UNIVERSITÀ DEGLI STUDI DI PADOVA

FACOLTÀ DI INGEGNERIA

Corso di Laurea in Ingegneria Informatica

TESI DI LAUREA

CONFIGURAZIONE E GESTIONE DI UNA RETE AZIENDALE

Relatore: *Prof. Sergio Congiu*

Laureando: *Lorenzo Mattiolo*

ANNO ACCADEMICO 2012 / 2013

– Nella vita non bisogna mai rassegnarsi, arrendersi alla mediocrità, bensì uscire da quella "zona grigia" in cui tutto è abitudine e rassegnazione passiva. –

Rita Levi-Montalcini

A me stesso e ad un bambino

che presto nascerà,

mio nipote

Indice

Prefazione

Questa tesi rappresenta la relazione di fine tirocinio, il cui scopo finale è la progettazione e lo sviluppo di un sistema scalabile e virtualizzato, e la creazione di un nuovo ambiente, portando l'attuale infrastruttura distribuita a un sistema ottimizzato in alta affidabilità. Il lavoro svolto è stato quello di monitorare e gestire una grande rete privata contenente una grande quantità di dati, permettendo l'implementazione di innumerevoli servizi per la buona gestione dell'azienda.

Al giorno d'oggi le reti informatiche sono di fondamentale importanza nella nostra quotidianità, ma non sempre ce ne accorgiamo. L'utilità e l'importanza di Internet, la più grande rete mondiale, è certamente nota a tutti, ma non è l'unico caso. In ogni azienda, ufficio o casa infatti, è ormai facile imbattersi in una rete privata. Per un'azienda, implementare una rete di calcolatori significa raggiungere quegli obiettivi e quella produttività che fino a qualche anno fa non erano nemmeno immaginabili ma che ora, con l'evoluzione della tecnologia, sono facilmente accessibili. Grazie a questo sviluppo, gli utenti di un'azienda riescono a comunicare e scambiare informazioni in modo rapido ed efficiente senza la necessità di trovarsi fisicamente nello stesso luogo, e condividono risorse quali potenza di calcolo, memoria, unità di memorizzazione e periferiche, gestiti in maniera centralizzata, favorendo un incremento della sicurezza e della competitività del sistema. Risulta evidente che la realizzazione di una rete di calcolatori presenta notevoli vantaggi: permette un'ottimizzazione dei costi, semplicità di gestione delle risorse, incremento della produttività, ed il guasto di una macchina, facilmente sostituibile, non blocca tutta la rete. Il settore però è in continua e soprattutto rapida evoluzione, le novità emergono veloci ed è una lotta continua per restare competitivi nel mercato. Tutto ciò genera una domanda sempre crescente di personale tecnico qualificato in grado di progettare, implementare e amministrare una rete, e di conseguenza determina un forte interessamento ed impegno nel settore da parte delle aziende, soprattutto per quel che riguarda sicurezza e affidabilità. E' importante dunque per un amministratore conoscere perfettamente tutti gli aspetti e le caratteristiche di una rete, in modo tale poterla monitorare, aggiornare e proteggere nel tempo.

L'informazione è un bene che aggiunge valore all'impresa. Dato che la maggior parte delle informazioni sono custodite su supporti informatici, ogni organizzazione

deve essere in grado di garantire la sicurezza dei propri dati, in un contesto dove i rischi informatici causati dalle violazioni dei sistemi di sicurezza sono in continuo aumento.

1. Introduzione

1.1. L'azienda

L'azienda per cui si è svolto il lavoro di analisi e configurazione del sistema informativo è Bellelli Engineering SpA, una società di progettazione e costruzione di impianti "chiavi in mano" e di materiali per le industrie operanti nel settore "Oil & Gas". Fondata nel 2002 con sede a Badia Polesine (RO), Bellelli Engineering è oggi una tra le più dinamiche società europee produttrici di impianti e processi per l'industria di petrolio e gas naturale cha vanno dalle attrezzature nei campi di estrazione fino a quelle di trattamento in raffineria. Grazie a continui investimenti nei processi produttivi ed al consolidamento della rete commerciale, oggi è una realtà che copre una buona parte del mercato medio – orientale, nordafricano e sudamericano.

Lo stabilimento di Badia Polesine resta comunque la sede principale dell'azienda e offre lavoro a circa un centinaio di dipendenti di cui fanno parte numerosi operai specializzati e laureati nelle aree tecnico-industriali.

Partendo da un disegno preliminare, vengono successivamente offerti servizi di ingegneria, acquisto di materiale e strumentazione, fabbricazione di impianti di processo, per giungere infine all'assemblaggio di unità o moduli montati su telaio. Un ulteriore servizio fornito da Bellelli Engineering consiste in un'accurata assistenza operativa post vendita per lo start-up degli impianti nei vari siti esteri.

Figura 1: Azienda - Esterno

Figura 2: Impianto

1.2. Descrizione del tirocinio

Il tirocinio ha avuto una durata complessiva di 6 mesi, strutturato in 500 ore suddivise in circa 25 settimane.

Durante tale periodo ho avuto l'opportunità di mettere in pratica le nozioni imparate durante il percorso di studi, di relazionarmi con la realtà del mondo del lavoro.

Il lavoro svolto è stato quello di monitorare e gestire una grande rete privata aziendale contenente una grande quantità di dati, permettendo l'implementazione di innumerevoli servizi per la buona gestione dell'infrastruttura informatica.

L'opportunità datami dall'azienda e dai collaboratori mi ha permesso di applicare le conoscenze apprese durante gli studi in un ambito diverso da quello universitario e più vicino all'ambito lavorativo futuro.

L'esperienza del tirocinio ha completato il mio percorso formativo di studi, in cui la parte teorica della materia viene applicata per la gestione, progettazione, e risoluzione dei problemi di connessione e di rete per il corretto funzionamento della struttura.

Le motivazioni che mi hanno spinto ad intraprendere questo percorso sono state molte, in particolare la possibilità di capire come funziona il mondo del lavoro, e la possibilità di mettere in pratica tutto quello che ho studiato nel corso degli anni di università.

2. La rete aziendale

In questo capitolo verrà trattata la rete aziendale in tutti i suoi aspetti più significativi, a livello di gestione ed operabilità. Il processo di analisi e configurazione, portato avanti nel periodo di permanenza in azienda, è stato riportato in questa relazione suddividendolo in paragrafi che si focalizzano ognuno in contesti diversi, così da rendere ancora più facile ed intuitivo reperire le informazioni.

Al termine di ogni paragrafo inoltre si è deciso di includere un breve ma completo approfondimento delle tecnologie affrontate, che oltre ad essere utile, rende completo questo documento.

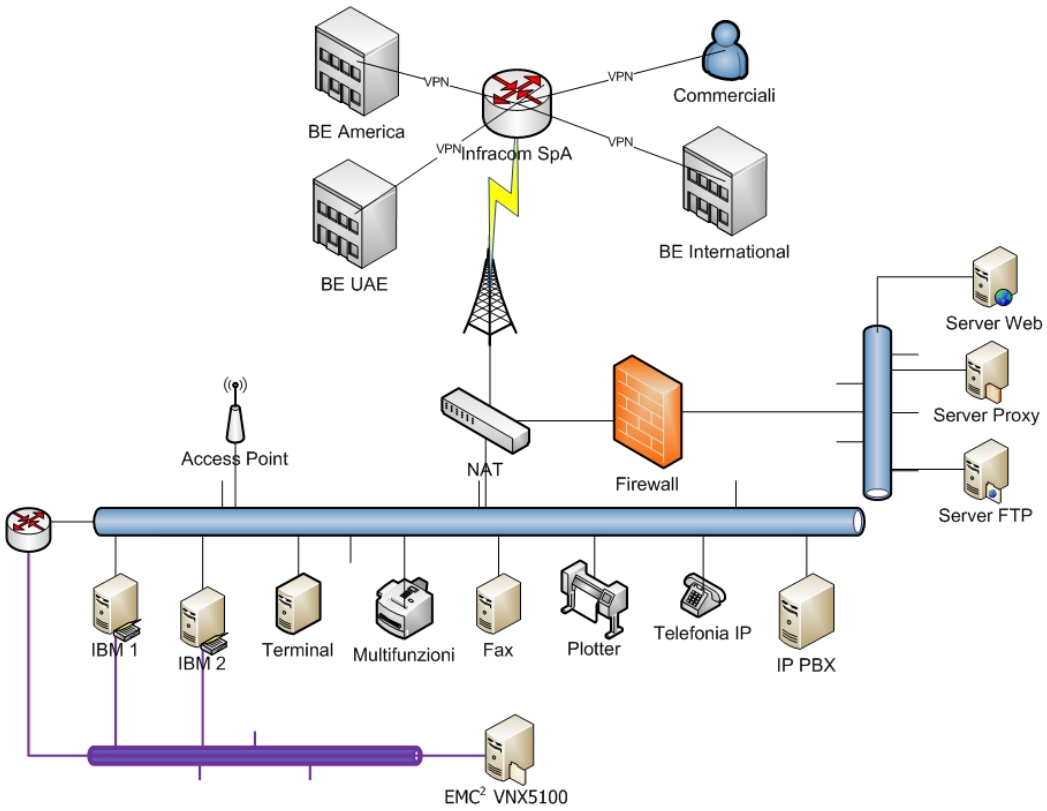

Figura 3: La rete - Schema concettuale

2.1. Connessione esterna

La connettività verso la rete Internet è offerta dalla società Infracom Italia S.p.A., un internet provider e compagnia telefonica che fornisce le aziende del territorio veneto. L'accesso è di tipo simmetrico in cui le velocità di download e upload equivalgono entrambi a 10Mbit/s mentre la banda minima garantita (Minimum Cell Rate) è di 10Mbit/s.

La rete aziendale utilizza un'antenna parabolica direzionale a griglia, posizionata sul tetto della fabbrica, per effettuare un ponte radio punto-punto, alle frequenze 2 e 5 GHz (per ridondanza), con un'altra antenna di proprietà di Infracom, situata a Badia Polesine (RO), e facente parte di una rete proprietaria di ponti radio che copre le provincie di Verona, Rovigo, Padova e Ferrara. L'antenna utilizzata presenta un guadagno di 17 dBi.

Sottoscrivendo un contratto con Infracom, l'azienda proprietaria della rete LAN, acquista oltre alla connessione Internet anche un pacchetto di indirizzi IPv4 pubblici, da utilizzare per pubblicare all'esterno svariati servizi. L'unico attualmente utilizzato e visibile dalla nuvola è 82.193.23.34 sul quale pervengono le richieste di connessioni VPN e su cui viene eseguito NAT.

Nel firewall, che è collegato all'antenna parabolica ed esegue la funzione di gateway per la rete aziendale verso Internet, è presente un software che gestisce le richieste di connessioni VPN utilizzando il protocollo IPsec.

Le connessioni VPN sono molto importanti soprattutto in aziende come questa in cui è presente più di una sede operativa e dove i commerciali e i dirigenti, che quotidianamente si spostano per raggiungere i clienti e non sono fisicamente in azienda, hanno bisogno di accedere in modo sicuro alle informazioni usufruendo della rete pubblica. Una VPN permette di estendere la propria rete privata, mantenendone la sicurezza intrinseca, senza il bisogno di affittare linee pubbliche ma utilizzando software con sistemi di autenticazione dell'utente e in alcuni casi di crittografia dei dati. Anche le varie sedi necessitano di entrare nella rete LAN di Badia Polesine tramite la rete Internet.

L'azienda utilizza un firewall hardware di proprietà di GateProtect per proteggere tutti i computer collegati in rete. Questo permette sicuramente una semplice manutenzione e gestione rispetto un firewall software. Oltre alle funzioni di NAT e

firewall, la soluzione comprende supporto VPN, antivirus, antispam, antispyware e il filtraggio dei contenuti.

