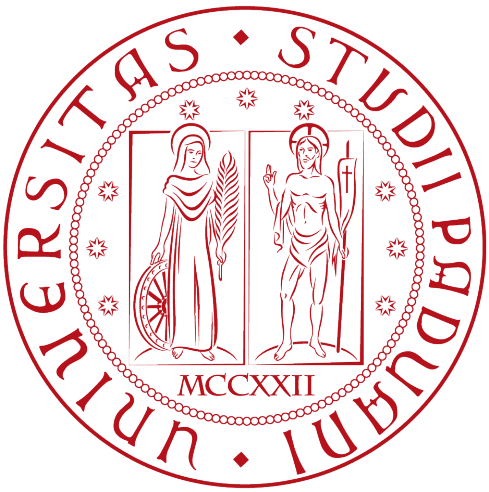
UNIVERSITÀ DEGLI STUDI DI PADOVA

Facoltà di Ingegneria

Corso di Laurea Triennale in Ingegneria Informatica



ANALISI E CONFIGURAZIONE DI UNA RETE AZIENDALE

Relatore
Prof. Marcello Dalpasso

Laureando
Daniele Simioni

Anno Accademico 2010/2011

Prefazione

Al giorno d'oggi le reti informatiche sono di fondamentale importanza nella nostra quotidianeità, 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 emorgono 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 affidabiltà.
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.

Indice

Introduzione

In questa tesi viene analizzata e descritta una rete aziendale.
Il problema della ditta proprietaria della rete presa in esame era quello di possedere documentazione incompleta ed imprecisa riguardo il sistema informatico, e questo rendeva dispendioso ogni intervento di manutenzione ordinaria e straordinaria. Si è deciso allora di procedere inanzitutto con un'accurata analisi del sistema per poi, quando era a disposizione un quadro completo della situazione, intervenire nei punti deboli della struttura con accorgimenti che si riteneva potessero fin da subito migliorare le prestazioni. Dopo tutto ciò si è prodotto questo documento che rappresenta una guida e un piccolo manuale di approfondimento del sistema informatico presente e delle tecnologie utilizzate, sperando che possa rappresentare un valido aiuto agli amministratori della rete.
Nel primo capitolo verrà fatta una panoramica dell'azienda in questione; verranno descritti i meccanismi produttivi e i prodotti realizzati, il settore e la fetta di mercato in cui opera. Nel secondo capitolo invece, la parte centrale di questo documento, verrà trattata la rete aziendale, ossia le tecnologie, i dispositivi, i protocolli, i mezzi trasmissivi e tutto ciò che riguarda e che è impiegato nel sistema informatico dell'azienda, con un accurato approfondimento dell'argomento trattato alla fine di ciascun paragrafo. Nel terzo ed ultimo capito verrà discusso il lavoro svolto e la documentazione prodotta.

CAPITOLO 1

L'azienda

L'azienda per cui si è svolto il lavoro di analisi e configurazione del sistema informatico è I.L.N.O.R. S.p.A.(Industria di Laminazione per Nastri di Ottone e Rame).
Nata nel 1961 con sede a Gardiagiano di Scorzé (Ve), ILNOR è oggi una tra le più dinamiche società europee produttrici di semilavorati di rame e di leghe di rame. Grazie a continui investimenti nei processi produttivi ed al consolidamento della rete commerciale, oggi è una realtà che produce nastri laminati a freddo in ottone, bronzo e rame destinati al settore automobilistico, elettronico, elettrico, idrosanitario e delle telecomunicazioni coprendo buona parte del mercato europeo e solo negli ultimi anni si è dedicata anche ai nastri stagnati, nichelati ed argentati elettricamente.
ILNOR inoltre è presente in Germania con la propria controllata, il Centro di Servizio Ilnor GmbH nei pressi di Stoccarda che ha la missione di soddisfare le richiesti dei clienti per lotti di piccole dimensioni in pronta consegna.
Lo stabilimento di Gardigiano di Scorzè resta comunque la sede principale dell'azienda e offre lavoro a circa 130 dipendenti di cui fanno parte numerosi operai specializzati e laureati nelle aree tecnico-industriali.
Il processo produttivo si divide principalmente in 5 passi successivi che vengono svolti in 5 aree differenti della fabbrica e in cui si identificano:

- Accettazione materie prime
- Fonderia
- Laminazione e ricottura
- Finitura
- Stoccaggio prodotto finito

ACCETTAZIONE MATERIE PRIME: Giornalmente vengono scaricate nel magazzino automatico delle materie prime le varie leghe di cui si costituiscono i prodotti finiti. Si presentano sotto forma di fine truciolato oppure come componenti riciclati e dopo aver superato severi controlli sulla qualità e la purezza della lega vengono codificate in modo da poter risalire al fornitore responsabile. L'impiego del magazzino automatico consente inoltre di minimizzare, utilizzando un'apposita procedura, l'entità di eventuali inquinamenti della lega.

Figura 1.1: Materia prima

FONDERIA:La ditta dispone di 5 impianti in parallelo per la fusione delle materie prime che operano a diverse temperature a seconda della lega da lavorare e che, a causa del notevole tempo richiesto per entrare a regime di funziomento, restano in funzione 24 ore su 24 obbligando la ditta a prevedere tre turni di lavoro al giorno. All'uscita del processo di fusione si ottiene un nastro grezzo su cui viene eseguita la fresatura della superficie e dei bordi per garantire fin da subito nastri esenti da alcun difetto superficiale.

Figura 1.2: Fonderia

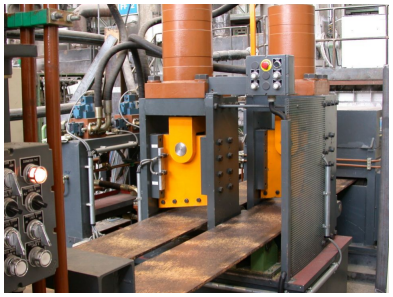


Figura 1.3: Fresatura

LAMINAZIONE E RICOTTURA: Tre laminatoi a freddo (sbozzatore, intermedio e finitore) provvedono alla riduzione dello spessore dei nastri al valore richiesto. In questo processo è molto curata l'interfaccia uomo-macchina in modo da rendere veloci e consapevoli le scelte che l'operatore è portato di volta in volta a prendere. Per migliorare ulteriormente le qualità del prodotto, una volta ottenuta la misura desiderata, il nastro viene introdotto in uno dei 4 forni a campana a disposizione dell'azienda dove viene ricotto con la tecnologia HICO/H2 in grado di ricuocere lamine di spessore fino a 0.05 mm in atmosfera di idrogeno.

Figura 1.4: Laminatoio

Figura 1.5: Forni a campana

FINITURA: Ottenuto il prodotto finito con le caratteristiche e lo spessore desiderato non resta che tagliare il nastro a seconda della larghezza richiesta. Per il taglio sono a disposizione due slitter ad alta velocità dotati di imballo automatizzato. Tutti i nastri di spessore fino a 1 mm vengono inoltre tenso-spianati al fine di ottenere strisce con bassa sciabolatura, ridotta curvatura e nessuna ondulazione. Se necessario è possibile procedere anche ad un detensionamento termico finale.

Figura 1.6: Slitter

STOCCAGGIO PRODOTTO FINITO: Il nastro alla fine dopo essere stato pesato viene depositato nel magazzino di stoccaggio in bobine multicoils (da 10 a 2000 kg) dove attende di essere prelevato e caricato nei camion che lo consegneranno al cliente. Periodicamente alcuni campioni vengono prelevati dal magazzino e sottoposti al controllo qualità in due moderni laboratori che testano la purezza della lega e le caratteristiche strutturali del nastro in modo da garantire al cliente un prodotto soddisfacente. Sono operativi inoltre gli standard di qualità UNI EN ISO 9001, ISO/TS 16949 (richiesto dal settore automobilistico) e UNI ES ISO 14001 (assicura la conformità alla legislazione ambientale).

Figura 1.7: Magazzino

Figura 1.8: Laboratorio

L'immagine sottostante rappresenta la mappa geografica dell'azienda. Sono evidenziati i reparti che saranno coinvolti nella stesura di questo documento in quanto significativi per la connettività della rete.

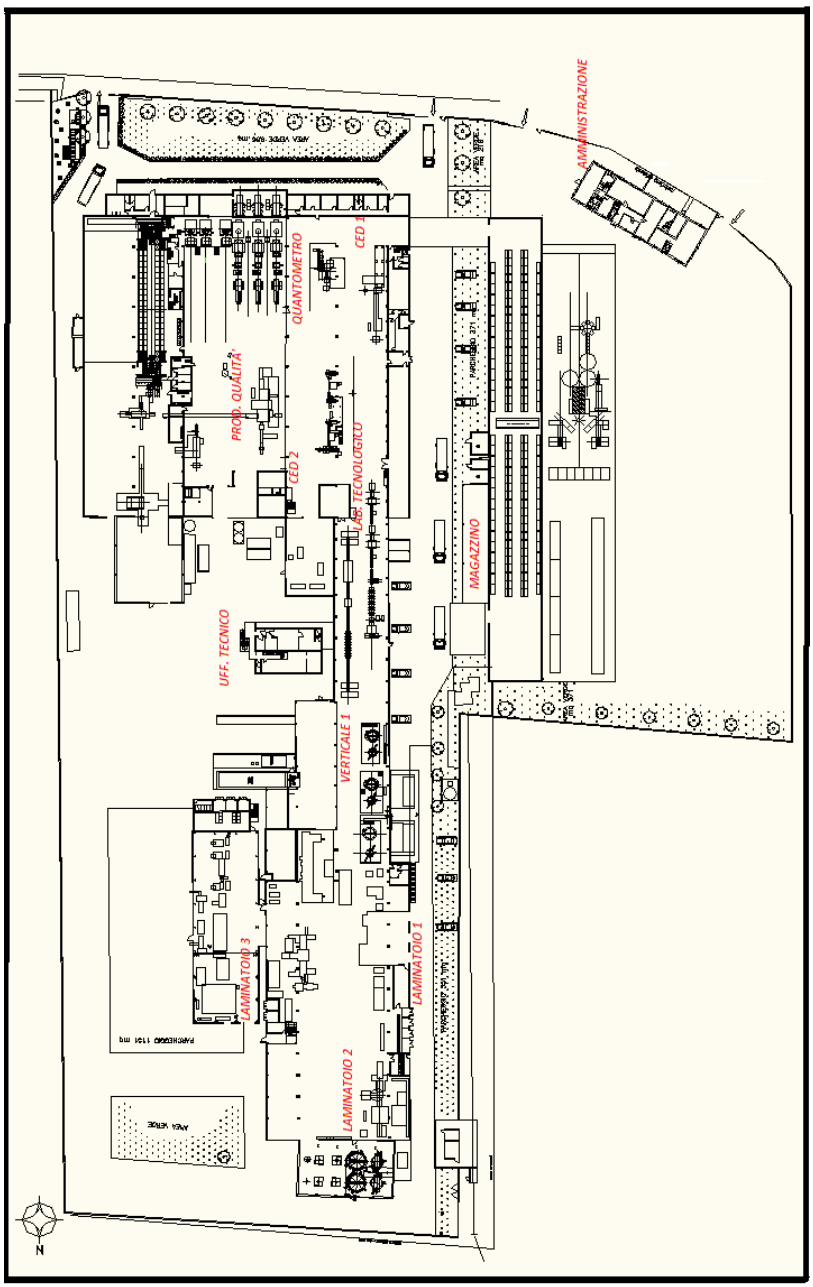


Figura 1.9: Piantina della fabbrica

CAPITOLO 2

La rete aziendale

In questo capitolo, come già preannunciato, 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 repererire 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.
Si comincerà con la connettività esterna, cioè come l'azienda si interfaccia con il mondo esterno, vero e proprio punto critico visto il ruolo che ricopre nel determinare la sicurezza del sistema; poi si parlerà dei server e dei loro servizi offerti agli utenti della rete interna, il cuore pulsante della produzione aziendale; si continuerà con la topologia di rete e i protocolli utilizzati che assieme ai mezzi trasmissivi e i dispositivi di rete influenzano principlamente le prestazioni; per terminare si tratterà la gestione dei collegamenti tramite patch panel e l'implementazione di resilient link, caratteristica imprescindibile di un sistema affidabile.

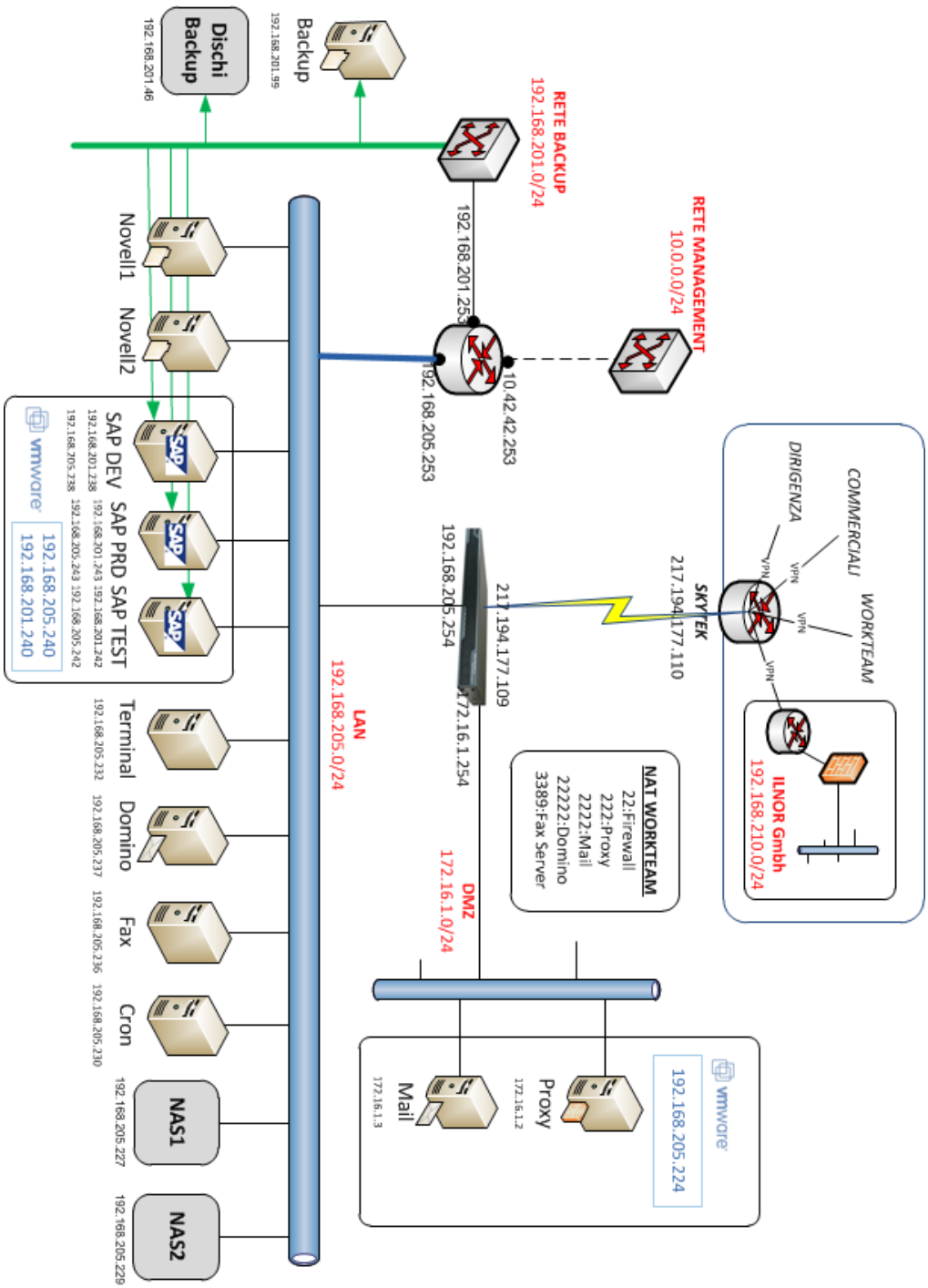


Figura 2.1: Schema concettuale della rete ILNOR

2.1 Connettività Esterna

La connettività verso la rete Internet è offerta dalla società Skytek srl, 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 4 Mbit/s mentre la banda minima garantita (*Minimum Cell Rate*) è di 2 Mbit/s.
La rete aziendale utilizza un'antenna parabolica direzionale a griglia, posizionata sul tetto della fabbrica sopra al CED1, per effettuare un ponte radio PDH[1] punto-punto, alle frequenze 2 e 5 GHz (per ridondanza), con un altra antenna di proprietà di Skytek, situata a Mira (VE) e facente parte di una rete proprietaria di ponti radio che copre le provincie di Padova, Rovigo, Treviso, Venezia e Vicenza. L'antenna utilizzata presenta un guadagno di 17 dBi[2], polarizzazione[3] orizzontale e verticale (per ridondanza) e la codifica dei dati BPSK/DSSS[4].

