SOLUZIONE AL TEMA DI SISTEMI PER L'INDIRIZZO INFORMATICO (SPERIMENTAZIONE ABACUS)

Dovendo procedere alla realizzazione di un progetto di rete locale risulta indispensabile partire dall'analisi della situazione preesistente all'interno dell'Istituto, che inciderà sulla scelta delle topologia e del tipo di strutture da implementare.

Facendo riferimento alle indicazioni della traccia sulla dislocazione dei computer e alla situazione tipica di un Istituto Tecnico, disposto in un unico edificio di 3 piani, è possibile ipotizzare che:

1. esistano delle connessioni di rete nei singoli uffici, nei laboratori e nella biblioteca, mentre risultano indipendenti le postazioni della dirigenza;

2. sia disponibile almeno una linea digitale veloce per la connessione ad Internet che arriva ad una borchia ubicata, secondo la normativa vigente sul cablaggio strutturato, in un apposito locale;

3. l'accesso alle singole reti sia di tipo peer to peer;

4. le macchine e i sistemi operativi siano eterogenei

5. ogni ambiente (ufficio, biblioteca, laboratorio) sia dotato almeno di una stampante

6. i dati da proteggere riguardino gli uffici di segreteria, la biblioteca e gli uffici di presidenza.

Per quanto riguarda inoltre la topologia della scuola ipotizziamo quanto segue:

1. i laboratori siano dislocati sul primo piano, mentre gli uffici e la biblioteca sono posti al pian terreno;
2. la superficie di ogni piano non superi i 1000mq;
3. il locale che ospita il punto di connessione telefonica e che spiterà le apparecchiature principali si trova al pian terreno ed è conforme alla normativa sulla sicurezza (assenza di tubi del gas, tubi dell'acqua, linee elettriche di potenza, …)
4. esistono dei percorsi di collegamento tra piani e locali;
5. la predisposizione dell'impianto elettrico è conforme alla norma.

Con queste informazioni è possibile realizzare un primo schema di architettura della rete di Istituto, distinguendo il cablaggio orizzontale da quello verticale.

