

Illustrazione di scenari tipo per una rete scolastica

2002 - Riccardo Aliani & Roberto Bisceglia

L'infrastruttura di rete

- Le schede di rete
- La cablatura
- I concentratori
- I router
- I print server
- I modem ed i TA ISDN/xDSL
- I gruppi di continuità
- I patch panels

Le schede di rete

Sono gli adattatori per connettere i computer alla rete. Di norma sono schede PCI e funzionano a 10 e a 100 Mbit.

Nei notebook possono essere integrate o su scheda PCMCIA.



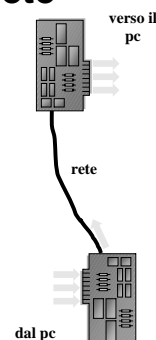
Scheda PCI 10/100



Scheda PCMCIA 10/100

Le schede di rete

- ◆ La scheda provvede a trasformare i dati da trasmettere in rete, serializzandoli e spostandoli a pacchetti lungo il cavo a cui è collegata
- ◆ Nel computer ricevente la scheda provvede invece ad intercettare i pacchetti ad essa diretti (o di *broadcast*, diretti cioè a tutta la rete) e a ricomporli per essere letti dal calcolatore



Quale Scheda scegliere ?

Esistono diversi tipi di schede di rete, ormai tutte di tipo PCI plug&play.

Si differenziano soltanto per il chipset (ad es. Realtek 8139, 3COM 905) e per alcune caratteristiche particolare.

La scelta è solo di carattere economico, tenendo conto che:

- ◆ Una scheda Realtek 8139B costa circa 15 €.
- ◆ Una scheda 3com 905 costa non meno di 60 €.

Cablaggio della rete

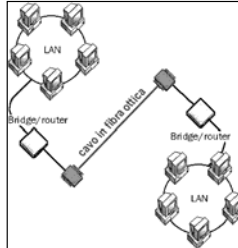
- ◆ Prima di procedere ad analizzare alcuni casi reali di progettazione, è necessario tener conto del tipo di cablaggio presente oppure, nel caso di sua inesistenza, delle possibilità (economiche e fisiche) di una sua realizzazione. I tipi sono:

1. *Cablaggio strutturato*
2. *Cablaggio non strutturato*

Il cavo a fibre ottiche

- ◆ Il costo del cavo è molto basso, ma i connettori e le apparecchiature a cui è connesso ne comportano una esclusione dalla categoria delle reti economiche

- ◆ Può risultare utile, date le sue virtù, come dorsale di rete o per connettere reti differenti tra di loro



Dove mettere i cavi ?

Spesso è il problema maggiore in quanto la maggioranza delle scuole non dispone di canalizzazioni di servizio nella muratura. La scelta può essere:

- ◆ Pavimentazione rialzata in pannelli e disposizione dei cavi nello spazio sottostante.
- ◆ Canaline in PVC a muro o a pavimento.
- ◆ Canaline a discesa dai controsoffitti.



La scelta dei cavi

Considerata la differenza dei costi di materiale e di installazione dei cavi UTP e STP, il fatto che la lunghezza delle singole tratte è al massimo è di pochi metri, la scelta preferibile è:

- ◆ Cablatura con cavi UTP certificati cat.5.

Gli errori da evitare

- ◆ Installazione di cavi non certificati, in particolare per le caratteristiche ignifughe.
- ◆ Installazione di cavi volanti.
- ◆ Installazione di cavi in canaline con cavi elettrici.
- ◆ Installazione di cavi troppo corti o troppo lunghi.
- ◆ Installazione di cavi in zone di passaggio o soggette a calpestio.

L'alternativa al cablaggio

- ◆ In situazioni di difficile installazione, si può considerare la soluzione di una rete wireless (senza fili)
- ◆ La rete wireless segue lo standard Ethernet 802.11b, con portata del segnale radio fino a 100 mt in ambiente chiuso e 300 mt all'aperto
- ◆ Questa soluzione limita la velocità ad un max di 11 Mbit/sec; risulta inoltre molto più costosa rispetto alla soluzione tradizionale



I Concentratori di rete

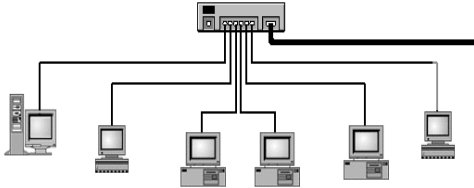
I concentratori di rete sono apparecchiature alle quali convergono i cavi provenienti da tutti i nodi di rete, e sono deputati allo smistamento dei pacchetti di dati.

Due sono i tipi di concentratori:

- ◆ Gli Hub
- ◆ Gli Switch

Gli Hub

Gli Hub sono apparati concentratori verso i quali sono convogliati i dati provenienti e destinati a ciascun computer. I pacchetti che a loro arrivano sono indirizzati a tutti i nodi, ma solo il destinatario è in grado di identificarli.



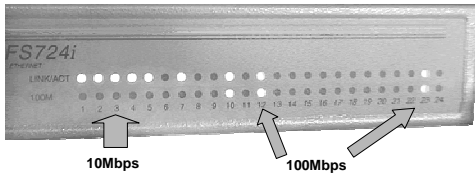
Gli Hub

Sono in pratica semplici ripetitori di segnale. Quando un pc trasmette verso l'hub, il suo segnale viene semplicemente ripetuto a tutti gli altri pc collegati alle altre porte dell' Hub.



