8 Le infrastrutture telematiche e Internet

Questo capitolo nasce dall'esigenza di aggiornare e approfondire alcuni aspetti tecnici già trattati nella prima edizione del presente studio e dalla consapevolezza dell'importanza che le tecnologie di rete e le modalità di accesso ad Internet rivestono nel progetto di una Biblioteca Digitale (BD).
Il capitolo si può considerare diviso in due parti. La prima parte, dedicata ai fondamenti, alle tecnologie e ai protocolli di rete è da considerasi propedeutica alla seconda, nella quale si affrontano gli aspetti più rilevanti della progettazione dell'infrastruttura di rete per la BD.

8.1 Fondamenti

8.1.1 LAN, WAN e accesso Internet

Una LAN (Local Area Network), o rete locale, è costituita da un insieme di risorse (computer, periferiche) connesse in rete in un'area geograficamente chiusa. Un esempio di LAN è quello di una rete dati presente all'interno di un edificio.

Una WAN (Wide Area Network) è una rete di dati pubblica che utilizza connessioni dedicate o satellitari per collegare più reti locali (LAN) ed avente dimensioni maggiori di una rete metropolitana (MAN[138]).

Quando più reti LAN o MAN sono interconnesse, l'oggetto risultante si dice un internet (con la minuscola), e trattasi di una rete geografica dal punto di vista organizzativo anche se il suo ambito spaziale è piccolo.

La Internet (con la maiuscola) e' quindi l'internet per antonomasia, ed è in assoluto la WAN più conosciuta.

[138] Rete locale in cui la distanza dei collegamenti tra i nodi può raggiungere la distanza di alcune decine di chilometri

8.1.2 Le Reti Virtuali Private (VPN)

Nell'ambito della BD, sempre più spesso emerge l'esigenza di connettere sedi remote e singoli utenti che, pur essendo all'esterno, hanno la necessità di accedere alle risorse interne delle singole biblioteche. In casi come questi è necessario affidarsi alle **Virtual Private Network (VPN)**.

Nella sua forma più semplice una VPN connette sedi e utenti remoti di una o più strutture attraverso Internet. La connessione viene protetta per mezzo di un tunnel cifrato. Tale soluzione permette l'abbattimento dei costi legati all'adozione di connessioni dedicate quali le CDN. Vi sono alcuni scenari principali per i quali risulta conveniente utilizzare una VPN, per ognuno dei quali sarà necessario implementare la soluzione di sicurezza ottimale.

Accesso remoto utente

Questo tipo di approccio consente agli utenti mobili, dotati di una connessione Internet cifrata, di accedere alla rete locale della biblioteca in modo protetto.

Connettività LAN to LAN

Questa soluzione riduce notevolmente i costi di linee dedicate. Le strutture remote accedono in questo modo ad un traffico LAN attraverso una connessione Internet ad alta velocità, generalmente attraverso un router.

8.1.3 Architettura di rete

Quella che segue è una rapida rassegna delle più diffuse architetture di rete e ha lo scopo di evidenziarne le caratteristiche principali e il possibile impiego nella Biblioteca Digitale.

8.1.3.1 Centralizzata

L'architettura centralizzata prevede un'unità centrale, detta *Mainframe*, a cui sono connesse tutte le postazioni della rete, dette *Terminali*.

Ogni terminale agisce come periferica interattiva di ingresso/uscita per l'accesso alle risorse di rete e le sue uniche attività sono quelle di inserimento dati da tastiera e visualizzazione risultati su schermo.
Tutte le attività computazionali e di accesso alle risorse sono gestite dall'unità centrale che condivide i cicli di processore e la memoria (RAM e disco) tra tutti i terminali connessi alla rete.

Si tratta della più antica architettura di rete esistente ed ha il pregio di una completa centralizzazione delle attività di gestione.
Sebbene il suo utilizzo si sia notevolmente ridotto nel tempo, l'architettura centralizzata è ancora molto utilizzata nella gestione di grandi archivi e sono ancora molti i produttori di hardware e software che sviluppano server, applicazioni e servizi su tecnologia mainframe (IBM, Sun Microsystems, Compaq, Honeywell).

8.1.3.2 Client/Server

Si tratta dell'architettura attualmente più diffusa e prevede uno o più server per la gestione centralizzata delle risorse di rete (archivi, stampanti, file, ecc...) e postazioni di lavoro costituite da computer autonomi che eseguono localmente tutte le attività (esecuzione locale delle applicazioni).

Gli utenti accedono alle risorse di rete attraverso le postazioni di lavoro in seguito ad un processo di autenticazione gestito centralmente da server adibiti a tale scopo. I server di autenticazione (domain controller) mantengono il database degli utenti in cui sono definiti i diritti di accesso alle risorse (profilo utente).

Il principale vantaggio di questa architettura è costituito dalla centralizzazione dei profili utente che consente un controllo efficiente delle risorse e la possibilità di autenticazione dell'utente qualsiasi sia la postazione dalla quale quest'ultimo faccia accesso.

8.1.3.3 Peer-To- Peer

Nota nel mondo Windows come Workgroup (gruppo di lavoro), l'architettura peer-to-peer è senz'altro la più diffusa nelle piccole LAN aziendali poiché non richiede particolari conoscenze sistemistiche per la sua implementazione e manutenzione.

In una rete peer-to-peer ogni postazione mette a disposizione delle altre alcune risorse gestite localmente, come file, stampanti, unità ZIP, ecc...; i diritti di accesso alle singole risorse sono stabiliti localmente alle postazione e ciò rappresenta il limite più significativo di questa architettura che non consente la centralizzazione delle attività di amministrazione delle risorse e dei servizi, rendendo il modello non applicabile a reti di medie e grandi dimensioni (in realtà già sopra le 50 postazioni).
In sostanza in una rete peer-to-peer ogni postazione (peer) agisce sia da client (quando richiede l'accesso ad una risorsa posseduta da un altro peer) che da server (quando concede l'accesso ad una sua risorsa).

Il punto di forza delle reti peer-to-peer, oltre alla semplicità nell'amministrazione, risiede nella diffusione capillare delle risorse che consente agli utilizzatori di accedere a quelle che risultino in posizione più conveniente, come la stampante più vicina, o gestite da computer più performanti. Ciò comporta, però, un aumento sensibile nei costi di gestione della rete poiché moltiplica le risorse oltre le reali necessità e aumenta drasticamente i costi di manutenzione della rete.

Il Peer-to-Peer e Internet

L'approdo della tecnologia peer-to-peer in Internet (P2P) è diretta conseguenza della richiesta crescente di distribuzione di grossi contenuti, soprattutto multimediali, da parte di un'utenza sempre più esigente e di una rete sempre più capillare.

Fino all'arrivo del peer-to-peer, i provider Internet affrontavano (e tutt'ora affrontano in larga misura) il problema della distribuzione dei contenuti attraverso la realizzazione di reti CDN (*Content Delivery Network*).
Nelle CDNs i contenuti resi disponibile da un sito www o ftp vengono replicati su server di appoggio detti *Cache Server*, distribuiti in rete (Internet) in prossimità di confini di flusso significativi come, ad esempio, presso i pop dei più importanti service provider commerciali (punti di accesso Internet).

Il P2P estende il concetto di diffusione dei contenuti proprio delle reti CDN, facendo partecipare alla rete di distrubuzione lo stesso utente finale (peer). In questo modo, se un utente richiede l'accesso ad uno specifico file (risorsa), la sua richiesta può essere soddisfatta da altri utenti, anch'essi connessi e partecipanti alla rete di distribuzione. La scelta di chi fornirà la risorsa richiesta sarà fatta sulla base di criteri di valutazione della velocità di trasferimento (peer più "vicino", peer con accesso a banda più larga, ecc..).

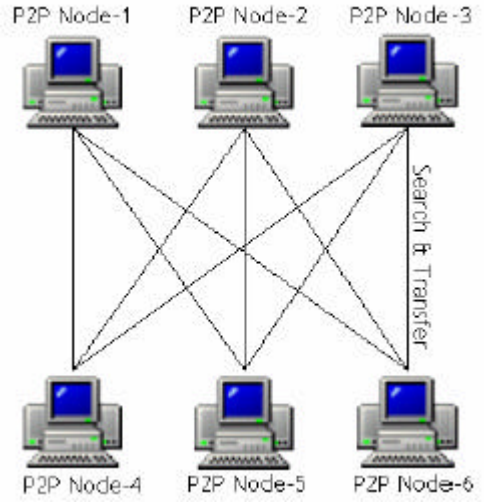
La prima grande esperienza di P2P è stata quella di Napster (1999), la grande rete di distribuzione di file musicali cresciuta in pochissimi anni fino a toccare la vetta di 1,57 milioni di utenti contemporanei nel febbraio del 2001.
Il fenomeno Napster, conclusosi nel 2002 dopo pochi anni dalla sua nascita per problemi legati al copyright, ha dimostrato le potenzialità delle tecnologie P2P nella distribuzione di contenuti di grandi dimensioni via Internet ed è stato seguito da molte altre esperienze tra le quali quella di KaZaA, Gnutella, Morpheus, FastTrack, Grokster, Groove, Chord, e molte altre.

Sebbene il concetto alla base delle varie implementazioni di P2P sia sempre lo stesso, ossia il fatto che l'utente finale partecipa a realizzare la rete di distribuzione, esistono attualmente diversi tipi di P2P [0].

Fondamentalmente le architetture P2P si possono distinguere in due grandi categorie: Centralizzato e Decentralizzato.

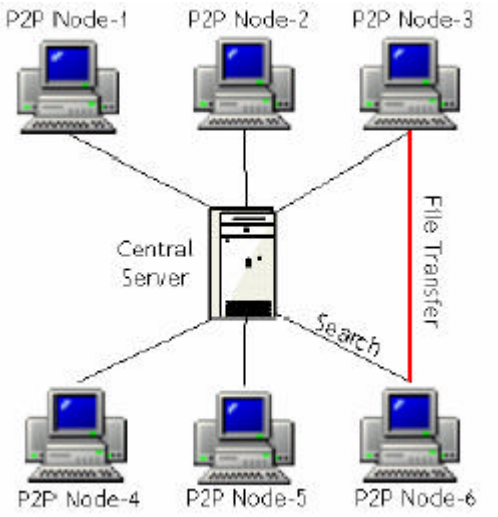
P2P Centralizzato

Si tratta di una architettura in cui esiste un nodo centrale (server) che mantiene gli indici delle risorse disponibili sui peer della rete e gestisce le funzioni di ricerca. In questo tipo di struttura ogni peer che richiede una risorsa effettua una ricerca sugl'indici del server il quale individua i peer in grado di soddisfare la richiesta. Una volta individuata la risorsa viene stabilita una connessione diretta tra il peer che ha fatto la richiesta ed uno di quelli che hanno la disponibilità della risorsa cercata, sulla base della presunta efficienza di trasferimento. Un esempio di P2P centralizzato e Napster.



P2P Decentralizzato

Nell'architettura decentralizzata non esiste un server che effettua operazioni di ricerca. Ogni nodo che richiede una risorsa inoltra una richiesta ai peer più prossimi i quali, a loro volta, la inoltrano ad altri peer. Il processo ha termine quando la risorsa è stata individuata e comunque dopo un numero prefissato di inoltri (hop). Un esempio di questo tipo di P2P è la prima versione di Gnutella.