Figura 2.2: Antenna parabolica a griglia

Il punto di trasmissione di Mira è collegato a sua volta con ponti radio PDH punto-punto alla frequenza di 11 Ghz verso le centrali di Cadoneghe (PD) a 155 Mbit/s e Mestre a 34 Mbit/s (per ridondanza su Cadoneghe).
La centrale di Cadoneghe (o Padova) è collegata a 3 anelli in fibra ottica 10 Gigabit/s. In due di questi anelli i dati seguono il percorso Milano-Padova-Francoforte-Milano mentre nell'altro seguono il percorso inverso; utile nel caso di guasto alle linee di collegamento tra due stazioni (vedi figura 2.3). Da Milano, Skytek, così come altri ISP minori, riceve la connettività alla rete mondiale grazie a contratti con ISP più importanti a livello nazionale ed internazionale.

[1] Plesiochronous Digital Hierarchy, protocollo di rete di livello fisico usata nelle reti di telecomunicazione per trasmettere grosse quantità di dati

[2] Decibel isotropic, guadagno in decibel rispetto ad un'antenna isotropica, unita' adimensionale che qualifica l'antenna stessa rispetto al radiatore isotropico.

[3] Indica la direzione dell'oscillazione del vettore campo elettrico durante la propagazione dell'onda nello spazio. Un apparato sintonizzato per ricevere un'onda elettromagnetica con una certa polarizzazione non è in grado di riceverne con polarizzazione opposta, anche se alla stessa frequenza.

[4] Binary Phase Shift Keying/Direct Sequence Spread Spectrum, tecnica di modulazione e tecnologia di trasmissione per segnali deboli a banda larga.

Nello specifico Skytek riceve connettività a livello nazionale da Interoute su due linee a 100 Mbit/s, da Fastweb su una linea a 100 Mbit/s e da Telecom sempre su una linea 100 Mbit/s. Tutti e quattro questi ISP sono presenti al MIX (*Milano Internet eXchange*), un punto di interscambio tra internet service provider in Italia e ad altri anelli di fibre. Il MIX è situato a Milano ed è il punto di interconnessione multipla più importante in Italia per quantità di traffico smistato (ce ne sono numerosi in tutto il mondo); le reti degli operatori Internet in Italia (ISP, carriers, content providers, ...) e le loro dorsali si collegano in questo luogo per scambiare traffico e distribuirlo in Europa e nel mondo.

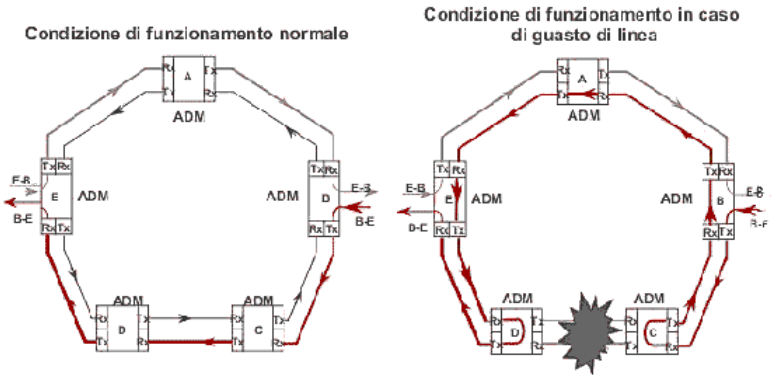


Figura 2.3: Verso di percorrenza di 3 anelli in fibra

Sottoscrivendo un contratto con Skytek, l'azienda proprietaria della rete LAN, acquista oltre alla connessione Internet anche un pacchetto di 10 indirizzi IPv4 pubblici, da 217.194.177.100 a 217.194.177.109, da utilizzare per pubblicare all'esterno svariati servizi. L'unico attualmente utilizzato e visibile dalla nuvola è 217.194.177.109 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 quotidinanamente 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 la sede tedesca di Stoccarda, non disponendo di server propri, necessita di entrare nella rete LAN di Gardigiano di Scorzè tramite la rete Internet.

Sull'indirizzo 217.194.177.109, come mostrato in figura 2.1, viene inoltre eseguito il NAT (*Network Address Translation*), per permettere alla ditta esterna Workteam, a seconda della porta (TCP o UDP) sulla quale effettua la richiesta, di accedere a determinati server della rete aziendale (oppure a determinati dispositivi, per esempio il firewall); dopo naturalmente aver stabilito una connessione VPN, mettendo in sicurezza il transito delle informazioni e autenticando l'identità del destinatario. Workteam è una ditta esterna che si occupa per conto della ditta committente della manutenzione e della gestione di dispositivi e servizi interni che si interfacciano con la rete pubblica; necessita quindi di un accesso remoto alle macchine. Nel firewall è presente una tabella impostata dagli amministratori di rete che permette, quando il tentativo di connessione viene fatto su una determinata porta e proviene da un determinato indirizzo IP, in questo caso quello della ditta Workteam, di tradurre l'indirizzo 217.194.177.109 nell'indirizzo privato della macchina nella rete interna a cui si vuole accedere; tutte le altre richieste provenienti da altri indirizzi IP o su altre porte vengono scartate. Questo processo è utile perchè in questo modo si permette solamente ad utenti selezionati di poter accedere a determinati elaboratori della rete interna e rendere completamente invisibili gli altri.
Per quel che riguarda la connettività esterna e la sua gestione, non si dispongono di informazioni più precise, sia perchè questo argomento non era previsto nel lavoro di analisi e configurazione della rete interna sia perchè gli stessi amministratori della rete non sono a conoscenza di ulteriori particolari ma ne affidano la gestione a ditte esterne come Workteam. Per completezza di informazione si è comunque voluto esporre un quadro generale della situazione rigurdante questo aspetto e da quello che si è potuto notare nel periodo di permanenza in azienda, le scelte fatte risultano appropriate alle esigenze e alle prestazioni desiderate.

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 etc) 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.

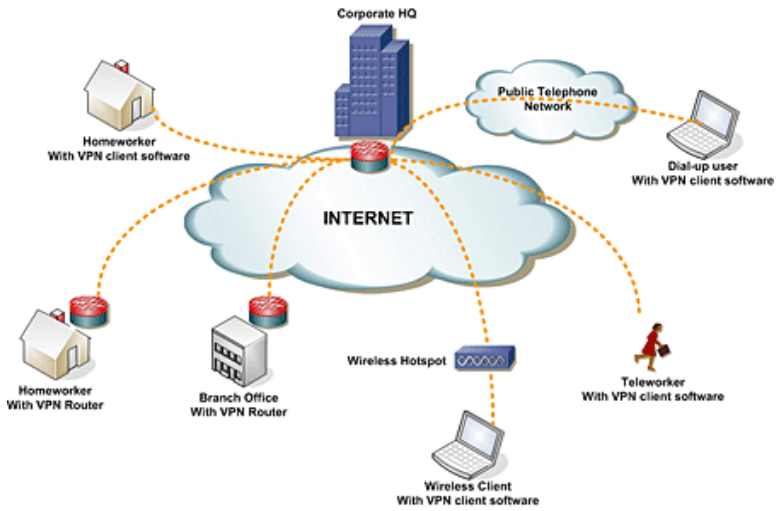


Figura 2.4: Schema di utilizzo di una connessione VPN

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.

HYBRID: Una Secure VPN può essere adoperata come parte di una Trusted VPN creando un terzo tipo di VPN: Hybrid VPN. È chiaro che le Secure VPN e le Trusted VPN hanno proprietà molto differenti; le Secure VPN danno sicurezza, ma non assicurano i percorsi mentre le Trusted VPN assicurano le proprietà dei percorsi come QoS, ma non la sicurezza da intrusioni. A causa di questi punti di forza e di debolezza sono state introdotte le Hybrid VPN. Una situazione tipica per il dispiegamento di un Hybrid VPN è quando un'azienda ha già una Trusted VPN e desidera sicurezza su una parte della VPN. Le parti sicure di una Hybrid VPN possono essere controllate da un cliente o dallo stesso provider che fornisce la VPN.

Una VPN ben strutturata può offrire grandi benefici per un'azienda:

- Estende la connettività geografica
- Migliora la sicurezza delle connessioni
- Riduce i costi per l'accesso sicuro ad una rete privata
- Riduce il tempo di transito per i clienti remoti
- Semplifica la topologia di rete, almeno in determinati scenari
- Mostra una buona economia di scala
- Fornisce la possibilità di reti globali

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, che l'implementazione di IPv6 che avrebbe risolto questo problema (vedi paragrafo 2.3.2) 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 IP 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 dipositivo 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.

I principali vantaggi del NAT sono:

- Risolve in parte problema carenza indirizzi IPv4.
- Non necessario cambiare indirizzi rete privata per accedere ad Internet.
- I dati viaggiano tra le reti in maniera trasparente.
- I protocolli più comuni funzionano bene.
- Traffico non raggiunge host interni se non definite specifiche regole.

Gli svantaggi:

- Non conforme dettami reti end-to-end (pacchetti non modificabili).
- Lavoro aggiuntivo per la CPU dei dispositivi che lo implementano.
- Introduce un "single point of failure".
- Penalizza peer-to-peer e programmi per condivisione file.
- Per certe applicazioni deve analizzare payload pacchetto e riscriverlo.
- Instradamento dipende anche da caratteristiche livello trasporto.

2.2 Server Interni

In azienda sono presenti fisicamente 9 server (alcune macchine presentano più server virtualizzati) distribuiti in due stanze, CED1 e CED2. La scelta di utilizzare due locali è stata presa per rendere meno affolate 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 CED1 sono presenti i server più importanti della rete principale, per quel che riguarda la linea produttiva e la gestione amministrativa, e quelli appartenti alla rete DMZ, mentre in CED2 sono stati posizionati i server meno importanti e alcuni duplicati di quelli in CED1 che serviranno in caso di emergenza per sostituire la loro copia principale. In CED2 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.
Di seguito verrà fatto un elenco delle macchine server attive in azienda: ne verrà spiegata la funzione, verranno elencati i software installati, verranno indicati i parametri che ne permettono l'individuazione in rete e verranno fornite tutte le altre informazioni utili a darne una descrizione completa.

DELL POWER EDGE 2650
Nome: Novell 1
Funzione: Contiene i disegni tecnici di progettazione macchine, i programmi di gestione degli impianti, il programma di interfaccia con il gestionale SAP della produzione e gestisce i profili della sicurezza.
Sistema Operativo: Netware 4.3
Indirizzo IP: /
Rete: LAN principale
Locazione: CED1 collegato allo switch 10.42.42.2
Note: Non utilizza i protocolli della pila TCP/IP ma quelli di IPX/SPX.

DELL POWER EDGE 2850
Nome: Novell 2
Funzione: È la copia integrale del server Novell 1 per sostituirlo in caso d'emergenza con un minimo intervento manuale. A seconda della criticità dei dati la copia viene effettuata ogni 15 min, ogni ora oppure ogni giorno.
Sistema Operativo: Netware 4.3
Indirizzo IP: /
Rete: LAN principale
Locazione: CED2 collegato allo switch 10.42.42.3
Note: Non utilizza i protocolli della pila TCP/IP ma quelli di IPX/SPX.

IBM HS22V
Nome: SAP DEV (sviluppo); SAP TEST (test)
Funzione: Utilizzati per lo sviluppo e il test di funzionamento del sistema gestionale SAP, un software enterprise sviluppato dalla multinazionale tedesca SAP AG. Ad esso si collegano gli utenti che neccessitano di testare nuovi programmi e i consulenti per sviluppare nuove procedure.
Sistema Operativo: Linux SuSe Enterprise Server 11 per entrambi
Indirizzo IP: 192.168.205.238/192.168.201.238; 192.168.205.242/192.168.201.242
Rete: LAN principale e rete di backup
Locazione: CED2 posto nella seconda posizione dello chassis
Note: Questo server è una blade server, cioè un server spogliato dell'alimentazione, del raffreddamento, della memoria e delle interfacce di rete; tutto viene incorporato e condiviso nello chassis su cui possono essere inseriti più blade server. Questa macchina inoltre contiene il software VMware ESXi 4.1 che si pone tra l'hardware e il sitema operativo e permette di virualizzare i servizi SAP DEV e SAP TEST sulla stessa lama.

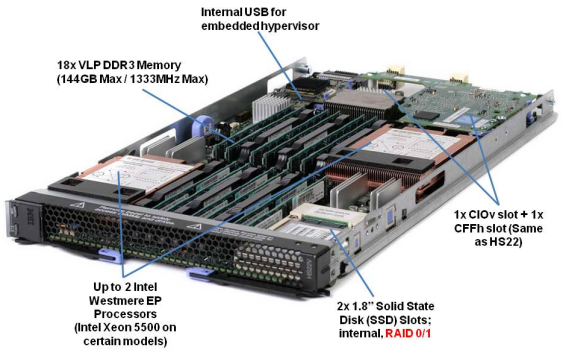


Figura 2.5: Blade server e i suoi componenti

IBM HS22V
Nome: SAP PRD (produzione)
Funzione: Utilizzato per il funzionamento del sistema gestionale SAP, un software enterprise sviluppato dalla multinazionale tedesca SAP AG. Ad esso si collegano tutti gli utenti autorizzati negli uffici e in reparto.
Sistema Operativo: Linux SuSe Enterprise Server 11
Indirizzo IP: 192.168.205.243/192.168.201.243
Rete: LAN principale e rete di backup
Locazione: CED2 posto nella prima posizione dello chassis
Note: Questo server è una blade server, cioè un server spogliato dell'alimentazione, del raffreddamento, della memoria e delle interfacce di rete; tutto viene incorporato e condiviso nello chassis su cui possono essere inseriti più blade server. Questa macchina inoltre contiene il software VMware ESXi 4.1 che si pone tra l'hardware e il sitema operativo e permette di virualizzare il servizio SAP PRD.

IBM BLADE CENTER H
Nome: Chassis
Funzione: Contiene i blade server e fornisce loro l'alimentazione, le interfacce di rete, il raffreddamento, ecc.
Sistema Operativo: Firmware proprietario
Indirizzo IP: 192.168.205.240/192.168.201.240
Rete: LAN principale e rete di backup
Locazione: CED2 collegato allo switch 10.42.42.3 e allo switch 10.42.42.171
Note: È identificato nella rete con un proprio indirizzo e attraverso le sue interfacce di rete (possiede alcune diverse di rete che gli permettono il collegamento con reti diverse) rende visibili tutti i blade server che contiene. È collegato inoltre ad una SAN, utilizzando la tecnologia SAS (*Serial Attached SCSI*), per permettere la memorizzazione dei dati dei blade server; funge da "ponte" tra la SAN e gli utenti della rete ethernet.

Figura 2.6: Chassis e blade server inseriti

IBM DS3524
Nome: Dischi memorizzazione SAN
Funzione: Fornisce supporti di storage ad alte prestazioni; in questo caso rappresentano l'hard-disk dei blade server collegati.
Sistema Operativo: Firmware proprietario
Indirizzo IP: /
Rete: SAN
Locazione: CED2 collegato attraverso interfaccia SAS allo chassis
Note: 10 dischi da 146 GB + 6 dischi da 300 GB. Sul dispositivo sono integrati inoltre degli switch (infrastuttura SAN), concettualmente simili a degli ethernet switch, sui quali vengono effettivamente realizzati i collegamenti attraverso l'interfaccia SAS, Serial Attached SCSI dove SCSI (*Small Computer System Interface*).