Il maggior rischio nelle reti IT consiste nella complessità di gestione e numerosità delle funzioni avanzate di sicurezza che vengono introdotte. Questo porta inevitabilmente al rischio di aumento esponenziale degli errori di configurazione.

Grazie alla semplice e intuitiva interfaccia di gestione eGUI® dell'apparato GPA 250 di gateprotect, si è riuscito facilmente ad ovviare a questo problema rispettando appieno le esigenze dell'azienda, rendendo inoltre più rapidi i processi di gestione aziendali. Per proteggere efficacemente la rete aziendale, il firewall identifica quali pacchetti di dati possono entrare o uscire dalla rete in base a regole ben definite. In questo modo gli amministratori di sistema hanno la possibilità di abilitare per ogni singolo utente o gruppo di utenti qualunque tipo di servizio con le relative opzioni di sicurezza aggiuntive, come i proxy o il filtro web. Autenticandosi sul firewall con il proprio PC, l'utente usufruisce di tutti i servizi a lui assegnati. Infine gli amministratori di sistema possono filtrare il traffico di rete evitando qualsivoglia traffico indesiderato.

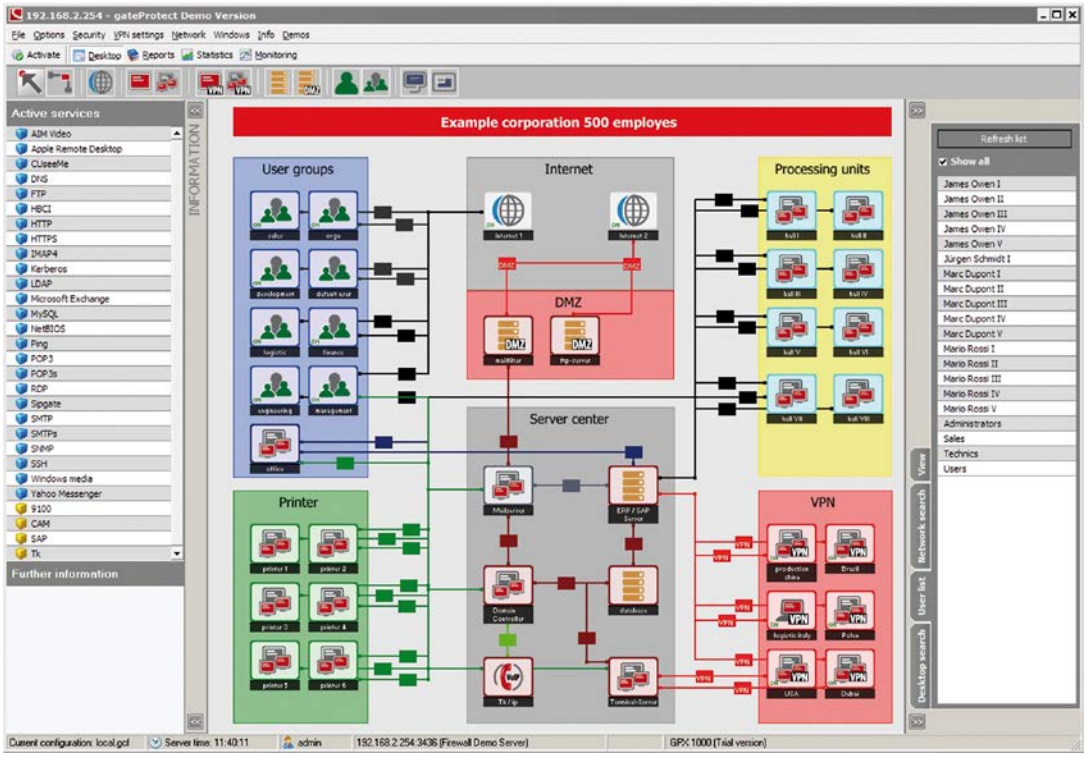

Figura 4: Interfaccia eGUI GateProtect

Mediante l'utilizzo del software di gestione dell'apparato GPA 250 di gateprotect, è stato inoltre possibile, senza difficoltà, la creazione tra la rete esterna e la rete interna di una speciale area chiamata DMZ (Demilitarized Zone), una zona demilitarizzata in cui sia il traffico esterno che quello interno sono fortemente limitati e controllati per poter implementare alcuni servizi che comunicano con l'esterno.

Tra le varie problematiche che ho affrontato insieme al mio tutor durante il periodo di permanenza nell'azienda, la più laboriosa è stata sicuramente l'aggiornamento e la configurazione del centralino telefonico di proprietà di 3CX. L'azienda era dotata inizialmente di un centralino PBX che permetteva agli utenti di effettuare un numero di chiamate interne ed esterne con un numero limitato di connessioni contemporanee. Vista la rapida crescita dell'azienda, che ha portato ad aumento accelerato di personale e l'apertura di nuove sedi all'estero, si è deciso di aggiornare il vecchio centralino alla nuova versione software sottoscrivendo il servizio di telefonia voip con il provider VoIPVoice, integrandolo con la già esistente linea PSTN per riutilizzare al meglio le attrezzature presenti in azienda. Questo sistema è risultato sicuramente molto più flessibile e soprattutto con costi di impianto e di esercizio notevolmente più bassi rispetto alla soluzione precedente.

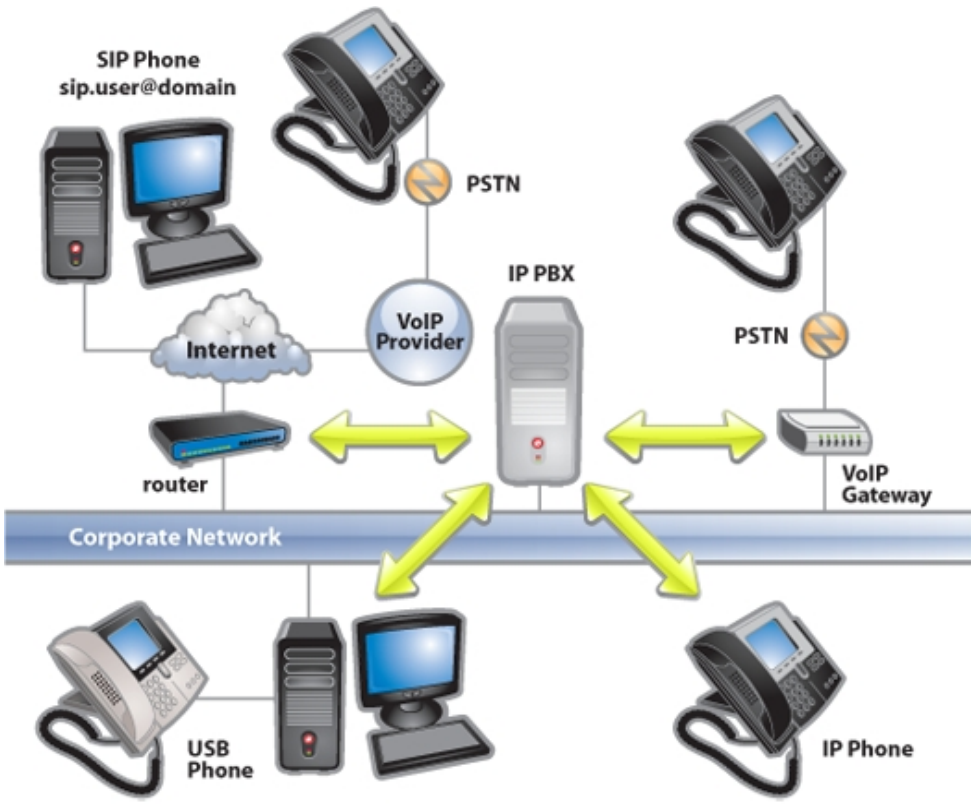

Figura 5: Schema concettuale centralino 3CX

2.1.1. VPN

Virtual Private Network o VPN è una rete di telecomunicazioni privata instaurata tra soggetti che utilizzano un sistema di trasmissione pubblico e condiviso come per esempio Internet. Le reti VPN utilizzano collegamenti che necessitano di autenticazione per garantire che solo gli utenti autorizzati vi possano accedere; per garantire la sicurezza che i dati inviati in Internet non vengano intercettati o utilizzati da altri non autorizzati, esse utilizzano sistemi di crittografia.

Oltre alla cifratura, una VPN sicura deve prevedere nei suoi protocolli dei meccanismi che impediscano violazioni della sicurezza, come ad esempio il furto dell'identità digitale o l'alterazione dei messaggi.

La VPN dal punto di vista operativo è un ottimo strumento di comunicazione per tutte quelle aziende con molteplici sedi, utenti remoti e partner dislocati in aree diverse che necessitano di accedere in modo sicuro ed a costi estremamente contenuti a servizi, dati o applicazioni normalmente disponibili solo quando direttamente connessi alla propria rete locale. Ad esempio la VPN risulta un ottimo strumento per tutte quelle aziende che vogliono dotare i loro dipendenti (es. personale mobile, rappresentanti commerciali …) di un accesso alla rete aziendale sicuro ed affidabile per consentire loro il download e l'upload di dati riservati, l'accesso a banche dati o l'esecuzione di applicazioni dedicate.

Esistono fondamentalmente tre tipologie di connessioni VPN:

- Trusted VPN
- Secure VPN
- Hybrid VPN

TRUSTED: La garanzia che la rete Trusted VPN offre è la sicurezza che nessun terzo non autorizzato possa usufruire del circuito del cliente. Questo implica che il cliente abbia un proprio indirizzo IP e una propria politica di sicurezza. Il cliente di una VPN si aspetta quindi che il fornitore della VPN mantenga l'integrità del circuito in modo da impedire l'accesso di intrusi.

Le aziende che utilizzano una Trusted VPN vogliono avere la sicurezza che i loro dati si muovano attraverso una serie di percorsi che hanno proprietà specifiche e che

sono controllati da un ISP (Internet Service Provider). È necessario dunque che nessuno al di fuori del fornitore possa cambiare nessuna parte della VPN. Queste reti non usano algoritmi di cifratura ma partono dal presupposto che un singolo soggetto fidato gestisca l'intera rete condivisa, e che quindi l'impossibilità di accedere al traffico globale della rete renda i singoli canali sicuri dato che il gestore della rete fornisce ad ogni soggetto solamente la sua VPN.

I protocolli che utilizzano questa filosofia sono: L2F (Layer 2 Forwarding, sviluppato da Cisco), L2TP (Layer 2 Tunnelling Protocol, sviluppato da Microsoft / Cisco), L2TPv3 (Layer 2 Tunnelling Protocol version 3) e MPLS (Multi Protocol Label Switching).

SECURE: Il vantaggio di utilizzare questo tipo di VPN è che i dati vengono criptati e possono essere trasportati in Internet come qualsiasi altro dato. Questo traffico criptato agisce come un “tunnel” tra due reti: anche se un intruso cercasse di leggere i dati non potrebbe decifrarne il contenuto né modificarli, dato che eventuali modifiche sarebbero immediatamente rilevate dal ricevente e quindi respinte.

Le Secure VPN sono particolarmente utili per permettere accessi remoti da parte di utilizzatori connessi ad Internet da zone non controllate dall'amministratore della rete, ed inoltre le proprietà di sicurezza di una VPN devono essere concordate da tutte le parti della VPN; gli amministratori delle due estremità del tunnel devono essere in grado di accordarsi sulle proprietà di sicurezza.

I protocolli più conosciuti che implementano una VPN sicura sono: IPsec (IP security, parte obbligatoria di IPv6), PPTP (point-to-point tunneling protocol, sviluppato da Microsoft), SSL/TLS, VPN Quarantine e ISPs.