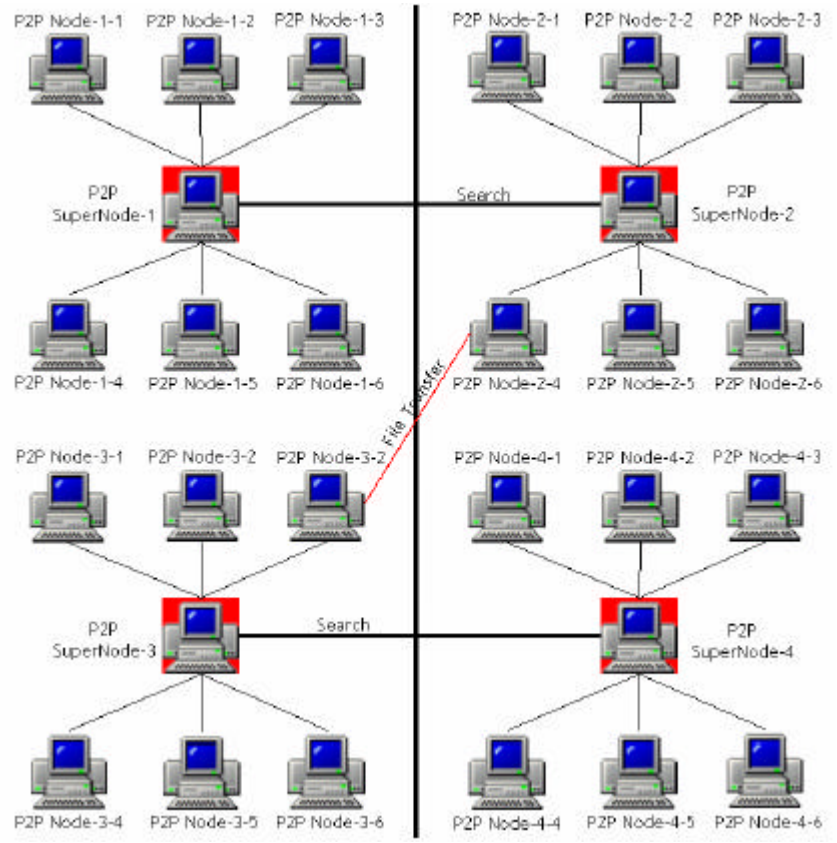


P2P Decentralizzato Controllato

Costituisce l'ultima generazione nell'architettura P2P ed è una variante del precedente a cui si aggiungono alcuni "super-peer" che hanno il compito di facilitare le operazioni di ricerca delle risorse distribuite tra i nodi.

Alcune implementazioni di P2P di ultima generazione [0] prevedono la segmentazione dei file in modo tale che nessun peer possieda l'intero file ma solo dei frammenti. In questo modo si raggiungono diversi scopi:

- nessun peer possiede il file completo: si possono applicare restrizioni nell'accesso alle risorse (rispetto del copyright);
- il download del file avviene recuperando i frammenti da più peer in parallelo: la velocità di trasferimento è approssimativamente quella permessa dalla larghezza di banda di downlink del peer richiedente (saturazione della banda);
- se un peer che trasmette un segmento ha dei problemi si perde solo il segmento e non l'intero file: è garantita la continuità nella distribuzione dei contenuti (fault tollerance).



Il P2P e la BD

Attualmente sono molti gli studi sull'impiego delle tecnologie P2P in ambito Biblioteca Digitale. L'interesse che queste tecnologie suscitano e senza dubbio dovuto alla ricerca di soluzioni atte a consentire la distribuzione dei contenuti multimediali, che sono il tratto caratteristico che distingue la BD da una biblioteca tradizionale.

Particolarmente interessante per l'ampiezza degli argomenti trattati e per l'alto valore scientifico risulta il lavoro svolto dallo *Stanford Digital Library Technologies Project*[139] nell'ambito del progetto *NSF Digital Libraries Foundation Phase 2*[140] della *National Science Foundation*, in collaborazione

[139] http://www-diglib.stanford.edu
[140] http://www.dli2.nsf.gov

con *Library of Congress*[141], *Berkeley University*[142], *Alexandria Digital Library Project*[143], *California Digital Library*[144] e altri.
Tra i moltissimi argomenti trattati nel campo del P2P[145] dallo Stanford Digital Library Technologies Project, ne emergono alcuni di particolare rilevanza tra cui quelli relativi ai metodi di ricerca dei contenuti e alla loro protezione.

8.1.3.4 Architettura ibrida: il caso WinFrame/MetaFrame

L'architettura di tipo ibrido rappresenta una sorta di ritorno al passato poiché introduce elementi tipici dell'architettura centralizzata su una struttura di tipo client/server, realizzando una felice fusione che trae forza dalle caratteristiche migliori di entrambe le architetture.

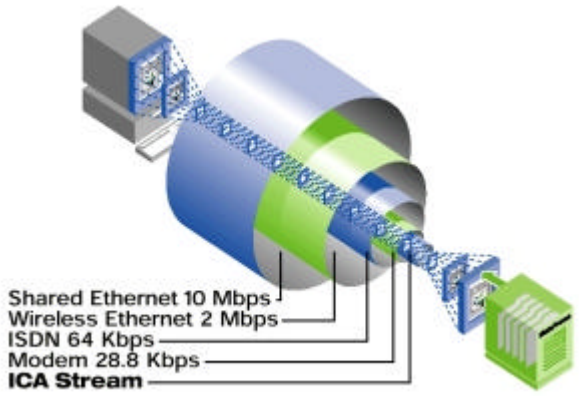
Quando si parla di architettura ibrida si fa soprattutto riferimento alle ultime generazioni di sistemi operativi Microsoft: Windows NT 4.0 Terminal Server Edition, Windows 2000/XP e la recentissima tecnologia .NET .
In realtà l'esplosione nell'uso delle architetture miste nasce dal successo del sistema operativo server WinFrame di Citrix[146].
Nato dall'integrazione tra la tecnologia NT di Microsoft e le funzionalità del protocollo ICA (*Indipendent Computing Architecture*) sviluppato dalla stessa Citrix, WinFrame consente ai client non solo di utilizzare le risorse di rete rese disponibili dal server (file, stampanti, ecc...) ma anche di accedere ad applicazioni windows in esecuzione sul server stesso, trasformando il client in una sorta di terminale grafico detto *Windows Terminal* o *Winstation* dal quale l'utente è in grado di utilizzare i programmi come se fossero in esecuzione sulla propria postazione.

Il funzionamento del protocollo ICA prevede che sulla rete transitino sostanzialmente i dati relativi alla pressione dei tasti della tastiera e ai

141 http://lcweb2.loc.gov/ammem/dli2
142 http://elib.cs.berkeley.edu
143 http://www.alexandria.ucsb.edu
144 http://www.cdlib.org
145 http://www-db.stanford.edu/peers
146 http://www.citrix.com

movimenti del mouse, mentre, per quanto riguarda le immagini, il protocollo effettua una memorizzazione temporanea delle immagini (caching) in un determinato momento e trasporta successivamente sulla rete solo le modifiche relative all'immagine di partenza (refresh). Questa modalità di funzionamento determina un'occupazione di banda estremamente limitata, valutabile, in media, tra 10 e 20 Kbps (1 Kbps= 1000 bit per secondo).

Nella figura che segue viene rappresentata graficamente l'occupazione di banda relativa di una connessione ICA rispetto alla larghezza di alcuni canali trasmessivi standard quali quelli rappresentati da una rete Ethernet, una rete Wireless, una connessione ISDN e una connessione con modem analogico.



Proprio grazie alla ridotta occupazione di banda il protocollo ICA rappresenta una delle migliori soluzioni per la realizzazione di strumenti di tele-lavoro, poiché risulta efficiente sia su normali connessioni Internet che su collegamenti punto-punto realizzati da modem analogici.

Un altro vantaggio dell'architettura ibrida con protocollo ICA è rappresentato dalla possibilità di realizzare servizi multipiattaforma. ICA infatti consente l'esecuzione remota di applicazioni windows native anche da postazioni DOS, Mac, Unix/Linux, Java e Windows CE.

A partire da Windows NT 4.0 Terminal Server Edition, parte della tecnologia di Citrix, ad esclusione del protocollo ICA, è stata inclusa nei sistemi operativi Microsoft sottoforma di un servizio detto *Terminal Service*[147]. Con la nascita di Terminal Service Microsoft a messo a disposizione la possibilità di realizzare architetture ibride senza l'aggiunta di altre componenti software, con il solo ausilio del protocollo RDP (*Remote Desktop Protocol*).

Per quanto riguarda il protocollo ICA, è bene sottolineare che la sua importanza non è calata poiché rappresenta ancora l'unico protocollo multipiattaforma in ambiente Microsoft (RDP non lo è) e il solo capace di realizzare efficienti connessioni anche su collegamenti a banda molto stretta (RDP non ha la stessa efficienza di banda). Attualmente Citrix distribuisce un prodotto che rappresenta l'evoluzione di WinFrame, chiamato *MetaFrame*, che si configura come un *add-on* ai sistemi operativi server di Microsoft.

Di recente si sono affacciati sul mercato altri interessanti prodotti per la realizzazione di architetture ibride come, ad esempio, il sistema *Tarantella*[148] basato su tecnologia Java che rappresenta una sorta di "meta sistema operativo" capace di interfacciarsi con diversi server di applicazioni quali Microsoft Terminal Server, Citrix MetaFrame, Mainframe, Unix/Linux server, attraverso i protocolli RDP, X11, VT e IBM 3270/5250.

L'importanza di una tale architettura nell'ambito della BD sarà oggetto di approfondimento più avanti nel paragrafo "*Investimento e accessibilità - I protocolli RDP e ICA*".

[147] http://www.microsoft.com/windows2000/techinfo/howitworks/terminal/rdpfandp.asp
[148] http://www.tarantella.com

8.2 Protocolli e tecnologie a confronto

8.2.1 Cenni generali

Lo scopo di un protocollo di comunicazione è permettere a due interlocutori di scambiare informazioni utilizzando una rete di telecomunicazioni. Un protocollo di comunicazione è definito da un insieme di regole, che possiamo suddividere in tre categorie:

- algoritmi, che specificano come gli interlocutori si comportano per accedere alla rete e come funziona la rete internamente;
- temporizzazioni, che determinano le tempistiche di esecuzione degli algoritmi;
- formati, che descrivono come devono essere strutturate le informazioni che gli interlocutori si scambiano.

Questa definizione può sembrare molto astratta; in realtà molte azioni quotidiane si basano su di un uso implicito di protocolli di comunicazione. Due esempi vicini alla nostra esperienza sono gli accessi al sistema telefonico ed al sistema postale. Quando si esegue una telefonata si devono seguire delle regole (un protocollo) per riuscire a comunicare: il protocollo prevede il sollevamento del microtelefono, la composizione del numero telefonico dell'interlocutore, l'attesa della risposta, e così via. Anche per accedere al sistema postale è necessario seguire un protocollo, che prevede ad esempio l'indicazione dell'indirizzo del destinatario in una posizione opportuna sulla busta (altrimenti difficilmente la lettera sarà recapitata).