DELL POWER EDGE 2850
Nome: Terminal
Funzione: Distribuisce la connettività agli utenti della rete aziendale e ne fornisce l'accesso a quei servizi per cui sono abilitati.
Sistema Operativo: Windows Server 2003
Indirizzo IP: 192.168.205.232
Rete: LAN principale
Locazione: CED1 collegato allo switch 10.42.42.2
Note: Implementa il servizio DHCP[5] (*Dynamic Host Configuration Protocol*) per gli utenti che si collegano alla rete, prevalentemente thin client[6].

DELL POWER EDGE 2650
Nome: Domino
Funzione: È utilizzato per la gestione della posta elettronica e dei documenti commerciali e di qualità creati su SAP. grazie anche all'aiuto di alcune procedure di gestione documentale.
Sistema Operativo: Linux SuSe Enterprise 9
Indirizzo IP: 192.168.205.237
Rete: LAN principale
Locazione: CED1 collegato allo switch 10.42.42.2
Note: Installato il software Lotus Domino 8.0, un prodotto IBM che fornisce strumenti enterprise per e-mail (Lotus Note) e strumenti collaborativi. Include inoltre un sistema di database nel formato NSF (*Network File System*).

[5]Protocollo di livello applicativo, permette ai dispositivi di ricevere dinamicamente ad ogni richiesta di accesso la configurazione necessaria per poter operare su una rete TCP/IP.

[6]Elaboratore con piccola o nessuna applicazione logica, dipendende dal server centrale per elaborare dati. La parola thin si riferisce alla piccola immagine di boot che questi client richiedono tipicamente per connettersi a una rete e partire con un web browser dedicato o una connessione di tipo remote desktop.

IBM X3250M2
Nome: Fax
Funzione: Si occupa della gestione dei fax aziendali.
Sistema Operativo: Windows Server 2003
Indirizzo IP: 192.168.205.236
Rete: LAN principale
Locazione: CED2 collegato allo switch 10.42.42.3
Note: Monta opportune schede ISDN fax e ha installato il software Extra-Fax 7.0 che si integra perfettamente in ambienti dove presente il software Lotus Domino.

DELL POWER EDGE 2650
Nome: Cron
Funzione: Sincronizza il server Novell 1 con il server Novell 2 e copia i database di Domino in NAS 1.
Sistema Operativo: Linux Ubuntu 9.10
Indirizzo IP: 192.168.205.230
Rete: LAN principale
Locazione: CED1 collegato allo switch 10.42.42.2
Note: Sono presenti script realizzati dagli amministratori di rete che eseguono le funzione di sincronizzazione.

IBM X3650
Nome: Proxy; Mail
Funzione: Tutta la navigazione Internet e la posta elettronica in entrata o in uscita passa attraverso questi server. Vengono eseguiti i dovuti controlli sui pacchetti in transito per aumentare la sicurezza e proteggere la rete interna.
Sistema Operativo: Linux SuSe Enterprise Server 11 per entrambi
Indirizzo IP: 172.16.1.2; 172.16.1.3 (la macchina fisica ha indirizzo 192.168.205.224)
Rete: DMZ (la macchina fisica appartiene alla LAN principale)
Locazione: CED1 collegato al firewall
Note: Sulla macchina fisica è presente il software VMware ESXi 4.1 ad un livello compreso tra l'hardware e il sistema operativo che permette di virtualizzare i due servizi Proxy e Mail sulla stessa macchina fisica. Nel server Proxy sono installati i programmi Squid (web server), Sarg (analizzatore log) e NTP Server (*Network Time Server*). Nel server Mail invece sono presenti i software MailScanner, SapmAssassin e ClamAv che proteggono il sistema da virus e spam.

CISCO LINKSYS NSS6100
Nome: NAS 1
Funzione: Contiene la copia dei dati del server Domino (backup mail e documenti interni) più i file utenti.
Sistema Operativo: Firmaware proprietario
Indirizzo IP: 192.168.205.227
Rete: LAN principale
Locazione: CED1 collegato allo switch 10.42.42.2
Note: 4 dischi da 1 TB in RAID 5.

CISCO LINKSYS NSS6100
Nome: NAS 2
Funzione: È la copia di NAS 1. La copia viene eseguita giornalmente solo per i dati modificati.
Sistema Operativo: Firmaware proprietario
Indirizzo IP: 192.168.205.229
Rete: LAN principale
Locazione: CED2 collegato allo switch 10.42.42.3
Note: 4 dischi da 1 TB in RAID 5.

HP DL360G6
Nome: Backup
Funzione: Esegue la copia dei database dei server SAP PRD, SAP TEST e SAP DEV.
Sistema Operativo: Linux SuSe Enterprise Server 9
Indirizzo IP: 192.168.201.99
Rete: Rete di backup
Locazione: CED2 collegato allo switch 10.42.42.171
Note: È installato il software HP Data Protector 6. Il server di backup salva i dati del server SAP PRD ogni 4 ore mentre quelli dei server SAP DEV e SAP TEST quotidianamente.

HP D2D2500
Nome: Dischi memorizzazione backup
Funzione: Contiene i dati dei server SAP PRD, SAP TEST e SAP DEV.
Sistema Operativo: Firmware proprietario
Indirizzo IP: 192.168.201.46
Rete: Rete di backup
Locazione: CED2 collegato allo switch 10.42.42.171
Note: 4 dischi da 1 TB in RAID 5. Settimanalmente i dati vengono riversati in cassetta su di un Autoloader DLT.

Figura 2.7: Autoloader DLT

2.2.1 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.

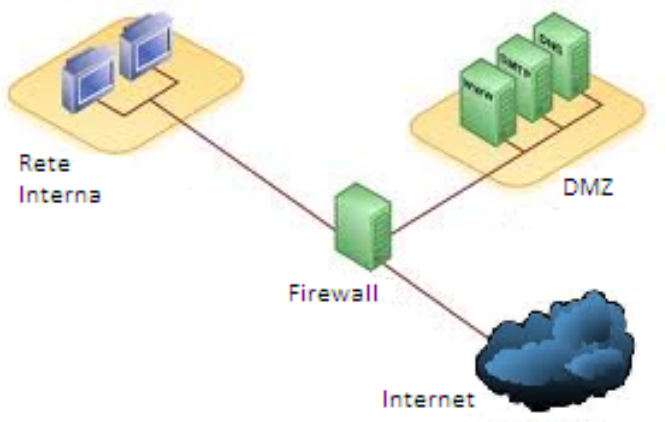


Figura 2.8: Schema di utilizzo di una rete DMZ

Le politiche di sicurezza attuata in presenza di DMZ sono:

- Tentativo connessione esterno verso DMZ: AUTORIZZATO.
- Tentativo connessione esterno verso LAN: VIETATO.
- Tentativo connessione interno verso DMZ: AUTORIZZATO.
- Tentativo connessione interno verso esterno: AUTORIZZATO.
- Tentativo connessione DMZ verso interno: VIETATO.
- Tentativo connessione DMZ verso esterno: RIFIUTATO.

Ricapitolando, la DMZ è un'area pubblica protetta, dove il traffico è strettamente regolato ed è utile per pubblicare servizi verso l'esterno minimizzando i rischi per la rete interna.

2.2.2 NAS e SAN

NAS

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 dunaue 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.

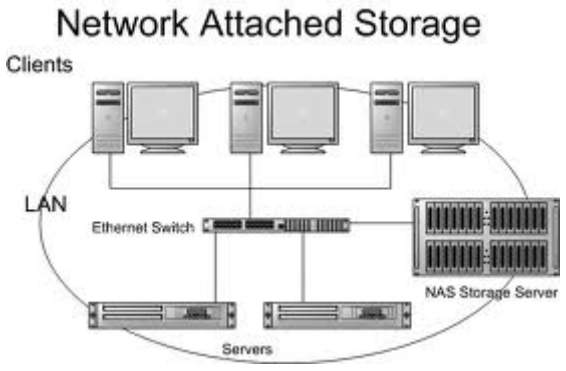


Figura 2.9: Dispositivi NAS in reti ethernet

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:
RAID0: 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.

SAN

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 traffico 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, ed iSCSI (Internet SCSI), quest'ultima 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. La virtualizzazione dello storage é il processo di astrazione dell'archiviazione fisica. Le risorse di storage fisici vengono aggregate in pool da cui viene creato il deposito logico e si presenta all'utente uno spazio per la memorizzazione dei dati trasparente alla posizione reale dei dischi.

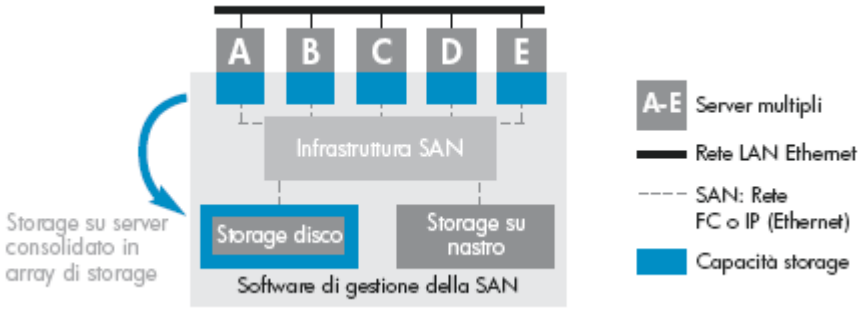


Figura 2.10: Architettura SAN

L'impiego di una qualsiasi tecnologia di networking proposta per le reti SAN rispetto alle precedenti soluzioni consente di:

- Raggiungere distanza superiori e prestazioni migliori.
- Facilitare e centralizzare la gestione dello storage
- Consolidamento dello storage e del clustering dei sistemi.
- Condividere i dati tra piattaforme diverse.

2.3 Topologia e Protocolli

La topologia della rete presa in considerazione si estende su una superficie di circa 20000 m^2 ed è organizzata in modo da prevedere un segmento privato per la sola gestione degli apparati di interconnessione e instradamento, 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 utenti della LAN[7] (*Local Area Network*) principale.
La rete di backup è necessaria perchè il software gestionale dell'azienda prevede da contratto che venga allestita una rete separata in cui oltre ai server che lo contengono dev'essere presente solamente un server di backup, certificato dalla ditta produttrice del software, che gestisce le operazioni di salvataggio e memorizzazione dei dischi su dispositivi di storage con una procedura accurata e appositamente implementata. Se ciò non fosse si perderebbe la garanzia di supporto e la conformità con l'azienda produttrice del software gestionale che fornisce oltretutto la lista in cui scegliere marca, modello e sistema operativo del server di backup. Questo metodo sebbene comporti un maggiore utilizzo di dispositivi e quindi maggiore spazio, dando l'idea talvolta di essere un sistema macchinoso e poco economico, permette una gestione più agevole delle operazioni di backup e separa il traffico generato dalle operazioni di salvataggio (possono diventare parecchie) da quello della rete principale che ne guadagna in prestazioni. Nella rete principale invece sono attivi i server e gli host necessari a svolgere le attività aziendali, siano essi elaboratori degli utenti o macchinari della catena produttiva. Un elenco completo dei server è presente nel paragrafo 2.2.
La prima operazione che si è deciso di svolgere per analizzare la rete è stata quella di rilevare la topologia della rete presente, individuare quindi la collocazione dei vari nodi. Si è cominciato analizzando la poca 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. Questo però non è stato sufficiente, la documentazione non era completa e spesso, essendo molto vecchia, è risultata essere imprecisa a causa di interventi successivi non segnalati. Si è proceduto quindi in maniera manuale.
Spostandosi nei vari reparti della fabbrica, dove gli amministratori della rete indicavano esserci dei dispositivi, si sono individuati gli armadi contenenti gli switch; per quelli di cui non si disponeva di informazioni si è individuato manualmente il patch panel a cui andavano a finire i cavi connessi alle loro porte. Questo però non era sufficiente perchè non si conosceva ancora la vera destinazione dei collegamenti. Per ognuno di questi switch allora si è presa

[7] Rete che raggiunge un'estensione di alcuni kilometri, si differenzia dalle PAN, *Personal Area Network* di alcuni metri, dalle MAN, *Metropolitan Area Network* che arrivano ad occupare intere città e dalle WAN, *Wide Area Network* che arrivano anche oltre.

in esame la tabella MAC e per ogni porta si sono individuati gli indirizzi MAC che ne facevano capo. Dopo aver inviato da un terminale della rete una richiesta in broadcast tramite il protocollo ICMP e aver ricevuto una risposta da ogni host attivo, grazie ad un software che permette di analizzare tutti i pacchetti che viaggiano in rete (Wireshark), si sono filtrati i risultati sugli indirizzi MAC della porta interessata ricavati in precedenza e ottenuto l'indirizzo IP corrispondente. A questo punto, avendo a disposizione l'indirizzo IP che rappresentava la destinazione della connessione, si è fatta una ricerca su un file fornito dagli amministratori contenente indirizzo IP, nome e reparto di tutte le macchine attive e operanti nella rete. Si è riuscito così a dare un nome e una collocazione alla destinazione del collegamento. Alcune volte però le corrispondenze della tabellla MAC dello switch per una determinata porta non erano singole ma presentavano una lunga lista di indirizi MAC. Questo stava a significare che il collegamento non era verso un host finale ma era verso un altro dispositivo e quella determinata porta vedeva tutti gli indirizzi MAC delle macchine che connesse a quel dispositivo. Incrociando questi risultati a quelli ottenuti in precedenza si è riuscito a tracciare una mappa completa della topologia della rete presente. Questo modo di procedere è risultato molto impegnativo e ha occupato molto tempo ma si è rivelato essere, tutto sommato, molto efficiente. In figura 2.12 è mostarata la disposizione degli switch delle reti nei vari reparti della fabbrica.
Una volta determinata la collocazione dei vari nodi della rete, ne si è analizzata la disposizione logica e si è notato che questa non era ottimale ma presentava invece uno schema molto sbilanciato che influiva sulle prestazioni e determinava una notevole debolezza strutturale in caso di guasto dei nodi intermedi. Per ovviare a questo problema è stata studiata una nuova collocazione logica degli switch in modo tale da dividere il traffico e bilanciare il carico tra i nodi. Per tutti gli interventi riguardanti i dispositivi di rete si rimanda al paragrafo 2.4. Si arriva così alla topologia finale (vedi figura 2.11) caratterizzata da una struttura ad albero bilanciato (o a stella) con connessioni punto-punto, che a differenza delle connessioni broadcast presentano collegamenti tra singole coppie di elaboratori. In questo modo la rete risulta più efficiente e oltre a garantire una facile individuazione di un guasto, permette, nel caso peggiore di una rottura dei nodi di livello più alto, la continuazione del lavoro sull'altra metà della rete. Il nodo di centro stella resta però un punto critico, a lui infatti sono collegati i server, il router e il firewall, oltre a tutti gli altri switch e host in cascata. Se tale nodo dovesse guastarsi la rete sarebbe praticamente inutilizzabile. Si è verificato dunque che fosse sovradimensionato e protetto con alimentazione ridondata; cosa che fortunatamente era già prevista dalla configurazione di rete iniziale.
Mentre si utilizzava il software di analisi per studiare la topologia si è notato che i pacchetti che viaggiano in rete, a livello di collegamento del modello ISO/OSI, implementano il protocollo Ethernet II e incapsulano a livelli più alti sia protocolli della pila TCP/IP che della pila IPX/SPX.