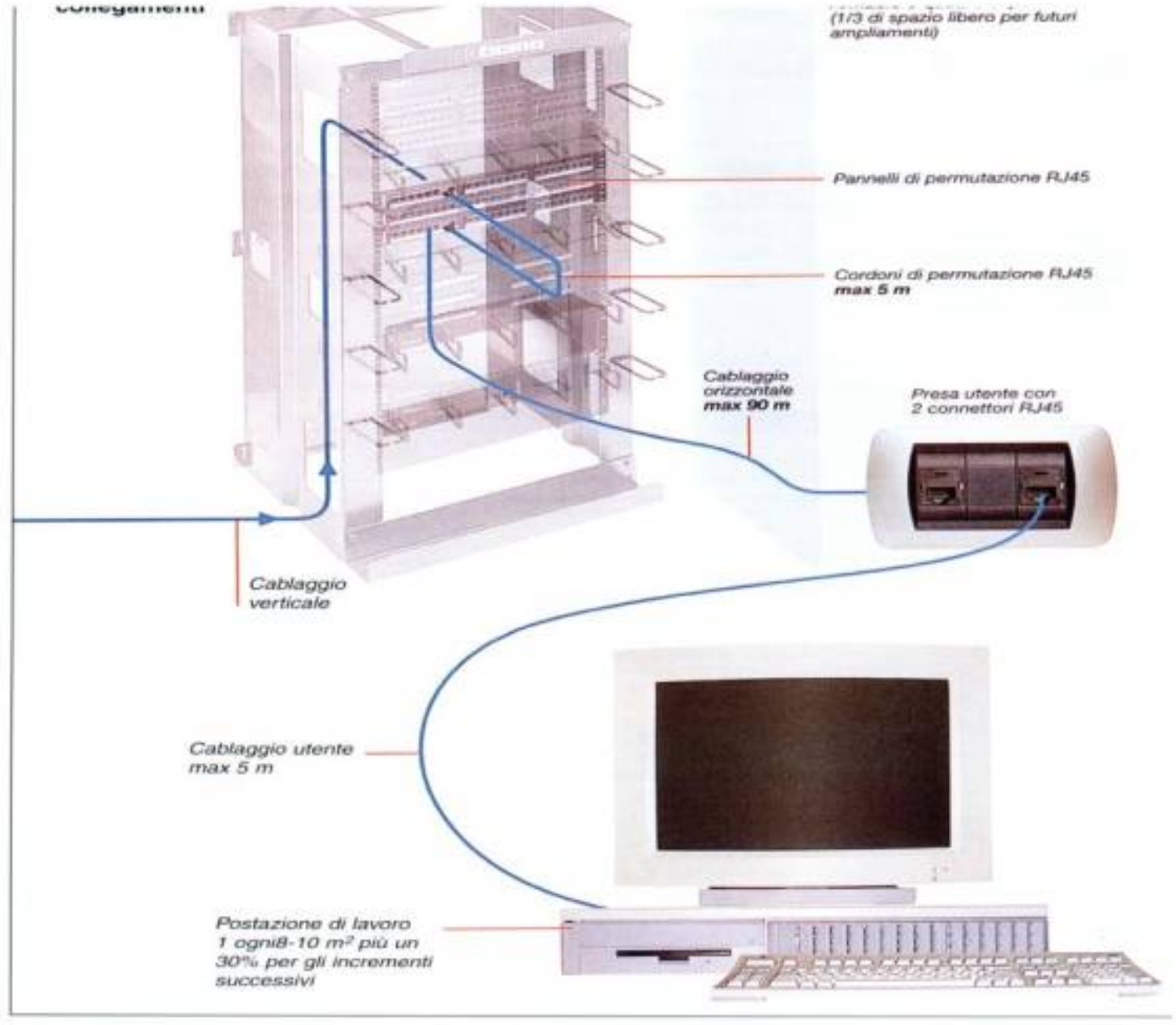
Cablaggio orizzontale

Primo piano ogni laboratorio è dotato almeno di un concentratore con porta di up link, dal quale si parte per realizzare la dorsale di piano fino a uno switch di piano.

Per ospitare lo switch, il patch panel e le apparecchiature elettroniche accessorie destiniamo un armadio (IDF) con una ridondanza di almeno il 30% sui collegamenti disponibili.

L'ubicazione dell'IDF deve essere scelta tenendo conto di due fattori importanti: la distanza dai concentratori e la vicinanza all'armadio verso il quale convergerà la dorsale di edificio.

Ipotizzando che le reti utilizzate siano Ethernet a 100Mbit, le distanze anzidette non devono superare i 100 metri tra il patch panel e la postazione utente.



Piano terreno ogni ambiente, tranne la Vicepresidenza e la Presidenza, è dotato di un concentratore con porta di up link, dal quale si parte per realizzare la dorsale di piano fino a uno switch di piano.

Allo stesso switch, con linee dirette, sono collegati gli uffici della Presidenza e della Vicepresidenza.

Un IDF di piano con una ridondanza di almeno il 30% sui collegamenti disponibili raccoglierà le apparecchiature del pian terreno con una struttura e un’ubicazione simili a quelle usate per il primo piano.