I protocolli per le reti di telecomunicazioni sono sovente molto articolati. Essi stabiliscono le modalità secondo le quali un utente può accedere ai servizi di rete e i meccanismi secondo cui tali servizi vengono forniti, quindi le regole secondo le quali gli utenti sono in grado di comunicare. Per la realizzazione dei protocolli di rete, le industrie si sono orientate, fin dalla nascita delle reti di telecomunicazioni, verso architetture a strati. Tali

strutture sono definite suddividendo l'insieme di regole per la comunicazione tra utenti in una serie di "protocolli più semplici" che, combinati, realizzano funzioni via via più complesse. Ogni strato (o livello) fornisce servizi agli strati superiori e li realizza basandosi sui servizi ad esso forniti dagli strati inferiori. Ovviamente gli strati superiori operano ad un livello logico di maggior complessità, e forniscono servizi più sofisticati rispetto agli strati inferiori. Ogni strato è in grado di richiedere o fornire servizi solamente agli strati adiacenti e ignora completamente che cosa accada negli altri strati della architettura; gli strati adiacenti comunicano mediante le cosiddette *primitive di interfaccia*.

Queste caratteristiche comportano molti vantaggi: permettono di semplificare la fase di progetto, di manutenzione e di aggiornamento del software, poiché il singolo strato è molto più semplice dell'insieme di regole complessivo; permettono di modificare uno strato del protocollo senza dover intervenire sugli altri strati, purché vengano rispettate le interfacce con gli strati adiacenti; inoltre, i servizi forniti dagli strati inferiori possono essere utilizzati da più strati adiacenti superiori contemporaneamente.

Questi concetti sono presenti in tutte le architetture delle reti di comunicazioni sviluppate verso la fine degli anni '60, quali ad esempio ARPANET, SNA (IBM) e DNA (Digital). Purtroppo però la stratificazione non è avvenuta nello stesso modo nelle diverse architetture: tutte le architetture di rete citate sono a strati, ma gli strati sono diversi tra loro, quindi le architetture non sono compatibili.

Questa situazione di incompatibilità ha portato alla necessità di stabilire standard comuni; l'ISO è l'organismo internazionale che si è occupato della standardizzazione delle architetture di rete e ha proposto una famiglia di standard nota con il nome OSI (Open Systems Interconnection), che ne descrive le caratteristiche (per ulteriori dettagli si veda l'appendice A).

Parallelamente al mondo dei protocolli si sviluppa l'altrettanto intricato universo delle tecnologie di trasmissione dati, costituito da un'ampia gamma di dispositivi hardware (schede di rete) e supporti fisici (cavi) pensati per soddisfare le esigenze di ogni tipo di clientela, dall'utente privato alla grande azienda.

8.2.2 La rete della Biblioteca Digitale

Senza voler troppo dilungarsi in dettagli tecnici, che vanno oltre lo scopo della presente sezione e per i quali si rimanda alle appendici A e B, un'analisi di tipo costi/benefici suggerisce, per la realizzazione della rete dati della BD, l'utilizzo della tecnologia Fast Ethernet (100 Mbps) su cablaggio di tipo UTP categoria 5e o 6 per i semplici collegamenti tra PC e, budget permettendo, su fibra ottica multimodale per i collegamenti di dorsale.

Lo stack di protocolli utilizzato sarà quello TCP/IP, che grazie alla sua grandissima diffusione, agli applicativi contenuti e alla capacità di transitare sulla rete Internet è di gran lunga la scelta più indicata.

L'elettronica di rete non dovrebbe prevedere l'utilizzo di hub, bensì l'impiego di switch (che forniscono prestazioni nettamente superiori ad un costo relativamente contenuto) e, dove necessario, di router (per ulteriori dettagli si veda l'appendice C).

L'accesso ad Internet sarà garantito da un collegamento dedicato di nuova generazione di tipo xDSL (si veda l'appendice D): ADSL nel caso di domanda di banda limitata e/o budget ridotto, HDSL nel caso di maggior richiesta di banda.

8.3 Principi di progettazione di rete per la Biblioteca Digitale

8.3.1 Introduzione

Scopo della presente sezione è la definizione dei principi che devono guidare il progetto dell'infrastruttura di rete nell'ambito di una biblioteca che si appresti a trasformarsi in una Biblioteca Digitale (BD) o, meglio, in una Biblioteca Ibrida, al cui interno una parte significativa e crescente di prodotti e servizi si orienti al digitale.

Affinché una biblioteca tradizionale si possa trasformare in BD è necessario, quindi, che la rete sia capace di sostenere la distribuzione e l'accesso ai contenuti in formato digitale (cataloghi, immagini, filmati, ecc...).

In molti casi una BD realizza una condivisione di risorse tra più biblioteche tradizionali estendendo la rete oltre i confini architettonici delle singole biblioteche e costituendo una rete di tipo geografico (LAN/WAN).

Inoltre la BD dovrà mettere a disposizione i propri contenuti "digitali" non solo agli utenti interni ma anche a coloro che accederanno via Internet attraverso portali opportunamente realizzati per la "navigazione" e la consultazione dei contenuti stessi (accesso Web).

L'accessibilità via Web alle risorse della BD implica la necessità di implementare forme di protezione delle risorse e di autenticazione dell'utenza che facciano uso delle più recenti tecnologie (Access List, Firewall, VPN, ecc..).

Poiché quella della BD è una rete fortemente orientata ai servizi, molto più di qualsiasi altro sistema di automazione tradizionale, saranno questi a determinare le tecnologie con le quali verrà implementata l'infrastruttura.

I paragrafi che seguono cercano di fornire le linee guida necessarie a chi, a vario titolo, si trova coinvolto nel progetto di una nuova rete o nella ristrutturazione di una esistente con il compito di renderla adatta a sostenere i servizi che caratterizzano una BD, individuando gli strumenti più opportuni al raggiungimento degli obiettivi prefissati

8.3.2 Chi partecipa al progetto di una rete?

È importante comprendere che il progetto della rete per la BD non deve essere considerata un'attività da delegare totalmente al progettista.
Al contrario è necessario che ogni Biblioteca partecipi attivamente all'individuazione delle tipologie e della qualità dei servizi che si intendono implementare, permettendo così al progettista di definire in modo appropriato gli obiettivi da raggiungere.

Poiché la BD è una struttura fortemente rivolta ai servizi è utile coinvolgere gli stessi utilizzatori (operatori della biblioteca e utenti finali) nella definizione delle reali esigenze e rendere tutti partecipi del cambiamento.

A tal fine è necessario che la Biblioteca individui uno o più referenti interni selezionati tra i propri tecnici e bibliotecari, che fungano da raccordo tra la Biblioteca stessa e il pool di progettisti che avrà il compito di realizzare l'infrastruttura di rete.

I referenti interni alla Biblioteca avranno quindi due importanti compiti:

- coinvolgere gli operatori e gli utenti della Biblioteca nel progetto della BD così che ognuno possa dare il proprio contributo alla definizione degli obiettivi;
- far comprendere ai progettisti il modo con cui le risorse saranno utilizzate in termini di intensità e qualità dei servizi.

In questo modo si ottengono due risultati fondamentali:

- si evita il rischio che alcuni operatori percepiscano le attività legate alla realizzazione della nuova struttura come estranee al proprio ruolo (cosa che purtroppo si verifica molto spesso) e che agiscano più o meno consciamente da freno allo svilupparsi dei nuovi servizi della BD;
- si permette ai progettisti di scegliere l'architettura e le tecnologie più adatte al raggiungimento degli obiettivi prefissati.

8.3.3 Gli Standard e la loro funzione

Il rispetto degli standard nella progettazione di una rete è un principio fondamentale quale che sia l' architettura e la tecnologia scelta poiché garantisce l'interoperabilità tra i sistemi.
È utile chiarire che il termine interoperabilità in questa sede sta ad indicare la capacità di sistemi realizzati da costruttori diversi (multivendor) di "comprendersi" e lavorare assieme e non deve essere confuso con il concetto di interazione tra strutture ed istituti di diversa natura quali biblioteche, archivi e musei.

Presupposto fondamentale per l'interoperabilità multivendor è la convergenza dei sistemi su un set di standard condivisi, ossia su di un insieme di regole che determinano prestazioni e funzioni dei sistemi stessi. In sostanza: due o più sistemi che rispettino uno standard X saranno in grado di costituire un sistema omogeneo più ampio che rispetti ancora le specifiche definite dallo stesso standard.

Progettare selezionando fornitori, materiali e servizi che rispettino determinati standard consente di svincolarsi dalle tipiche costrizioni derivanti dalla scelta di sistemi proprietari quale, ad esempio, il vincolo eccessivo che si crea col fornitore primario del sistema. Ciò permette alla rete di crescere e adeguarsi nel tempo potendo attingere ogni volta alla soluzione più adeguata sia in termini economici che prestazionali, agendo in modo efficace sulla leva della concorrenza. Un sistema proprietario

potrebbe, inoltre, non trovare più in futuro alcun supporto tecnico/commerciale se il fornitore, per qualsiasi motivo, decidesse di abbandonare quello specifico prodotto.

Nella realizzazione di una rete una questione non irrilevante è quella che concerne la fase di collaudo finale dell'intera infrastruttura al fine di attestarne la reale rispondenza alle specifiche fissate in fase di progetto. All'esito di questa attività, in genere, è vincolato il pagamento dei fornitori e installatori del sistema. Anche sotto questo aspetto gli standard offrono un aiuto fondamentale in quanto forniscono il set di test da effettuare sia sull'intero sistema che su ognuna delle parti costituenti.

La scelta di uno standard influenzerà anche la successiva fase di selezione delle applicazioni e dei servizi a cui la rete fornirà supporto. Di conseguenza: più diffuso e condiviso è lo standard prescelto, più sarà ampia la scelta dei software compatibili, con evidenti riflessi positivi sulla capacità dell'infrastruttura di fornire le funzionalità desiderate.

Cercando di riassumere, possiamo dire che muoversi nel rispetto degli standard permette di:

- garantire le prestazioni dell'infrastruttura di rete;
- assicurare la capacità di scambiare informazioni con sistemi confinanti o remoti;
- svincolarsi da particolari fornitori/installatori;
- garantire supporto tecnico alla rete;
- scegliere la miglior soluzione sulla base del rapporto costi/benefici desiderato;
- valutare in modo certo le prestazioni della rete;
- costruire un ambiente compatibile per applicazioni e servizi.

Naturalmente il rispetto degli standard presuppone la conoscenza di quelli disponibili e la capacità di scegliere quelli più adatti alla rete che si intende realizzare.
Nella realizzazione delle infrastrutture di rete, con particolare riferimento alle LAN, si parla ormai da tempo di cablaggio strutturato, intendendo con questa definizione una serie di regole che consentono di realizzare una distribuzione degli accessi alla rete in grado di sostenere sviluppi e mutazioni degli ambienti di lavoro.
Nell'ambito del cablaggio strutturato, che sarà oggetto di uno specifico paragrafo, esistono alcuni importanti standard ampiamente utilizzati a cui è necessario fare riferimento (vedi appendice E). Tali standard tendono a coprire tutte le fasi del progetto, dell'installazione, dell'esercizio e della manutenzione dell'infrastruttura di rete.

Ogni standard garantisce delle prestazioni e impone allo stesso tempo dei costi. Per questo motivo è importante affrontare tutti gli aspetti che vengono passati in rassegna nei prossimi paragrafi al fine di essere preparati ad operare la scelta più conveniente.
In ogni caso nessun progetto di infrastruttura di rete deve trascurare la questione degli standard: dal committente al progettista fino al tecnico che si occupa del cablaggio fisico, tutti gli attori che concorrono alla realizzazione della rete devono concordare su standard condivisi e soprattutto dimostrare di essere in grado di garantire tali standard.