Come nella maggior parte della LAN viene quindi utilizzata l'architettura Ethernet, che oltre a gestire l'accesso al mezzo di trasmissione in caso di competizione tra due o più nodi in connessioni broadcast, trasferisce informazioni senza errori e divide le informazioni in unità trasferibili sul mezzo trasmissivo. Offre ottime garanzie riguardo affidabilità e prestazioni e opera sia a livello collegamento sia in parte a livello fisico. La rete aziendale non presenta però una tecnologia ethernet omogenea perchè al suo interno vengono utilizzati differenti mezzi di connessione e differenti velocità di trasmissione che comportano la presenza di tre diversi standard: 100BaseTX, 1000BaseTX e 1000BaseSX. Per quello che riguarda i mezzi di connessione e la scelta del loro utilizzo si rimanda alla lettura del paragrafo 2.5.
Neanche a livelli più alti, ossia quelli più vicini all'utente, come abbiamo visto c'è omogeneità. Viene usata infatti sia la suite di protocolli TCP/IP che IPX/SPX. I protocolli della pila TCP/IP vengono utlizzati, così come in tutte le reti del mondo, sia per lavorare e comunicare all'interno della rete privata ma soprattutto per poter interagire con la rete Internet, in grado quest'ultima di gestire solo tali protocolli. I protocolli della pila IPX/SPX invece vengono utilizzati perchè sono presenti dei server Novell il cui sistema operativo è Netware 4.3. Solo dalla versione 5 di tale sistema operativo Novell ha deciso di gestire i protocolli TCP/IP quindi per adesso è necessario usufruire della pila IPX/SPX. Per l'elenco completo delle macchine Novell e la loro funzione si rimanda al pargrafo 2.2. I server Novell non sono comunque l'unico motivo per cui si utilizzano questi protocolli. All'interno della rete sono infatti presenti delle macchine il cui sistema operativo è MS-DOS, anch'esso non recente, e la cui funzione è quella di controllare i processi della catena di produzione nei reparti e i parametri che gestiscono i macchinari. Neanche MS-DOS originariamente infatti supportava TCP/IP avendo visto la luce anni prima dell'invenzioni di tali protocolli. Negli elaboratori il cui sistema operativo è diverso da Netware o DOS è necessario siano presenti pacchetti software, appositamente installati, che permettano l'elaborazione dei pacchetti appartenenti ai protocolli IPX/SPX. Nella rete aziendale la verifica non è stata necessaria perchè dato il loro totale funzionamento, tutte le macchine interessate da tali protocolli, già disponevano degli accorgimenti necessari; semmai bisognerà fare attenzione che il supporto sia abilitato quando verranno installate in rete nuove macchine.
Utilizzando il software Wireshark, che analizza i pacchetti di rete, è stato appreso, come detto in precedenza, che i protocolli IPX/SPX vengono incapsulati a livello collegamento in pacchetti Ethernet II la cui caratteristica è quella di avere un campo nell'header lungo 2 byte e nel quale viene specificato il tipo di dato incapsulato nel campo dati. Dopo aver studiato la struttura della trama di Ethernet II è stato individuato il campo "type" e identificato il valore che rappresentava il tipo di dati incapsulati.
Per IPX/SPX tale valore in esadecimale vale 0x8137.

Anche se la presenza di pacchetti IPX/SPX nella rete non presenta nessun danno per le prestazioni è auspicabile che i server Novell attualmente presenti vengano presto sostituiti con macchine e sistemi operativi più recenti, ricchi di moderne funzionalità e a cui è garantito totale supporto tecnico. In questo modo si ottiene una rete omogenea, che lavora solamente con protocolli TCP/IP, più facile da gestire a da controllare. Per le macchine in cui gira il sistema operativo MS-DOS vale lo stesso discorso per quanto riguarda l'omogeneità dei protocolli in rete ma grazie alla loro semplicità d'utilizzo e la scarsa avidità di risorse che permette loro di svolgere molto bene le proprie funzioni, non si sente il bisogno di sostituirle con elaboratori più recenti. Almeno per ora.

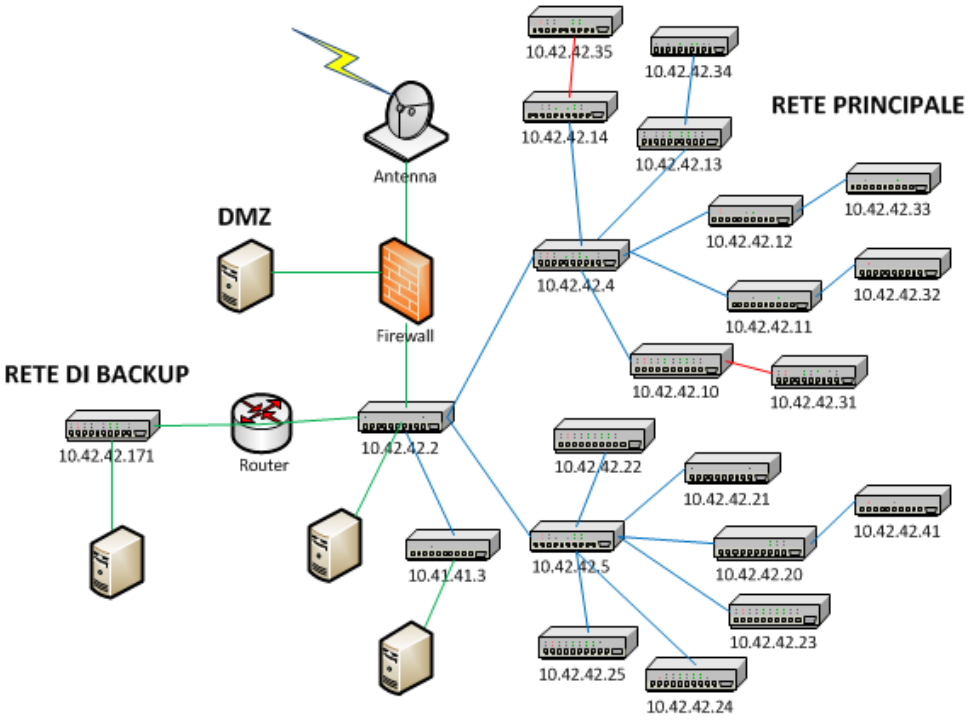


Figura 2.11: Topologia della rete aziendale
(collegamenti blu = fibra, verde = UTP cat6, rosso = UTP cat5e)

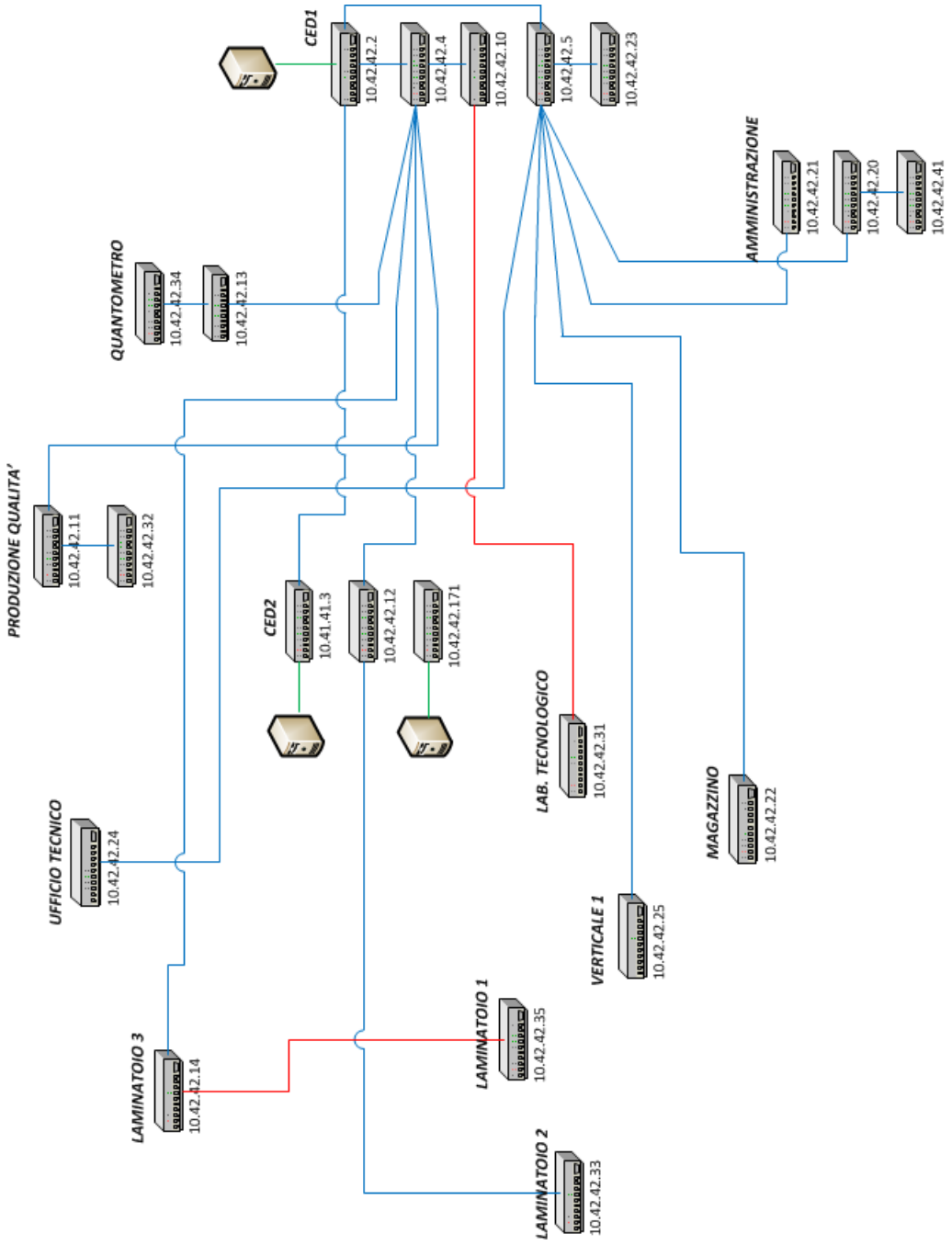


Figura 2.12: Distribuzione switch nei reparti
(collegamenti blu = fibra, verde = UTP cat6, rosso = UTP cat5e)

2.3.1 Ethernet/802.3

Ethernet è un protocollo nato fondamentalmente per gestire l'invio di un frame sul mezzo fisico e la competizione tra due o più utenti che volessero utilizzare contemporaneamente quest'ultimo in una connessione broadcast. Si è sviluppato agli inizi degli anni '70 da ricercatori di Xerox Palo Alto Research Centre (PARC) a cui si uninoro agli inizi degli anni '80 Intel Corporation e Digital Equipment Corporation per definirne uno standard (*Ethernet II* o *DIX Ethernet*) che costituì poi la base per lo standard IEEE 802.3 del 1985.
Oltre che per alcune caratteristiche del livello fisico i due standard si distinguono soprattutto dal fatto che 802.3 divide il livello di collegamento del modello ISO/OSI nel sotto-livello MAC (*Media Access Control*) e nel sotto-livello LLC[8] modificando di conseguenza il formato del frame. Sia lo standard IEEE 802.3 che Ethernet II definiscono specifiche di livello fisico (caratteristiche funzionali di transceiver e repeater, codifica dei dati, mezzi trasmissivi ecc.), e specifiche di livello di collegamento. Le specifiche di livello collegamento di Ethernet v2 contengono le specifiche di controllo di accesso al mezzo trasmissivo (MAC) e la definizione dei codici per la gestione delle communicazioni, mentre 802.3 contiene solo le specifiche MAC e i codici per le communicazioni affidabili sono contenuti nell'intestazione LLC definita nello standard IEEE 802.2. Ormai da diversi anni gli apparati elettronici disponibili in commercio sono conformi anche alle specifiche 802.3; essi vengono normalmente identificati con il nome originale Ethernet e usati come sinonimi.

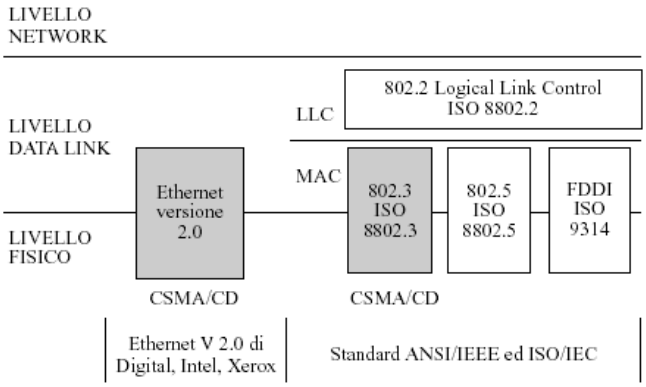


Figura 2.13: Differenze Ethernet II - 802.3

[8]Sottolivello che sta sopra al MAC nascondendo i vari tipi di architettura di rete. Fornisce al livello superiore tre modalità di servizio: logical data link, servizio non affidabile e non orientato alla connessione; data link connection, servizio affidabile e orientato alla connessione e logical data link, non orientato alla connessione ma che prevede una conferma di ricezione.

Di seguito veranno descritte le specifiche di accesso al mezzo trasmissivo e il metodo di contesa, caratteristiche comuni ai due standard.
Ethernet, così come 802.3, è l'implementazione della più generale tecnologia per reti locali CSMA/CD (*Carrier Sense Multiple Access with Collision Detection*). Come indicato dalle parole "multiple access", inizialmente si può pensare ad una serie di nodi che inviano e ricevono frame tramite una linea di connessione condivisa, l'espressione "carrier sense", a sensore di portante, significa che tutti i nodi sono in grado di distinguere una linea inattiva da una occupata mentre "collision detect", con rilevazione di collisione, significa che un nodo rimane in ascolto mentre trasmette e può quindi capire quando un frame, che sta trasmettendo, subisce un'interferenza da un frame trasmesso da un altro nodo.
Il protocollo è di tipo *best effort*, cioè si basa sul principio di fare "del proprio meglio" senza dare nessuna garanzia all'utente riguardo le prestazioni del servizio e utilizza un algoritmo del seguente tipo:

- Prima di trasmettere la stazione aspetta che il canale sia libero;
- Appena è libero inizia a trasmettere;
- Se c'è una collisione, viene inviata una sequenza di 32 bit per Ethernet v2.0 e di 32-48 bit per IEEE 802.3 detta "sequenza di jamming", per avvisare le altre stazioni;
- Se la trasmissione non riesce la stazione attende una quantità di tempo casuale e poi riprova.

La quantità di tempo che si lascia passare è regolata da un apposito algoritmo, il *binary backoff exponential algorithm*:

- Dopo una collisione il tempo si considera discretizzato (slotted) con uno slot time pari a 51,2 microsecondi (a 10 Mbps corrisponde al tempo di andata e ritorno in un segmento di lunghezza massima (2500 m), di un frame di lunghezza minima (512 bit))[9]
- Il tempo di attesa prima della prossima ritrasmissione è un multiplo intero dello slot time e viene scelto a caso in un intervallo i cui estremi dipendono da quante collisioni sono avvenute;
- Dopo n collisioni, il numero r di slot time da lasciar passare è scelto a caso nell'intervallo 0<=r<=2k-1, con k=min(n, 10);
- Dopo 16 collisioni si rinuncia (inviando un messaggio di errore al livello superiore).

[9]Se si vuole aumentare la velocità di un certo fattore, diciamo 10, nello stesso dominio di collisione si deve diminuire di 10 volte la lunghezza massima della rete o aumentare di 10 volte la lunghezza minima del frame.

La crescita esponenziale dell'intervallo garantisce una buona adattabilità ad un numero variabile di stazioni, infatti se il range fosse sempre piccolo, con molte stazioni si avrebbero praticamente sempre collisioni mentre se il range fosse sempre grande, non ci sarebbero quasi mai collisioni ma il ritardo medio causato da una collisione sarebbe molto elevato.
Le prime tecnologie ethernet/802.3 utilizzavano topologia a bus (broadcast) dove tutte le stazioni condividevano il mezzo trasmissivo. Raggiungevano una velocità trasmissiva di 10 Mbps, limitavano la distanza tra due stazioni a circa 4 km e permettevano la presenza di massimo 1024 host[10]. In queste reti inizialmenete venivano utilizzati cavi coassiali e i collegamenti erano implementati con un *giunto a T* o, nel caso di un cavo più spesso, un sistema di accoppiamento detto *tap* che perforava il cavo con una vite dalla punta dorata andandone a toccare l'anima in acciaio. Successivamente all'introduzione di dispositivi come hub e switch, che permettevano un tipo di collegamento diverso, vennero utilizzati i doppini in rame e le fibre ottiche nelle reti a 10 Mbps, in una topologia a stella e non più a bus. Vedi tabella 2.1.