Gli Hub

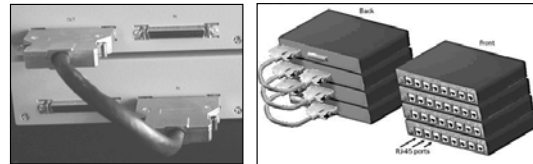
Ovviamente l'hub va scelto in base alla velocità consentita dalle schede e dai cavi; esistono quindi hub a 10, 100 o 1000Mbps, oppure hub "autosense" che riconoscono in automatico la velocità del nodo connesso



Gli Hub

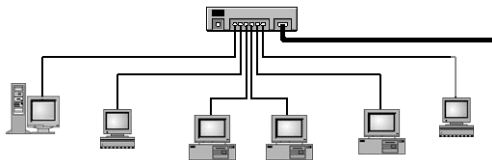
Esistono hub a 4, 8, 16, 24 porte; superato questo limite è necessario connettere "in catena" più hub, per aumentare il numero di nodi collegabili

Gli hub più costosi possono essere impilati (stackable) a seconda delle esigenze fino a formare un unico grande hub, con oltre 144 porte



Gli Switch

Gli Switch sono Hub intelligenti in grado di propagare i dati solo al segmento interessato e non a tutta la rete.



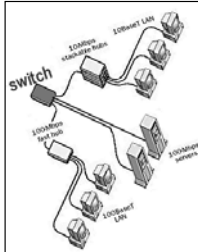
Gli Switch

In pratica si crea una tabella degli indirizzi abbinati alla porta, in modo che i pacchetti destinati ad un certo indirizzo finiscano solo nella porta abbinata a tale indirizzo, senza andare a disturbare le altre tratte. Il risultato è una maggiore velocità di trasmissione.



Gli Switch

- ◆ Grazie alle sue doti, lo switch riesce a velocizzare lo smistamento delle informazioni
- ◆ Può essere usato in qualsiasi condizione come sostituto dell'hub, ma dato il suo costo notevolmente superiore viene impiegato nei nodi centrali di smistamento, in modo da segmentare una rete in sezioni più piccole e meno congestionate



Hub vs. Switch

Considerato che gli Switch sono intelligenti, si capisce che questi sono da preferire agli Hub.

Tuttavia è legittimo considerare anche la variabile del costo.

- Un Hub a 16 porte 10/100 costa circa 80 €
- Uno Switch 16 porte 10/100 costa circa 400 €

Dove mettere il Concentratore ?

Il concentratore è un apparecchio vitale per la rete. Se non funziona, la rete non funziona.

Per questo è consigliabile installarlo in un locale protetto, ovvero in un apposito armadio.

Fortemente sconsigliato lasciarlo appoggiato ad un tavolo, a disposizione di tutti.

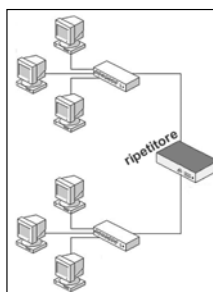
Gli errori da evitare

- ◆ Acquistare un concentratore con un numero di porte inferiore o al limite della necessità
- ◆ Acquistare un concentratore a 10 Mbit anziché uno a 10/100 Mbit.
- ◆ Collocare il concentratore in un luogo sbagliato.
- ◆ Collocare il concentratore in una zona sprovvista di presa elettrica.

I Ripetitori

Quando la distanza tra due punti della rete supera la misura massima consentita dal cavo, si ricorre a dei dispositivi di amplificazione e ripulitura del segnale detti *ripetitori*.

Il ripetitore permette anche di spostare le trasmissioni tra differenti mezzi di distribuzione, come i cavi coassiali e le fibre ottiche.

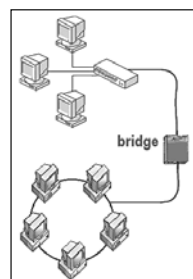


I Bridge

Si utilizzano in reti di dimensioni elevate o con molto traffico.

Consentono di collegare segmenti di rete con architetture o addirittura protocolli differenti.

Possono filtrare le trasmissioni tra due segmenti di rete, riducendone il traffico grazie a tabelle di instradamento gestite nella loro memoria.



I Router

Apparecchiatura che si occupa di instradare i pacchetti da una rete ad una altra rete, lavorando a livello di protocollo ed in modo intelligente.

Solo i pacchetti con una destinazione conosciuta e certa vengono instradati.

I router più utilizzati sono quelli che collegano la LAN ad Internet attraverso connessioni ISDN o ADSL.



I Modem

Quando la rete si estende tramite linee telefoniche, entrano in gioco i *modem*.

Sono strumenti che trasformano i dati per essere idonei al trasporto tramite telefono.

Un modem comunica sempre con un altro modem (dall'altra parte del telefono), mai con un computer

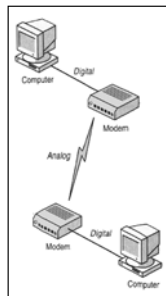
Il modem di solito è fisicamente connesso al computer o ad un router



I Modem

I modem analogici sono lenti in quanto debbono convertire il segnale da inviare (digitale) in suono (analogico) e viceversa (*MODulazione-DEModulazione*).

Attualmente la velocità massima di un modem analogico in ricezione è di 56 Kbps e di 33.6 Kbps in trasmissione, dati peraltro teorici, in quanto risentono notevolmente della qualità della linea.



I Terminali ISDN e xDSL

Se si dispone di una linea ISDN è possibile installare un Terminal Adapter. La velocità massima possibile è di 64 Kbps utilizzando un solo canale, 128 Kbps per due canali.

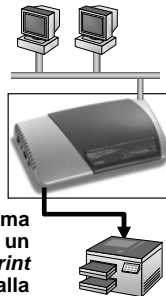
Disponendo di una connessione xDSL si possono utilizzare terminali appositi. La velocità massima possibile è di 1.28 Gbps.



I Print Server

Nel caso si necessiti di una stampante di rete, questa può essere condivisa da un computer (che diventa print server) oppure direttamente connessa alla rete (nel caso disponga di scheda di rete interna), ma sempre dipendente da un server che ne gestisce la coda di stampa

Per rendere completamente autonoma una stampante, è necessario un piccolo apparecchio detto *Print Server*, che si connette alla rete e alla stampante e gestisce le richieste di stampa degli utenti connessi



I Gruppi di continuità

Noto anche come *UPS*, garantisce alimentazione elettrica continua e stabilizzata ai server anche durante i black-out (grazie a batterie).