Questi meccanismi non implementano di per sé una rete virtuale, ma solo un colloquio sicuro tra due terminali. In questi casi il meccanismo di rete virtuale deve essere realizzato mediante un protocollo apposito che viene poi incapsulato, vedi SSH, TLS, SOCKS, OpenVPN.

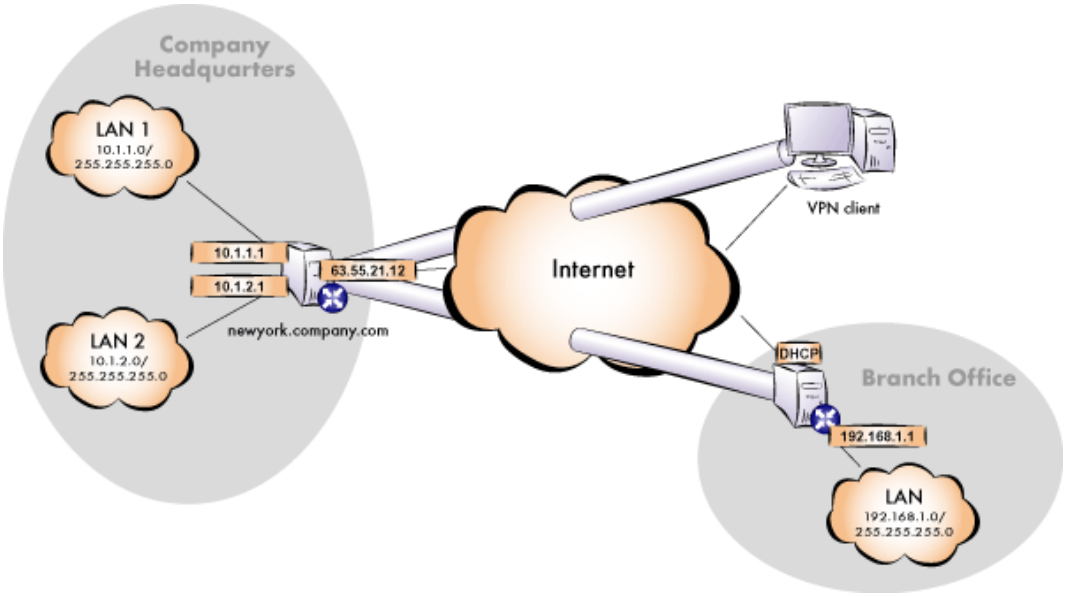

Figura 6: Schema di utilizzo di una rete VPN

2.1.2. NAT

NAT (Network Address Translation) è una tecnica usata per sostituire nell'intestazione di un pacchetto IP un indirizzo, sorgente o destinazione, con un altro indirizzo.

Nel suo impiego più diffuso viene usato per permettere ad una rete che usa una classe di indirizzi privata di accedere ad Internet usando uno o più indirizzi pubblici. E' stato studiato nel momento in cui ci si è accorti che lo spazio di indirizzamento IPv4 non era poi così grande come era sembrato al momento della sua creazione. All'inizio si credeva fosse una soluzione temporanea, e che l'implementazione di IPv6, che avrebbe risolto questo problema, sarebbe arrivata presto, invece la rapida crescita dell'accesso ad Internet e il ritardo nell'adozione di IPv6 ha reso il NAT una pratica molto comune. Col l'andare del tempo però si sono scoperte nuove potenzialità nell'utilizzo di tale soluzione ed è stata impiegata, con delle varianti per soddisfare altre esigenze; di seguito vengono presentati i metodi più comuni nell'utilizzare tale tecnica evidenziando le situazioni in cui risultano utili.

TRASLAZIONE STATICA: Il principio del NAT statico consiste nell'associare un indirizzo IP pubblico ad un indirizzo IP privato interno alla rete, fare cioè la

traduzione, in entrata o in uscita dalla rete interna del pacchetto IP modificandone l'indirizzo sorgente e/o di destinazione. Alcuni host possono avere la necessità di utilizzare un proprio ben determinato indirizzo pubblico in uscita pur conservando il proprio indirizzo privato. In questo caso tramite il NAT statico si può fare una mappatura 1:1 in cui è garantito il mascheramento, ma l'unicità dell'host in uscita permette di tradurre solamente l'indirizzo IP sorgente lasciando inalterata la porta TCP/UDP.

La traslazione di indirizzo statico permette quindi di connettere dei terminali della rete interna a Internet in maniera trasparente, ma non risolve il problema della penuria di indirizzo nella misura in cui n indirizzi IP smistati sono necessari per connettere n terminali della rete interna.

TRASLAZIONE DINAMICA: La NAT dinamica permette di condividere un indirizzo IP fra più terminali in indirizzamento privato, così tutti i terminali della rete interna sono virtualmente visti dall'esterno con lo stesso indirizzo; ed è la ragione per cui il termine IP masquerading è talvolta usato per designare il meccanismo di traslazione di indirizzo dinamico. Per poter condividere i diversi indirizzi IP privati su un unico indirizzo pubblico, il NAT dinamico usa il meccanismo di traslazione della porta (PAT, Port Address Translation o NAPT, Network Address and Port Translation), cioè l'attribuzione di una porta (TCP o UDP) sorgente diversa ad ogni richiesta in maniera tale da poter mantenere una corrispondenza tra le richieste provenienti dalla rete interna e le risposte dei terminali su Internet, tutte indirizzate all'unico IP pubblico disponibile.

PORT FORWARDING: Le tecniche di traduzione di indirizzo presentate in precedenza permettono solamente di collegare delle richieste che provengono dalla rete interna verso quella esterna mentre il contrario risulta impossibile visto che un utente esterno non è a conoscenza degli indirizzi privati della macchina da raggiungere nella rete interna (a meno che non sia stata impostata a priori una corrispondenza nel dispositivo che esegue la traduzione). Per superare questo ostacolo è stata proposta un'estensione del NAT detta Port Forwarding o Port mapping che consiste nel configurare il dispositivo che effettua la traduzione degli indirizzi in modo tale che riesca a trasmettere ad un terminale specifico della rete

interna, tutti i pacchetti ricevuti su una particolare porta. Esiste inoltre un meccanismo derivato del NAT, detto Port Triggering, che permette di autorizzare la connessione su certe porte se si verifica una determinata condizione.

Alcune applicazioni usano più di una porta per scambiare i dati con il server, e se il dispositivo che traduce gli indirizzi si aspettasse una risposta solo su una determinata porta, verrebbero eliminati numerosi pacchetti in arrivo su altre porte.

DOUBLE NAT: Talvolta è necessario far comunicare tra loro due LAN, ad esempio due sedi di una stessa azienda che utilizzano VPN, connesse ad Internet tramite IP masquerading. In alcuni casi però capita che le LAN utilizzino gli stessi range di indirizzi IP, quindi non è possibile collegarle direttamente, ma sarebbe necessario rinumerare una delle due reti, ovvero riassegnare indirizzi IP in una diversa sottorete a tutti gli host. Questa operazione è normalmente faticosa, comporta disservizi e spese, per cui spesso si preferisce ricorrere a configurazioni di Double NAT, che nascondono reciprocamente le due reti, permettendo loro di comunicare come se non usassero indirizzi IP sovrapposti.

2.1.3. Firewall

Il firewall è un apparato hardware che, lavorando ai livelli di rete, di trasporto e applicativo del modello ISO/OSI, filtra tutti i pacchetti entranti ed uscenti di una rete o di un computer applicando regole che ne contribuiscono alla sicurezza. In questo caso si parla di firewall perimetrale e può essere realizzato anche con un normale computer, con almeno due schede di rete, e software apposito. I firewall prevedono comunque la possibilità di filtrare ciò che arriva da una qualsiasi rete esterna sulla base di diversi tipi di criteri, non sempre relativi alla sicurezza informatica, ma volti a limitare gli utilizzi della rete sulla base di decisioni politiche, come per esempio la censura di siti Internet con contenuti non pertinenti con l'attività lavorativa che possono distrarre il lavoratore.

Oltre al firewall a protezione perimetrale ne esiste un secondo tipo, definito Personal Firewall, che si installa direttamente sui sistemi da proteggere e che effettua un controllo su tutti i programmi che tentano di accedere ad una rete esterna

dall'elaboratore sul quale è installato. Rispetto ad un firewall perimetrale, il personal firewall è eseguito sullo stesso sistema operativo che dovrebbe proteggere, ed è quindi soggetto al rischio di venir disabilitato da un malware che prenda il controllo del calcolatore con diritti sufficienti. A suo favore, però il personal firewall ha accesso ad un dato che un firewall perimetrale non può conoscere, ovvero può sapere quale applicazione ha generato un pacchetto o è in ascolto su una determinata porta, e può basare le sue decisioni anche su questo.

Usualmente la rete viene divisa dal firewall in due sottoreti: una, detta esterna, comprende la rete non sicura (solitamente Internet), mentre l'altra, interna, comprende una sezione più o meno grande di un insieme di computer locali. In alcuni casi però è possibile che si crei l'esigenza di avere una terza sottorete, detta DMZ (zona demilitarizzata), adatta a contenere quei sistemi che devono essere isolati dalla rete interna ma che comunque necessitano di essere protetti dal firewall. Spesso inoltre un firewall, a seconda delle esigenze, integra anche la funzione di gateway, esegue operazioni di NAT e gestisce connessioni VPN.

Esistono varie tipologie di firewall, in ordine crescente di complessità:

Packet Filter: Si limita a valutare gli header di ciascun pacchetto, decidendo quali far passare e quali no sulla base delle regole configurate.

Stateful inspection: Tiene traccia di alcune relazioni tra i pacchetti che lo attraversano, ad esempio ricostruisce lo stato delle connessioni TCP.

Deep inspection: Effettuano controlli fino al livello 7 della pila ISO/OSI, ovvero valutano anche il contenuto applicativo dei pacchetti.

Application layer firewall: Apparati che intercettano le connessioni a livello applicativo. A questa categoria appartengono i proxy. In tali casi, la configurazione della rete privata non consente connessioni dirette verso l'esterno ma sono permesse solo alcune connessioni in modo selettivo, e solo per i protocolli che supporta.

Il firewall resta comunque solo uno dei componenti di una strategia di sicurezza informatica, e non può quindi in generale essere considerato sufficiente per proteggere in modo totale una rete che necessita di molti accorgimenti hardware e software.

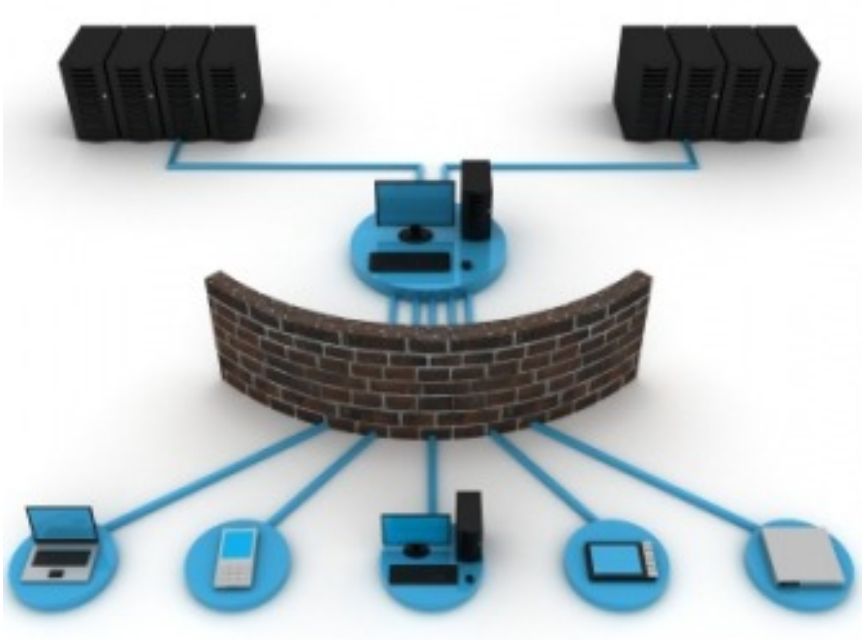

Figura 7: Rappresentazione schematica del firewall

2.1.4. DMZ

Quando alcuni terminali della rete interna devono essere accessibili dall'esterno (server web, server di posta, server FTP pubblico, ecc.), è spesso necessario creare una nuova interfaccia verso una rete a parte, accessibile sia dalla rete interna che da quella esterna, senza per altro rischiare di compromettere la sicurezza dell'azienda. Questa nuova rete è chiamata DMZ (DeMilitarized Zone), è un'area in cui sia il traffico proveniente dall'esterno che quello LAN sono fortemente limitati e controllati; in pratica si crea una zona cuscinetto tra interno ed esterno che viene attestata su una ulteriore interfaccia di rete del firewall oppure viene creata aggiungendo un firewall.