Figura 2.14: Cavo coassiale

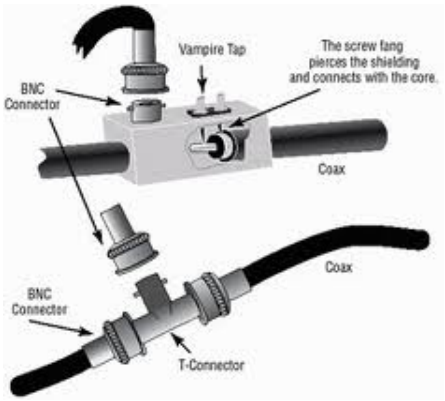


Figura 2.15: Accoppiamento con cavo coassiale: giunto a T e tap

[10]Valore determinato dal fatto che l'algoritmo di backoff esponenziale, che regola l'accesso al canale trasmissivo, prevede un massimo di 2^{10} slot di tempo in cui scegliere di trasmettere dopo una collisione.

L'utilizzo degli switch (Ethernet Switching) introdusse, oltre ad un nuovo metodo di connessione per i cavi, la tecnologia a matrice di commutazione che permette di instradare i pacchetti verso l'interfaccia di destinazione senza propagarli a tutte le altre così da permettere la divisione del dominio di collisione ed eliminare la contesa per il mezzo trasmissivo. Per maggiori dettagli si veda paragrafo 2.4. L'Ethernet Switching segnò l'abbondono dei cavi coassiali e permise di avere una rete con più di 1024 host e un'estensione maggiore rispetto a prima, senza doverla ridurre in caso di aumento di velocità di trasmissione.

Nome	**Standard**	**Descrizione**
Xerox Ethernet	Ethernet II	Prima implementazione
10BASE5	802.3 (8)	Coassiale, connessione tap, 500m
10BASE2	802.3 (10)	Coassiale, giunto a T, 200m
10BASE-T	802.3 (14)	UTP cat3 e cat5e, 100m
10BASE-FL	802.3 (15-18)	Fibra ottica
10BASE-FB	802.3 (15-17)	Fibra ottica, adatta per dorsali

Tabella 2.1: Alcune delle prime versioni Ethernet/802.3 a 10 Mbps

Quelli appena elencati sono solo alcuni tra i primi standard ethernet utilizzati. Col passare degli anni sono state introdotte numerose altre versioni dello standard 802.3 e con l'evoluzione della tecnologia, la velocità di trasmissione è aumentata prima di un fattore 10 (100 Mbps, *Fast Ethernet*), poi di un fattore 100 (1000 Mbps, *GigabitEthernet*), 1000 (10000 Mbps, *10GigabitEthernet*) e anche più. Vedi tabella 2.2. Queste versioni pur mantenendo l'approccio dell'algoritmo CSMA/CD incrementano la velocità di trasmissione agendo sul tipo di cavi utilizzati, sulla codifica dei dati (abbandonando la codifica Manchester) e sulla frequenza di trasmissione. E' possibile realizzare comunque schede di rete che mantengano la compatibilita' con i vari standard.

Nome	**Standard**	**Mezzo trasmissivo / Distanza massima**
100BASE-TX	802.3u	UTP cat5e e STP, 100m
100BASE-FX	802.3u	Fibra multimodale, 1a finestra
1000BASE-SX	802.3z	Fibra multimodale 1a finestra, 220m/550m
1000BASE-LX	802.3z	Fibra monomodale 2a finestra, 5km
1000BASE-T	802.3ab	UTP cat5e,100 m,
1000BASE-TX	802.3ab	UTP cat6, 100m
10GBASE-S	802.3ae	Fibra multimodale, 65 m
10GBASE-L	802.3ae	Fibra monomodale 2a finestra, 10km
10GBASE-E	802.3ae	Fibra monomodale 3a finestra, 40km

Tabella 2.2: Alcuni dei più comuni standard 802.3

Gli acronimi usati per le implementazioni del livello fisico sono tutti del tipo NBaseA, dove N rappresenta la velocità di trasmissione, Base indica che l'implementazione opera in banda base, ed A è una sigla legata al tipo di cavo utilizzato e ad altre caratteristiche salienti.

Ogni scheda di rete prodotta nel mondo possiede un indirizzo di 6 byte univoco e memorizzato in una memoria non volatile. Questo indirizzo è detto indirizzo MAC o indirizzo fisico e costituisce l'identificativo di ogni nodo a livello di collegamento. Rappresenta nelle trame ethernet il destinatario e la sorgente. Per il fatto che esso sia universalmente univoco e non modificabile rappresenta il solo metodo identificativo sicuro per un host in rete ed è utilizzato dagli switch per decidere dove instradare ciascun pacchetto. I 6 byte vengono rappresentati in coppie di cifre esadecimali separate dai due punti e a ciascun produttore di dispositivi ethernet viene fornito un prefisso diverso che dovrà costituire la parte iniziale dell'indirizzo.
Bisogna ricordare inoltre che in una rete che utilizza tecnologia ethernet non è possibile effettuare connessioni che realizzano cicli tra i vari nodi. In alcuni casi questo è auspicabile perchè così si ha la possibilità di raggiungere un nodo nel caso un collegamento non funzionasse, ma senza aver attivato oppurtuni protocolli che gestiscono la ridondanza di collegamenti un frame potrebbe viaggiare all'infinito nella rete, con devastanti effetti sulle prestazioni. Questo argomento verrà trattato approfonditamente nel paragrafo 2.7.
Il frame ethernet costituisce l'unità elementare di informazione scambiata tra elaboratori[11], in figura 2.16 la rappresentazione delle diverse tipologie.
Il primo modello di trama è stato definito nei primi anni '80 dallo standard Ethernet II. La seconda, dopo Ethernet II, è Ethernet 802.3. Alla fine degli anni '80, venne creata una terza trama: Ethernet 802.2. Si differenzia dalla 802.3 per l'aggiunta di 3 campi da 1 byte, sottratti al campo dati (che diventa lungo al massimo 1497 byte). Una quarta ed ultima variante della trama ethernet è la SNAP, simile a 802.2, in cui vengono aggiunti due campi tra cui il campo "tipo" utilizzato già in Ethernet II; vengono sottratti altri 5 byte al campo dati (che si riduce ad un massimo di 1492 byte).

[11] Tra i pacchetti trasmessi deve sempre intercorrere un tempo base di 9.6 microsecondi, detto Inter Packet Gap o Inter Frame Spacing, utile per differenziarli.

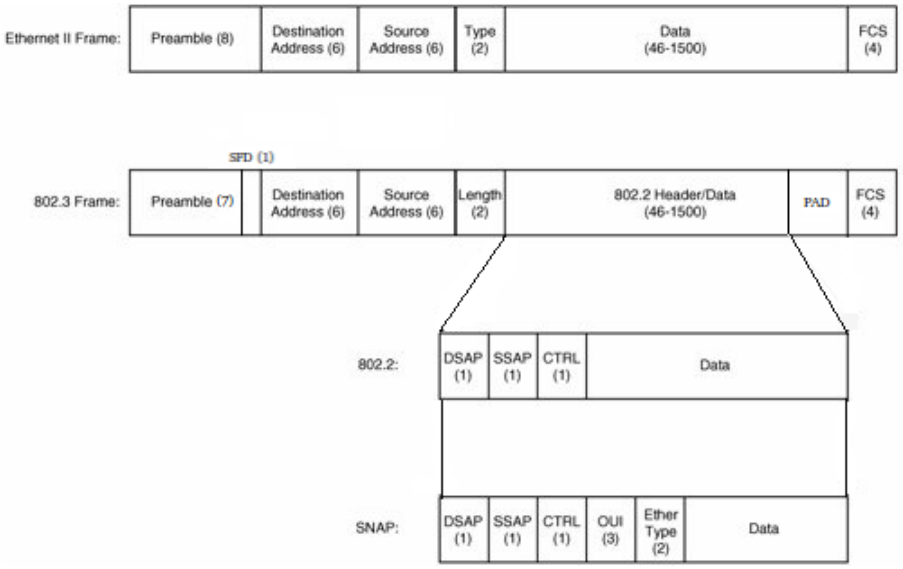


Figura 2.16: I 4 diversi tipi di trame

PRE (*Preamble*)
Preambolo. Sequenza di 1 e 0 che consente al ricevente di sincronizzare la comunicazione svegliando l'adattatore per l'arrivo della trama.

SFD (*Starting Frame Delimiter*)
Presente solo in 802.3 ed è composto da un byte, la cui sequenza di bit è 10101011 (in esadecimale AB). Dichiara che dal prossimo byte avrà inizio il frame vero e proprio, a partire dall'indirizzo di destinazione del frame.

DA (*Destination Address*)
Indirizzo destinazione. Il primo bit ha un significato particolare: se vale 0, la destinazione è una singola unità, altrimenti è un gruppo. Anche il secondo bit ha un significato speciale: se vale 0, l'indirizzo ha valore globale, altrimenti ha soltanto valore locale.

SA (*Source Address*)
Indirizzo sorgente. Rappresenta sempre una singola unità, per cui il primo bit è sempre 0.

TYPE
Possono esistere diversi tipi di frame (IPv4, IPv6, ARP, IPX, ecc.). In questo caso il campo assume un valore da 1536(0x0600) in su al fine di consentire ad alcuni pacchetti di usare il frame Ethernet v2 e ad altri la versione originale 802.3 nello stesso segmento ethernet.

LENGHT
Indica la lunghezza dei dati e può avere un valore minore o uguale a 1500.

PAYLOAD
Sono i dati veri e propri. Minimo 46 byte massimo 1500 dopodichè viene suddiviso in più frame.

PAD
Si aggiungono degli zeri per raggiungere la lunghezza minima del frame di 64 byte così da rilevare le collisioni. Presente solo in 802.3.

FCS (*Frame Check Sequence*)
Il mittente calcola su tutta la parte precedente del frame un valore di controllo secondo un algoritmo CRC (*Cyclic Redundancy Check*). Il ricevente farà lo stesso non appena ricevuto il frame confrontando il valore di questo campo con quello da lui calcolato.

DSAP (*Destination Service Access Point*)
Indica a quale processo di alto livello bisogna consegnare la trama.

SSAP (*Source Service Access Point*)
Indica il processo software di provenienza.

OUI (*Organization Unique Identifier*)

Identificativo universale del fornitore/produttore.

2.3.2 TCP/IP

Nei primi anni settanta, la Defence Advanced Research Project Agency (DARPA) finanziò l'Università di Stanford e la BBN (Bolt, Beranek and Newman) per lo sviluppo di un insieme di protocolli di comunicazione da utilizzarsi per lo sviluppo di reti a commutazione di pacchetto, per l'interconnessione di calcolatori eterogenei. Fu così che nacque l'Internet Protocol Suite i cui due protocolli più noti sono il TCP (Transmission Control Protocol) e l'IP (Internet Protocol). TCP/IP è dunque una serie di protocolli, utilizzabili gratuitamente da tutti perché di pubblico dominio e grazie a ciò ottenero un elevato successo diventando i più utilizzati nelle comunicazioni. Il sistema di protocollo TCP/IP è stato sviluppato scomponendolo in più moduli ciascuno con un compito preciso che svolgono gli uni dopo gli altri in un ordine preciso, con un sistema stratificato. I dati che circolano sulla rete sono trattati successivamente per ogni livello, che aggiunge un elemento d'informazione (detto intestazione) e poi li trasmette al livello successivo. Concettualmente, mandare un messaggio da un programma su una macchina ad un programma su un'altra, significa trasferire tale messaggio giù attraverso tutti i vari livelli e, tramite l'hardware, raggiungere l'altra macchina, risalire gli strati software in successione fino al livello di applicazione dell'utente destinazione. Lo scopo di un sistema a livelli è di separare il problema in differenti parti secondo il loro livello di astrazione. in cui ognuno comunica con un livello adiacente (quello sopra o quello sotto) usando i servizi del livello inferiore e fornendone a quello superiore.

La pila dei protocolli TCP/IP è organizzato concettualmente in quattro livelli e si distingue per questo dal modello ISO/OSI; inoltre ad ogni livello il pacchetto cambia d'aspetto dato che gli si aggiunge un'intestazione e quindi le denominazioni cambiano seguendo i livelli.

- Livello Accesso di rete (TRAME)
- Livello Internet (DATAGRAMMA)
- Livello Trasporto (SEGMENTO)
- Livello Applicazione (MESSAGGIO)

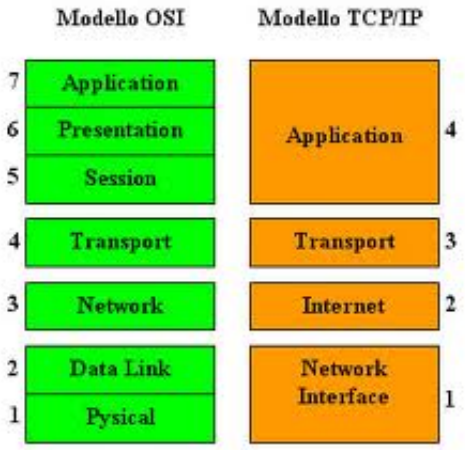


Figura 2.17: Differenza pila ISO/OSI - TCP/IP

APPLICAZIONE: A livello più alto, l'utente invoca i programmi applicativi che permettono di accedere ai servizi disponibili attraverso la rete; gestisce l'interattività tra l'utente e la macchina. Un programma applicativo interagisce con uno dei protocolli di livello trasporto per inviare o ricevere dati e li passa al livello trasporto nella forma richiesta.

TRASPORTO: Lo scopo primario del livello trasporto è consentire la connessione in rete fra due utenti ovvero permettere la comunicazione tra un livello applicativo ed un altro; una comunicazione di questo tipo è spesso detta end-to-end.
Il livello di trasporto deve accettare dati da molti utenti e da molti programmi di uno stesso utente contemporaneamente e, viceversa, deve smistare i pacchetti che gli arrivano ai vari specifici programmi; deve quindi usare delle

porte, di origine e di destinazione, per identificare l'applicazione del destinatario e della sorgente. Per assegnare ad ogni processo la sua porta, valore intero decimale, vengono utilizzati due approcci: *Central Authority*, in cui un'autorità centrale assegna i valori delle porte per servizi di interesse comune a più utenti e li pubblica su una lista; oppure *Dynamic Binding*, dove è il software di rete ad assegnare la porta e per conoscere il valore di un altro computer bisogna inviargli una richiesta.
I principali protocolli che fanno parte di questo livello sono TCP e UDP (User Datagram Protocol). In genere il TCP viene utilizzato per quelle applicazioni che richiedono un servizio orientato alla connessione, come ad esempio la posta elettronica e il file sharing, mentre l'UDP prende sempre più piede per le applicazioni in tempo reale come l'on-line gaming o lo streaming audio e video. La differenza fra i due protocolli risiede nella maggiore affidabilità nel trasporto dei dati di TCP che offre una serie di servizi appositamente pensati (gestione del flusso attraverso l'uso del protocollo Sliding Window, della congestione con la tecnica Multiplicative Decrease Congestion Avoidance/Slow Start Recovery) e controlla che dati giungano a destinazione senza errori ed in sequenza mediante un meccanismo di acknowledgement e ritrasmissione dopo la scadenza di un timeout; UDP invece punta molto sulla velocità di trasmissione a scapito della sicurezza.