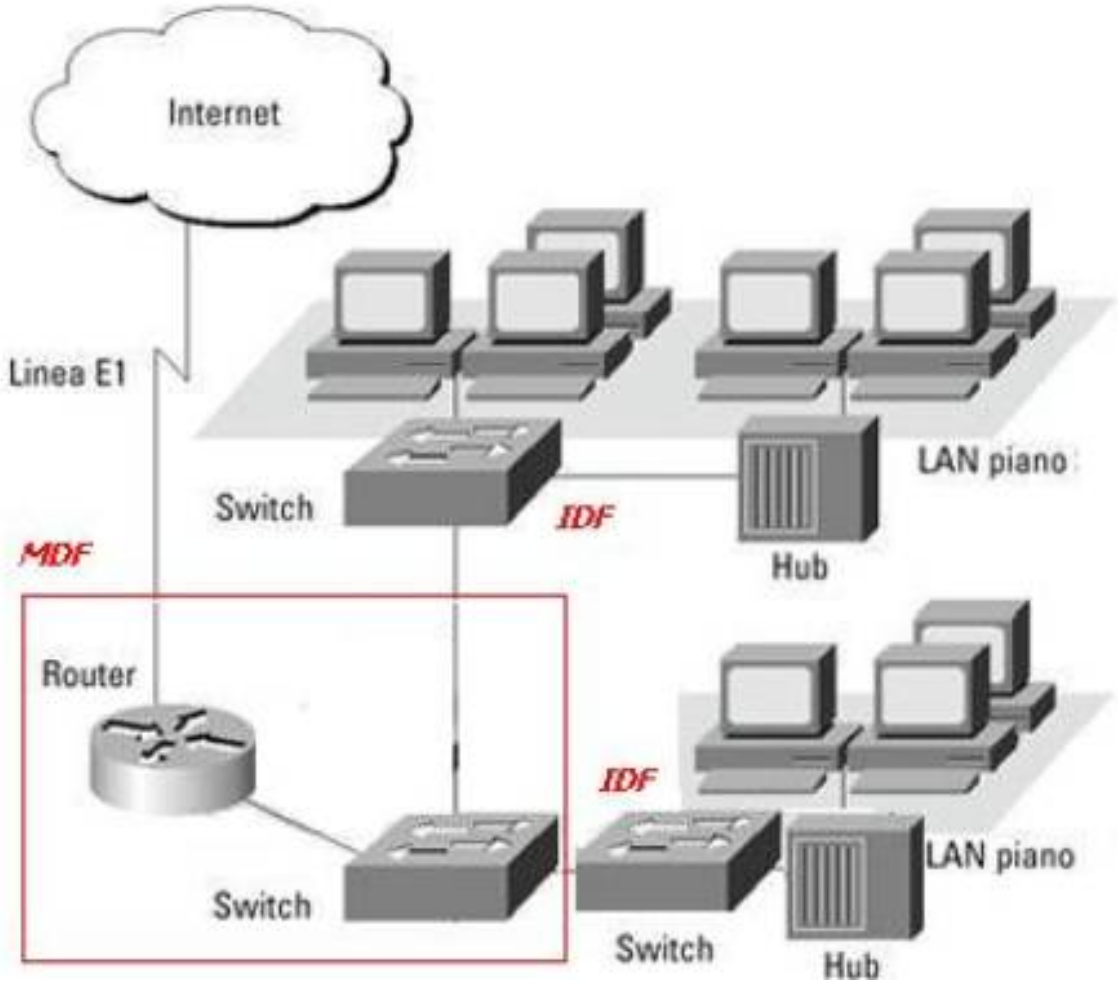
Cablaggio verticale

Sul pianterreno, un ulteriore armadio (MDF) ospiterà il “core switch”, la dorsale di edificio, il patch panel, il router e le apparecchiature elettroniche di supporto.

Considerando la consistenza delle strutture realizzate la rete non necessita di una dorsale particolarmente veloce. Potrebbe quindi essere mantenuto un collegamento a 100Mbit.

Qualora si volesse potenziare la dorsale, la scelta andrebbe fatta tra fibra ottica e gigabit su doppino di rame.

Ovviamente la scelta del tipo di switch da utrilizzare dipende dal tipo di dorsale che si vuole implementare.



Definita l’architettura di massima della rete passiamo ad analizzare l’organizzazione logica della rete e lo specifico delle strutture hardware da utilizzare.