Nel caso di gare, un capitolato tecnico dovrà riportare in modo preciso e dettagliato l'elenco degli standard prescelti in riferimento, anche, alle specifiche prestazionali definite dal progetto.

8.4 Obiettivi della progettazione (concetti generali)

I paragrafi che seguono rappresentano una rassegna degli obiettivi che la progettazione della rete della BD deve perseguire allo scopo di realizzare

una infrastruttura capace di soddisfare le esigenze dei servizi e delle applicazioni.

Efficienza e affidabilità

Garantire l'efficienza a l'affidabilità della rete significa consentire ad applicazioni e servizi di raggiungere il livello di fruibilità desiderato.
Questo importante obiettivo si raggiunge quando, esaminate le esigenze dei servizi e delle applicazioni, si opera la scelta tecnologica che meglio si adatta alla rete che si deve realizzare.
Per far ciò è necessario saper valutare il flusso dati che i servizi e le applicazioni generano (quantità di dati che transita attraverso la rete) in relazione anche al livello prestazionale desiderato, determinare i potenziali colli di bottiglia ed avere un ampia visibilità sulle diverse tecnologie disponibili nonché sui costi e i benefici che ciascuna di esse comporta.
Con il termine "tecnologie" si intendono quelle relative ai tipi di cablaggio (mezzi trasmissivi), ai dispositivi passivi e attivi di rete (hub, switch, router, bridge e firewall) e ai sistemi operativi (windows, unix, mac, ecc..).

Stabilità

Con il termine stabilità si intende la capacità di una rete e delle sue postazioni di rimanere inalterate ed immuni da interventi non autorizzati.
Una rete correttamente progettata deve consentire solo ad alcuni soggetti autorizzati la possibilità di cambiare la configurazione dei servizi, delle applicazioni e delle postazioni di lavoro.
La rete deve inoltre possedere sufficiente ridondanza di risorse in modo da limitare al minimo la frequenza e la lunghezza dei periodi di inattività dovuti a malfunzionamenti di alcune sue parti (servizi, applicazioni, dispositivi e postazioni).

Scalabilità

Per scalabilità si intende la capacità di una rete di sopportare, senza cali sensibili nelle prestazioni, incrementi del numero dei servizi, delle applicazioni disponibili e delle postazioni di lavoro.

Questo scopo si raggiunge attraverso una corretta analisi delle possibili esigenze future della rete ed una progettazione che segua i principi del "cablaggio strutturato".

Sicurezza

Il concetto di sicurezza all'interno di una rete abbraccia molti aspetti, tutti egualmente importanti e vitali.

In un progetto di rete ben realizzato deve essere garantita l'integrità e la protezione dei dati sensibili, la protezione delle risorse da accessi indesiderati, il controllo degli accessi esterni alla rete (per esempio da Internet) e l'accessibilità alla rete stessa.

Tutti questi aspetti devono essere garantiti attraverso i più attuali strumenti hardware e software quali i sistemi di backup, le protezioni rese disponibili dai diversi "file system", i sistemi antivirus, i profili utente, le liste di accesso, i firewall ed i router.

Accessibilità

Garantire l'accessibilità ad una rete significa permettere ad utenti esterni riconosciuti di utilizzare risorse da postazioni remote.

Ciò risulta necessario nel caso di utenti che accedano via Internet alle risorse rese disponibili dalla rete, nei casi in cui sia utile avere a disposizione strumenti di tele-lavoro o nei casi di collaborazione con strutture esterne.

Il concetto di accessibilità è strettamente legato a quello di sicurezza data l'ovvia necessità di autenticare gli accessi esterni, realizzabile tramite l'integrazione tra le tecnologie delle reti virtuali private (VPN) e le funzionalità di router e firewall.

Le VPN, in particolare, risultano fondamentali nella realizzazione dell'infrastruttura di rete per la BD in quanto consentono di estendere in modo sicuro le LAN oltre i confini delle singole biblioteche.

Controllo dei costi e salvaguardia dell'investimento

Il controllo dei costi è un aspetto che è fondamentale affrontare in fase di progetto poiché influisce direttamente sulla scelta delle tecnologie (su base costi/benefici) e determina la capacità di mantenere nel tempo il grado di efficienza della rete.

Salvaguardare l'investimento significa scegliere tecnologie che abbassino il più possibile il grado si obsolescenza della rete e garantiscano bassi costi di gestione ed upgrade.

Questo scopo viene raggiunto anche attraverso l'utilizzo di tecnologie RDP e ICA (Citrix MetaFrame) per la realizzazione di "server di applicazioni" che mantengano bassi i livelli di risorse necessarie sulle singole postazioni di rete.

8.4.1 Efficienza e affidabilità - Analisi dei flussi dati

L'efficienza e l'affidabilità di una rete, spesso, sono le caratteristiche che più delle altre vengono percepite dagli utilizzatori dei servizi poiché determinano, rispettivamente, velocità di accesso e disponibilità delle risorse.

Sebbene altri fattori concorrano al raggiungimento del livello di fruibilità delle risorse e dei servizi di cui gli utenti della rete necessitano, questo aspetto risulta senz'altro essere il più significativo in quanto influenza in modo determinante le scelte tecnologiche.

Come è già stato accennato in precedenza, il rispetto dei requisiti di efficienza e affidabilità è possibile solo se si è stati in grado di determinare, il più precisamente possibile, le esigenze di servizi e applicazioni in termini di flusso dati prodotto. Da questa analisi, infatti, deriva la capacità di individuare i potenziali colli di bottiglia e selezionare la tecnologia più opportuna per la realizzazione dell'infrastruttura di rete.

Esigenze dei servizi, delle applicazioni e degli utenti: la raccolta delle informazioni

Alla base dell'analisi dei flussi sta la raccolta dei dati relativi alle esigenze che caratterizzano l'attività degli utenti ed il funzionamento di servizi e applicazioni [0].
Sebbene anche il progettista sia, anche in questa fase, pienamente coinvolto, il contributo più importante al buon esito di questa attività viene dato dai responsabili del progetto per il committente (i referenti della Biblioteca) e da tutti i futuri utilizzatori della rete che si rendano disponibili a fornire dettagli sulla loro attività e sulle modalità con cui utilizzano o intendono utilizzare le diverse risorse.

In sostanza sono due gli aspetti che caratterizzano il flusso dati prodotto da un'applicazione o da un servizio: il modo di operare di questi e il tipo e l'intensità d'uso che ne fanno le diverse categorie di utenti.

Per quanto concerne il primo aspetto (modo di operare dei servizi) è necessario conoscere in maniera approfondita le applicazioni e la loro implementazione e, perciò, risulta fondamentale una stretta collaborazione tra i responsabili del progetto, che devono individuare il set di applicazioni/servizi su cui focalizzare l'attenzione, il supporto tecnico offerto dai fornitori delle applicazioni e il progettista della nuova rete.
In generale ogni applicazione/servizio ha le proprie caratteristiche e utilizza la rete secondo criteri specifici: un servizio di posta elettronica, ad esempio, invierà sulla rete pacchetti di dimensione e con modalità del tutto diverse da un'applicazione che gestisca la videoconferenza.

Nonostante questa specificità, si possono comunque fare alcune considerazioni [0] utili nella valutazione dei flussi prodotti dai servizi in rete, pur ricordando che l'analisi non può essere completa senza che sia stata affrontata la questione relativa alle modalità e intensità d'uso che gli utenti fanno di questi servizi, questione di cui si parlerà più avanti nel presente capitolo.

Categoria	Dimensione media in MB (1MB=1.000.000 byte)
E-mail	0,01
Fogli elettronici	0,1
Schermate (Terminali Windows)	0,5
Documenti	1
Immagini	10
Oggetti Multimediali	100
Database	1000

A questo proposito vediamo una tavola che illustra in modo sintetico le dimensioni approssimative di alcuni tipi di “contenuti” che possono transitare sulla rete.
Sebbene l’entità dei contenuti sia molto importante nel dimensionamento di una rete dati, altrettanto importante è la frequenza con cui tali contenuti vengono richiesti e inviati dalle postazioni di rete e dai server.
Per fare un esempio concreto di consideri l’attività di ricerca su un database.
Mediamente, una query (ricerca) su database ha una dimensione di circa 4 KByte, ossia 32 kbit (1 byte = 8 bit). Supponendo che su una rete vi siano 10 operatori che eseguono 1 ricerca ogni 2 minuti, ovvero 120 secondi, l’occupazione media di banda può essere così calcolata:

banda = 32 kbit * 10 / 120 sec. = 2,7 kbps (2.700 bit per secondo)

Sebbene questo valore sia ben lontano dalla capacità di trasporto di una rete FastEthernet (100 Mbps = 100.000 kbps), è necessario considerare che a seguito di una ricerca con esito positivo è probabile che l’operatore acceda al contenuto trovato all’interno del database e ciò comporta un ben più consistente trasferimento di dati. Supponendo che si tratti di documenti e che le probabilità di successo di una ricerca siano del 30%, facendo riferimento alla tabella precedente, si ottiene un trasferimento di

circa 1 Mbyte per operatore ogni 30 ricerche su 100, ossia 8 Mbit * 30 / 100 = 2,4 Mbit = 2400 kbit, da cui si ottiene la seguente occupazione media di banda:

banda = 2400 kbit * 10 / 120 sec. = 200 kbps (200.000 bit per secondo)

che va a sommarsi a quella dovuta all'attività di ricerca.

Nel casso di una BD i contenuti possono in realtà essere ben più consistenti di un semplice documento, come accade nel caso di immagini, filmati e file audio. Da ciò è facile dedurre quanto importante sia una corretta analisi delle attività svolte sulla rete al fine di dimensionare correttamente l'infrastruttura e permettere un efficiente uso dei servizi e delle applicazioni.

D'altra parte un'analisi completa delle caratteristiche dei servizi non può limitarsi alla sola dimensione dei contenuti e al traffico medio prodotto. Vi sono infatti altri parametri che concorrono a descrivere completamente uno specifico flusso dati sulla base delle caratteristiche dei servizi.
In particolare si possono individuare le seguenti classi di servizi:

- *servizi di tipo "best-effort"*
  non prevedono nessun controllo rispetto al modo con cui la rete soddisfa le richieste; la rete non offre per questi servizi alcuna garanzia; gli utenti devono adattarsi allo stato che la rete ha nel momento in cui fanno richiesta dello specifico servizio; esempi di questo tipo sono i servizi Internet quali WWW, FTP, e-mail;
- *servizi specificati "deterministici"*
  prevedono la possibilità di misurare i requisiti necessari al servizio e poterne determinare la disponibilità in rete; una volta che le risorse necessarie al servizio sono disponibili la rete deve disporre di strumenti (tipicamente basati su metodo statistici) per il mantenimento di tali risorse entro limiti prestabiliti; esempi di servizi

deterministici sono la teleconferenza e lo streaming audio/video che rientra nella categoria dei servizi di distribuzione di contenuti multimediali, molto utilizzati in ambito BD;

- *servizi specificati "garantiti"*
  si tratta dei servizi con i criteri più restrittivi e rappresentano un sottoinsieme dei deterministici in quanto, in genere, necessitano di specifiche risorse di rete in misura strettamente garantita; i meccanismi che la rete deve mettere a disposizione di questo tipo di servizi sono analoghi a quelli utilizzati per i servizi deterministici con in più una garanzia stabilita da appositi contratti e politiche di servizio; si tratta soprattutto di servizi critici che operano su rete geografica quali la telemedicina, le transazioni bancarie, ecc.. e raramente si trovano impiegati nell'ambito della BD.