Se non è prevista una zona DMZ, nel malaugurato caso in cui un servizio in LAN fosse compromesso in seguito ad una vulnerabilità, l'aggressore potrebbe raggiungere anche gli altri host della rete, dato che in LAN non esiste isolamento tra il server e gli altri nodi. Se lo stesso problema si verificasse in DMZ, l'attaccante avrebbe grosse difficoltà a raggiungere la LAN, poiché il traffico verso la rete LAN è fortemente limitato dal firewall. Architetture più complesse possono implicare la presenza di più zone DMZ distinte con il relativo controllo del traffico su tutti i lati creando diversi livelli di protezione per evitare le intrusioni.

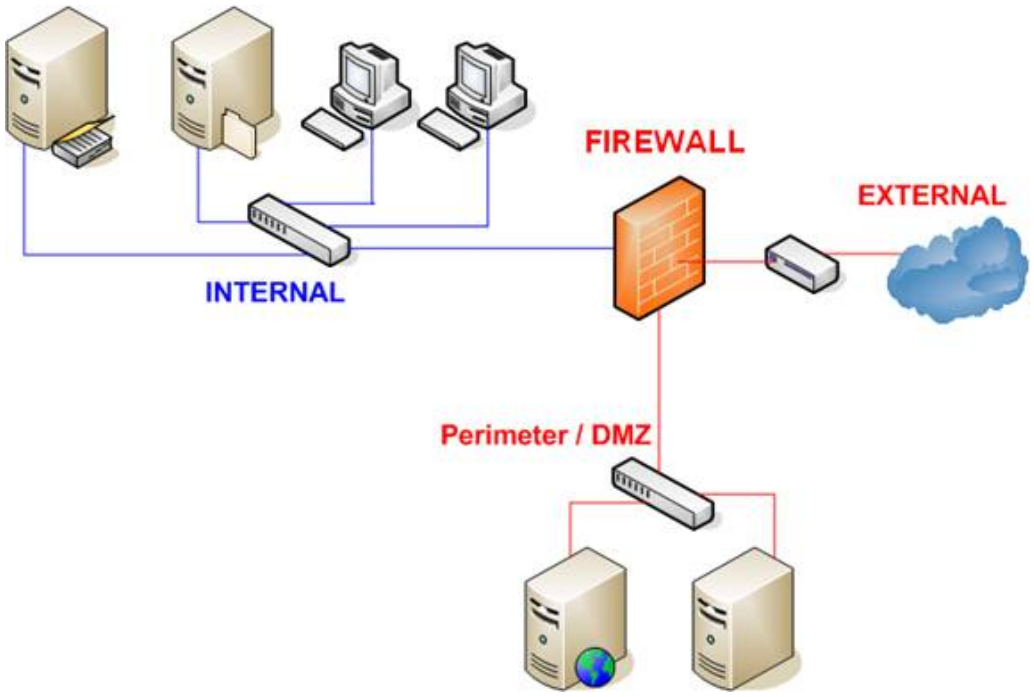

Figura 8: Rappresentazione rete DMZ

2.1.5. PBX e IP PBX

Il PBX è una centrale telefonica per uso privato. E' usato nelle aziende per fornire una rete telefonica interna. Il vantaggio di avere un centralino telefonico aziendale è quello di poter risparmiare sul numero di canali di fonia da chiedere in affitto ad un provider del servizio telefonico anziché avere una linea dedicata per ciascun utente

all’interno dell’azienda: infatti il numero di canali disponibili garantiti in uscita può essere dimensionato in base al traffico medio dell’azienda.

Ogni centralino svolge, di base, questi tre compiti:

- instaura una connessione (circuito) fra gli apparati telefonici dei 2 utenti, mappando il numero chiamato in un telefono fisico, verificando che questo non sia impegnato;
- mantiene questa connessione per tutto il tempo necessario tramite un meccanismo di segnalazione;
- fornisce informazioni sulla durata e il costo della connessione.

Oltre alle funzioni base, possono essere presenti svariate altre funzionalità. Tra i più comuni vi è l’IVR (Interactive Voice Response), sistema interattivo con menù vocali preregistrati selezionabili tramite tastiera.

L’IP PBX invece è un sistema di commutazione telefonica per aziende in grado di passare le chiamate tra gli utenti VoIP (Voice over IP) sulle linee locali; inoltre, consente a tutti gli utenti di condividere un certo numero di linee telefoniche esterne. Un sistema IP PBX standard può anche passare chiamate da un utente VoIP a un utente telefonico tradizionale oppure tra due utenti telefonici tradizionali, come un sistema PBX convenzionale. Con un sistema PBX convenzionale, è necessario separare le reti per la comunicazione vocale e per la comunicazione dei dati. Uno dei principali vantaggi di un sistema IP PBX è che utilizza reti di dati e reti vocali convergenti. Ciò vuol dire che è possibile stabilire l’accesso alla rete, ma anche le comunicazioni VoIP e le comunicazioni telefoniche tradizionali, utilizzando una singola linea (vedi fig.5, paragrafo 2.1).

In un IP PBX è possibile utilizzare tre tipi di codec VoIP:

- G.711 μ-law
- G.711 A-law
- G.723.1

G.711 è uno standard sviluppato per l'utilizzo con i codec audio. Nello standard G.711 sono definiti due algoritmi principali: l'algoritmo μ-law, utilizzato in Nord America e in Giappone e l'algoritmo A-law, utilizzato in Europa e in altri paesi. Il codec audio G.723.1 è utilizzato soprattutto nelle applicazioni VoIP e per l'uso è

richiesta una licenza. Il codec G.723.1 è un tipo di codec di elevata qualità e ad alta compressione.

Un sistema IP PBX può offrire i codec G.711 e G.723.1. Per impostazione predefinita, il primo codec da utilizzare è G.723.1. Tra i codec più comuni troviamo perciò:

- G.711: larghezza di banda 64kbps; questo codec richiede un'elaborazione molto bassa. Necessita di un minimo di 128Kbps per la comunicazione a due vie.
- G.723.1: larghezza di banda da 5.3kbps a 6.3kbps; questo codec offre un'elevata compressione con alta qualità audio e richiede una maggiore elaborazione rispetto al codec G.711. Il codec G.723.1. utilizza una larghezza di banda ridotta ma offre una qualità audio più alta.

2.1.6. VoIP

Il VoIP, Voice over IP (Voce tramite protocollo Internet), è una tecnologia che rende possibile effettuare una conversazione telefonica sfruttando una connessione Internet o una qualsiasi altra rete dedicata a commutazione di pacchetto che utilizzi il protocollo IP senza connessione per il trasporto dati.

Con VoIP si intende l'insieme dei protocolli di comunicazione di strato applicativo che rendono possibile tale tipo di comunicazione. Grazie a numerosi provider VoIP è possibile effettuare telefonate anche verso la rete telefonica tradizionale (PSTN). In realtà più in generale VoIP consente una comunicazione audio-video real-time, unicast o multicast, su rete a pacchetto (es. videotelefonata, videochiamata e videoconferenza).

Il vantaggio principale di questa tecnologia sta nel fatto che essa elimina l'obbligo di riserva della banda per ogni telefonata (commutazione di circuito), sfruttando l'allocazione dinamica delle risorse, caratteristica dei protocolli IP (commutazione di pacchetto). Vengono instradati sulla rete pacchetti di dati contenenti le informazioni vocali, codificati in forma digitale, e ciò solo nel momento in cui è necessario, cioè quando uno degli utenti collegati sta parlando.

Le conversazioni VoIP non devono necessariamente viaggiare su Internet, ma possono anche usare come mezzo trasmissivo una qualsiasi rete privata basata sul protocollo IP, per esempio una LAN all'interno di un edificio o di un gruppo di edifici. I protocolli usati per codificare e trasmettere le conversazioni VoIP sono solitamente denominati Voice over IP protocols. Uno dei vantaggi di questa tecnologia è che permette di fare leva su risorse di rete preesistenti, consentendo una notevole riduzione dei costi in ambito sia privato che aziendale, specialmente per quanto riguarda le spese di comunicazione interaziendali e tra sedi diverse. Una rete aziendale, infatti, può essere sfruttata anche per le comunicazioni vocali, permettendo di semplificare l'installazione e il supporto e di aumentare il grado di integrazione di uffici dislocati sul territorio, ma collegati tramite l'infrastruttura di rete.

La tecnologia VoIP richiede due tipologie di protocolli di comunicazione in parallelo, una per il trasporto dei dati (pacchetti voce su IP), ed una per la segnalazione della conversazione (ricostruzione del frame audio, sincronizzazione, identificazione del chiamante, etc). Nella grande maggioranza delle implementazioni VoIP, per il trasporto dei dati, viene adottato il protocollo RTP (Real-time Transport Protocol). Invece per la seconda tipologia di protocolli necessari alla telefonia via Internet, il processo di standardizzazione non si è ancora concluso. Al momento, sono coinvolti tre enti internazionali di standardizzazione: ITU (International Telecommunications Union), IETF (Internet Engineering Task Force) ed ETSI (European Telecommunication Standard Institute) con alcuni consorzi (per esempio, Softswitch, H.323ORG, Vivida ecc.). La gestione delle chiamate voce sulla rete IP, al momento, è indirizzata verso due differenti proposte, elaborate in ambito ITU e IETF, che sono rispettivamente H.323 e SIP (Session Initiation Protocol).

2.2. La rete interna

La rete interna è organizzata in modo da prevedere un segmento privato per la gestione delle operazioni di backup, un segmento DMZ nel quale risiedono i servizi che vengono proposti sulla rete pubblica ed infine un segmento privato che contiene i server e gli host degli utenti della LAN principale.

La rete di backup gestisce le operazioni di salvataggio e memorizzazione dei dati su dispositivi di storage con una procedura accurata e appositamente implementata. L'utilizzo di questa rete, sebbene comporti un maggiore utilizzo di dispositivi e quindi maggiore spazio, risultando un sistema poco economico, permette una gestione più agevole delle operazioni di backup, e principalmente separa il traffico generato dalle operazioni di salvataggio da quello della rete principale, che ne guadagna in termini di prestazioni.

Nella rete principale invece sono attivi i server e gli host necessari a svolgere le attività aziendali, siano essi elaboratori degli utenti, telefoni IP o stampanti multifunzione.