INTERNET: Questo livello gestisce la comunicazione tra una macchina ed un'altra anche non connesse alla stessa rete; accetta una richiesta di inoltro di un pacchetto da un livello di trasporto insieme all'identificazione della macchina alla quale il pacchetto deve essere inviato.
Il principale e più importante protocollo di questo livello è IP, Internet Protocol, su cui si basa la comunicazione della rete Internet. Esso è fondamentale perché, anche se di per sé realizza una trasmissione non sicura, fornisce il supporto necessario per tutti gli altri protocolli affidabili. Accetta i pacchetti di livello di trasporto, li spezzetta se necessario e li incapsula nei datagramma di base di questo livello, riempie gli header necessari ed usa l'algoritmo di routing per decidere a chi deve mandare questo pacchetto. Si tratta di routing diretto, quando sorgente e destinatario appartengono alla stessa rete, indiretto quando appartengo a reti diverse ed è neccessario instradare il pacchetto attraverso un router.
Il livello Internet gestisce i datagrammi in ingresso verificandone la validità ed usa l'algoritmo di routing per decidere se il datagramma deve essere inoltrato o processato localmente; in quest'ultimo caso il software elimina l' header del datagramma e sceglie quale protocollo di trasporto gestirà il pacchetto. I protocolli di questo livello sono caratterizzati dal fatto che non forniscono garanzie (pacchetti possono essere persi o consegnati fuori ordine) e non sono orientati alla connessione (ogni pacchetto è indipendente e può seguire un percorso diverso).

Il protocollo IP attualmente utilizzato si chiama IPv4 ma ha i giorni contati. Esso prevede un metodo di identificazione di ogni host connesso ad una rete tramite l'assegnazione di un indirizzo binario a 32 bits suddivisi in quattro gruppi con i rispettivi valori scritti in decimale che permette la gestione di 2^{32} ovvero 4 miliardi di utenti. Concettualmente, ciascun indirizzo IPv4 è una coppia NetID-HostID, dove il NetID identifica la rete dove è connesso l'host mentre l'HostID identifica l'host su quella rete. Gli indirizzi IPv4 inoltre sono divisi in cinque classi distinguibili dai tre bit di ordine più alto e presentano un diverso numero di bit utilizzato per identificare un host all'interno della rete. In ogni classe di indirizzi è presente un gruppo di indirizzi, detti indirizzi privati, riservati alle reti locali e non visibili dall'esterno, allo scopo di ridurre le richieste di indirizzi pubblici; i pacchetti relativi a tali reti non vengono instradati dai router nella rete Internet e quindi non entreranno in conflitto con analoghi indirizzi posti su altre reti locali.

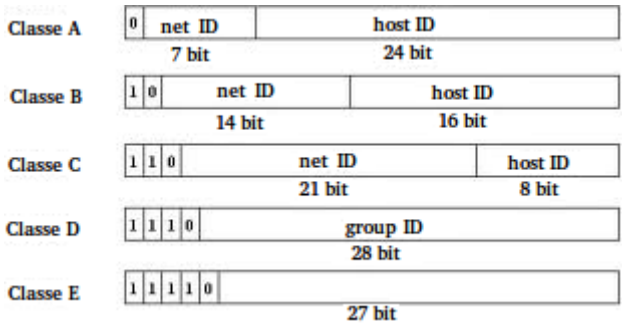


Figura 2.18: Classi indirizzi IPv4

Private IP Networks	Class of Networks	Number of Networks
10.0.0.0 through 10.0.0.0	A	1
172.16.0.0 through 172.31.0.0	B	16
192.168.0.0 through 192.168.255.0	C	256

Figura 2.19: Intervalli indirizzi privati

Ad oggi però la nostra società è costantemente innondata da i più svariati dispositivi elettronici dotati di un accesso Internet che neccesita di un indirizzo IP, vedi smartphone, tablet, navigatori e console, e questo fatto ha decretato l'inevitabile esaurirsi degli indirizzi disponibili. Per superare questo ostacolo si pensò alla creazione di un nuovo protocollo che incrementasse lo spazio di indirizzamento.
Fu così che già nei primi anni '90 si cominciò a lavorare al progetto del un nuovo protocollo che inizialmente venne chiamato IPng o IP New Generation ma a cui poi fu assegnato un numero di versione ufficiale noto come IPv6[12] in cui i bits riservati per l'indirizzo sono 128, rappresentati in 8 gruppi di 4 cifre esadecimali, che permettono di indirizzare $3,4 \cdot 10^{38}$ nodi; numero a dir poco sufficiente per le esigenze presenti e future. Lo spazio di indirizzamento di IPv6 è suddiviso in base ai bit più significativi che specificano i diversi usi dell'indirizzo.

Prefisso	Utilizzo
0000 0000	Riservato
0000 0001	Non assegnato
0000 001	Riservato per assegnazioni NSAP
0000 010	Riservato per assegnazioni IPX
0000 011	Non assegnato
0000 1	Non assegnato
0001	Non assegnato
001	Aggregatable Global Unicast Addresses
010	Non assegnato
011	Non assegnato
100	Non assegnato
101	Non assegnato
110	Non assegnato
1110	Non assegnato
1111 0	Non assegnato
1111 10	Non assegnato
1111 110	Non assegnato
1111 1110 0	Non assegnato
1111 1110 10	Indirizzi da usare su una linea locale
1111 1110 11	Indirizzi da usare in un sito locale
1111 1111	Indirizzi di tipo multicast

Figura 2.20: Utilizzo prefissi indirizzi IPv6

Oltre ad aumentare lo spazio di indirizzamento l'IPv6 incrementa la sicurezza e la confidenzialità dei pacchetti, è in grado di configurare automaticamente alcuni parametri di rete, supporta nativamente la QoS per servizi in tempo reale, ha un header di lunghezza fissa, i datagram sono non frammentabili dai router (se necessario possono solo gli host) ed elimina il campo checksum, già presente negli altri strati dello stack.

[12]La discontinuità nella numerazione delle versioni è dovuta al fatto che la versione 5 venne usata qualche tempo addietro per un protocollo sperimentale

La transizione ad IPv6 comporta però vari problemi di compatibilità con IPv4. La politica adottata consiste in un graduale passaggio da un protocollo all'altro, cercando di far coesistere le due versioni di IP in un'unica rete. Per far ciò la strada seguita consiste nel costruire router e switch in grado di interpretare entrambi i protocolli, utilizzare sistemi operativi in grado di generare indirizzi IPv6 e di interpretarli e aggirare la non interpretabilità di IPv6 via software.
Tutte le soluzioni finora create possono essere suddivise in tre categorie:

Tunneling: Incapsula il pacchetto IPv6 in un pacchetto IPv4 oppure integra l'indirizzo IPv4 nell'indirizzo IPv6.
NAT-PT: Traduzione con metodo NAT degli indirizzi IPv4 e IPv6.
Dual-stack: Un campo Version identifica la versione del protocollo.

ACCESSO DI RETE: Il quarto ed ultimo strato è costituito da una interfaccia di rete che accetta il datagramma IP e lo trasmette, dopo averlo incapsulato in apposite trame, sull'hardware di rete (mezzo trasmissivo).

2.3.3 IPX/SPX

La suite di protocolli IPX/SPX, derivata da Xerox XNS, venne introdotta originariamente da Novell per lo scambio di pacchetti in rete dove presenti macchine con sistema operativo NetWare, un sistema operativo sviluppato da Novell che ebbe grande successo negli anni ottanta come primo vero sistema operativo di rete introducendo sul mercato di larga scala i concetti di condivisione delle informazioni in rete e avendo il suo punto di forza nel software per i client compatibile con diverse piattaforme. NetWare conquistò la una posizione dominante sul mercato sviluppando lo standard local area network (LAN) partendo da un concetto molto semplice: condivisione dei file invece che dei dischi. A causa della popolarità di NetWare tra la fine degli anni 1980 e la metà degli anni 1990, l'IPX divenne un protocollo di internetworking molto diffuso ma già alla fine degli anni novanta, con il boom della connettività Internet, la pila TCP/IP, utilizzata per le communicazioni nella rete mondiale, divenne dominante anche sulle LAN dove prima invece primeggiava IPX/SPX.
Il supporto nativo al TCP/IP per i servizi di file e stampa normalmente associati a Novell venne introdotto con NetWare 5.0 solamente nel 1998 in cui Novell riconobbe finalmente l'importanza di Internet, passando la sua interfaccia primaria, da IPX/SPX a TCP/IP; IPX/SPX era ancora supportato, ma l'enfasi era passata su TCP/IP. Anche il sistema operativo MS-DOS, che vide la luce prima dell'introduzione di TCP/IP, utilizza per lo scambio di pachetti in rete i protocolli di IPX/SPX. In sistemi operativi in cui il supporto a IPX/SPX non è previsto di default dev'essere appositamente abilitato, e in alcuni casi devono essere installati specifici pacchetti software aggiuntivi affinchè vengano elaborati.
IPX/SPX prende il nome, come TCP/IP, dai due protocolli più importanti, IPX e SPX appunto. Altri importanti procolli di questa collezione sono NCP per interazioni client/server nella condivisione di risorse anche da remoto e SAP che ad intervalli di tempo pubblica gli indirizzi dei server e i servizi disponibili.
L'Internetwork Packet Exchange (IPX) è un protocollo di rete che offre un servizio senza connessione, inaffidabile, senza correzione di errori e senza nessuna garanzia sulle prestazioni. Visto dunque che IPX non garantisce la spedizione dei pacchetti, i livelli più alti devono fornire i servizi per l'invio sicuro. A livello Trasporto NetWare usa il protocollo Sequenced Packet Exchange (SPX), protocollo affidabile che gestisce circuiti virtuali, esegue il controllo di flusso oltre che degli errori e garantisce la sequenzialita' dei pacchetti scambiati. Raramente vengono persi o danneggiati durante la trasmissione su una singola rete e in tal caso è prevista la richiesta di ritrasmissione.

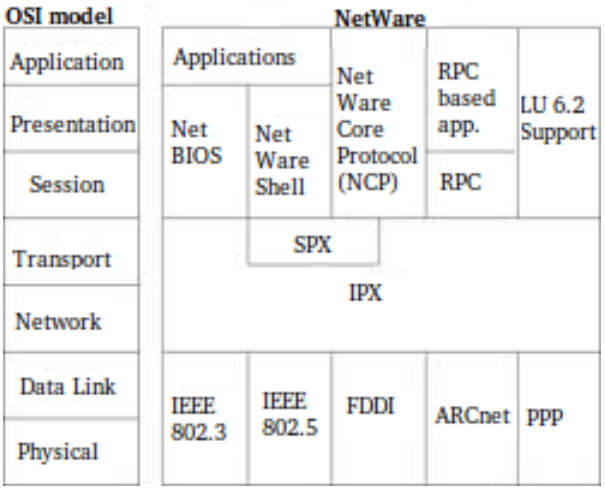


Figura 2.21: I principali protocolli della pila IPX/SPX

Gli host per i protocolli di IPX/SPX hanno indirizzi di nodo a 48-bit, che di default sono settati sull'indirizzo MAC dell'interfaccia di rete, mentre le reti sono identificate da un indirizzo esadecimale a 32-bit all'interno dell'intervallo: 0x1 - 0xFFFFFFFE. L'indirizzo di nodo viene unito all'indirizzo di rete in modo da creare un identificativo unico per l'host sulla rete nel formato rete:nodo. Siccome l'indirizzo di nodo è solitamente identico all'indirizzo MAC della scheda di rete, la traduzione tra indirizzo di livello rete e indirizzo di livello collegamento, come avviene in TCP/IP, non è necessaria.

IPX inoltre può essere trasmesso su ethernet usando uno dei quattro seguenti tipi di incapsulazione nella trama di livello collegamento:

802.3 (raw): Usato nei sistemi legacy[13] e prevede che i dati IPX inizino immediatamente dopo il frame header 802.3. Questi ultimi iniziano sempre con due byte 0xFF per differenziare questo tipo di incapsulazione IPX.
Ethernet II: comprende un frame header Ethernet II seguito dai dati IPX.
802.2 (SNAP): Comprende un frame header 802.3, un header LLC (3 byte: 0xAA, 0xAA, 0x03), un header SNAP (5 byte: 0x00, 0x00, 0x00, 0x81, 0x37) e i dati IPX. I campi 0xAA dell'header LLC stanno per protocollo 'SNAP'. I primi tre byte dell'header SNAP sono un OUI seguiti da 2 byte dell'EtherType IPX.
802.2 (Novell): Comprende un frame header 802.3 (destination, source, length) seguito da un header LLC (3 byte - 0xE0, 0xE0, 0x03) seguito dai dati IPX. Il campo 0xE0 dell'header LLC sta per protocollo 'Novell'.

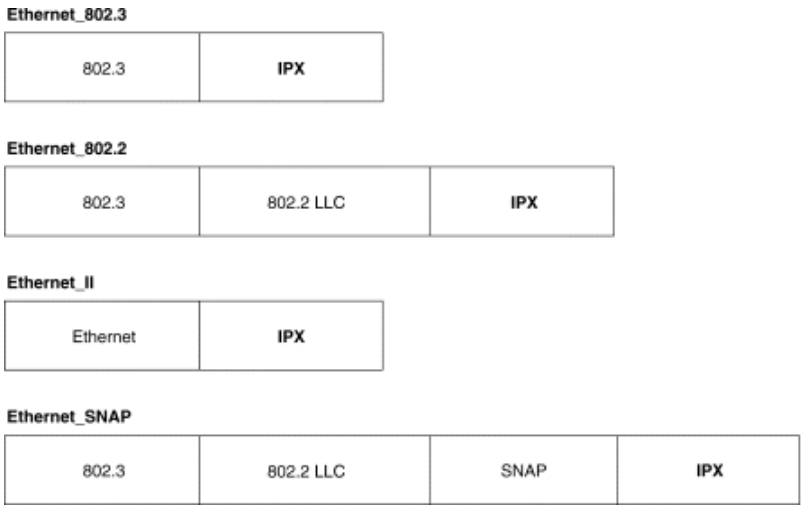


Figura 2.22: Metodi di incapsulamento

[13]Sistema informatico che l'utente non vuole o non può rimpiazzarla, che utilizzano tecnologie meno recenti e per questo motivo sono molto difficili da interfacciare con i sistemi più recenti

2.4 Dispositivi di rete

Nella rete aziendale, allo stato attuale, sono presenti 22 switch, un firewall e un router. Principalmente sono stati individuati mentre si studiava la topologia di rete e venivano ispezionati i reparti segnalati dagli amministratori ed evidenziati in figura 1.9 e 2.12.
All'inizio però erano presenti anche due hub. Il primo, individuato assieme agli altri dispositivi, era situato nel laboratorio elettronico, vicino al reparto verticale1. Al dispositivo, che faceva capo ad uno switch in sala CED1, erano collegati due macchinari del laboratorio elettronico. Risultava necessario questo ripetitore perchè altrimenti la distanza tra i due macchinari e lo switch a cui erano connessi era superiore a 100 m, cosa che lo standard ethernet non permette. Attualmente, visto che di recente nel reparto verticale1 è stato installato lo switch 10.42.42.25 che dispone di porte libere, l'hub è stato rimosso e i collegamenti spostati, seguendo un percorso adeguato e facilmente realizzabile grazie alla comoda posizione delle macchine che limitava gli ostacoli da superare. In questo modo si è diviso il dominio di collisione tra le due macchine che non saranno più in competizione per l'accesso al mezzo.
Il secondo hub invece non era presente negli armadi ispezionati e in cui erano stati trovati tutti gli altri dispositivi.
Mentre si studiava la topologia, nel paragrafo 2.3, si è detto che venivano esaminate le tabelle MAC degli switch e segnalate le porte per le quali erano presenti più di un indirizzo MAC, questo perchè stava significare che la connessione era verso un altro dispositivo e non verso un terminale. Una volta terminata la mappa completa della disposizione degli switch, si è notato che una porta dello switch 10.42.42.14, situato nel reparto laminatoio3, presentava ancora una lista di indirizzi MAC. Questo stava a significare senza dubbio che a quella porta era connesso un'altro dispositivo. Anche se tutti i locali segnalati dagli amministratori erano stati esaminati, si è proceduto alla ricerca di questo dispositivo, che si pensava dovesse essere un altro switch, negli armadi situati all'interno della fabbrica e adiacenti al laminatoio3. Fortunatamente, dopo alcuni tentativi, in un armadio polveroso e dimenticato, è stato ritrovato non uno switch, ma un altro hub a cui questa volta erano collegati molti macchinari del reparto laminatoio1.
Questa volta non si potevano spostare tutti i cavi nello switch 10.42.42.14 del laminatoio3 o in altri switch vicini, sia perchè non si disponeva di tante porte libere sia perchè stendere nuovi cavi in quel reparto per un collegamento in sicurezza avrebbe richiesto molto tempo e un lavoro costoso vista la complicata posizione dei macchinari. Si è deciso dunque di installare un nuovo switch, 10.42.42.35, nell'armadio "dimenticato" del laminatoio1, collegandolo con il cavo già utilizzato in precedenza, allo switch più vicino, il 10.42.42.14 del laminatoio3.