Servizi deterministici

Al fine di caratterizzare e gestire servizi di tipo deterministico è necessario individuare quali sono i requisiti prestazionali che la rete deve garantire.
In generale si distingue tra:

- *Affidabilità*: continuità nella disponibilità delle risorse; risulta direttamente proporzionale alla capacità della rete di fornire informazioni sullo stato delle risorse in modo deterministico e accurato;
- *Capacità*: misura della possibilità di trasferimento di informazioni; dipende dalla larghezza di banda (capacità torica dell'infrastruttura di rete) e dal "throughput" o produttività (capacità reale dell'infrastruttura, delle postazioni e dei protocolli di alto livello);
- *Ritardo*: intervallo di tempo tra la trasmissione delle informazioni e la loro ricezione da parte dei destinatari; include i ritardi dovuti a tutti i componenti, dall'infrastruttura agli host.

Nel recente passato erano poche e generalmente costose le tecnologie in grado di consentire l'implementazione di servizi di tipo deterministico. Nel caso di necessità di questo tipo, in effetti, si parlava quasi esclusivamente di reti ATM (Asynchronous Transfer Mode).
I recenti sviluppi hanno reso disponibili alcune funzionalità tipiche della rete ATM anche per tecnologie decisamente più economiche quale, ad esempio, FastEthernet [0].
Da qualche tempo, infatti, sono comparsi dispositivi FastEthernet in grado di gestire code di priorità basate su parametri ti tipo QoS (Quality of Service) che permettono di "garantire" determinate risorse (soprattutto in termini di capacità e ritardo) a specifici flussi dati, consentendo un'efficiente distribuzione dei contenuti multimediali, così importanti per una BD[149].

Sulla questione relativa alle modalità d'uso dei servizi e delle applicazioni da parte degli utenti è importante comprendere quanto sia fondamentale il contributo dei responsabili del progetto per il committente.
Questi, infatti, dovranno essere in grado di coinvolgere ampi settori di operatori della Biblioteca (i futuri utenti della rete) al fine di comprenderne bisogni e abitudini ed essere in grado di "dimensionare" opportunamente i servizi.
In questo modo, inoltre, si raggiunge un secondo importante scopo, ossia quello di una ampia, condivisa e consapevole partecipazione di tutti alle attività connesse alla realizzazione della nuova rete: ciò costituisce la più solida base su cui realizzare una infrastruttura che risponda alle reali esigenze.

Per la raccolta delle informazioni relative alle modalità d'uso dei servizi risulta estremamente utile fare ricorso a questionari specifici appositamente realizzati.
Di seguito vediamo un modello esemplificativo.

[149] Significativi a questo proposito sono gli switch CISCO della famiglia Catalyst (http://www.cisco.com)

Settore	**Opere a stampa antiche e moderne**
Attività	**Acquisizioni** **Catalogazione (immissione dati; cattura)** **Inventariazione** **Legatura e Restauro**
Ubicazione	**Stanze: 5, 6, 7**
Numero unità operative	**8**
Ore di lavoro giornaliere	**6**

Uso del PC e delle risorse di rete

a) Per quante ore giornaliere si utilizza o si prevede di utilizzare il computer?

meno di 1 ora	da 1 a 3 ore	da 3 a 5 ore	più di 5 ore
	X		

b) Indicare le percentuali d'uso delle risorse di rete (Intranet/Internet)

Percentuale di accesso a risorse interne alla Biblioteca	**80%**
Percentuale di accesso a risorse esterne (via Internet)	**20%**

c) Si fa o si prevede di fare uso di posta elettronica?

Si	No
X	

Uso di applicazioni specifiche

Indicare le applicazioni che sono o saranno utilizzate e le relative modalità d'uso

Applicazioni/Servizio	Categoria	Modalità d'uso
SBN, Tinlib	**Cataloghi e Basi Dati**	**Catalogazione**
Word, Excel, PowerPoint, Publisher **CD-Rom in rete**	**Office Automation** **Cataloghi Multimediali**.	**Redazione, Consultazione** **Consultazione**
. .	. .	. .
.	.	.

Naturalmente tra gli utilizzatori della rete della BD non ci sono soltanto gli operatori interni ma anche e soprattutto gli utenti, sia quelli che accedono alle risorse dall'interno, ossia da una delle strutture che costituiscono la BD stessa, sia gli utenti provenienti da Internet.

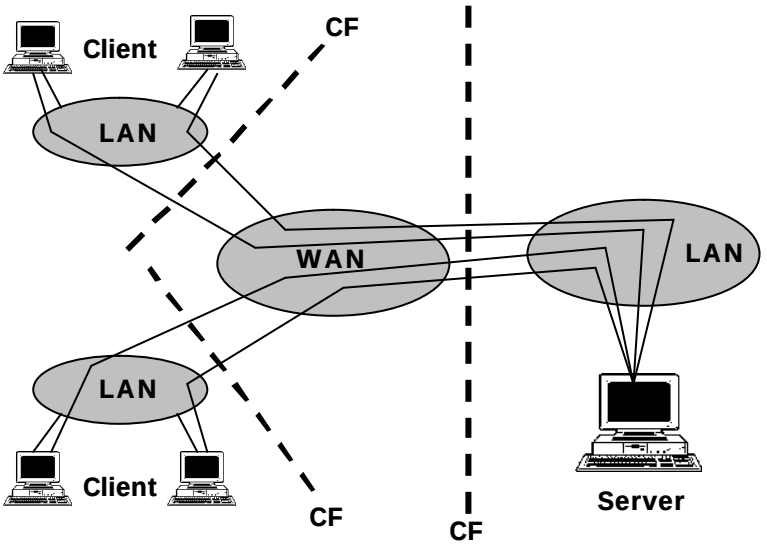
L'analisi di questa categoria di utilizzatori risulta assai più complicata e, in genere, è utile fare riferimento ai dati statistici di affluenza (quando disponibili) o cercare informazioni da altre esperienze di BD realizzate e già

in attività. Se esiste già un portale delle biblioteche che partecipano al progetto della nuova rete può essere utile rilevare il numero di contatti su diversi archi temporali (giornaliero, mensile, annuale), nonché i dati relativi ai picchi di accesso (numero massimo di contatti contemporanei).

Il concetto di collo di bottiglia

L'analisi dei flussi dati permette l'individuazione dei cosiddetti *colli di bottiglia*, ossia quei fenomeni in cui il flusso dati supera le capacità della rete creando un rallentamento nelle attività.
Normalmente i colli di bottiglia si formano in prossimità dei *confini dei flussi* cioè in quei segmenti di rete in cui diversi flussi si consolidano a formare un flusso composto relativo a diversi servizi e postazioni. Un tipico esempio di confine di flusso è il router che connette la LAN alla WAN e/o la LAN a Internet.

Individuare i colli di bottiglia permette di dimensionare opportunamente gli "snodi" critici della rete in modo da soddisfare i criteri di efficienza e affidabilità.



CF = Confine dei Flussi

Il processo di dimensionamento, naturalmente, influisce in modo determinante sulla scelta delle tecnologie, da quelle relative al cablaggio

(rame, fibra, wireless) a quelle che riguardano i dispositivi di interconnessione quali hub, switch e router.

Il concetto di collo di bottiglia, infine, consente di comprendere a pieno la funzione di uno dei componenti più importanti di una infrastrutture di rete: la *dorsale*.
Per dorsale si intende il tratto di cablaggio che collega due distinte aree telematiche, ossia due zone in cui si trovano i dispositivi attivi e passivi di interconnessione di rete, tipicamente raccolti in armadi attrezzati ed elettrificati. Da queste aree telematiche si dipartono i cablaggi verso le postazioni utente.
Le dorsali in genere realizzano, in una topologia stellare, il collegamento tra diversi edifici nonché quello tra i piani all'interno di ciascun edificio. In questo senso appare chiaro come esse siano il luogo dove potenzialmente si concentrano i colli di bottiglia.
Per queste ragioni è estremamente importante che il progetto della rete tratti con cura il dimensionamento delle dorsali, operando le scelte tecnologiche più adatte.

Hub, Switch e Router

L'analisi dei flussi, come è stato ampiamente sottolineato, influisce in modo determinante sulla tecnologie da impiegare per la realizzazione della rete [0].
In particolare è determinante nella scelta dell'elettronica di rete, ossia nella selezione dei dispositivi attivi di interconnessione quali hub, switch e router.
Per comprendere pienamente il significato di questa affermazione, vediamo quali sono le caratteristiche che distinguono questi tre tipi di dispositivi in riferimento alla gestione dei flussi dati.

Prima di tutto occorre dare due definizioni:

- *Bandwidth domain*: insieme di dispositivi (postazioni di lavoro, server, stampanti, ecc..) che condividono la stessa banda (segmento di rete)
- *Broadcast domain*: insieme di dispositivi che scambiano messaggi di broadcast e multicast

Al fine di comprendere pienamente il senso dei due insiemi (domini) è necessario chiarire il significato di broadcast e multicast in contrapposizione a *unicast*.
All'interno di una rete i pacchetti (messaggi) che trasportano i dati possono essere di tre tipi diversi:

- pacchetti *unicat*, ossia pacchetti diretti ad un unico destinatario;
- pacchetti *broadcast*, ossia pacchetti diretti a qualsiasi host della rete in grado di riceverli; i pacchetti di questo tipo sono utilizzati per rendere noto a tutti gli host un preciso stato della rete come, ad esempio, la disponibilità di una stampante, la condivisione di un disco da parte di un server, ecc .., o per svolgere alcune funzioni fondamentali come la risoluzione dei nomi e l'assegnazione degli indirizzi via DHCP;
- pacchetti *multicast*, ossia pacchetti diretti ad un gruppo specificato di host della rete; i pacchetti di questo tipo sono in genere utilizzati da alcune applicazioni che trasferiscono dati a più destinatari contemporaneamente al fine di evitare l'inutile moltiplicazione dei messaggi sulla rete; si tratta in genere di applicazioni e servizi per la distribuzione in rete di contenuti multimediali e di videoconferenza.

A differenza dei pacchetti unicast, i broadcast vengono elaborati da tutti gli host della rete ed un loro eccesso può costituire motivo di drastica diminuzione dell'efficienza dell'infrastruttura. Inoltre alcuni dispositivi di accesso alla rete (schede di rete), trattano i messaggi di tipo multicast come dei broadcast, indipendentemente dal fatto che tali messaggi siano o

meno diretti a quello specifico host, aumentando ulteriormente il carico di lavoro della postazione.

La definizione di questi due tipi di insiemi (bandwidth e broadcast domain), unitamente alla stima dell'entità dei flussi dati relativi ai diversi servizi, serve ad individuare due tipologie di problemi che è possibile affrontare e risolvere selezionando opportunamente l'elettronica di rete, ampiamente descritta nell'appendice C.

Protocollo	**Numero massimo di postazioni**
IP	500
IPX	300
AppleTalk	200
NetBIOS	200
Mixed	200

In particolare si può dire che un eccessivo flusso dati all'interno di un "bandwidth domain" può provocare un calo di efficienza ed affidabilità legato a fenomeni quali l'eccessivo numero di collisioni nel caso di reti Ethernet o l'insostenibile allungamento dei tempi di attesa del "token" nelle reti Token Ring o FDDI (Fiber Distributed Data Interface).