Durante il periodo di permanenza nell'azienda, è stato svolto inoltre un'attenta analisi di tutti i nodi della rete, completando la scarsa documentazione disponibile riguardante i collegamenti degli switch e delle macchine ai patch panel, in modo tale da poter individuare quali connessioni terminassero verso altri nodi della rete o avessero come destinazioni host finali. Se non si teneva uno schema aggiornato del modo in cui le varie sezioni della rete si interfacciano ai patch panel, veniva applicata un'etichetta / targhetta identificativa ad ogni porta in modo tale da tenere comunque traccia delle destinazioni e poter effettuare connessioni rapide e precise. In alcuni patch panel però è capitato non fossero presenti né le etichette sulle porte né uno schema che potesse in qualche modo dare informazioni sulla destinazione del collegamento. Una volta individuate le destinazioni finali delle connessioni o eventualmente la collocazione del relativo patch panel utilizzando un tester per reti LAN, si è provveduto immediatamente ad applicare delle etichette / targhette sulle porte del patch panel assegnando, in formato stringa, il nome della porta a cui erano connesse o, nel caso il collegamento fosse verso un dispositivo di rete, il reparto in cui si trovava il patch panel a cui era collegato.

Tutto ciò che riguarda il patch panel e il modo con cui si effettuano le connessioni solitamente non influisce sulle prestazioni e sulla qualità delle tramissioni in rete; avere però a disposizione una struttura ben organizzata, facilmente gestibile e di cui si conosce bene la topologia rende la vita molto più facile agli amministratori in caso di manutenzione.

Si è constatato che la rete aziendale non presenta una tecnologia ethernet omogenea perché al suo interno vengono utilizzati differenti mezzi di connessione e differenti velocità di trasmissione, che comportano la presenza di tre diversi standard: 100BaseTX, (mezzo trasmissivo UTP cat5e, utilizzato per collegare gli host agli switch), 1000BaseTX (mezzo trasmissivo UTP cat6, utilizzato per collegare gli switch ai server) e 1000BaseSX (mezzo trasmissivo fibra ottica). La fibra ottica è utilizzata solo per collegamenti a 1000 Mbps tra gli switch della rete di backup in modo tale da non creare colli di bottiglia dove il traffico di pacchetti è elevato.

I server presenti fisicamente in azienda (alcune macchine presentano più server virtualizzati) sono distribuiti in due stanze, SiteA e SiteB. La scelta di utilizzare due locali è stata presa per rendere meno affollate e più agevoli le stanze ma soprattutto per proteggere i server, e quindi garantire la continuazione della produzione nel caso si verificasse un incendio, un allagamento o altri eventi simili in uno dei due reparti. In sala SiteA sono presenti i server più importanti della rete principale, per quel che riguarda la linea produttiva e la gestione amministrativa, e quelli appartenenti alla rete DMZ, mentre in SiteB sono stati posizionati i server meno importanti e soprattutto alcuni duplicati di quelli in SiteA che serviranno in caso di emergenza per sostituire la loro copia principale. In SiteA sono presenti anche i server che contengono il software gestionale dell'azienda, che oltre a far parte della rete LAN principale aderiscono alla rete di backup, e il server che ne gestisce le operazioni di salvataggio.

Server IBM X3650 M4

Rappresenta il cuore di tutta la rete informatica aziendale al quale spetta il compito di gestirne le operazioni fondamentali. Sistema scalabile e virtualizzato, con una serie di caratteristiche ben definite che consentono la massima connettività, la continuità del servizio e l’integrità dei dati.

Processore	**Intel Xeon 6Core E5-2620 2.00 GHz /15MB Processore Intel Xeon**
Numero di processori installati	**2**
Ctrl Disco	IBM ServeRAID M5014 SAS/SATA controller on riser card / PCI-Express / supports RAID-0/1/10/5/50 /
Numero dischi installati	**2 x 300GB SAS**
Memoria installata	**128 GB (con 16 moduli da 8GB)**
Memoria RAM max.	768 GB
Alloggiamenti RAM (totali/disponibilità)	18 DIMM (2 DIMM)
Cache di secondo livello interna	12MB
Scheda di rete	**8 Porte Gigabit**
Dispositivi	DVD
Alimentatore	**2 x 550W ridondato**
Dimensioni	443,6mm 698mm 85,4mm
HBA	**QLogic 8Gb FC Dual Port HBA**

Figura 9: Caratteristiche IBM X3650 M4

Questo server, denominato come IBM1, sito nella sala server SiteA, presenta più server virtualizzati: un server virtualizzato con sistema operativo Windows Server 2008 R2 utilizzato per la gestione del documentale aziendale Arxivar, il programma gestionale Microsoft Dynamics AX 2012 e i disegni tecnici di progettazione degli impianti; un server virtualizzato con sistema operativo Windows Server 2003 che distribuisce la connettività agli utenti della rete aziendale e ne fornisce l'accesso ai servizi ai quali sono abilitati e gestisce i profili di sicurezza.

Esiste un altro server denominato IBM2, sito nella sala server SiteB , che è la copia integrale del server IBM1. Servirà a sostituirlo in caso d'emergenza.

Entrambi sono collegati mediante un segmento privato in fibra ottica, standard 1000BaseSX, da una coppia di switch Brocade DS300B, interfaccia 802.3z da 8Gbps, da 24 porte ciascuno. Insieme costituiscono la Storage Area Network di tutto il sistema.

Server EMC^2 VNX5100

Rappresenta la struttura di storage del sistema informativo aziendale. Collegata al segmento SAN, questa soluzione è composta da due piattaforme EMC^2 VNX 5100, una esattamente la copia dell'altra, che, servirà in caso di disastro o blocco di uno dei due siti.

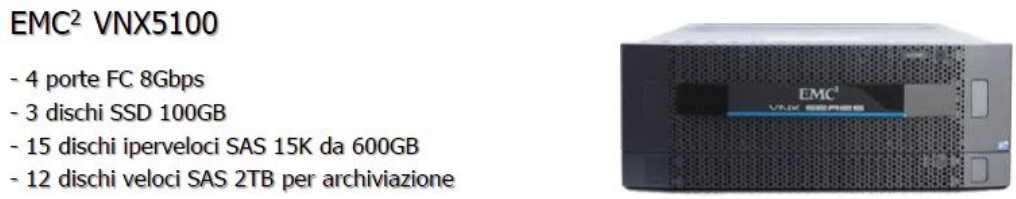

Figura 10: Soluzione storage VNX5100

Presenta inoltre una suite di programmi con i quali le permetterà un'ottimizzazione automatica per garantire le massime prestazioni di sistema, il minor costo di storage e al tempo stesso una protezione dei dati da errori localizzati, da interruzioni dell'attività e da guasti irreparabili.

2.2.1. Server

Il server indica genericamente un componente o sottosistema informatico che fornisce, a livello logico e a livello fisico, un qualunque tipo di servizio ad altre componenti (tipicamente chiamate client) attraverso una rete di computer, all'interno di un sistema informatico o direttamente in locale su un computer. Rappresenta dunque un nodo terminale della rete opposto all'host client e fornisce i dati richiesti da altri elaboratori, facendo quindi da Host per la trasmissione delle informazioni virtuali.

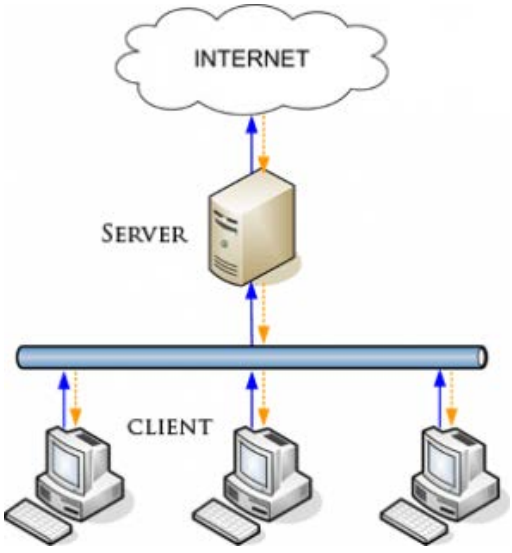

Figura 11: Rappresentazione schematica client-server

Tra i servizi che vengono tipicamente erogati da un server o più server e che ne identificano a sua volta le varie tipologie, si possono citare:

- File server, permette agli utenti di accedere ai file situati sul server come se fossero sul proprio calcolatore, agevolando la condivisione di informazioni;
- Database server, permette di gestire intere banche dati;
- FTP server, fornisce alla rete accesso a cartelle pubbliche o con autenticazione;
- Web server, usato per ospitare un sito web (es. server HTTP);
- Application server, usato per far funzionare un programma applicativo sul Web (applicazione Web) e condividerne le funzionalità tra gli utenti;
- Mail server, usato per la gestione della posta elettronica;
- Print server, permette di mettere in comune una o più stampanti tra gli utenti di una rete con la eventuale gestione dei diritti di accesso;
- DHCP server, per l'assegnazione automatica di indirizzi IP ai computer host;
- Proxy server, fornisce una cache di accesso al Web e la possibilità di controlli di autenticazione e di filtro

2.2.2. NAS e SAN

Un Network Attached Storage (**NAS**) è un dispositivo collegato ad una rete di computer la cui funzione è quella di condividere tra gli utenti della rete un'area di storage (o disco). Il NAS (Network Attacched Storage) è un server con un sistema operativo preinstallato (firmware), una scheda di rete e diversi hard disk destinati all'immagazzinamento dei dati. Il sistema operativo integrato permette di specificare i diritti di accesso alle cartelle e ai file rendendoli disponibili su diverse piattaforme, implementando i protocolli più diffusi come FTP (File Transfer Protocol), NFS (Network File System) e Samba, per esportare i dati in una rete TCP/IP.

Normalmente un NAS consente l'eventuale rimozione ed aggiunta di dischi “a caldo”, senza la necessità di disattivare l'unità (hot-swap). Uno tra i più importanti vantaggi offerti dai NAS è quello di permettere di centralizzare

l'immagazzinamento dei dati in un solo dispositivo altamente specializzato e accessibile a tutti i nodi della rete. Nell'ambito dell'adozione di una soluzione NAS un eventuale svantaggio potrebbe essere costituito invece dall'enorme quantità di dati che viene a transitare sulla rete.

I NAS sono dunque indicati per ambienti in cui conta l'economicità di acquisto e la flessibilità di gestione, e in cui le prestazioni siano un fattore secondario. La suite TCP/IP utilizzata per lo scambio di dati è adatta per inviare e ricevere piccole quantità di informazioni, ma poco indicato per quelle situazioni dove sia richiesto un traffico dati elevato.

Sistemi NAS permettono inoltre di implementare schemi RAID (Redundant Array of Independent Disks) garantendo una migliore gestione della sicurezza dei dati. Il RAID è un sistema informatico che usa un insieme di dischi rigidi per condividere o replicare le informazioni e i benefici sono di aumentare l'integrità dei dati, la tolleranza ai guasti e le prestazioni rispetto all'uso di un disco singolo. Il RAID può essere implementato sia con hardware dedicato sia con software specifico su hardware di uso comune, e i dati vengono partizionati in segmenti di uguale lunghezza (configurabile) e scritti su dischi differenti. Con il passare degli anni, sono nate diverse implementazioni del concetto di RAID e ognuna presenta vantaggi e svantaggi:

- RAID 0: Divide i dati equamente tra due o più dischi con nessuna informazione di parità o ridondanza (operazione detta di striping). I dati sono condivisi tra i dischi e i dischi non possono essere sostituiti visto che sono tutti dipendenti tra di loro.
- RAID1: Crea una copia esatta (mirror) di tutti i dati su due o più dischi. È utile nei casi in cui la ridondanza è più importante che usare tutti i dischi alla loro massima capacità. Ogni disco può essere gestito autonomamente nel caso l'altro si guasti.
- RAID2: Divide i dati al livello di bit (invece che di blocco) e usa un codice di Hamming per la correzione d'errore che permette di correggere errori su singoli bit e di rilevare errori doppi.
- RAID3: Usa una divisione al livello di byte con un disco dedicato alla parità. È estremamente raro nella pratica e uno degli effetti collaterali è che non può eseguire richieste multiple simultaneamente.