Sia le indicazioni esplicite sulla sicurezza, sia considerazioni ovvie sulla necessita di controllare gli accessi e proteggere dati, applicazioni e configurazione, suggeriscono di utilizzare un'architettura Client-Server.

Le alternative d'ambiente per reti protette, in questo memento sono praticamente due: Windows e Linux (Unix lo tralasciamo dato che la realtà scolastica lo rende sovradimensionato). Nello specifico si può pensare Windows 2003 e Linux in una delle versioni disponibili sul mercato, di cui quella più diffusa e alla quale faremo riferimento è Red Hate.

A prescindere dal sistema operativo, valgono alcuni criteri organizzativi di carattere generale:

1. l'accesso è garantito da un server di account
2. la stampa passa attraverso un apposito server
3. le risorse condivise sono gestite da un server dedicato
4. i dati sensibili possono essere gestiti o attraverso specifiche protezioni previste direttamente dal DBMS o attraverso un server di database: la seconda sembra ridondante
5. l'accesso condiviso ad Internet è garantito dal router
6. per la rete conviene utilizzare indirizzi IP di classe C, visto che il router gestisce il NAT
7. non risulta conveniente usare un doppio protocollo per risorse ed internet, visto che i server fanno riferimento tutti a TCP/IP
8. per controllare le attività degli studenti compreso il loro eventuale accesso ad internet conviene utilizzare per le workstation sistemi operativi protetti quali Windows XP o lo stesso Linux. Qualora però, come ipotizzato nella soluzione, siano presenti in rete sistemi operativi variegati, risulta indispensabile avvalersi delle utility per il bloccaggio dei profili o addirittura le funzioni di terminal server previste per i sistemi operativi di rete
9. ogni classe avrà una sua cartella sul server come ogni gruppo all'interno della classe e gli account dovranno essere gestiti ad albero sfruttando le caratteristiche di ereditarietà dei diritti di accesso
10. la segreteria, il preside ed il vicepreside avranno loro ambienti protetti e potranno accedere ad altre risorse secondo un piano di sicurezza definito localmente
11. i server di rete avranno una collocazione che dipende dal loro livello di importanza e dalla loro visibilità, soprattutto per ridurre il broadcast. In particolare risulta conveniente collegare i server di laboratorio e di ufficio sugli switch di piano, mentre quelli di risorse vanno insieme al router sul core switch
12. per evitare intrusioni via internet dovrebbero essere sufficienti le funzioni di Natting e Patting del router. Qualora però si volesse un margine di sicurezza maggiore si potrebbere ricorrere ad un firewall fisico da porre tra la rete ed il router
13. per evitare i soliti conflitti di indirizzi IP conviene sfruttare le funzioni di DHCP ormai presenti su tutti i server e il DNS dinamico

Con riferimento ai sistemi operativi specifici riteniamo che:

1. l'Active Directory di Windows 2000 sia ridondante per la situazione esaminata
2. si possa sfruttare Linux come firewall e router
3. la visibilità trasversale tra i due ambienti debba essere garantita con l'installazione di Samba
4. per la posta elettronica attraverso server esterni siano sufficienti i client a corredo dei sistemi operativi (Outlook Express, Nautilus, Mozzilla, …)
5. per posta elettronica interna si possano usare Exchange e SendMail/Postfix