Salvaguarda l'integrità e la correttezza dei dati conservati sui server ed evita lente ripartenze della rete.

Se controllabile tramite computer, permette partenza e arresto dei server programmati.

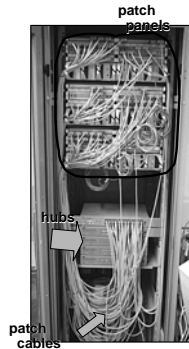


I Patch Panels

In reti formate da molti nodi tutti i cavi vengono convogliati verso un armadio, detto anche *rack*.

Nel rack i cavi vengono collegati ad uno o più pannelli modulari detti *patch panels*.

Da qui, tramite cavi detti *patch cables*, sono collegati agli hub o alle altre apparecchiature.

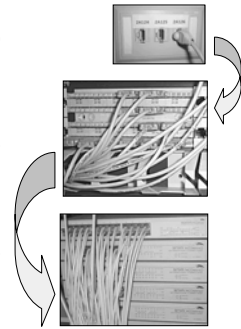


I Patch Panels

In questa maniera i cavi e i dispositivi di rete sono protetti dentro i rack, contro eventuali manomissioni

È facile spostare e riconfigurare le prese di rete, spostando i patch cables

La struttura modulare consente futuri ampliamenti



Organizzazione dell'aula

- Disposizione dell'aula
- Tavoli e sedie
- Impianti elettrici
- Illuminazione

Disposizione dell'aula

La disposizione dell'aula dipende, ovviamente, dal locale utilizzato.

Di norma le soluzioni possibili sono:

- ◆ Postazioni frontali
- ◆ Postazioni disposte sul perimetro
- ◆ Postazioni ad isola
- ◆ Postazioni a penisola

Esempi di aule



Aula frontale



Aula perimetrale



Aula a penisole



Aula a isole

La legge 626/94

Per la legge 626/94 e la legge 422/2000 uno studente non può essere considerato "lavoratore", in quanto non sta almeno 20 ore settimanali al computer.

Il D.M. Sanità 2 giugno 2000, stabilisce alcuni parametri ergonomici e relativi alla protezione dell'inquinamento elettromagnetico che devono essere considerati.

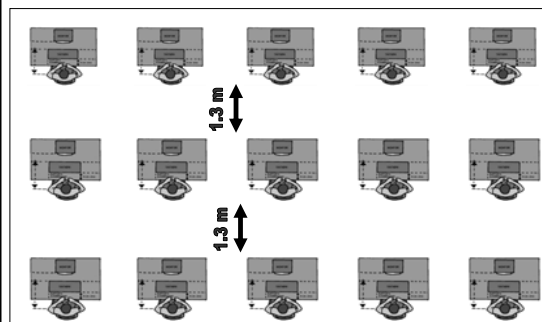
L'inquinamento elettromagnetico

I computer ma, soprattutto, i monitor sono fonti di inquinamento elettromagnetico.

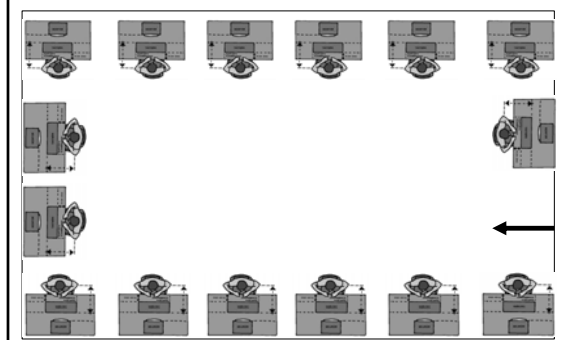
Per questo motivo è indispensabile evitare la concentrazione o la vicinanza di più computer.

La disposizione dell'aula frontale o a pettine richiede pertanto che tra uno studente e la fila vicina vi siano almeno 1.3 m, tali da limitare l'emissione a $0.2 \mu\text{Tesla}$.

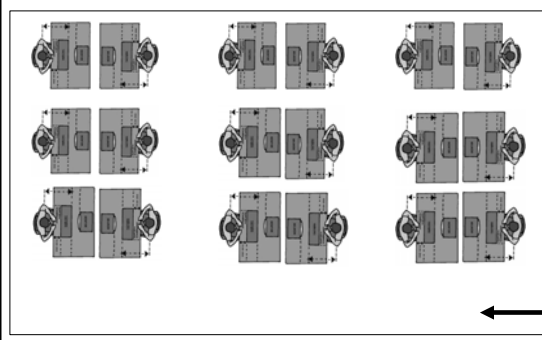
Aula frontale



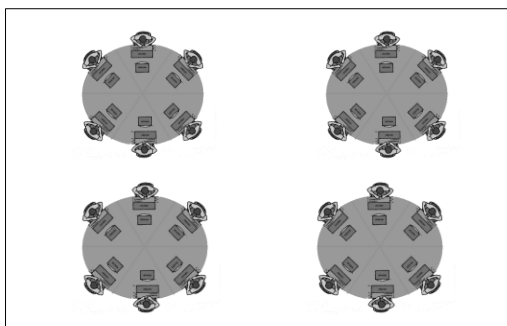
Aula perimetrale



Aula a penisole



Aula a isole



Quale aula scegliere ?

Di norma un'aula informatica viene creata in un locale preesistente.

Ciò comporta necessità di adattamenti che, spesso, si scontrano con l'ottimizzazione del lavoro.

Gli impianti delle aule frontali, a penisole o a isole devono essere fatte a pavimento, con un "pavimento galleggiante" o provenire dai soffitti, con idonee canalizzazioni.

Per le aule perimetrali, gli impianti possono correre lungo i muri in canaline in PVC.

Per questo, le aule perimetrali sono le più semplici ed economiche da realizzare.

Tavoli e sedie

I tavoli devono possibilmente essere di dimensioni adeguate, con ripiano per tastiera, spazio per il mouse e passacavi integrati.

Le sedie devono essere ergonomiche ed a norma della L.626/94.

