizzato il grado di riconoscere e certificare l'identità della stazione prima di concedere l'accesso alla rete.
È quindi bene verificare che l'*Access Point* supporti uno o più sistemi di autentica di rete.

Esempio di configurazione di un Access Point

Vediamo ora un esempio di come è possibile configurare un *Access Point* per realizzare una rete con tecnologia *wireless*.

Access Point (AP):

Nel manuale del dispositivo troviamo ovviamente tutte le istruzioni passo-passo su come procedere. Per prima cosa colleghiamo l'AP all'infrastruttura di rete cablata come nell'esempio *Infrastructure* e procediamo con il *set-up* dell'IP perché sia contattabile dalla rete locale.

Molti di questi dispositivi dispongono di un'interfaccia di tipo *Web* per semplificarne la configurazione. Il manuale d'uso specifica l'indirizzo IP di *default*, cioè l'indirizzo di rete che il dispositivo possiede quando esce della fabbrica.

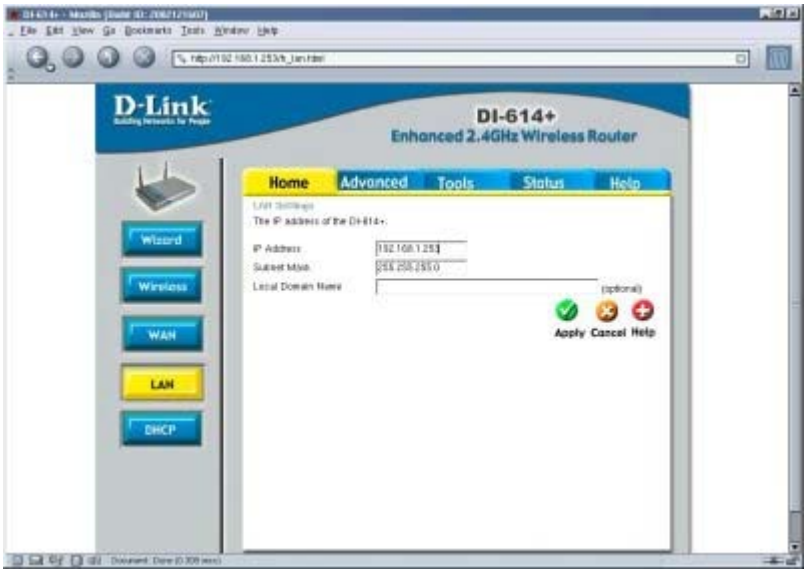
Nel nostro caso: 192.168.0.1 (con *netmask* 255.255.255.0).

Se la nostra rete *Ethernet* possiede lo stesso indirizzamento sarà subito possibile contattarlo tramite il *browser*, altrimenti dovremmo configurare una *workstation* sulla rete 192.168.0.0 con *netmask* 255.255.255.0 per poter configurare l'*Access Point*.

Aprendo il *browser* digiteremo come indirizzo l'IP specificato nel manuale di istruzioni del dispositivo.

Esempio: http://192.168.0.1

A questo punto è possibile configurare il dispositivo attraverso una serie di menu.
Per cambiare l'indirizzo IP è sufficiente cliccare su LAN e scegliere l'indirizzo IP proposto dal nostro progetto di rete.



Si procede con il *set-up* della rete *wireless*. Il parametro standard da impostare è l'SSID (*Service Set ID*) cioè il nome della nostra rete *wireless*, senza questo l'apparato utilizzerà quello di *default*. È importante notare che viene abilitata la crittografia *WEP* per 3 classi di utenti distinte. Questi parametri dovranno essere configurati allo stesso modo anche sulle stazioni.

Un'altra restrizione di accesso alla rete è possibile grazie alle funzioni di *MAC filtering*. Nell'esempio l'accesso *wireless* è consentito solo a 3 calcolatori di cui ovviamente occorre conoscere il *MAC Address*.

Infine per evitare che le configurazioni possano essere manomesse occorre impostare l'accesso tramite *password* al dispositivo.