- RAID4: Usa una divisione a livello di blocchi con un disco dedicato alla parità. Permette ad ogni disco appartenente al sistema di operare in maniera indipendente quando è richiesto un singolo blocco.
- RAID5: Usa una divisione dei dati a livello di blocco con i dati di parità distribuiti tra tutti i dischi. Questa è una delle implementazioni più popolari, sia in hardware che in software. Il blocco di parità è letto solamente quando la lettura di un settore dà un errore.
- RAID6: Usa una divisione a livello di blocchi con i dati di parità distribuiti due volte tra tutti i dischi. Nel RAID6 il blocco di parità viene generato e distribuito tra due blocchi di parità, su due dischi separati.
- RAID 0+1: È la combinazione in ordine di RAID 0 e RAID 1.
- RAID 1+0: È la combinazione in ordine di RAID 1 e RAID 0.

Una Storage Area Network (**SAN**) è una rete o parte di una rete ad alta velocità (generalmente Gigabit/sec) costituita da dispositivi di memorizzazione di massa, in alcuni casi anche di tipologie e tecnologie differenti e apparecchiature di interconnessione dedicate. Il suo scopo è quello di rendere tali risorse di immagazzinamento (storage) disponibili per qualsiasi computer (generalmente application e DDBB server) connesso ad essa. La SAN quindi è una rete dedicata allo stoccaggio aggregato alle reti di comunicazione dell'azienda. I computer con accesso al SAN hanno un'interfaccia di rete specifica collegata al SAN, oltre alla loro interfaccia di rete tradizionale; il traffico SAN è completamente separato dal traffco utenti e sono i server applicativi che giocano il ruolo di interfaccia tra la rete di dati e la rete utenti.

I protocolli attualmente più diffusi, usati per la comunicazione all'interno di una SAN, sono FCP (Fiber Channel Protocol), utilizzato con connessioni in fibra e cavi in rame ad alta velocità (sia arriva fino 10/20 Gigabit/s) tra server e array di dischi; iSCSI (Internet SCSI), quest'ultimo lavora sopra la pila TCP/IP ed è utilizzato per connessioni a basso costo tra host e SAN in reti ethernet. Server multipli, prodotti da fornitori diversi, su cui si eseguono sistemi operativi diversi possono essere tutti connessi ad una SAN che può essere interconnessa a più reti anche di natura diversa. Il vantaggio di un'architettura di questo tipo è che tutta la potenza di calcolo dei server è utilizzata per le applicazioni, in quanto i dati non risiedono direttamente

in alcuno di questi. Ogni server che effettua una connessione verso una SAN necessita di una speciale scheda denominata host bus adaptor (HBA), tipica del protocollo e del cavo utilizzato per il collegamento. Sebbene spesso trascurato, il software di gestione della rete SAN, costruito in moduli o integrato in un unico strato, è forse la parte più importante e oltre a fornire la possibilità di implementare sistemi RAID permette la virtualizzazione dello storage.

2.2.3. Cavo UTP

UTP è l'acronimo di Unshielded Twisted Pair e identifica un cavo non schermato utilizzato comunemente per il collegamento nelle reti ethernet. Quando si parla di cavo non schermato si intende che esso, al contrario di un cavo schermato (STP, S/STP, S/UTP), non è rivestito da un involucro mettalico, tipicamente una calza di rame stagnato, che serve a ridurre i disturbi in ambienti dove le interferenze elettromagnetiche sono elevate. UTP è composto da otto fili di rame intrecciati a coppie. Ciascuna coppia è intrecciata con passo diverso e ogni coppia è intrecciata con le altre. L'intreccio dei fili ha lo scopo di ridurre il crosstalk o diafonia. La diafonia è un'interferenza elettromagnetica dovuta a due cavi vicini di un circuito o di un apparato elettrico. Dato un filo in cui scorre corrente infatti, viene generato un campo magnetico; se questo campo è variabile ed è presente un secondo conduttore che forma una spira chiusa, allora viene generata una tensione che può disturbare il segnale. In questo caso l'effetto è proporzionale alla distanza, all'area della spira, al suo orientamento e all'intensità della corrente. La diafonia inoltre, come la distorsione, l'attenuazione e la sensibilità ai segnali esterni variano al variare della frequenza del segnale; occorre pertanto chiedersi quale sia la frequenza di segnale adatta per ogni determinata applicazione.

Intrecciando i fili in rame (binatura) si riduce questo effetto perchè in questo modo i campi magnetici prodotti, essendo grandezze vettoriali, producono tensioni indotte tali da annullarsi a vicenda. In questo modo però si va incontro anche al fenomeno del delay skew, ovvero una variazione nel ritardo di propagazione del segnale sulle singole coppie dovuta al diverso passo di binatura delle coppie in un cavo multi coppia.

I cavi UTP seguono le specifiche standardizzate in TIA/EIA21 che li dividono in varie categorie in base ad esempio al numero di intrecci e alle capacità di trasportare segnali.

- Categoria 1: (TIA/EIA-568): usata per la rete telefonica generale, ISDN e per i citofoni.
- Categoria 2 (non riconosciuta): Usata per le reti Token Ring a 4 Mbit/s.
- Categoria 3: (TIA/EIA-568): Usata per reti con frequenze fino a 16 MHz, diffusa in reti Ethernet a 10 Mbit/s.
- Categoria 4 (non riconosciuta): Usata per reti con frequenze fino a 20 MHz, ad esempio Token Ring a 16 MHz.
- Categoria 5 (non riconosciuta): Usata per reti con frequenze fino a 100 MHz, ad esempio 100BaseTX; è utilizzabile anche per 1000BaseT.
- Categoria 5e (TIA/EIA-568): Usata per reti con frequenze fino a 120 MHz, ad esempio FastEthernet e GigabitEthernet; “e” sta per “enhanced” cioè “migliorato”.
- Categoria 6 (TIA/EIA-568): Usata per reti con frequenze fino a 250 MHz, usata in 1000BaseT e utilizzabile anche per reti 10GigabitEthernet.
- Categoria 6a (TIA/EIA-568): In sviluppo per reti con frequenze fino a 500 MHz, usata in 10GigabitEthernet.

La lunghezza massima di un cavo UTP a prescindere dallo standard ethernet utilizzato è di 100 m, superato tale valore il segnale che arriva al destinatario degrada troppo.

Un cavo UTP termina con dei connettori di tipo 8P8C (8 position 8 contact), che si innestano direttamente nell'interfaccia del dispositivo sia esso una scheda di rete, un hub, uno switch o un router. Questi connettori sono chiamati anche RJ-45 (dall'inglese Registered Jack tipo 45) e costituiscono un'interfaccia fisica specifica usata nell'attestazione di cavi elettrici a coppie di conduttori incrociati. Va ricordato inoltre che negli standard 10BaseT, 100BaseTX e 1000Base-TX vengono utilizzate solo due delle quattro coppie di fili (2 e 3), una per la trasmissione dei segnali e una per la ricezione, mentre in 1000BaseT si utilizzano tutte e 4 le coppie di conduttori. Se si devono collegare due dispositivi simili come per esempio PC-PC, SWITCH-HUB o PC-ROUTER si utilizza un cavo di tipo cross (incrociato) mentre se si

devono connettere dispositivi diversi come per esempio PC-SWITCH, uno diritto. I cavi diritti presentano gli 8 fili nello stesso ordine in entrambi i 2 connettori, mentre quelli cross presentano una sequenza diversa: in 1000BaseT, sono invertite le coppie 2-3 e 1-2 mentre in 10BaseT, 100Base-TX e 1000BaseTX sono scambiate solamente le coppie 2-3, cioè quelle in cui viaggiano i dati. Nella costruzione del cavo, ovvero nel crimpare i connettori, alle sue estremità si possono seguire due standard: TIA/EIA 568A o TIA/EIA 568B che presentano le coppie 2 e 3 scambiate di posto. Non ha importanza quale dei due standard si sceglie nelle proprie connessioni perché non influiscono sulle prestazioni, ma è necessario mantenere la stessa logica di scelta per l'intera rete. Da alcuni anni, tuttavia, grazie a nuove generazioni di chip d'interfaccia, le schede di rete dei dispositivi sono in grado di supportare l'autosensing, una caratteristica che consente di utilizzare qualsiasi tipologia di cavo conforme agli standard per interconnettere qualsivoglia combinazione di apparato senza preoccuparsi di sceglierne uno dritto o incrociato.

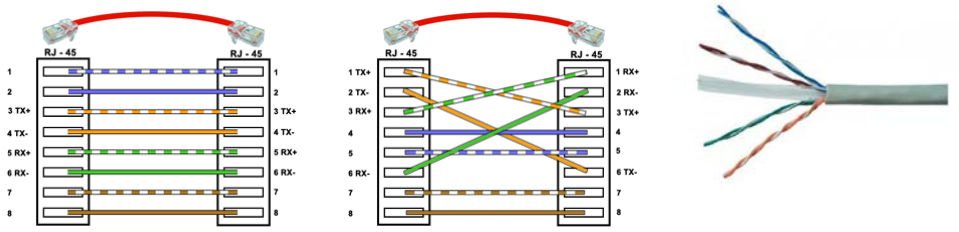

Figura 12: Da sinistra a destra, cavo UTP dritto, incrocia e UTP cat6

2.2.4. Fibra ottica

Le fibre ottiche sono filamenti di materiali vetrosi o polimerici, realizzati in modo da poter condurre la luce. In un sistema ottico come le fibre, i segnali vengono trasmessi sotto forma di fotoni che non hanno carica elettrica e quindi non possono essere influenzati da campi elettrici e magnetici. Attraverso i fotoni inoltre si esclude qualsiasi forma di crosstalk dato che la bassa perdita di flusso luminoso, che può avvenire all'interfaccia di bordo della fibra, è trattenuta dal rivestimento opaco che la avvolge, garantendo così che segnali ottici non interferiscano con altri provenienti da fibre poste in prossimità. Ogni singola fibra ottica è composta da due strati concentrici di materiale trasparente estremamente puro: un nucleo cilindrico centrale (core), ed un mantello (cladding) attorno ad esso.

La fibra ottica funziona come una specie di specchio tubolare. La luce che entra nel core ad un certo angolo si propaga mediante una serie di riflessioni sulla superficie di separazione fra i due materiali del core e del cladding. Le fibre ottiche sfruttano il principio della deviazione che un raggio di luce subisce quando attraversa il confine fra due materiali diversi (core e cladding nel caso delle fibre); la deviazione dipende dagli indici di rifrazione dei due materiali, il cladding in questo caso deve avere un indice di rifrazione minore rispetto al core. Oltre un certo angolo di rifrazione, a meno che la fibra non compia curve troppo brusche, il raggio rimane intrappolato all'interno del materiale. C'è da dire però che una parte del raggio luminoso, quindi una parte del segnale viene comunque disperso fuori dal core in quantità diverse a seconda dell'angolo di rifrazione.

Le fibre ottiche sono di due tipi:

- Multimodali: Raggi diversi possono colpire la superficie con diversi angoli (detti modi), proseguendo quindi con diversi cammini.
- Monomodali: Sono così sottili che si comportano come una guida d'onda: la luce avanza in modo rettilineo, senza rimbalzare.

Per quanto riguarda le fibre multimodali il diametro del core è di 50 µm o 62,5 µm, più o meno la dimensione di un capello, mentre per le fibre monomodali il diametro è di 8 µm o 10 µm. Per entrambe il diametro del cladding è di 125 µm.