Lo spazio tra i tavoli deve essere adeguato al passaggio degli alunni, senza che ciò crei problemi ai computer delle file vicine.



Impianti elettrici

Gli impianti devono essere a norma. L'aula deve avere adeguate protezioni con interruttori magnetotermici per aree ed uno generale.

Ciascuna postazione deve avere un numero congruo di prese (almeno 3) plurivalenti (italiane e Shucko).

Devono essere previste prese per hub, stampante di rete, plotter, etc.

Da evitare, invece, l'uso di prolunghe volanti.



Illuminazione

L'aula deve essere dotata di adeguata illuminazione artificiale.

L'illuminazione naturale deve, possibilmente, arrivare dal lato sinistro dei computer ed essere adeguatamente filtrata da tende o veneziane.



Gli errori da evitare

- ◆ Collocare l'aula in un locale inadeguato per dimensioni.
- ◆ Collocare l'aula in un locale inadeguato dal punto di vista della sicurezza.
- ◆ Installare collegamenti elettrici volanti (prolunghe, ciabatte, etc.).
- ◆ Non prevedere un adeguato carico della rete elettrica.
- ◆ Collocare i tavoli in modo che sia difficile accedere alle postazioni.
- ◆ Collocare le postazioni con forte illuminazione frontale o posteriore.
- ◆ Collocare l'hub in zona facilmente accessibile e incontrollabile.
- ◆ Collocare computer a ridosso dei termosifoni.

I Computer

I computer di un'aula in rete non necessariamente devono essere dello stesso tipo e caratteristiche.

E', infatti, normale disporre di computer acquistati in fasi successive.

Anche computer preesistenti possono entrare in rete, semplicemente installando una scheda di rete e configurandoli adeguatamente.

Sono necessari alcuni requisiti minimi, tali da consentire un utilizzo soddisfacente.

Requisiti minimi dei computer

Per consentire il funzionamento corretto dei sistemi operativi e dei più noti programmi applicativi, i computer dovrebbero avere le seguenti caratteristiche:

- ◆ CPU: Pentium > 120 Mhz.
- ◆ RAM: > 32 Mb
- ◆ Scheda video: SVGA > 4 Mb
- ◆ Hard Disk: > 1 Gb

Stampanti

L'errore da evitare è quello di dotare ciascun computer di una stampante di basso livello.

La soluzione migliore potrebbe essere quella di installare una stampante laser di buona qualità ed una stampante ink-jet a colori.

Le stampanti possono essere collegate a computer e condivise a tutta la rete, oppure dotate di scheda di rete ed installate come nodo.

Risorse condivise: i dischi

- ◆ La rete può consentire grossi risparmi nell'acquisto dell'hardware dei client
- ◆ Ogni macchina può diventare file server e condividere dischi o cartelle, quindi è inutile acquistare pc client con dischi enormi
- ◆ La macchina che funge da file server può inoltre essere dotata di dischi speciali, quali lettore CD/DVD, masterizzatore, ZIP, ecc.

I client senza Cdrom ? Sì, avete letto bene.

Altro Hardware condiviso

In una rete diverso può essere l'hardware installato su uno o più computer e condiviso a tutta la rete:

- ◆ Masterizzatore
- ◆ Scanner
- ◆ CDrom o DVDrom
- ◆ Scheda di acquisizione video
- ◆ Fotocamera digitale
- ◆ Dischi ottici

I Sistemi operativi

In una aula in rete possono convivere senza problemi sistemi operativi diversi appartenenti alla famiglia Microsoft Windows:

- ◆ Windows 3.11 Workgroups
- ◆ Windows 95, 95 OSR2
- ◆ Windows 98, 98 SE
- ◆ Windows ME
- ◆ Windows NT 4 Server
- ◆ Windows NT 4 Workstation
- ◆ Windows 2000 Professional
- ◆ Windows XP Professional

I File System

E' il modo con il quale i sistemi operativi memorizzano i dati sulle memorie di massa.

- ◆ MS-Dos e Windows 95, release B esclusa, utilizzano F.A.T. 16 bit.
- ◆ Windows 95 rel.B, Windows 98, Windows ME e Windows XP Home utilizzano anche la F.A.T. 32 bit.
- ◆ Windows NT, Windows 2000 e Windows XP Professional usano anche NTFS.

I File System

Qualora si utilizzino sistemi NT, Windows 2000 o Windows XP Professional, è consigliabile l'utilizzo, nella partizione di sistema, di NTFS. Questo file system infatti:

- ◆ E' più veloce e frammenta meno i file.
- ◆ Permette di concedere autorizzazioni di accesso ai singoli file o cartelle, ad utenti o gruppi di utenti.

I Protocolli di comunicazione

Con il termine “*protocollo di comunicazione*” si indica l'insieme di regole di comunicazione che debbono essere seguite da due o più interlocutori affinché siano in grado di capirsi.

Ad es.: il protocollo alla base della comunicazione tra docente e allievi durante una lezione potrebbe avere queste caratteristiche.

- ◆ Il docente parla in una lingua comprensibile agli allievi.
- ◆ Gli allievi ascoltano il docente.
- ◆ Quando vogliono intervenire gli allievi alzano la mano ed attendono il permesso del docente per iniziare a parlare.
- ◆ Durante l'intervento degli allievi il docente ascolta.
- ◆ Al termine dell'intervento il docente risponde.

Esempio di Protocollo di rete

- ◆ A contatta B: “Init”
- ◆ B risponde ad A: “Ack”
- ◆ A inizia a mandare pacchetti di dati a B
- ◆ B riceve i pacchetti di dati
- ◆ Il protocollo termina quando A invia “Fine” a B
- ◆ B risponde con “AckFine”

I Protocolli di comunicazione

- ◆ Con il termine “*protocollo di comunicazione*” si indica l'insieme di regole che debbono essere seguite da due o più interlocutori affinché siano in grado di capirsi.
- ◆ Sono riconosciuti e aggiornati da organismi internazionali (es. ISO)
- ◆ Nel corso degli anni, si sono sfolpiti in numero; i più famosi ed adottati col sistema operativo Windows sono NetBEUI e TCP/IP.