Questa soluzione sebbene il dominio di collisione è stato diviso ed è stata eliminata la contesa per l'accesso al mezzo da parte di tutti quelli utenti, non è comunque definitiva. Il cavo utilizzato per collegare lo switch del laminatoio1 con lo switch del laminatoio3 è un UTP cat5e, steso sotto il pavimento della fabbrica, che non potendo sostenere velocità superiori, anche a causa della distanza tra i due dispositivi quasi al limite consentito dallo standard utilizzato, è stato collegato a porte a 100 Mbps diventando di fatto un collo di bottiglia per i pacchetti in transito. Rispetto infatti a tutti gli altri collegamenti tra switch questo presenta una velocità di trasmissione 10 volte inferiore. Inoltre, collegare i cavi direttamente alle porte dello switch senza passare prima per un patch panel, ovviamente non presente, è sconveniente se non adirittura contro produttivo. Per maggiori spiegazioni sui problemi riguardanti i patch panel si rimanda alla lettura del paragrafo 2.6.
Dei 22 switch attualmente attivi nella rete, solamente 20 erano presenti nella configurazione iniziale; due sono stati aggiunti per motivi diversi nel corso delle modifiche effettuate.
Uno di questi è il 10.42.42.5, aggiunto al primo livello di connettività al pari di 10.42.42.4 (vedi figura 2.11), switch sul quale prima gravava il carico di tutto il traffico distribuito ai nodi dei vari reparti. E' stato posizionato in sala CED1 e adesso il carico del traffico risulta più bilanciato; se dovesse rompersi uno dei due switch di primo livello, metà della rete resterebbe comunque attiva. Si è scelto di installare uno switch identico a 10.42.42.4, con tutte le porte in fibra ottica (10.42.42.2 e 10.42.42.3 oltre a 4 porte in fibra ottica hanno porte in rame che possono lavorare a 1000 Mbps per le connessioni a server, router e firewall mentre tutti gli altri switch presentano porte in rame a 100 Mbps e solamente una/due porte di uplink, in rame o fibra a seconda del trasduttore installato, che viaggiano a 1000 Mbps), adatto per lo scopo di portare la connettività a tutti gli altri nodi della rete. Si è avuto cura inoltre, vista l'importanza dello switch 10.42.42.5, di connettere sia lui che 10.42.42.4 all'alimentazione ridondata, proteggendoli da un'eventuale interruzione elettrica così da mantenere attivi almeno i nodi ai livelli più alti e più importati.
Il secondo degli switch aggiunti è il 10.42.42.35, in laminatoio1, ed è colui che è andato a sostituire l'hub come spiegato in precedenza.
Un'ulteriore modifica alla configurazione iniziale degli switch è stata apportata prima di redigere la mappa della topologia definitiva in figura 2.11.
Nel reparto amministrazione infatti, i 3 switch presenti, inialmente erano collegati in cascata. Questo però, sebbene le connessioni tra gli switch venissero fatte a 1000 Mbps, presentava comunque un quarto livello di connettività e quindi un calo delle prestazioni per gli utenti collegati. Vista la possibilità di utilizzare una dorsale in fibra già presente e non utilizzata verso sala CED1, si è deciso di collegare lo switch 10.42.42.21 direttamente allo switch 10.42.42.5 del CED1 e mantenere in cascata solamente 10.42.42.20 e 10.42.42.41.

C'è da aggiungere infine che man mano uno switch veniva preso in esame, con l'aiuto di un portatile, ci si collegava alla porta seriale (standard RS232 presente su tutti gli switch) per poterne configurare alcuni parametri e renderne più facile la gestione. Si accedeva così al software di configurazione (firmware) che oltre a tante altre cose, permetteva di impostare indirizzo ip, maschera di rete, e gateway predefinito; parametri che definivano una rete di management costituita dagli switch. Una volta definita la rete degli switch era facile accedere alla configurazione di un dispositivo da un qualsiasi terminale della rete principale utilizzando il protocollo telnet[14].
Per fare ciò bisognava però aggiungere una corrispondenza nella tabella di routing del terminale dal quale si voleva accedere alla rete di management. Nella rete aziendale infatti, di default, quando un elaboratore della rete principale tenta di comunicare con una rete esterna indirizza i pacchetti al gateway predefinito, il firewall, che si interfaccia solamente con la rete Internet. Per spostarsi sulla rete di management, ma può valere anche per la rete di backup, è neccessario far seguire ai pacchetti in uscita un percorso diverso: invece di andare al firewall devono dirigersi al router, il gateway verso le reti di backup e management. Questo si ottiene eseguendo sul terminale, da riga di comando, l'istruzione "ROUTE ADD 10.0.0.0 MASK 255.0.0.0 192.168.205.253" per la rete management e "ROUTE ADD 192.168.201.0 MASK 255.255.255.0 192.168.205.253" per la rete di backup; il primo parametro è l'indirizzo di rete da raggiungere, il secondo è la maschera di rete mentre il terzo è l'indirizzo ip del gateway al quale consegnare i pacchetti in uscita.
Per quanto riguarda firewall e router non sono state apportate modifiche.
Il firewall presente in sala CED1, oltre ad essere collegato allo switch 10.42.42.2 di centro stella, è connesso a 1000 Mbps con un cavo UTP cat6 all'antenna situata sopra al CED1, che porta la connettività Internet e di cui funge da gateway predefinito. Il router, anch'esso situato in sala CED1, svolge solo il ruolo di gateway per la rete principale verso la rete di backup e verso la rete di management degli switch.

[14]Protocollo di rete non sicuro utilizzato per fornire all'utente sessioni di login remoto di tipo riga di comando tra host in rete.

2.4.1 Hub

Un ripetitore o hub è generalmente un dispositivo elettronico che riceve in ingresso un segnale debole e lo ritrasmette in uscita con un segnale più alto e potente, cosicché la propagazione del segnale può essere garantita a lunghe distanze senza eccessivo degrado.
Il dispositivo lavora al livello fisico del modello ISO/OSI e non gestisce l'arbitraggio dell'accesso al mezzo trasmissivo, lasciando che gli host di una ethernet collegati lo facciano tramite l'algoritmo CSMA/CD. Ogni nodo che si collega ad un hub fa parte quindi del medesimo dominio di collisione. Il traffico, le collisioni ed i frame ritrasmessi vengono replicati su tutte le porte dell'hub, frazionando e sottraendo banda passante in egual misura ad ogni utenza della rete; le uniche connessioni possibili tra il dispositivo e gli host sono half-duplex[15].

Vi sono tre categorie di hub:

Passivi: Non necessitano di alimentazione, si limitano a connettere i cavi.
Attivi: Necessitano di alimentazione, poiché amplificano il segnale.
Ibridi: Hub avanzati, permettono collegamento tra più tipologie di cavo.

Oltre a ritrasmettere il segnale ricevuto ed eventualmente il segnale di jam nel caso di una collisione, un hub ha il compito di ripristinare simmetria e posizione del segnale rigenerando, se necessario, il preambolo del frame. Il ritardo introdotto da un hub per svolgere queste operazioni è generalmente di pochi microsecondi ed è quindi quasi ininfluente

[15] Un sistema half-duplex fornisce una comunicazione in entrambe le direzioni, ma con la possibilità di usare soltanto una direzione alla volta.

2.4.2 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 traffico, 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[16] raddoppiando la banda passante.

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

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

[16] Un sistema full-duplex permette la comunicazione in entrambe le direzioni e, diversamente dall'half-duplex, la permette simultaneamente. Il mezzo trasmissivo però deve avere due canali indipendenti.

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.
Spesso su alcune porte possono essere montati trasduttori utilizzati per aggiungere ad uno switch 100Base-TX una o due porte di tipo 1000Base-X per il collegamento verso il resto della rete (uplink) o per un server veloce.
Macchine più evolute invece sono dotate di funzionalità che permettono di collegarsi tra loro ed essere viste come un unico dispositivo. In questo caso rami con caratteristiche di velocità e capacità inferiori, che prima collegavano le macchine, confluiscono ordinatamente su rami con caratteristiche superiori, con velocità che arrivano anche a 10Gbps. Questo tipo di collegamento viene detto "stack".
Uno switch di fascia medio-alta inoltre è tipicamente dotato di un agente di gestione, ovvero un piccolo 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.

2.4.3 Router

Nella tecnologia delle reti a commutazione di pacchetto[17] un router è un dispositivo che lavora a livello di rete e permette la connessione di reti di livello collegamento eterogenee garantendo il passaggio di un pacchetto da una rete ad un'altra grazie a un indirizzo IP e a una maschera (con cui viene fatto l'AND logico a livello di bit) per ogni rete a cui si interfaccia.
La funzione di instradamento è basata dunque sugli indirizzi IP di livello di rete, a differenza dello switch che instrada sulla base degli indirizzi di livello collegamento.
Possiamo dividere il routing dei pacchetti in due forme: diretto e indiretto. Il routing diretto si realizza tra due macchine connesse alla stessa rete ed è immediato mentre il routing indiretto si realizza tra due macchine non interfacciate alla stessa rete dove il mandante è obbligato a passare il datagramma al router per la decisione. In questo caso il procedimento si fa un pò più complicato perchè il mittente incapsula il datagramma e lo manda al router più vicino, questo estrae il datagramma e il software al livello di rete sceglie il prossimo router sulla strada per la destinazione. Il datagramma viene di nuovo incapsulato in frame di livello di collegamento e il procedimento si ripete finché si trova un router che può mandare il pacchetto direttamente al destinatario.
Gli elementi della tabella di instradamento (Routing Table) non sono singoli calcolatori ma intere reti, ovvero sottoinsiemi anche molto ampi dello spazio di indirizzamento. Questo è fondamentale per la scalabilità delle reti, in quanto permette di gestire reti anche molto grandi facendo crescere le tabelle di instradamento in modo meno che lineare rispetto al numero di host.
Per garantire la massima affidabilità e lo sfruttamento ottimale dei collegamenti in caso di reti complesse costituite da molte sottoreti diverse e variamente interconnesse, i router possono costruire le loro tabelle di instradamento del tutto autonomamente e in modo dinamico, scambiandosi periodicamente informazioni su come raggiungere le varie reti che collegano l'un l'altro comprese le eventuali nuove sottoreti. Per fare questo sono stati messi a punto dei protocolli di routing appositi, come OSPF, RIP e BGP, attraverso i quali i router si scambiano informazioni sulle reti raggiungibili. In alternativa è pur sempre idealmente possibile, ma non sempre effettivamente realizzabile a causa della complessità delle reti, una configurazione delle tabelle di routing IP in maniera manuale e statica. In un router possono inoltre essere implementate diverse politiche di scheduling e di gestione dinamica della coda per la QoS dei vari protocolli.

[17] Tecnica di accesso multiplo a ripartizione nel tempo, utilizzata per condividere un canale di comunicazione tra più stazioni in modo non deterministico, si distingue dalla modalità di trasferimento a commutazione di circuito che è invece tipicamente usata nelle comunicazioni telefoniche.

Come per lo switch esistono più tipologie di instradamento che possono essere utilizzate da un router:

- Cut-Through
- Store-and-Forward

I vari processi di elaborazione per l'indirizzamento e l'instradamento modificano l'header del pacchetto, ad esempio decrementando il campo TTL[18] e aggiornando il campo checksum. Questo processo introduce dei sensibili ritardi aggiuntivi sulla linea di uscita e sono motivo di miglioramento da parte dei produttori di router.
In generale i router, in quanto sistemi embedded, hanno il loro sistema operativo e necessitano di essere configurati manualmente non essendo dispositivi plug and play. A seconda della tipologia del router la configurazione avviene tramite un'interfaccia basata su web (accessibile digitando l'indirizzo IP del dispositivo nel browser) o attraverso un'apposita console a riga di comando su porta seriale.

[18] Determina il numero massimo di elaboratori che possono essere attraversati da un pacchetto.

2.4.4 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. Per un approfondimento sul concetto di DMZ si veda il paragrafo 2.2.1.
Spesso inoltre un firewall, a seconda delle esigenze, integra anche la funzione di gateway, esegue operazioni di NAT e gestisce connessioni VPN . Questi meccanismi sono spiegati in dettaglio nel paragrafo 2.1.1 e 2.1.2.

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 necessità di molti accorgimenti hardware e software.

2.5 Mezzi di connessione/trasmissione

Per i collegamenti tra i vari dispositivi della rete aziendale vengono utilizzate due diverse categorie di mezzi trasmissivi: elettrici, con cavi in rame UTP cat5e e cat6 e ottici, con la fibra ottica.
La fibra ottica è utilizzata per collegamenti a 1000 Mbps tra gli switch della rete in modo tale da non creare colli di bottiglia dove il traffico di pacchetti è elevato. A parte per 10.42.42.2, 10.42.42.3, 10.42.42.4 e 10.42.42.5 che presentano nativamente delle porte in fibra ottica, per tutti gli altri switch, che dispongono soltanto di porte per cavi in rame a 100 Mbps, è stato necessario installare dei trasduttori (forniti dalla casa costruttrice degli switch) negli appositi slot. In questo modo si possono utilizzare una o al massimo due porte (uplink) per dispositivo a 1000 Mbps; per cavi in rame o in fibra ottica a seconda del tipo di trasduttore.
Non è stato comunque possibile effettuare una connessione in fibra a 1000 Mbps tra lo switch 10.42.42.10 del CED1 e lo switch 10.42.42.31 del laboratorio tecnologico perchè non è presente nessuna dorsale tra i due reparti che ne permette il collegamento. Non si conosce il motivo per cui quando sono state realizzate le altre dorsali in fibra ottica presenti in azienda non sia stato raggiunto anche il laboratorio tecnologico ma di certo questo è un grave difetto che se non altro andrebbe risolto al più presto portando anche in quel reparto una connessione in fibra a 1000 Mbps. Anche lo switch 10.42.42.35 del laminatoio1 è raggiunto da una connessione con cavo in rame cat5e a 100 Mbps ed il perchè è già stato spiegato nel paragrafo 2.4.
Le dorsali di fibra ottica installate in azienda sono di tipo multimodale e presentano due differenti diametri di core: alcune sono a 50 μm mentre altre a 62,5 μm. Lo schema è mostrato in figura. Questa differenza non rappresenta un problema per quanto riguarda le prestazioni della rete ed entrambe le tipologie di fibra rientrano nello standard 1000BaseSX. Questo standard prevede una lunghezza massima di 220 m per la fibra con core da 62,5 μm e di 550 m per per la fibra da 50 μm, entrambi con lunghezza d'onda 850 nm. Anche se utilizzare due diametri di core differenti nelle dorsali non rappresenta un problema, lo potrebbe diventare il fatto di utilizzare una bretella (così si chiama il pezzo di fibra che va dalla dorsale al dispositivo) con core di diametro diverso rispetto a quello usato nella dorsale. Se i core, cioè dove effettivamente viaggia l'informazione sotto forma di luce, non sono dello stesso diametro e non sono perfettamente allineati si potrebbe andare incontro ad attenuazione e distorsione con conseguente perdita di pacchetti e peggioramento delle prestazioni. Si è eseguito dunque un controllo su tutte le fibre utilizzate, sostituendo le bretelle nel caso i due diametri non coincidessero e controllando anche che non effettuassero curvature troppo strette quando venivano raggruppate all'interno degli armadi perchè questo avrebbe potuto danneggiare la fibra e compromettere la qualità delle trasmissioni.
Nell'analizzare le fibre si è notato infine che esse utilizzano due tipi differenti

di connettori: ST per le connessioni al patch panel e SC per le connessioni verso i dispositivi. Anche in questo caso, usare due tipi di connettori differenti non presenta problemi e di conseguenza non si effettuano cambiamenti. I cavi in rame utilizzati, come già detto, sono di due tipi e presentano differenti caratteristiche; di conseguenza vengono impiegati per scopi differenti. I cavi UTP cat5e vengono utilizzati per le connesioni verso gli utenti finali dove la velocità di 100 Mbps è sufficiente a soddisfare le attuali esigenze mentre i cavi UTP cat6 vengono impiegati nelle connessioni a 1000 Mbps verso i server, il router e il firewall. In questo scenario si ha a che fare dunque sia con lo standard 100BaseTX che con lo standard 1000BaseTX, dove la lunghezza massima per un collegamento garantito è di 100 m per entrambi. L'utilizzo di tre differenti standard di rete anche se in un primo momento potrebbe creare confusione, in questo caso risulta una scelta adeguata e garantisce buone prestazioni senza creare il minimo problema di compatibilità. Ogni mezzo trasmissivo infatti ha vantaggi e svantaggi determinati per lo più dal costo, dalla larghezza di banda[19], dalla massima velocità di comunicazione consentita e dalla massima estensione geografica garantita. È importante dunque trovare un equilibrio tra tutti questi fattori ed individuare ciò che si adatta meglio alle proprie esigenze.