D'altra parte, come spiegato in precedenza, un numero eccessivo di host (postazioni/server) e servizi all'interno di un "broadcast domain" può causare un ulteriore appesantimento del flusso complessivo e portare ad un congestionamento della rete dovuto ai troppi messaggi broadcast e multicast che le postazioni devono elaborare.
La tabella che segue riporta i limiti consigliati per quanto riguarda il numero di postazioni in un broadcast domain in funzione del protocollo di rete utilizzato:

Facendo riferimento alle considerazioni appena fatte e ai dettagli tecnici riportati nell'appendice C, si può affermare che per ridurre gli

inconvenienti determinati dall'eccessiva dimensione dei "bandwidth domain" è necessario utilizzare degli switch al posto dei meno "intelligenti" hub, cosicché si è in grado di sezionare il flusso in maniera opportuna. La questione relativa all'eccesso di broadcast e multicast, invece, si risolve con l'introduzione di router in grado di fermarne la diffusione oltre limiti accettabili.

Un'altra questione che l'analisi dei flussi mette in evidenza è la presenza di servizi di tipo deterministico che necessitino di precisi requisiti di affidabilità, capacità e ritardo, come per esempio i servizi di teleconferenza o quelli di distribuzione di contenuti multimediali.
In questo caso è necessario ricorrere a tecnologie e dispositivi in grado di gestire i flussi in base a parametri quali, ad esempio, il QoS o CoS (Class of Service).

8.4.2 Stabilità - Ridondanza

La ridondanza è un concetto molto importante nell'ambito della rete di una BD poiché consente di mantenere stabili le risorse e il livello di fruibilità dei servizi in una struttura che, come si è detto più volte, ai servizi è interamente orientata.

In ambito informatico quando si parla di ridondanza si intende la disponibilità di strumenti alternativi di accesso alle risorse, da utilizzarsi in parallelo o in sostituzione a quelli normalmente utilizzati.

Per chiarire meglio questo concetto, si consideri l'accesso al database del catalogo di una biblioteca: cosa accade se il server che gestisce il database smette di funzionare? Può un servizio essenziale come l'accesso al catalogo subire un "fermo macchina" che lo rende inaccessibile? Quanto può essere lungo il periodo di inattività del servizio di accesso al catalogo prima che il disagio causato dal disservizio sia considerato inaccettabile?
Vediamo un altro esempio; si consideri il server web che gestisce il portale di accesso esterno alle risorse di una BD: cosa accade nel caso di un

fermo macchina, o nel caso che la connettività al server web subisca una interruzione dovuta alla linea fisica, al provider o ai dispositivi di accesso quali firewall e router? Può una BD rinunciare ad una delle caratteristiche che la contraddistinguono così fortemente da una biblioteca tradizionale, ossia l'accessibilità delle risorse oltre i propri confini architettonici?

Per ovviare ai disservizi causati dal malfunzionamento hardware e software dei componenti di una rete è necessario dotare l'infrastruttura di una certa percentuale di risorse duplicate (ridondanza) in grado di sostenere i servizi per il tempo necessario alla "riparazione" delle parti malfunzionanti (*Fault Tollerance*).

Nella maggior parte dei casi, più che garantire l'assoluta continuità dei servizi, la ridondanza consente di ridurre drasticamente il loro periodo di inattività. Ciò è dovuto al fatto che, generalmente, esiste un tempo non nullo di sostituzione della la risorsa primaria (non più disponibile a causa del malfunzionamento) con quella secondaria (backup).
In altri casi, invece, la sostituzione avviene in tempo reale senza che l'utenza si accorga di alcunché.

A questo punto vediamo un elenco delle principali forme di ridondanza con una breve descrizione delle modalità di funzionamento.

Ridondanza Hardware

Si tratta della duplicazione di alcune componenti hardware critiche quali, ad esempio, dischi fissi, schede di rete, alimentatori, ecc...
Le tecniche di ridondanza hardware sono generalmente applicate sui server e hanno lo scopo di permettere la sostituzione rapida o in tempo reale di alcuni componenti particolarmente soggetti a rotture, il cui mancato funzionamento è causa di interruzione di servizi essenziali.
Sul mercato esistono attualmente soluzioni che consentono una ridondanza completa di tutto l'hardware che compone il server, dalla

scheda madre ai processori, dalla RAM ai dischi fissi, dalle schede di rete agli alimentatori, ecc... A fronte di un costo superiore a quello della ridondanza classica, ossia limitata ai componenti più critici, queste soluzioni hanno il pregio di coprire tutti i possibili malfunzionamenti e possiedono, in genere, meccanismi automatici di sostituzione a tempo zero.

Server di Backup

Il concetto si server di backup estende quello di ridondanza hardware fino ad includere l'intera macchina comprensiva di sistema operativo, applicazioni e servizi.

In questo senso si tratta di una ridondanza sia hardware che software che permette una tolleranza sia alle "rotture" che ai malfunzionamenti propri dei servizi.

Una tipico impiego dei server di backup è quello relativo alla gestione dei servizi di autenticazione degli utenti (*domain controller*), di archiviazione di file (*file server*) e di accesso a banche dati, opac, server web, server ftp, ecc... In questi casi la ridondanza viene spesso utilizzata anche per implementare tecniche di *load balancing* per la distribuzione del carico di lavoro su più server, cosicché i i server di backup svolgono il duplice compito di garantire continuità ed efficienza ai servizi.

Backup delle linee di connessione **(Dorsali/Link)**

Questo tipo di backup ha lo scopo di garantire continuità di connessione su collegamenti critici quali le dorsali e le connessioni WAN.

L'implementazione di questo genere di ridondanza consiste nella duplicazione di parte dell'elettronica di rete (switch e router) e di alcuni collegamenti fisici (dorsali e linee di accesso WAN). Un caso tipico è quello di una o più linee ISDN (con relativo router) utilizzate come connessione di backup di una linea HDSL.

Ridondanza di periferiche di rete

Si tratta della più semplice tra le tecniche di ridondanza e consiste nella duplicazione di periferiche di rete quali stampanti, plotter, fax, ecc...

8.4.3 Scalabilità - Cablaggio strutturato

Per cablaggio strutturato si intende una infrastruttura di rete fonia/dati realizzata su un'insieme di regole definite dagli standard americani, internazionali ed europei, definite allo scopo di rendere la rete estremamente razionale, maneggevole e scalabile.

Tra i principi fondamentali del cablaggio strutturato c'è il concetto di topologia stellare.
Secondo questo principio, ogni edificio viene suddiviso in aree telematiche omogenee e per ciascuna area viene definito un centro stella (tipicamente rappresentato da un armadio che ospita i dispositivi passivi ed attivi di interconnessione) da cui di dipartono i cavi di rete che raggiungono le postazioni utente.
A sua volta, ogni centro stella è collegato agli altri attraverso un centro stella di livello superiore.
La struttura gerarchica ha termine in un centro stella di edificio che, oltre a svolgere il ruolo di accentratore dei cablaggi, realizza l'accesso al mondo esterno (Internet) e/o agli altri edifici tramite router (campus).

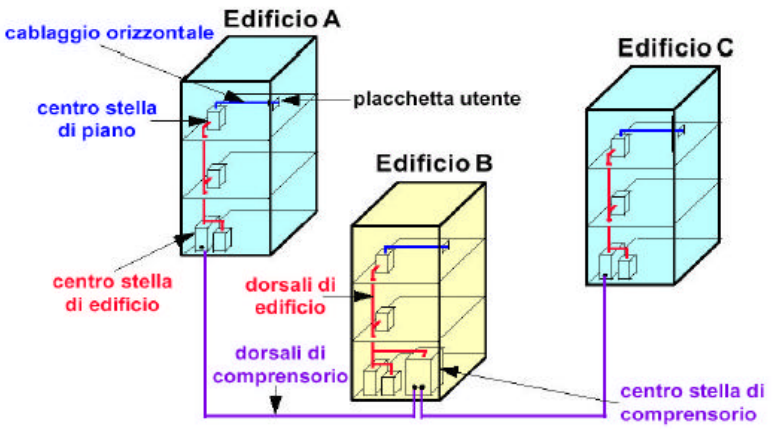
Secondo le regole del cablaggio strutturato, inoltre, ogni postazione di lavoro deve essere raggiunta da una doppia presa di rete. Ciò permette, nel caso si tratti di una postazione di lavoro che necessita di una linea telefonica, di connettere sia una workstation (PC, Notebook, Mac, Unix, ecc.) che un telefono o, nel caso di postazioni al pubblico, di connettere due workstation.
In definitiva, quando si parla di presa di rete nel cablaggio strutturato, si deve sempre considerare una presa doppia (dati/dati, fonia/dati, fonia/fonia).

Gli standard di riferimento per il cablaggio strutturato sono quelli già analizzati nello specifico capitolo (si veda 8.3.3 Gli Standard e la loro funzione) e contengono tutte le prescrizioni, dai materiali alle procedure, che progettisti e installatori devono seguire per la corretta realizzazione della rete.

In particolare tra le regole del cablaggio strutturato ne esistono alcune specificatamente orientate alla progettazione di una infrastruttura in grado di sostenere cambiamenti nell'assetto e nella distribuzione delle postazioni di lavoro.

Secondo queste regole il progettista deve prevedere almeno 2 (EN50173) o 3 (EIA/TIA 568) prese di rete per postazione di lavoro (scrivania) e deve considerare la possibilità di una postazione di lavoro ogni 10 m^2, distribuendo le prese in posizioni facilmente raggiungibile con una "patch cord" (cavo di rete che collega il computer/telefono alla relativa presa).

In questo modo si riducono drasticamente i casi in cui un riassetto delle postazioni di lavoro imponga un nuovo cablaggio o lo spostamento delle prese esistenti.



Naturalmente solo le prese attive (ossia quelle realmente utilizzate per connettere un computer o un telefono) saranno collegate ai dispositivi attivi di rete (hub e switch) mentre tutte le altre (regolarmente attestate sui pannelli di accentramento all'interno degli armadi) saranno pronte per futuri utilizzi. In definitiva l'insieme dei centri stella (armadi) realizza una

matrice di connessioni in grado di assegnare, per esempio, lo stesso numero telefonico alla postazione di uno specifico utente, anche nell'eventualità che questo si sposti all'interno della rete.

Cercando di riassumere, possiamo dire che tra i vantaggi di un cablaggio strutturato troviamo:

- durata e garanzia del cablaggio: gli standard permettono di ottenere dagli installatori una garanzia variabile tra i 15 e i 25 anni;
- versatilità dei punti presa: ogni punto può essere utilizzato sia come presa dati che come linea telefonica;
- scalabilità della rete: l'aggiunta di una postazione di lavoro all'interno dell'area cablata non comporta alcun costo;
- "mobilità" dell'infrastruttura: lo spostamento delle postazioni di lavoro all'interno dell'area cablata non comporta alcun costo aggiuntivo;
- robustezza: la topologia stellare comporta un naturale isolamento dei guasti ed impedisce che questi si ripercuotano sull'intera infrastruttura.

Per completezza di analisi è utile sottolineare alcuni aspetti critici relativi alla scelta di un cablaggio strutturato che, in una certa misura, rappresentano degli svantaggi.
In particolare si può dire che:

- il cablaggio strutturato comporta l'installazione di punti presa in "soprannumero" e quindi impone costi di posa in opera sensibilmente maggiori rispetto ad un tradizionale cablaggio non strutturato in cui si posano solo i cavi necessari al raggiungimento delle postazioni previste al momento della realizzazione dell'infrastruttura;
- per progettare e realizzare una rete secondo i principi del cablaggio strutturato è necessario fare ricorso a professionisti certificati in

grado di garantire gli standard che questo tipo di cablaggio richiede, e ciò, ovviamente, determina un aumento dei costi di realizzazione.