I Protocolli TCP/IP

Acronimo di Transmit Control Protocol e Internet Protocol.

E' un insieme di protocolli utilizzati dalle reti locali e da Internet.

Il TCP si occupa della suddivisione dei messaggi in "pacchetti", mentre l'IP pensa ad inviarli al corretto destinatario.

I Protocolli TCP/IP

Sono protocolli di basso livello; ciò significa che essi lavorano vicino al livello fisico della rete.

La loro funzione è di fornire servizi ai protocolli superiori e alle applicazioni (es. FTP, Telnet, HTTP).

L'indirizzo IP, o IP address, è un campo composto da 32 bit che definisce la rete e ciascuna macchina connessa.

Il TCP/IP è il protocollo di base di Internet.

Gli Indirizzi IP

Un indirizzo IP a 32 bit può essere visto come una coppia di due numeri: il numero di rete e il numero di host o nodo. Il numero di bit usato per il numero di rete dipende dalla classe di indirizzo.

Esistono cinque classi di indirizzi IP, tre le principali:

- ◆ Classe A: permette di avere 126 reti con 16777213 host ciascuno.
- ◆ Classe B: permette di avere 16382 reti, di 65534 host ciascuno.
- ◆ Classe C: permette di avere 2097150 reti, di 254 host ciascuno.

Gli Indirizzi IP

Poiché possono essere utilizzati sia da Internet che in reti locali, sono stati definiti dei range di IP privati che non sono assegnati ad host di Internet:

- ◆ 10.0.0.0 - 10.255.255.255
- ◆ 172.16.0.0 - 172.16.255.255
- ◆ 192.168.0.0 - 192.168.255.255

Questi devono essere utilizzati in una rete locale che utilizzi il TCP/IP.

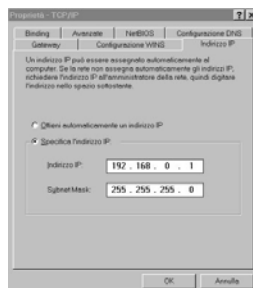
Configurare gli IP

Configurare gli IP di una rete con sistemi Windows è estremamente semplice. Nelle "Proprietà di rete", alla voce TCP/IP è sufficiente indicare un indirizzo diverso per ciascun computer della rete. Ad esempio

- ◆ 192.168.0.1 con sottomaschera di rete 255.255.255.0 per il primo computer.
- ◆ 192.168.0.2 con sottomaschera di rete 255.255.255.0 per il secondo computer.
- ◆ 192.168.0.3 con sottomaschera di rete 255.255.255.0 per il terzo computer.

Configurare gli IP

Ad esempio in Windows 98 è sufficiente indicare i valori negli spazi:



Configurare gli IP

In Windows 2000 è sufficiente indicare i valori negli spazi:



Configurare gli IP

La configurazione precedentemente descritta si definisce "statica".

Attivando in un server DHCP in un dominio NT/2000 è possibile rendere "dinamica" l'assegnazione degli indirizzi IP.

In questo modo il client riceve dal server un IP "disponibile" ad ogni collegamento, secondo modalità definite in uno "scope".



Test della rete

Al termine dell'installazione della rete, del TCP/IP e della definizione degli IP statici è necessario provvedere al test della rete, per verificare se tutti gli host parlano tra di loro.

E' sufficiente cliccare sull'icona "Risorse di rete" e vedere tutti i computer di rete, purchè essi siano attivi ed abbiano condiviso o una stampante o altra risorse "Condividi file e stampanti".

La verifica della funzionalità del TCP/IP è necessario utilizzare un comando DOS, il comando "ping".

Test della rete

Il comando "ping" manda una serie di pacchetti di dati ad un host identificato dal suo indirizzo IP.

Ad esempio:

C:\>ping 192.168.0.1

Se l'host è attivo e TCP/IP funziona, si avrà una risposta.

```
C:\WINDOWS> ping 192.168.0.1
Pinging 192.168.0.1 with 32 bytes of data:
Reply from 192.168.0.1: bytes=32 time=1ms TTL=64
Reply from 192.168.0.1: bytes=32 time=2ms TTL=64
Reply from 192.168.0.1: bytes=32 time=1ms TTL=64
Reply from 192.168.0.1: bytes=32 time=1ms TTL=64

Ping statistics for 192.168.0.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 2ms, Average = 1ms
```

Protezione dei computer

Proteggere i computer significa garantire una funzionalità duratura degli stessi.

Le protezioni da considerare sono:

- ◆ Protezione del BIOS.
- ◆ Protezione Antivirus.
- ◆ Protezione delle impostazioni.
- ◆ Limitazioni dell'uso di alcuni software.
- ◆ Protezione da cancellazioni e modifiche di file.
- ◆ Ripristino delle condizioni operative.

Protezione del BIOS

La prima protezione da attivare è quella del BIOS.

La procedura è semplicissima, basta entrare nelle impostazioni del BIOS al momento dell'avvio (di norma premendo il tasto <CANC> e definire una password per "Supervisor".

Da quel momento non sarà più possibile modificare le impostazioni.

Protezione Antivirus

L'accesso alla rete Internet o l'uso di floppy disk è spesso causa di attacchi virali.

Ogni computer deve essere dotato di antivirus che deve essere aggiornato almeno ogni 15 giorni.

Un antivirus non aggiornato perde la maggior parte delle sue capacità di protezione.

Protezione delle impostazioni

E' utile proteggere le impostazioni di base del sistema operativo (impostazioni del desktop, stampanti, etc.).

Tale protezione può essere effettuata agendo sul registro, utilizzando il tool apposito (Poledit per Windows 9x e NT, Criteri di protezione in Windows 2000 o XP), ovvero utilizzando software di terze parti.

Limitazione dell'uso di alcuni software

Tale opportunità è data solo se il file system è NTFS (Windows NT, 2000, XP pro).

Con esso è possibile bloccare l'accesso o l'esecuzione fino a livello di singoli file.