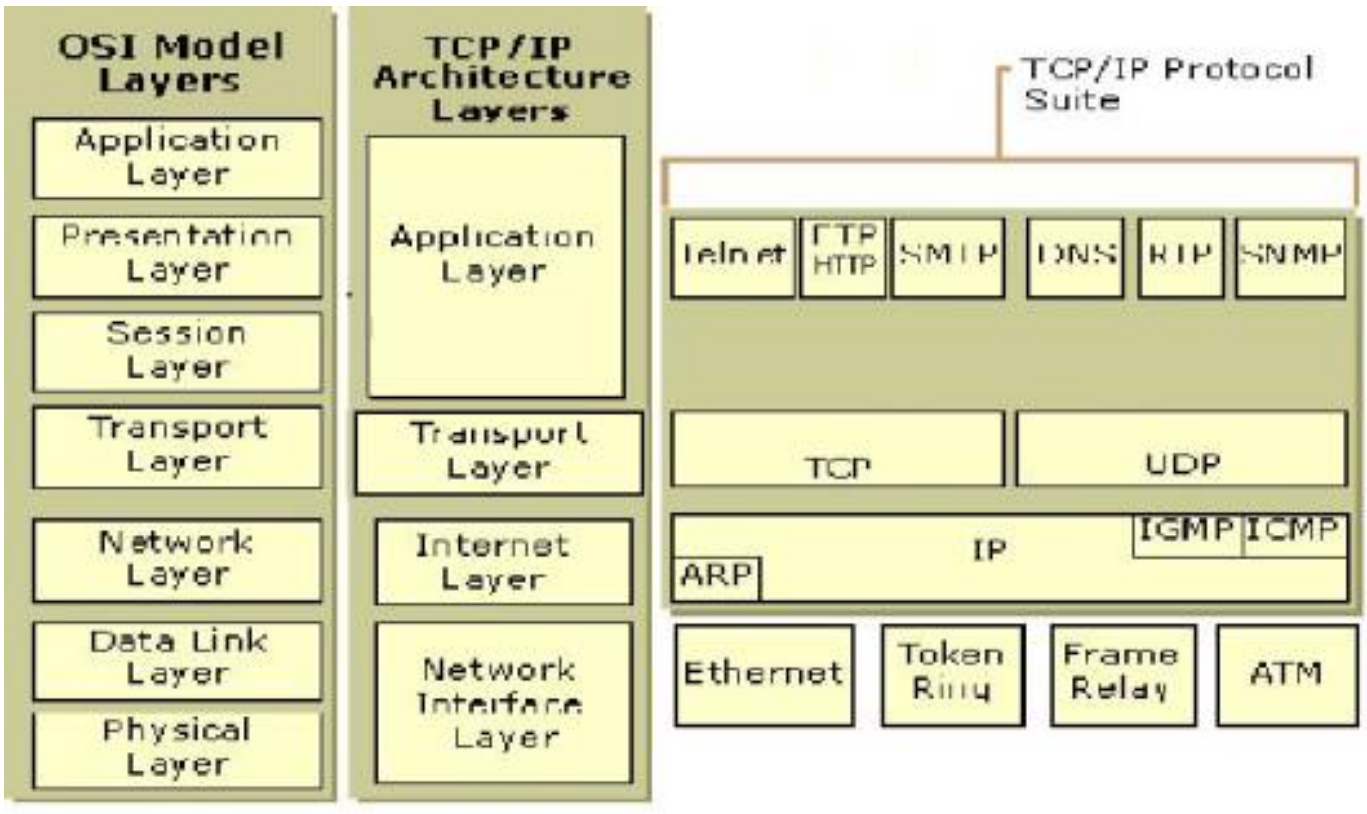
Configurazione dei Client

A prescindere dal sistema operativo (cambia solo l'interfaccia), sui client bisogna configurare correttamente il protocollo, la predisposizione per il DHCP, il DNS, l'accesso al dominio, il riferimento al router (gateway).

Per completare le risposte alle richieste della traccia contenute nel punto 2, possiamo precisare che:

1. la scelta della connessione Ethernet corrisponde ai livelli 1 e 2 del modello OSI
2. le attività del router fanno riferimento al livello 3 e 4
3. i servizi e le applicazioni fanno riferimento ai livelli superiori

La figura seguente illustra la relazione esistente tra modello OSI e TCP/IP



A cura di: Domenico Capezzuto e Antonio Garavaglia Itis Lagrange Milano,

Umberto Torelli Itis Feltrinelli Milano