D'altra parte, a fronte di un maggiore investimento iniziale (costo di primo impianto) si riscontra una sensibile riduzione dei costi a medio e lungo termine, nonché di quelli di manutenzione e gestione, determinata dalla maggiore versatilità presentata da una soluzione strutturata.

Reti Wireless

Le reti wireless, ampiamente trattate nell'appendice B, possono essere considerate a ragione come la massima espressione della scalabilità nel campo delle reti e, quindi, come una sorta di estensione "senza fili" del cablaggio strutturato.

In effetti il wireless trova largo impiego come tecnologia utile a coprire aree in cui risulta difficile o addirittura impossibile la posa dei cavi. In questo tipo di applicazioni ciò che si viene a determinare è una rete mista wired/wireless, nella quale ad un cablaggio tradizionale in rame e/o fibra si aggiungono aree coperte da comunicazioni wireless.

Nel caso specifico di Biblioteche locate in ambienti con vincoli architettonici il wireless può essere la soluzione ideale (se non l'unica) per riuscire a realizzare l'infrastruttura di rete necessaria ai servizi della BD, grazie al basso "impatto ambientale" che lo contraddistingue e all'estrema mobilità delle postazioni di lavoro.

Sebbene in alcuni casi il wireless possa anche sostituire interamante il tradizionale cablaggio, realizzando così una struttura estremamente versatile, è utile ricordare che una tale soluzione non copre le comunicazioni telefoniche e, soprattutto, non elimina né la necessità di cablare le dorsali in rame o fibra, né quella di realizzare gli armadi di

centro stella che consentono di mettere in comunicazione gli access point con l'elettronica di rete alloggiata negli armadi stessi.

Negli ultimi tempi l'utilizzo di tecnologie wireless nell'ambito dei progetti di BD ha subito una crescita sensibile grazie soprattutto all'aumento delle prestazioni in termini di larghezza di banda previste dai recenti standard.

Tra i vantaggi più evidenti che i responsabili dei progetti tendono a sottolineare c'è, naturalmente, quello della grande libertà di movimento delle postazioni di rete, ancora più evidente laddove vi è un uso sensibile di computer portatili.
Un altro vantaggio indiscutibile è la diminuzione dei costi di primo impianto grazie alla drastica riduzione di opere di cablaggio e muratura.

Dal punto di vista degli svantaggi tutti i progetti realizzati evidenziano una difficoltà di gestione delle procedure di sicurezza e protezione della rete (vedi appendice B), che aumenta sensibilmente il costo di gestione e rende più arduo il compito di realizzare un efficiente controllo degli accessi alle risorse.
Al secondo posto tra gli svantaggi c'è la questione della scarsa interoperatività multivendor tra i dispositivi wireless, che può rendere impossibile l'accesso di utenti con dispositivi mobili (pc portatili, PDA , ecc..) corredati di dispositivi wireless non corrispondenti alle specifiche della rete che li deve ospitare.
Infine va ricordato che le prestazioni di una rete wireless sono ancora di gran lunga inferiori a quelle di un cablaggio classico in rame e fibra.

Nonostante tutte le limitazioni esposte, l'impiego del wireless in alcune strutture ad accesso pubblico, quali le biblioteche, le università e i centri di ricerca è molto diffuso e in continua crescita, soprattutto negli Stati Uniti. Per avere conferma di ciò si provi ad eseguire una ricerca su un qualsiasi motore Web (ad esempio Google) utilizzando come chiave wireless AND library, limitatamente ai siti .EDU in lingua inglese.

8.4.4 Sicurezza - Profili utente

La maggior parte dei sistemi operativi di rete attuali, tra cui Windows NT/2000/XP, Novell e Linux, consentono la creazione di profili utente in grado di regolare le modalità di accesso alle risorse e ai servizi di rete fin nei minimi dettagli.
In tal modo è possibile determinare esattamente le risorse che un utente (interno o esterno alla Biblioteca) potrà utilizzare, in che modo vi accederà e in che misura.

Usati congiuntamente agli strumenti di protezione messi a disposizione dai file system (per esempio da NTFS di Windows), i profili utente sono fondamentali per la realizzazione di politiche di protezione dei dati sensibili.

Chi opera in Biblioteca sa bene quanto sia arduo il compito di mantenere operative le postazioni di lavoro (soprattutto quelle al pubblico) senza incorrere in continue perdite di configurazione determinate da volontarie o involontarie modifiche al sistema operativo e da installazioni non autorizzate di software, magari scaricato da internet e quindi potenzialmente molto dannoso.
L'attività di manutenzione delle postazioni al pubblico è, tra l'altro, una delle voci di costo che più di ogni altra influisce negativamente sul costo di gestione della rete.
I profili utente sono molto utili per evitare questi inconvenienti poiché permettono di mantenere fissate le configurazioni delle postazioni di lavoro, stabilizzando nel tempo il livello di accessibilità alle risorse e ai servizi, e abbassando, contemporaneamente, i costi di gestione.

Infine è interessante sottolineare come i profili utente siano lo strumento più adatto alla realizzazione del *posto di lavoro virtuale*, ossia quello spazio distribuito in cui lo specifico utente ritrova, indipendente dalla postazione da cui accede alla rete, i suoi strumenti di lavoro, le sue ricerche, i

contenuti selezionati e tutto ciò che qualifica la sua attività all'interno della BD.

I sistemi di protezione tramite Router e Firewall

I dispositivi quali router e firewall (di cui si parla in dettaglio nell'appendice C) sono gli apparati con i quali si realizza e si protegge la connessione della BD con l'esterno.

Mentre i router, che sono principalmente addetti alla gestione della connettività, implementano protezioni basate essenzialmente su delle *Access List*, i firewall possono fare dei controlli anche sul contenuto delle comunicazioni consentendo un livello di sicurezza molto efficace: con i firewall è possibile, ad esempio, impedire l'accesso ad alcuni siti internet sulla base dell'argomento trattato.

Per quanto riguarda le Access List, queste consentono essenzialmente di regolare l'accesso alle risorse sulla base di un controllo incrociato tra gli indirizzi IP, le porte TCP/UDP e i servizi, e risultano molto utili come primo strumento di blocco degli accessi indesiderati alle risorse della BD.

A proposito dei firewall, è necessario sottolineare che esistono sia in versioni software (da installare su appositi server), che in forma di apparato dedicato da collocare in uno degli armadi di distribuzione del cablaggio.
Un firewall in forma di apparato dedicato è senz'altro da preferire a quello software poiché più efficiente e più semplice da amministrare e mantenere non essendo vincolato a eventuali problemi esterni quali, ad esempio, quelli del sistema operativo del server ospite.

8.4.5 Accessibilità delle risorse – Reti Virtuali Private

Come è stato più volte sottolineato una BD ha come caratteristica fondamentale la condivisione delle risorse tra biblioteche distinte.

La necessità di estendere le singole reti delle biblioteche oltre i limiti architettonici prevede la possibilità di realizzare canali di comunicazione sicuri e protetti da accessi non autorizzati.

Nella realizzazione di canali protetti per la connessione tra singole LAN è necessario utilizzare alcune complesse tecnologie di criptaggio, integrità e autenticazione basate su sistemi a chiave pubblica e privata e su meccanismi di riconoscimento legati all'uso di certificati elettronici.
Sebbene l'approfondimento di tali tecnologie vada ben oltre lo scopo del presente studio, è utile sottolineare come tutte queste confluiscano nella realizzazioni di Reti Virtuali Private (VPN).

Data l'importanza delle VPN nell'ambito della BD si ritiene opportuno descriverne alcuni aspetti di carattere generale.

Reti Virtuali Private

Con l'evolversi dell'attività, per condividere via Internet le informazioni e le risorse, le biblioteche devono collegare alla propria rete centrale un numero sempre maggiore di sedi e utenti remoti che concorrono alla realizzazione della BD. In passato ciò era possibile mediante la creazione di una WAN privata, che utilizzava linee dedicate verso le sedi remote e server dial-access per il supporto degli utenti residenti e di quelli in telelavoro. Per una biblioteca di medie e piccole dimensioni, una WAN privata tradizionale può essere molto costosa da creare e gestire. Per la connessione di siti e utenti remoti alla rete principale della biblioteca oggi è disponibile un'alternativa, la rete privata virtuale (VPN - Virtual Private Network). La VPN opera in assoluta sicurezza e permette l'accesso completo ai dati di una WAN privata sfruttando tutte le caratteristiche di Internet.

I vantaggi della VPN

Maggiore convenienza: gli utenti remoti possono collegarsi alle risorse di rete centralizzate attraverso un link locale verso un Internet Service Provider, al prezzo di una chiamata locale.
Maggiore flessibilità: i nuovi utenti/strutture vengono aggiunti con facilità senza nuove apparecchiature o linee dedicate.
Maggiore affidabilità: le VPN sfruttano i mezzi delle vaste infrastrutture della rete pubblica e l'esperienza delle biblioteche che le controllano.
Maggiore sicurezza: le VPN utilizzano il "tunneling" e i sistemi di cifratura per proteggere il traffico privato. Il tunneling crea una connessine peer-to-peer temporanea tra l'utente remoto e quello centrale, bloccando l'accesso a chiunque si trovi all'esterno.
Cosa serve per creare una VPN: le biblioteche che fanno parte della BD possono creare e gestire una propria VPN, ma è sicuramente più semplice affidarsi ad un Internet Service Provider. In tal caso ci si deve semplicemente collegare al provider utilizzando un router o un modem.

Le VPN esistenti sono generalmente di due tipi: dial e dedicate. Le prime permettono di sfruttare i bassi costi dei servizi dial-up normali mentre le altre possono utilizzare i servizi frame relay o le linee dedicate, soprattutto quando è necessario un collegamento remoto ad alta velocità e capacità.

8.4.6 Investimento e costi di gestione

L'aspetto relativo ai costi di realizzazione e gestione di una rete (TCO, *Total Cost of Ownership*) è senz'altro uno dei più rilevanti poiché influisce sia sulle possibilità di realizzare una infrastruttura con le caratteristiche desiderate sia sulla capacità di mantenere nel tempo la qualità dei servizi implementati.

Ancora una volta è utile ribadire che la BD è una struttura fortemente orientata ai servizi e, come tale, risente fortemente dell'evoluzione delle tecnologie informatiche. Ciò, senza alcun dubbio, implica che la rete della

BD deve essere sempre mantenuta aggiornata, pena la perdita di qualità dei propri servizi.

È oramai opinione comune che le tecnologie informatiche, e soprattutto quelle che riguardano il trattamento e la diffusione dei contenuti multimediali, si evolvano così rapidamente che gli aggiornamenti hardware e software di una rete sono diventati la voce di costo predominante su tutte le altre spese di manutenzione di una rete.

Volendo fare un'analisi dettagliata dei costi che è necessario sostenere per la rete della BD si possono individuare due voci principali:

- investimento iniziale: per la realizzazione della rete e dei servizi;
- costi di gestione: per la manutenzione della rete, l'adeguamento delle licenze, l'aggiornamento dei software e dei servizi, i canoni di abbonamento (Internet, banche dati on-line, ecc..).