Per Windows 9X è possibile con l'uso di tools appositi.

Protezione da cancellazioni e modifiche di file

E' possibile proteggere i computer da cancellazioni di file, modifiche non volute, purchè non sia fortemente compromesso il sistema operativo.

Windows Me e Windows XP dispongono di un tool per il ripristino delle condizioni preesistenti ai danneggiamenti.

Tale operazione può essere fatta anche con software di terze parti.

Ripristino delle condizioni operative

Può essere effettuato utilizzando schede hardware particolari che impediscono le modifiche degli hard disk ed anche la loro formattazione.

Un altro sistema altrettanto efficace è la clonazione degli hard disk, con creazione di un'immagine di tutto il contenuto, che può facilmente e velocemente essere ripristinata.

Gli errori da evitare

- Sottodimensionamento dell'infrastruttura di rete.
- Errata scelta del locale.
- Mancanza di scalabilità.
- Assenza di protezioni o protezioni eccessive.
- Inaffidabilità delle connessioni
- Inadeguatezza dell'impianto elettrico e delle norme di sicurezza.

Rete didattica

In un aula in rete locale è possibile installare una rete didattica.

La rete didattica ha la funzione di favorire l'interazione docente-alunno.

Ad esempio è possibile mostrare il proprio desktop agli alunni, osservare il loro ed intervenire direttamente, scambiare messaggi, file, conversare, etc.

Due tipi di reti didattiche:

- ◆ Reti didattiche hardware
- ◆ Reti didattiche software



Rete didattica hardware

Si tratta di una rete che si affianca alla LAN, con proprie schede e propria cablatura.

Ha il vantaggio di utilizzare una via di trasporto autonoma, e quindi di non influire con le attività della LAN.

Ha lo svantaggio di essere molto costosa; spesso il costo a postazione equivale a quello di un computer

Rete didattica software

Si tratta di una rete software che utilizza come trasporto la LAN attraverso i protocolli di rete.

Ha il vantaggio di essere riutilizzabile, di offrire tutte le caratteristiche della rete hardware ad un costo decisamente inferiore.

Ha lo svantaggio di utilizzare la rete e, quindi, di rallentarla. In alcuni casi non supporta lo streaming video. Necessita di hardware potente.

Quale rete didattica ?

Le reti hardware hanno gli svantaggi di essere più costose, soggette a manutenzione da parte dell'installatore, di essere difficilmente trasportabili in altra aula e di essere soggette a veloce obsolescenza.

Per questo, considerati i continui aggiornamenti, è consigliabile l'installazione di una rete software.

La condivisione di Internet

Condividere l'accesso ad Internet significa disporre di una connessione che viene ripartita a tutti i computer.

Tenendo conto della suddivisione della banda, la soluzione migliore ad oggi è quella di una connessione ADSL 640 Kb.

Possibile, per un numero limitato di postazioni, l'utilizzo di una linea ISDN 128 Kb.

La connessione può essere:

- ◆ Con router
- ◆ Con proxy server

Il NAT ed il PAT

I router o i proxy devono avere la capacità di indirizzare le chiamate dai client di rete verso l'esterno e di distribuire correttamente i pacchetti di risposta.

Ciò avviene attraverso due meccanismi:

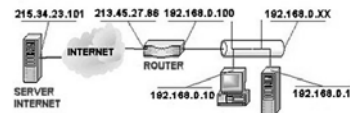
- ◆ NAT (Network Address Translation): viene utilizzato per nascondere la rete locale, in modo tale da permettere a più computer l'uscita verso Internet utilizzando un unico indirizzo IP.
- ◆ PAT (Port Address Translation): viene utilizzato per cambiare la porta di uscita o quella di ingresso quando da più client si fa accesso contemporaneamente a server esterni.

Il NAT ed il PAT

Se ad esempio il PC 192.168.0.10 vuole andare a visitare il sito Web 215.34.23.101, invia un pacchetto al gateway (router o proxy) 192.168.0.100; il NAT sostituisce l'IP sorgente con quello pubblico del gateway stesso, es. 213.45.27.86 e lo manda a destinazione.

Il server Web risponde al gateway il quale sostituisce l'IP al contrario e lo consegna al PC.

Se avvengono più richieste dalla LAN, il PAT si incarica di cambiare le porte sorgenti e, poi, destinatarie per evitare conflitti.



La connessione con router

Il router è una apparecchiatura attiva in grado di connettere due reti: la rete Internet e la LAN.

Una volta installato tutto il traffico verso e da Internet passa attraverso di esso.

Vantaggi:

- ◆ Semplicità di installazione.
- ◆ Nessuna necessità di manutenzione o di amministrazione.

La connessione con router

Il router ISDN o ADSL viene connesso, attraverso una porta RJ45 Ethernet o Fast Ethernet, al resto della rete ed è, quindi, considerato un vero e proprio nodo.

Ad esso è assegnato un indirizzo IP statico; tutte le macchine della rete devono porre come gateway l'indirizzo IP del router. Tutto il traffico da e verso Internet passerà così attraverso il router.



La connessione con proxy

Il proxy server è un programma, residente su un computer, che invia e riceve le chiamate ad Internet e le instrada a o da un terminale ADSL o ISDN.

Vantaggi:

- ◆ Presenza di una cache.
- ◆ Possibilità di definire gli utenti che possono accedere ad Internet.
- ◆ Possibilità di installare filtri.
- ◆ Report del traffico.
- ◆ Possibilità di firewalling.

La connessione con proxy

La connessione Internet attraverso proxy server ha quindi dei vantaggi.

Tuttavia è da ricordare che il proxy server ha un costo non indifferente, che impegna pesantemente un computer in particolare nel sistema dei dischi e che necessita di configurazioni abbastanza raffinate.

I proxy server più noti sono Microsoft Proxy server 2, ormai obsoleto, Microsoft ISA server e Wingate.