Le fibre monomodali sono certamente più costose ma riescono a reggere velocità più elevate e distanze ben più lunghe, prima che sia neccessario un amplificatore ottico, rispetto alle multimodali.

All'esterno della fibra vi è una guaina protettiva polimerica detta “racket” che serve a dare resistenza agli stress fisici e alla corrosione evitando il contatto fra la fibra e l'ambiente esterno.

Le fibre multimodali possono essere divise ulteriormente in due categorie:

- Step Index: L'indice di rifrazione è costante lungo tutta la sezione del core e cambia improvvisamente allorquando si incontra il cladding.
- Graded Index: L'indice di rifrazione cambia gradualmente dal core al cladding, permettendo l'uso di luce multi cromatica.

Le fibre multimodali subiscono il fenomeno della dispersione intermodale, per cui i diversi modi si propagano a velocità leggermente diverse all'interno della fibra e

questo limita la distanza massima a cui il segnale può essere ricevuto correttamente. Se la frequenza è troppo alta infatti, due modi di impulsi consecutivi possono arrivare a confondersi. Per ovviare a questo problema si adottano delle fibre multimodali graded index o fibre monomodali.

Il dispositivo trasmettitore in un impianto in fibra ottica è l'elemento che trasforma il segnale elettrico in impulsi luminosi da lanciare nella fibra stessa. Questi dispositivi elettro-ottici possono essere classificati in tre famiglie principali dove la differenza sostanziale risiede nel modo in cui le sorgenti lanciano gli impulsi luminosi nelle fibre:

- LASER: Light Amplification by Stimulated Emission of Radiation, generano impulsi solo al centro del nucleo.
- LED: Light Emitting Diode, illumina completamente il nucleo di una fibra multimodale e con molti modi copre l'intero diametro. Led monocromatici vengono utilizzati per ovviare al problema della dispersione cromatica dovuta al fatto che la luce trasmessa si compone in realtà di fasci di colore diverso, con lunghezza d'onda diverse ed è quindi probabile confondere i modi di impulsi consecutivi.
- VCSEL: Vertical Cavity Surface Emitting Laser, più focalizzati dei Led nell'immettere potenza.

Se in una fibra analizziamo l'andamento dell'attenuazione in funzione della lunghezza d'onda, notiamo che esistono tre frequenze ben precise in cui c'è minore attenuazione. Queste tre zone, chiamate finestre di trasmissione, sono quelle in cui operano le varie sorgenti ottiche. La prima finestra è centrata intorno al valore di 850nm ed è preferibile adoperarla con sorgenti di tipo led su fibre multimodali. La seconda finestra opera a 1300nm ed è caratterizzata da una attenuazione minore rispetto alla precedente. I dispositivi che operano in seconda finestra possono essere sia led su fibre multimodali che laser su fibre monomodali. Infine nella terza finestra l'attenuazione è più bassa ed è caratterizzata da una lunghezza d'onda di 1310/1550nm. Per lavorare in questa zona è necessario utilizzare esclusivamente emettitori laser con fibre monomodali.

I rivestimenti esterni delle fibre possono essere di tipo “tight” o “loose”. Il rivestimento di tipo tight viene detto anche aderente in quanto la fibra è fissata rigidamente alla guaina, il diametro esterno generalmente è di 900 micron ed è

utilizzata maggiormente nelle reti LAN interne e per le bretelle di permutazione. Nel tipo loose detto anche lasco le fibre ottiche vengono posate all'interno di un tubo rigido di materiale termoplastico e immerse in un gel tamponante che offre una migliore protezione all'umidità.

Nell'uso pratico, un collegamento bidirezionale viene realizzato utilizzando una coppia di fibre, una per ciascuna direzione. Le fibre ottiche sono collegate agli apparati di telecomunicazione mediante connettori che allineano meccanicamente il core della fibra con la sorgente luminosa e con il ricevitore. Un connettore comporta una attenuazione di circa 0,5 dB, ed è molto sensibile alla polvere, per questo motivo connettori e cavi inutilizzati vengono normalmente coperti. Esistono diversi tipi di connettori per le estremità delle fibre, i più comuni sono quattro: SC, LC, ST (innesto a baionetta), FC (innesto a vite).

Nel caso se ne avesse bisogno, due tratti di fibra ottica dello stesso tipo possono essere giuntati mediante fusione, rispettando le specifiche dei rispettivi standard, ottenendo un ottimo accoppiamento del core. Questa operazione è effettuata in modo semiautomatico mediante apparecchiature che allineano automaticamente i cladding o addirittura i core e ne controllano la fusione. Una giunzione ben eseguita comporta una attenuazione inferiore a 0,05 dB.

2.2.5. Lo switch

Lo switch è un dispositivo che non si limita a replicare il segnale, ma agisce sui frame ricevuti instradandoli verso la destinazione esatta. Mediante questa capacità tiene i domini di collisione separati, col vantaggio di occupare banda passante solo sulle porte effettivamente interessate dal traffco, lasciando libere le altre. Opera anche sulla gestione dei frame per cui se trova la rete occupata, utilizza un buffer per immagazzinare i frame attendendo che la rete si liberi e permettendo il collegamento di segmenti ethernet di tecnologie fisiche e velocità differenti (non è permessa però la connessione di reti di livello collegamento eterogenee come Token Ring ed Ethernet a meno che non si tratti di un cosidetto switch transazionale).

Operando a livello 2 del modello ISO/OSI, lo switch è in grado di identificare l'indirizzo MAC del mittente e del destinatario del frame; lo switch dispone di una

memoria volatile (MAC table), che viene riempita con le associazioni fra le porte ed i MAC osservati su di esse, in modo da poter tracciare le connessioni fra porte in funzione. Il riempimento di questa tabella è basato sull'apprendimento passivo progressivo degli indirizzi sorgente contenuti nei frame inoltrati (transparent learning o backward learning) che lo switch associa univocamente alla rispettiva porta di provenienza. Le associazione della MAC table vengono dimenticate dopo un certo tempo e se lo switch inizialmente non conosce ancora a quale porta è collegato un determinato indirizzo, inoltra il frame su tutte le porte. In alternativa è pur sempre possibile, una configurazione del forwarding database in maniera manuale e statica da parte dell'amministratore di rete.

L'isolamento fra i domini di collisione permette di non impiegare CSMA/CD evitando la propagazione di collisioni e frame non inerenti alla specifica porta e adottando la modalità full-duplex raddoppiando la banda passante.

Esistono 3 tipologie di instradamento del pacchetto utilizzate da uno switch:

- Cut-Through
- Store-and-Forward
- Fragment-Free

Nella prima tipologia lo switch si limita a leggere l'indirizzo MAC del destinatario e quindi manda il contenuto del frame contemporaneamente alla sua lettura. In questo caso l'invio dei frame non attende la ricezione completa dello stesso. Questo tipo di switch è quello con latenza minore. Negli switch store-and-forward invece viene letto l'intero frame e ne viene calcolato il cyclic redundancy check (CRC) confrontandolo con il campo FCS all'interno del frame. Solo se i due valori corrispondono il frame viene mandato al destinatario. Questi tipi di switch consentono di bloccare frame contenenti errori ma hanno una latenza maggiore. L'ultima tipologia è un compromesso tra le due precedenti in quanto si leggono i primi 64 bytes del frame in modo da rilevare solo alcune anomalie. Gli switch fragment-free e cut-through possono essere impiegati solamente nello switching simmetrico ovvero dove trasmettitore e ricevitore operano alla stessa velocità, gli switch store-and-forward invece consentono anche lo switching asimmetrico. Le tre tipologie però si differenziano solo se il buffer di trasmissione è vuoto e se il link di uscita è libero. Nel caso contrario le tre tipologie si riducono all'unica store-and-forward.

Uno switch di fascia medio-alta inoltre è tipicamente dotato di un programma software (firmware) che permette di controllarne e monitorarne il funzionamento. Questo è accessibile sia attraverso una porta seriale (gestione out-of-band) che attraverso la rete (gestione in-band). In questo caso, dopo aver configurato lo switch con indirizzo IP, maschera di rete e gateway (necessari per configurare un dispositivo in rete) risponde ai protocolli SNMP, telnet e/o ssh, HTTP. Grazie a questo agente di gestione e all'operabilità a livello di frame, gli switch possono essere configurati in modo da supportare VLAN, aggregazione (802.3ad/LACP), controllo d'accesso basato sugli indirizzi MAC o su autenticazione (802.1x), STP (802.1d), RSTP (802.1w), QoS MAC-based (802.1p) e mirroring sulle porte.

3. Gestione del Sistema Informativo

3.1. Gestione delle identità e degli accessi

L'autenticazione degli utenti è necessaria per vari motivi nel corso del lavoro quotidiano; l'accesso alla rete, alle applicazioni, ai dati e alla posta elettronica ne sono esempi tipici.

Gli utenti possono collegarsi tramite un unico accesso a tutte le risorse, applicazioni e dati a cui l'utente è autorizzato ad accedere. Per gestire questi accessi controllati è necessaria, in una rete basata su prodotti Microsoft, un'infrastruttura di Active Directory che fornisca il supporto di base per molti servizi richiesti dall'organizzazione, tra cui messaggistica e collaborazione, gestione dei sistemi e servizi di protezione.

All'interno del sistema informatico dell'azienda, l'Active Directory è il servizio directory incentrato sulla rete incluso in Microsoft Windows Server 2008.

A causa dei differenti uffici dove sono situati gli utenti, come ad esempio proposal department, administration department, technical department, è necessario gestire le informazioni relative ad ogni utente e il loro utilizzo delle risorse informatiche con un unico sistema di autenticazione coerente che possegga le caratteristiche necessarie per rendere il più efficace possibile la gestione di queste informazioni.

L'azienda gestisce una grande quantità di dati personali relativi ad ogni utente, e tali dati sono soggetti alla legge sulla privacy (d. lgs 30 giugno 2003, n.196):

"I sistemi informativi e i programmi informatici sono configurati riducendo al minimo l'utilizzazione di dati personali e di dati identificativi, in modo da escluderne il trattamento quando le finalità perseguite nei singoli casi possono essere realizzate mediante, rispettivamente dati anonimi od opportune modalità che permettono di identificare l'interessato solo in caso di necessità."

Il Codice prevede, per chi intende trattare dati, una serie di obblighi e di diritti. Infatti chiunque voglia utilizzare i dati personali di un soggetto deve informarlo, preventivamente, indicando con chiarezza le finalità per cui prevede di utilizzare tali dati e le relative modalità di utilizzo. Inoltre deve avere il consenso da parte del

soggetto interessato. In base a tale legge, l’azienda deve adempiere l’obbligo della protezione e trattamento dei dati dei singoli utenti. Per fare ciò ogni utente appartiene ad un gruppo ed ogni gruppo può accedere, tramite username e password, solo ad alcune risorse che vengono affidate in base alle competenze del loro ruolo all’interno dell’azienda. Anche le risorse, dati e servizi, vengono suddivisi in gruppi, il cui accesso verrà permesso o negato ai vari gruppi in base alla necessità.

3.1.1. Active Directory

Active Directory è un insieme di servizi di rete meglio noti come directory service adottati dai sistemi operativi Microsoft. Si fonda sui concetti di dominio (inteso come un mondo in cui vengono concentrate tutte le risorse della rete a partire da: account utente, account computer, cartelle condivise, stampanti ecc) e di Directory. L'insieme dei servizi di rete di Active Directory, ed in particolare il servizio di autenticazione Kerberos, realizzano un'altra delle caratteristiche importanti: il Single Sign-On (SSO). Tramite tale meccanismo un utente, una volta entrato nel dominio ed effettuato quindi il login ad esso da una qualsiasi delle macchine di dominio, può accedere a risorse disponibili in rete (condivisioni, mailbox, intranet ecc.) senza dover effettuare nuovamente l'autenticazione. Questo facilita di molto la gestione degli utenti.

il sistema di autentificazione:

- È organizzato e presentato come una directory.
- È supportato un metodo comune di richiesta, indipendentemente dal tipo di dati richiesto.
- Le informazioni con caratteristiche simili sono gestite in modo analogo.