Vediamo queste due voci nel dettaglio.

Investimento iniziale

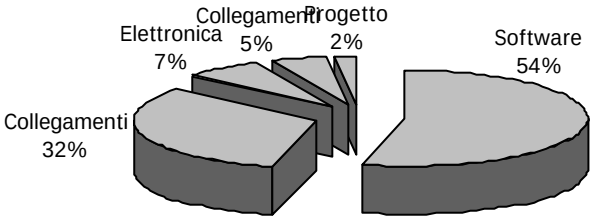
Questa voce rappresenta l'investimento iniziale che la Biblioteca deve sostenere per la realizzazione della rete e comprende:

- progetto
  - costi di progetto
  - redazione del capitolato tecnico
- cablaggio
  - materiali per il cablaggio (cavi, armadi, ecc..)
  - manodopera per il cablaggio
- apparati
  - elettronica di rete (hub, switch, router, ecc..)
  - server di rete

- postazioni (PC, MAC, ecc..)
- stampanti, scanner e altre periferiche speciali

- software
  - acquisto delle licenze dei sistemi operativi e dei software applicativi
  - attivazione abbonamenti (banche dati on-line, servizi di reference, ecc..)
  - configurazione della rete (servizi, applicazioni, profili di accesso, ecc...)
- collegamenti (WAN/Internet)
  - attivazione e abbonamento

Per i pesi relativi di ciascuna di queste voci sul costo totale dell'investimento si può orientativamente fare riferimento al seguente grafico:



Per quanto riguarda la fase di progetto è necessario considerare che esiste un costo aggiuntivo relativo al lavoro del personale interno che collabora alla fase di analisi e raccolta dati propedeutica alla stesura del progetto stesso.

In alcuni casi, inoltre, può essere necessario far precedere il progetto da uno studio di fattibilità, allo scopo di valutare i costi e pianificare le attività successive, dal progetto esecutivo alla realizzazione dell'infrastruttura.

Costi gestione

Come si è detto in precedenza il costo di gestione complessivo di una rete è composto da tutte quelle voci che riguardano manutenzione e aggiornamento, sia hardware che software, e cioè:

- cablaggio
  - assistenza
  - sostituzione di parti malfunzionanti
  - aggiunta di cablaggio
- apparati
  - assistenza all'elettronica di rete
  - manutenzione server e postazioni
  - aggiunta di risorse e periferiche
- software
  - licenze e aggiornamento dei software e dei sistemi operativi
  - canoni di abbonamento (banche dati on-line, servizi di reference, ecc..)
  - assistenza
- collegamenti (WAN/Internet)
  - canone di abbonamento annuale

In generale un'analisi completa dei costi di gestione risulta essere un'attività piuttosto complessa che non deve però essere trascurata pena la mancanza di risorse finanziarie necessarie al corretto sviluppo dei servizi.

Per quanto riguarda la questione delle licenze d'uso e degli aggiornamenti software è bene sottolineare che la maggioranza dei prodotti commercializzati propone soluzioni interessanti che permettono un

abbattimento dei costi di gestione, che vanno dai contratti di assicurazione a quelli di affitto del software.

I contratti di assicurazione software in genere prevedono che a fronte di un prezzo di acquisto iniziale maggiore, il fornitore offra un contratto che copre i costi degli aggiornamenti per un numero di anni successivi al primo (tipicamente 3 anni).

Le formule di affitto software rappresentano una soluzione per quanti preferiscano un costo ridotto ma ricorrente ad uno iniziale più elevato che esclude gli oneri di aggiornamento. L'affitto in genere si concretizza nel pagamento di una sorta di abbonamento annuo il cui importo viene calcolato in percentuale relativa al costo totale dell'acquisto del software. Sebbene questa soluzione sia comprensiva di licenze d'uso e aggiornamenti già nel medio periodo (circa 3 anni) la spesa totale risulta sensibilmente superiore a quella rappresentata dalle altre soluzioni (acquisto, contratto di assicurazione). Nonostante questo, però, l'affitto rappresenta una soluzione interessante in quanto riduce sensibilmente l'investimento iniziale e permette di pianificare facilmente la spesa annuale per il mantenimento dei servizi.

Sulla letteratura tecnica, intorno alle considerazioni sulle voci di costo che concorrono alla definizione del TCO, si trova spesso un riferimento ai costi di tipo *fuzzy*. Con il termine *fuzzy costs* si intendono quei costi che spesso sfuggono alle pianificazioni come, ad esempio, i costi relativi a perdita di produttività dovuta ad inefficienza della rete, alla necessità di modifiche o ampliamenti dell'infrastruttura, ad errate politiche di acquisto di licenze software, ecc.. .

Un recente studio condotto da The Gartner Group[150] ha indicato che molte organizzazioni commettono errori di valutazioni del TCO per circa il 50% del valore reale e che i costi trascurati sono composti in gran parte da *fuzzy costs* e dai costi sostenuti per la formazione degli operatori sull'uso della rete e dei servizi.

[150] http://www.gartner.com

Investimento e accessibilità - I protocolli RDP e ICA

I protocolli RDP e ICA permettono la realizzazione di quella architettura di rete ibrida di cui si parla nel paragrafo “8.1.3.4 Architettura ibrida: il caso WinFrame/MetaFrame” ed il loro impiego nell’ambito della BD sta assumendo un ruolo sempre più rilevante.

L’importanza di questi protocolli è legata alla possibilità di utilizzare dei ***Windows Terminal*** al posto dei tradizionali computer (PC, Mac, ecc...) per la realizzazione di postazioni di lavoro leggere (*Thin Client*), efficienti, facili da amministrare ed estremamente stabili.
La caratteristica principale di un Thin Client, infatti, è quella di non eseguire alcuna applicazione in locale ma di fungere da semplice terminale grafico per sessioni di lavoro in esecuzione su appositi server. Da questa caratteristica deriva il termine Thin (leggero), ad indicare l’esiguità di risorse a bordo della postazione.
A differenza di un computer tradizionale, un Windows Terminal non possiede parti meccaniche in movimento quali, dischi, lettori CD/DVD, unità floppy/ZIP, ventole, ecc... e ciò lo rende estremamente economico, resistente all’uso e difficile da manomettere.
Grazie al numero esiguo delle risorse hardware e alla totale assenza di parti meccaniche in movimento, un terminale Windows ha una durata di gran lunga superiore a quella di un computer tradizionale ed un costo sensibilmente inferiore
Quella che segue è una tabella riassuntiva dei benefici nell’uso dei Thin Client a confronto con una soluzione tradizionale

Thin Client	PC Tradizionali
Nessuna parte meccanica in movimento: poche rotture, scarsa necessità di manutenzione, lunga vita media del prodotto	Ridotta vita media del prodotto
Sistema operativo, driver e dispositivi di memorizzazione sul server (*Server Based Computing*): semplicità nell'amministrazione, aggiornamenti hardware e software centralizzati	Sistema operativo, driver e dispositivi di memorizzazione sulla postazione (*Desktop Based Computing)*: aggiornamenti hardware e software da effettuare su ogni postazione
Accesso ad applicazioni e servizi controllato: postazione estremamente stabile	Elevata complessità nella realizzazione del controllo su applicazioni, servizi e configurazione del sistema operativo locale: postazione potenzialmente instabile
Postazioni economiche	Postazioni costose
Postazioni semplici da implementare	Elevato tempo di implementazione delle postazioni
Semplici amministrazione remota	Difficili da amministrare in remoto
Resistenti all'attacco di virus	Vulnerabilità all'attacco di virus
Basso consumo energetico	Alto consumo energetico
Silenzioso	Generalmente rumoroso
Dimensioni ridotte	Ingombrante

Il basso grado di obsolescenza di un Windows Terminal, la stabilità della sua configurazione e il basso impatto in termini di amministrazione e TCO, rende la scelta dei thin client la più adatta a realizzare postazioni di accesso al pubblico, soprattutto nell'ottica della salvaguardia dell'investimento.

Data la totale assenza di meccanismi in movimento, i Thin Client sono particolarmente adatti alla realizzazione di postazioni in sale studio nelle quali sia necessario l'uso di dispositivi silenziosi. Il loro ridotto ingombro, inoltre, fa sì che possano essere posizionati in luoghi inaccessibili all'utente (sotto un tavolo, dietro ad un monitor, ecc...) salvaguardando lo spazio di lavoro.

Sebbene le postazioni di accesso al pubblico di una biblioteca siano il naturale impiego dei Thin Client, è necessario sottolineare che questo tipo di dispositivo è assolutamente adatto a svolgere le normali attività di ufficio, dall'uso della suite Microsoft Office (Word, Excel, PowerPoint, Access) alla navigazione Web, dall'uso della posta elettronica all'accesso a banche dati, ecc...

Tra i produttori più importanti di soluzioni thin client (a cui si può fare riferimento per ulteriori dettagli) citiamo la storica Wyse[151], la nuova ChipPC[152] e l'italiana CompuMaster[153].

[151] http://www.wyse.com
[152] http://www.chippc.com
[153] http://www.compumaster.it

Riferimenti Bibliografici

Peer-to-Peer File Sharing, The Effects of File Sharing on a Service Provider's Network, An Industry White Paper, Sandvine Incorporated, July 2002 (www.sandvine.com/solutions/pdfs/P2PWhitePaper.pdf)

A Content - Centric Distribution Strategy: The Secure, Mediated Peer-to-Peer Content Delivery Network as Best Value for Rich Downloadable Content and On-Demand Streaming, CenterSpan Communications Corporation, Fall 2002
(www.centerspan.com/technology/ new_content_whitepaper.pdf)

Beverly Yang, Hector Garcia-Molina, Efficient Search in Peer-to-Peer Networks, Computer Science Department, Stanford University (http://dbpubs.stanford.edu:8090/pub/2001-47)

Arturo Crespo, Hector Garcia-Molina, Routing Indices for Peer-to-peer Systems, Computer Science Department, Stanford University (http://dbpubs.stanford.edu/pub/2001-48)

Neil Daswani, Hector Garcia-Molina and Beverly Yang, Open Problems in Data-Sharing Peer-to-Peer Systems, Stanford University (http://dbpubs.stanford.edu/pub/2003-1)

Diane Teare, Designing Cisco Networks, Cisco Press, 1999
Wireless LAN Security, Enabling and Protecting the Enterprise, Symantec Enterprise Security Withe Paper, 2002
(http://securityresponse.symantec.com/avcenter/reference/symantec.wlan.security.pdf)

Andy Dornan, Emerging Technology: Wireless Lan Standards, Network Magazine, Feb 2002
(http://www.networkmagazine.com/article/NMG20020206S0006)

Andy Dornan, Bluetooth: At the Blue Screen, or Biting Back?, Network Magazine, Oct 2002 (http://www.networkmagazine.com/article/NMG20020930S0017)

Andy Dornan, Emerging Technology: Ultra-WideBand Wireless – Fat Pipes from Thin Air?, Network Magazine, May 2002 (http://www.networkmagazine.com/article/NMG20020603S0002)

Joel Conover, First Things First, Network Computing, July 2000 (http://tecun.cimex.com.cu/tecun/software/Soporte_tecnico_Redes/Enterasys/Wireless/Roamabout/Documentos/Articlewlan.pdf)

James D. McCabe, Reti di Computer, analisi e progettazione, McGraw-Hill, 1999

McDysan and Spohn, ATM: Theory and Applications, McGraw-Hill, 1995