La configurazione del proxy

La configurazione del proxy server è diversa a seconda del tipo, ma in generale si effettua sul server dedicato allo scopo, indicando quali protocolli il proxy deve far transitare (HTTP, FTP, POP3, SMTP, SOCKS, NTTP) e quali utenti hanno i relativi diritti.

I computer di rete sono, di solito, configurati con un apposito programma client che registra i dati del server e configura, di conseguenza, le applicazioni che debbano utilizzare il server.

I Firewall

Aprire la propria rete locale ad Internet può essere pericoloso. Le porte, infatti, sono bidirezionali e possono essere sfruttate da malintenzionati (molto più frequenti di quello che si pensi) per entrare nel vostro sistema e creare guai.

Per questo motivo è consigliabile l'installazione di un Firewall (muro di fuoco).

Il Firewall controlla tutto ciò che entra o esce dalla rete a cui è abbinato usando una tecnica d'ispezione denominata *stateful inspection*.

Essa consiste nel comparare tutti i dati in transito con profili di sicurezza predefiniti per garantire che tutto ciò che transita attraverso il firewall sia autorizzato.

I Firewall

I Firewall possono essere software o hardware.

I Firewall software svolgono egregiamente la funzione anche se la loro configurazione spesso è difficile e la loro attività tende a rallentare il transito di dati.

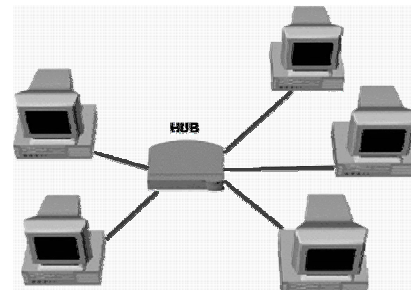
Tra i più noti Firewall software: McAfee Firewall, BlackIce Defender, ZoneAlarm, Symantec Firewall.

I Firewall hardware sono apparecchiature che vengono connesse tra il router o il terminale ADSL/ISDN e la rete e hanno il compito di filtrare tutti i pacchetti in transito.

Sono autoconfiguranti e di semplice installazione e particolarmente resistenti agli attacchi tipo DoS. Hanno, purtroppo, un costo elevato.



Aula in rete paritetica



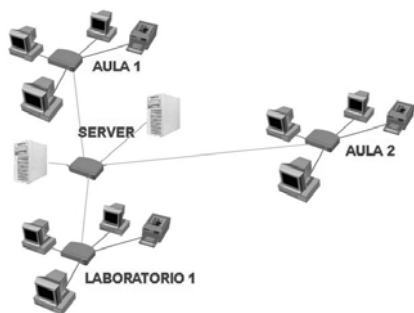
Vantaggi

- Semplicità di installazione
- Semplicità di gestione
- Non serve un System Administrator
- Non si impegna un computer come server

Svantaggi

- Difficoltà di controllare gli accessi
- Assenza di report delle attività
- Necessità di definire gli utenti in ciascuna postazione
- Necessità di definire eventuali policies in ciascuna postazione
- Maggiore vulnerabilità

Aula o aule in rete a dominio



Vantaggi

- Controllo e limitazione degli accessi.
- Report delle attività.
- Gestione centralizzata .
- Maggiore sicurezza.
- Possibilità di Intranet
- Miglioramento condivisione Internet (proxy server, filtri, etc.)

Svantaggi

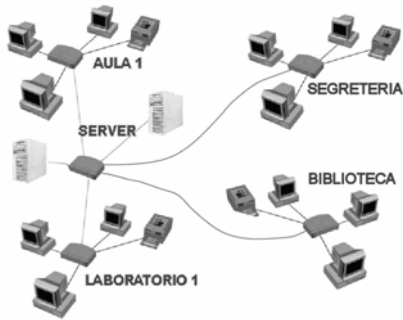
- Installazione e configurazione complessa.
- E' necessario un System Administrator.
- Si impegnano uno o più computer come server.
- Costi aggiuntivi per le licenze client.
- Se si blocca il server si blocca tutta la rete.

Rete d'Istituto

- ◆ Optando per la soluzione con aggiunta di uno o più server, si viene a formare, via via che vengono connessi nuovi ambienti, una rete d'Istituto, che può arrivare ad abbracciare l'intero edificio.
- ◆ La rete d'Istituto porta dei reali miglioramenti sia alla didattica sia all'organizzazione funzionale della scuola.



Rete d'Istituto



Il Dominio

Per gestire efficacemente una rete estesa a più parti dell'edificio, al limite anche a più edifici e per consentire l'accesso ad utenti con diverse caratteristiche, è necessario creare un dominio (domain).

Il Dominio

Rappresenta l'insieme dei computer, delle periferiche di rete, degli utenti che possono fare accesso ed i loro permessi.

La "sede" del dominio è il SERVER.

Per avere un dominio è necessario disporre di almeno un server (inteso come computer) dedicato e di un sistema operativo server.

Administrator

Come in tutti i domini, anche in quelli di rete deve esserci chi "detiene il potere".

E' Administrator, colui che definisce gli utenti, concede loro i permessi, determina le politiche di rete, crea i suoi "aiutanti": i server operators ed i backup operators.

E' buona norma che Administrator sia uno solo e che la password sia nota solo a lui.



La scelta di Administrator

Administrator in una rete scolastica deve essere un docente in possesso di buone conoscenze sistemiche, dotato di pazienza, di desiderio di imparare e di una buona quota di tempo disponibile.

E' auspicabile, se non doveroso, che Administrator sia nominato Figura obiettivo o, quanto meno, adeguatamente retribuito.

E' fortemente sconsigliabile lasciare la funzione a ditte esterne o a consulenti estranei alla scuola.

I Collaboratori di Administrator

Si tratta di utenti della rete alle quali sono assegnati particolari "poteri", ad esempio quello di fare backup, di installare software, di gestire gli account (escluso quello di Administrator...), di condividere directory e stampanti.

La scelta di questi "power users" deve essere fatta tra docenti o tecnici in possesso di buone conoscenze sistemiche di base.