Il servizio directory viene implementato mediante l’uso di cinque categorie di directory:

- Directory ad uso specifico
- Directory delle applicazioni
- Directory incentrate sulla rete
- Directory a scopo generale

- Metadirectory

L’ amministratore Active Directory ha il controllo completo sul modo in cui vengono presentate le informazioni nella directory. Queste informazioni sono raggruppate in contenitori denominati unità organizzative (OU), spesso organizzati in modo da semplificare l'archiviazione gerarchica dei dati. I tipi di dati archiviati nella directory vengono definiti tramite uno schema che ne specifica le classi denominate oggetti. Un oggetto utente, ad esempio, corrisponde alla classe Utente definita nello schema, gli attributi dell'oggetto utente contengono informazioni, quali nome, password e numero di telefono dell'utente. L'amministratore può aggiornare lo schema in modo da includere nuovi attributi o classi, quando ve ne è la necessità.

La struttura logica di Active Directory è considerata come una serie di directory logiche denominate domini. L'insieme dei domini è denominato foresta poiché i dati della directory in ogni dominio in genere sono organizzati in una struttura ad albero che rispecchia l'organizzazione.

L’implementazione e la progettazione della struttura logica consiste nelle seguenti operazioni:

1. Requisiti di progettazione della struttura logica: Le funzionalità di Active Directory per la delega amministrativa sono fondamentali nella progettazione della struttura logica. L'amministrazione delle OU organizzative può essere delegata per ottenere l'autonomia o l'isolamento di un servizio o dei dati. La delega amministrativa viene effettuata per soddisfare i requisiti legali, operativi e organizzativi della struttura.
2. Progettazione della foresta: Un modello di progettazione della foresta viene selezionato dopo aver determinato il numero appropriato di foreste nel processo di progettazione del servizio; ad esempio, quando sono necessarie diverse directory o le definizioni degli oggetti cambiano all'interno di un'organizzazione.
3. Progettazione del dominio: Viene selezionato un modello di dominio per ogni foresta.
4. Progettazione radice della foresta: Le decisioni relative alla radice della foresta si basano sulla progettazione del dominio. Se viene selezionato un modello di dominio singolo, quest'ultimo funziona da dominio radice della

foresta. Se viene selezionato un modello di dominio regionale, il proprietario della foresta deve determinare la radice della foresta.

5. Pianificazione dello spazio dei nomi di Active Directory: Una volta determinato il modello di dominio per ogni foresta, è necessario definire lo spazio dei nomi per la foresta e i domini.
6. Infrastruttura DNS per supportare Active Directory: Dopo aver progettato le strutture di dominio e la foresta di Active Directory, è possibile completare la progettazione dell'infrastruttura Dynamic Name System (DNS) per Active Directory.
7. Creazione della progettazione di un'unità organizzativa: Le strutture delle OU sono univoche per il dominio a differenza della foresta, quindi ogni proprietario di dominio è responsabile della progettazione della struttura della OU per il proprio dominio.

3.2. Gestione del sistema informatico

Tra le varie attività svolte presso l'azienda durante il periodo di tirocinio, quella sicuramente più importante in termini di responsabilità è stata la gestione di tutto il reparto macchine. L'attività di gestione ha avuto lo scopo di garantire la disponibilità del sistema informativo a tutti gli utenti per i tempi necessari, in modo sicuro e senza interruzioni, tenendo dati e funzioni aggiornati attraverso vari compiti di analisi e pianificazione.

Per quanto riguarda la gestione operativa del sistema, venivano attuati salvataggi periodici soprattutto dei personal computer a disposizione degli utenti, installazione di nuovi posti di lavoro, monitoraggio delle prestazioni dei sistemi (con eventuali aggiornamenti dei software in dotazione) e approvvigionamento dei materiali di consumo (in particolar modo materiali di consumo delle multifunzioni aziendali). Inoltre, in casi eccezionali, venivano programmati interventi tecnici specialistici come per esempio la sostituzione di un computer guasto con annesso il recupero dei dati più importanti.

Un'altra attività di grande interesse per la produttività aziendale, è indubbiamente l'assistenza agli utenti, attività costante di supporto nell'utilizzo del sistema. Ogni

dipendente periodicamente, veniva istruito e / o aggiornato sulle funzionalità del software di gestione Microsoft Dynamycs AX e sulle nuove funzionalità del software di gestione documentale Arxivar, entrambi usati quotidianamente durante le ore lavorative.

Per mantenere uno storico aggiornato di tutti gli interventi, degli aggiornamenti e delle risorse aziendali, nell'ultimo periodo di permanenza in azienda, insieme al mio tutor abbiamo iniziato ad implementare un database con il software applicativo FileMaker.

FileMaker è un database multi piattaforma che gestisce le risorse dati tramite la sua interfaccia. Uno strumento molto potente e utile, in grado di manipolare direttamente entità come tabelle di ricerca, schermi, rapporti, ecc. Inoltre fornisce delle API per permettere agli sviluppatori terzi di realizzare dei programmi che si integrino con il software stesso e ne aumentino le potenzialità.

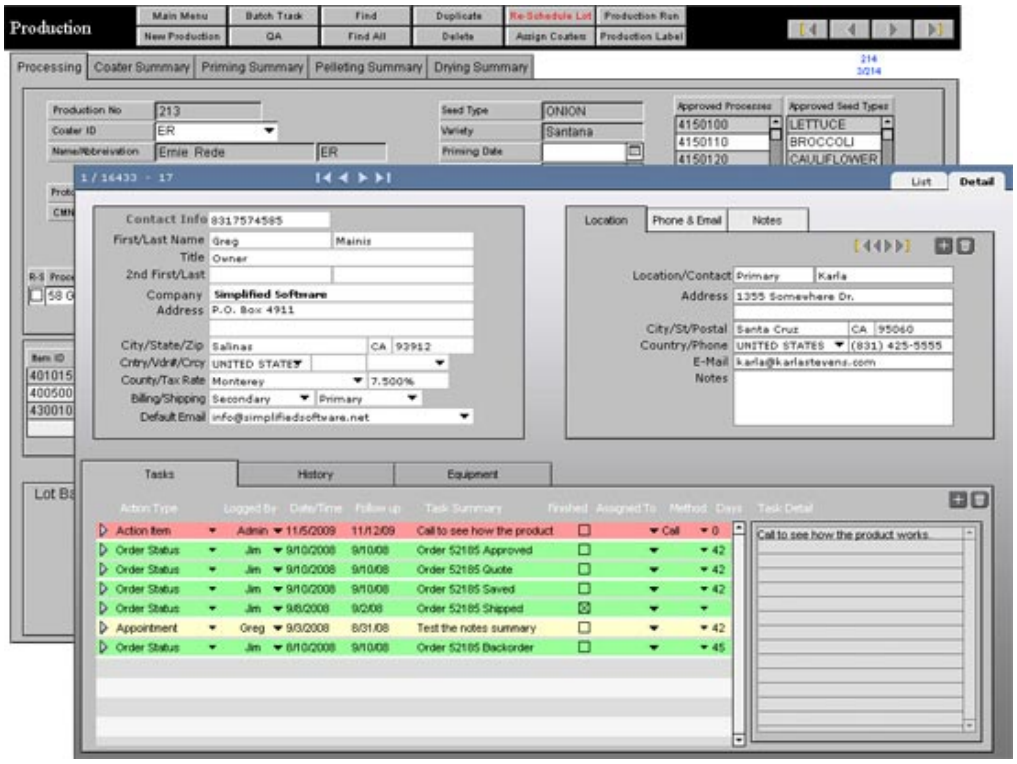

Figura 13: Interfaccia utente FileMaker

4. Conclusioni

Dopo circa sei mesi di Tirocinio, posso fissare alcuni punti, i quali rappresentano gli obiettivi fondamentali per il mio arricchimento formativo acquisito da questa esperienza:

- Capacità di applicare in un caso specifico, come la rete aziendale, tutto ciò che ho imparato dal mio percorso di studi;
- Capacità di relazionarmi con l'ambiente lavorativo, con i colleghi, con il personale e con gli organi amministrativi;
- Acquisizione di responsabilità che il ruolo impone;

Questi sono gli obiettivi fondamentali raggiunti, che erano anche quelli prefissati. L'azienda Bellelli Engineering SpA mi ha dato la possibilità di imparare molto, affidandomi ad una equipe composta da personale altamente qualificato e competente, tra cui il tutor aziendale ed altri collaboratori.

Le mansioni che mi sono state affidate sono passate dalle più semplici, fino ad arrivare a compiti con maggior responsabilità; ma non è mai mancato il supporto del tutor e dei colleghi.

Si è visto come sia difficile e dispendioso gestire una rete; essa infatti richiede il lavoro di tecnici esperti con approfondite conoscenze in molti ambiti, dall'hardware al software passando per i server, i dispositivi di rete, senza dimenticare i mezzi trasmissivi e molto altro. Tutto questo a prescindere se si dispone o meno della documentazione riguardante le tecnologie adottate.

La continua crescita ed evoluzione delle tecnologie di rete porterà questa guida, a distanza di qualche anno, ad essere di poca utilità. L'unica cosa indispensabile sarà di mantenere uno storico aggiornato di tutti gli interventi che si eseguiranno sulla rete aziendale e un database delle tecnologie adottate. In questo modo, anche nel caso di un passaggio di consegne tra responsabili incaricati ad amministrare il sistema informatico, si possa disporre di tecnici informati e preparati, con un conseguente beneficio per l'azienda.

Riguardo la situazione del sistema informatico aziendale, il poco tempo a disposizione ha impedito però di svolgere un lavoro ampio e completo, che trattasse tutti o perlomeno la maggior parte degli aspetti che determinavano l'inefficienza e la

poca sicurezza della rete. Ci si è concentrati dunque sulle specifiche che permettevano migliorie immediate e che richiedevano interventi brevi ed economici mentre quelli per cui era previsto un lavoro più impegnativo e più costoso sono stati segnalati agli amministratori con la speranza, che dopo averne valutato i pro e i contro a loro volta, possano essere eseguiti al più presto, portando a termine in modo completo il lavoro iniziato con questa tesi.

In conclusione posso affermare che l'esperienza del tirocinio ha completato il mio percorso formativo, arricchendo con aspetti pratici lo studio universitario.

Bibliografia

[1] Bruce S. Dave e Larry L. Peterson, Reti di calcolatori, Terza Edizione (2012), Apogeo Editore

[2] Andrew S. Tanenbaum, Reti di calcolatori, Quinta Edizione (2011), Pearson Education

[3] Wikipedia: http://it.wikipedia.org

[4] VoipVoice: http://www.voipvoice.it

[5] 3CX: http://www.3cx.it

[6] Intel: http://www.intel.com

[7] IEEE: http://www.ieee.org

[8] Cisco: http://www.cisco.com

[9] Microsoft: http://www.microsoft.com

[10] Infracom: http://www.infracom.it

[11] Gate Protect: http://www.gateprotect.com

[12] Fondazione Ingegneri Padova: http://www.fondazioneingegneripadova.org

[13] TechNet Microsoft: http://technet.microsoft.com

[14] VMware: http:/www.vmware.com

[15] FileMaker: http:/www.filemaker.com

[16] IBM: http:/www.ibm.com

[17] EMC^2: http:/www.emc.com

[18] Documentazione Bellelli Engineering SpA

Elenco delle figure