Il Progetto di Rete

Considerando che le aule o i laboratori possono essere delle tipologie già descritte, restano da considerare:

- ◆ La connessione tra le aule.
- ◆ I Server di rete
- ◆ I Sistemi operativi Server
- ◆ I Sistemi operativi Client
- ◆ La condivisione di accesso ad Internet

La connessione tra le aule

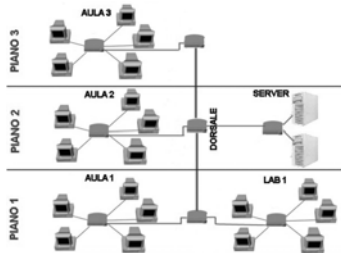
Una delle scelte strategiche è il progetto della connessione tra le aule e con la sala server.

Se la sala server è equidistante dalle aule, è possibile connettere gli hub/switch di aula all'hub/switch dei server.



La connessione tra le aule

Se le aule sono poste su piani diversi o a diverse distanze, è necessario installare una dorsale.



La dorsale

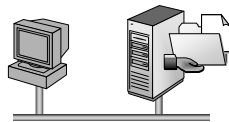
La dorsale è la cablatura che collega aule poste a diverse distanze o su piani diversi, ai server.

E' costituita da un cavo UTP cat.5 o, in caso di lunghe distanze o volendo una connessione più efficace, in fibra ottica.

Ad ogni piano è necessario installare un bridge o uno switch che si collega con l'hub/switch della LAN d'aula.

I Server di rete

◆ Sono computer che, possedendo maggiori risorse o capacità elaborative degli altri, le mettono a disposizione della rete



- ◆ Sono *dedicati* i server che lavorano esclusivamente per la rete, rispondendo anche a più richieste contemporanee dei client
- ◆ Sono *non dedicati* i server che, oltre ad offrire risorse alla rete, sono utilizzati correntemente anche come client

L'hardware per i Server

I server di rete hanno bisogno di un hardware abbastanza potente.

In particolare sono importanti il tipo ed il numero di CPU, la quantità di memoria RAM, il sistema dischi, la scheda di rete.

Anche il cabinet deve essere adeguato sia per quanto riguarda l'alimentazione, sia per quanto riguarda il raffreddamento.

Alcune specifiche

- ◆ Processore: uno o, meglio, due o più processori almeno a 1.5 GHz.
- ◆ RAM: almeno 512 Mb.
- ◆ Dischi fissi: almeno 2 da 40 Gb, sistema EIDE 100 o SCSI (Ultra 2 SCSI o Ultra 160 SCSI).
- ◆ Controller RAID 1 o 0+1 per mirroring o mirroring/striping dei dischi.
- ◆ Doppio alimentatore ridondante.
- ◆ Ventole supplementari.

Alcune specifiche: i dischi

- ◆ L'organizzazione del dominio risiede sui dischi del server: va assicurata protezione totale, anche in caso di guasto ad un disco
- ◆ Si ricorre di solito a controller RAID SCSI (Ultra 2 o Ultra 160), più costosi ma con prestazioni migliori.
- ◆ Alternativa più economica, ma altrettanto valida, è l'uso di controller e dischi EIDE 100. Il costo si riduce del 70 %.



Alcune specifiche: i dischi

- ◆ RAID (Redundant Array of Independent Disks) è un sistema hardware o software per l'accelerazione/protezione dei dati memorizzati su disco fisso. Consente tre livelli base:
- ◆ RAID 0 (striping): i dati da scrivere vengono divisi e inviati a due o più dischi in contemporanea.
- ◆ RAID 1 (mirroring): i dati da scrivere vengono replicati su un disco gemello
- ◆ RAID 5 (striping con parità): i dati da scrivere vengono divisi ed inviati ad almeno tre unità, con registrazione di parità

Livelli RAID a confronto

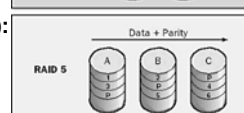
RAID 0 (striping): i dati da scrivere vengono divisi e inviati a due o più dischi in contemporanea



RAID 1 (mirroring): i dati da scrivere vengono replicati su un disco gemello



RAID 5 (striping con parità): i dati da scrivere vengono divisi ed inviati ad almeno tre unità, con registrazione di parità



Livelli RAID a confronto

	RAID 0 striping	RAID 1 mirroring	RAID 5 stripe parità
Velocità scrittura	Elevata	Normale	Buona
Velocità lettura	Elevata	Normale	Buona
Protezione dati	Nessuna	Completa	Elevata
Perdita spazio	Nessuna	Metà del totale	Un terzo del totale
Sostituzione a caldo	Impossib.	Si	Si

Errori da evitare

- ◆ Sottodimensionare il server.
- ◆ Utilizzare il server per compiti diversi.
- ◆ Installare scheda audio.
- ◆ Installare una scheda video costosa.
- ◆ Installare un monitor costoso.
- ◆ Installare un masterizzatore.
- ◆ Lasciare il server accessibile a tutti.

Collocazione dei Server

Per quanto possibile i server non devono essere collocati in un aula o in un laboratorio.

Un qualsiasi locale arieggiato, dotato di impianto elettrico adeguato, non accessibile a chiunque, è l'ideale per contenere i server.



La protezione dei Server

- ◆ Collegare il server ad un gruppo di continuità (UPS).
- ◆ Non lasciare mai il server accessibile, ma bloccarlo con password.
- ◆ Consentire l'accesso ai server solo all'utente Administrator.
- ◆ Verificare periodicamente lo stato dei servizi e visualizzare gli eventi.
- ◆ Installare regolarmente i Service Pack e gli aggiornamenti.
- ◆ Non installare programmi inutili nel server

Errori da evitare: Software dei server

- ◆ Scegliere un sistema che non assicuri assistenza adeguata all'administrator.
- ◆ Sottodimensionare o sovradimensionare la versione del software.
- ◆ Sovradimensionare il software rispetto alla potenza del server.
- ◆ Scegliere un sistema a cui vanno aggiunti molti servizi di terze parti.