[19] L'insieme delle frequenze che possono essere trasmesse senza attenuazione eccessiva o costante

2.5.1 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[20], 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 multicoppia.

Figura 2.23: Cavo UTP

[20] gabbia di Faraday

I cavi UTP seguono le specifiche standardizzate in TIA/EIA[21] 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 1000BaseTX vengono utizzate 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.

[21] Telecommunications Industry Association/Electronic Industries Alliance

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, 100BaseTX 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 perchè 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.

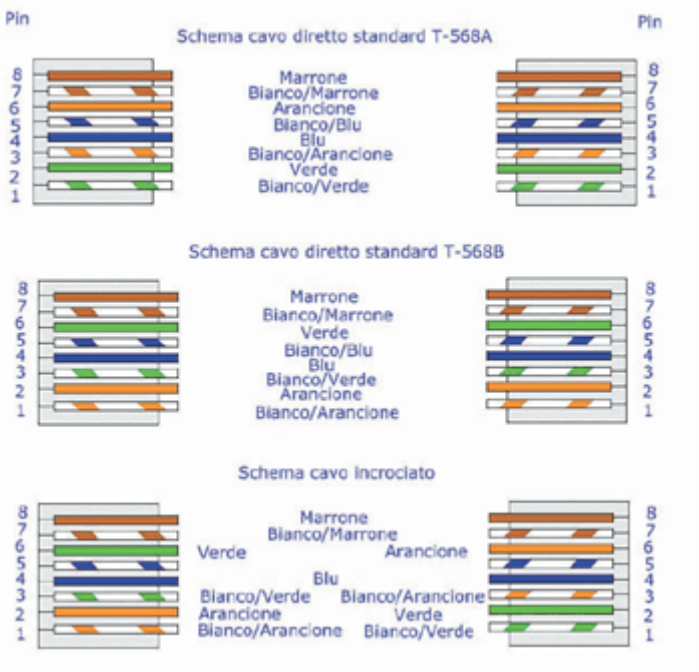


Figura 2.24: Schema dei cavi nelle diverse tipologie

2.5.2 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.

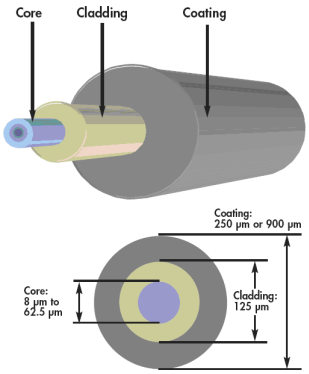


Figura 2.25: Fibra ottica

La fibra ottica funziona come una specie di specchio tubolare. La luce che entra[22] nel core ad un certo angolo si propaga mediante una serie di riflessioni alla 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[23] 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.

[22] La presenza di luce corrisponde ad un bit a '1', l'assenza ad uno '0'.

[23] Rappresenta il fattore numerico per cui la velocità di propagazione di una radiazione elettromagnetica viene rallentata rispetto alla sua velocità nel vuoto quando questa

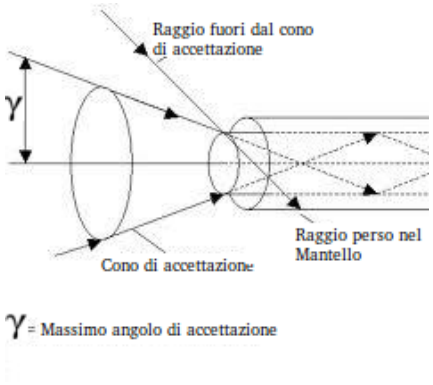


Figura 2.26: Metodo di propagazione nella fibra

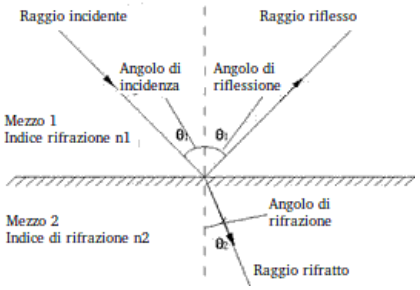


Figura 2.27: Angoli del fascio luminoso

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[24], rispetto alle multimodali.
All'esterno della fibra vi è una guaina protettiva polimerica detta "jacket" che serve a dare resistenza agli stress fisici e alla corrosione evitando il contatto fra la fibra e l'ambiente esterno.

attraversa un materiale

[24] Anche se la fibra è caratterizzata da una bassissima attenuazione intervengono comunque fenomeni fisici come le impurità, i difetti di fabbricazione e le caratteristiche intrinseche al mezzo che degradano il segnale.

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 multicromatica.

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.

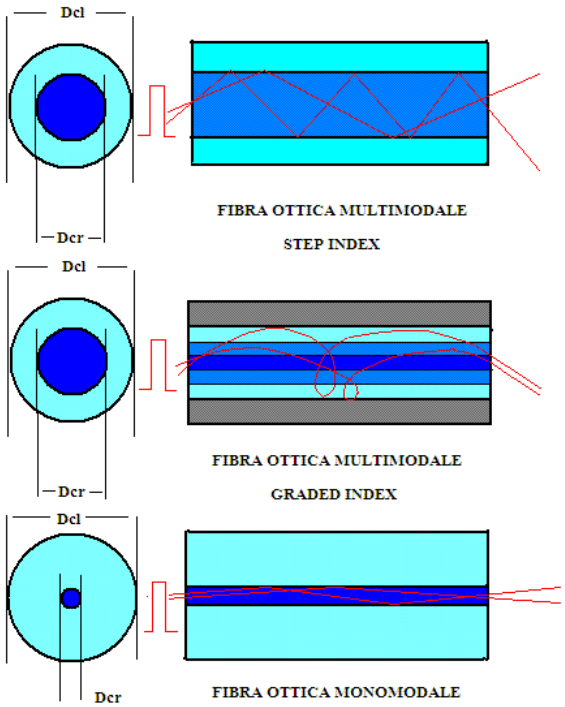


Figura 2.28: Tipi di fibre ottiche

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 piu' bassa ed è caratterizzata da una lunghezza d'onda di 1310/1550 nm. Per lavorare in questa zona è necessario utilizzare esclusivamente emettitori laser con fibre monomodali.

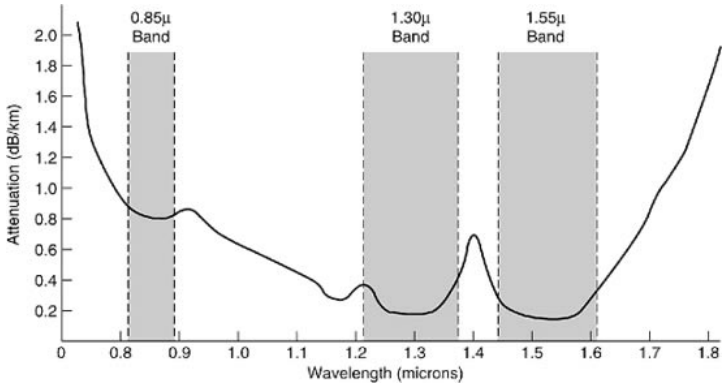


Figura 2.29: Finestre di trasmissione

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).

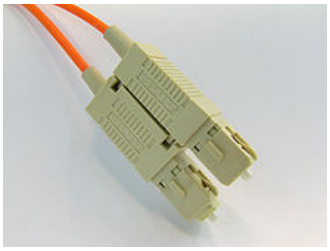


Figura 2.30: Connettore SC

Figura 2.31: Connettore LC

Figura 2.32: Connettore ST

Figura 2.33: Connettore FC

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.

Riassumendo infine i principali vantaggi delle fibre rispetto ai cavi in rame nelle telecomunicazioni si ha:

- Immunità alle interferenze elettromagnetiche (possono essere danneggiate solo da radiazioni alfa e beta).
- Maggiore velocità di trasmissione.
- Minore attenuazione[25] quindi maggiori distanze raggiungibili da un segmento (alcuni standard permettono lunghezze fino a 100 km).
- Assenza di diafonia.
- Minore peso ed ingombro.
- Minore potenza contenuta nei segnali.
- Maggiore resistenza alle condizioni atmosferiche.
- Assenza di problemi legati ai rischi di scariche.

[25] Si stanno studiando nuove fibre dette a *cristallo fonico* che consentono un attenuazione nell'ordine di 1dB/km

2.6 Gestione dei Collegamenti

In ogni stanza, dove presenti dispositivi di rete o server, sono presenti patch panel per cavi in rame e per fibre ottiche.
Spesso, se non si tiene uno schema aggiornato del modo in cui le varie sezioni della rete si interfacciano ai patch panel, viene 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 nè le etichette sulle porte nè uno schema che potesse in qualche modo dare informazioni sulla destinazione del collegamento.
Si è visto nel paragrafo 2.3, dove si studiava la topologia di rete, come la mancanza di informazioni sulla destinazione di un collegamento venisse affrontata e risolta. Una volta individuate le destinazioni finali delle connessioni o eventualmente la collocazione del relativo patch panel, si è provveduto immediatamente ad applicare delle etichette/targhette sulle porte del patch panel indicando il nome della macchina 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.
In sala CED1 si è notato essere presenti dei collegamenti, provenienti da macchine del reparto quantometro, che invece di attraversare il patch panel, presente e funzionante, terminavano direttamente nelle porte dello switch 10.42.42.23. Una volta staccati i cavi non si avrebbe avuto nessun riferimento sulla loro provenienza. In questo caso, dopo aver verificato la destinazione delle connessioni con il solito metodo e aver applicato le etichette sulle porte del patch panel, i cavi che prima finivano direttamente sullo switch sono stati dirottati al patch panel. Ora con un semplice collegamento tra le porte dello switch e quelle del patch panel si ripristina il collegamento originale; mantenendo però questa volta un riferimento sulla destinazione.
C'è da ricordare infine che in laminatoio1, dove è stato sostituito l'hub con lo switch, non è presente il patch panel e il collegamento tra gli switch avviene direttamente sulle loro porte. In questo caso non è possibile dirottare i cavi come si è fatto in precedenza, ma è auspicabile venga installato un patch panel il prima possibile in modo da permettere una gestione migliore delle connessioni e portare il collegamento in fibra ottica.
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.

2.6.1 Patch Panel

Il patch panel o sezionatore è un sistema che interfaccia tra di loro sezioni diverse di un cablaggio. Tipicamente è composto da una serie di pannelli forati, sul retro dei quali sono raccordate le sezioni di cablaggio.
Il cablaggio del patch panel è progettato in modo tale da raggruppare in maniera logica, per tipo e per utilizzo, tutti i cablaggi raccordati, in modo che sia agevole testarli, monitorarli o interconnetterli, con una flessibilità di impiego maggiore rispetto a un impianto fisso. Il vantaggio di poter disporre di questi dispositivi risiede nel fatto che tecnici e amministratori di rete possono modificare rapidamente la topologia, senza perdite di tempo e spese aggiuntive dovute ad interventi su cavi e altre attrezzature di commutazione. Sono in commercio patch panel sia per i cavi in rame che per le fibre ottiche e i modelli più sofisticati possiedono una struttura modulare. La struttura modulare permette di comporre patch panel in grado di instradare connessioni di diversi tipi di segnale sullo stesso pannello, risparmiando spazio se il numero dei segnali è limitato.

Figura 2.34: Sezione di cablaggio in patch panel

Figura 2.35: Patch panel per cavi in rame

In un pannello alto un'unità rack solitamente è possibile alloggiare 24/26 moduli. Il termine rack indica un sistema standard d'installazione di componenti hardware (server, switch, router, firewall, patch panel) ed è caratterizzato da una larghezza di 19 pollici (482,6 mm) e un'altezza di 1,75 pollici (44,45 mm) per ogni unità ospitata. Spesso alloggiate all'interno si trovano anche ventole di raffreddamento e gruppi di continuità integrati per i dispositivi hardware. Si preferisce non riempire mai completamente l'armadio rack, lasciando spazio tra un componente e l'altro in modo da permettere una migliore circolazione di aria e una più semplice gestione dei collegamenti.

Figura 2.36: Patch panel montati su rack

2.7 Resilient Links

Per migliorare ulteriormente la qualità della rete aziendale si è deciso di studiare ed implementare dei resilient links. L'obiettivo è quello di costruire una rete, anche molto estesa, performante e resistente a buona parte dei guasti che si possono verificare ai dispositivi e ai loro collegamenti.
Per raggiungere lo scopo inizialmente si era deciso di utilizzare il protocollo STP ma poi, verificato che tutti gli switch interessati dai resilient links supportavano anche RSTP, si è deciso di adottare tale protocollo. RSTP è un'evoluzione del protocollo STP e permette una convergenza dell'albero di copertura, in caso la topologia della rete venga modificata o si verifichi un guasto, molto più rapida rispetto al suo predecessore. Studiando RSTP si è appreso che i valori dei parametri necessari al funzionamento, impostati di default dagli switch, risultavano essere adeguati al caso della rete aziendale presa in esame. L'unica cosa da configurare erano le porte degli switch in modalità EDGE o POINT-TO-POINT a seconda dell'elaboratore a cui erano connesse, e specificare che il root bridge fosse 10.42.42.2, il centro stella situato in CED1. E' stato scelto tale switch perchè è il dispositivo centrale della rete e rispetto a 10.42.42.3 è collegato ai server più importanti.
A questo punto non restava altro che individuare i possibili collegameni ridondati da implementare. Dopo un accurato studio a tavolino, tenendo ben presente lo schema delle dorsali in fibra ottica e dei cavi in rame (in figura 2.37 e 2.38), sono stati individuate e realizzate le connessioni descritte nello schema in figura 2.39.
Per lo switch 10.42.42.35 del laminatoio1 non è stato possibile realizzare nessun collegamento ridondanto perchè come già ampiamente spiegato nei paragrafi 2.4, 2.5 e 2.6 l'unico cavo in rame che lo raggiunge è già utilizzato per la connessione alla rete tramite lo switch 10.42.42.14 del laminatoio3. E' evidente dunque, ancora una volta, quanto importante sia installare un patch panel in quel reparto e stendere in modo adeguato nuovi cavi, possibilmente in fibra ottica.
I collegamenti ridondati realizzati, a causa della poco sensata distribuzione delle dorsali in fibra e dei pochi switch a disposizione con porte a 1000 Mbps, non rappresentano la soluzione ottimale, ma solamente la migliore realizzabile sotto il profilo delle prestazioni, cercando di utilizzare il più possibile fibra ottica e porte a 1000 Mbps, e dell'economicità delle connessioni.
Molti collegamenti sono stati realizzati in rame a 100Mbps, sfruttando le dorsali dei cavi UTP cat5e invece della fibra ottica, perchè, come già detto, la maggior parte degli switch supporta al massimo due porte di uplink a 1000 Mbps, non sufficienti per realizzare tutte le connessioni necessarie. Sarebbe dunque una buona idea, nel momento ci fosse la necessità di sostituire uno switch, installarne uno che preveda la connessione a 1000 Mbps in fibra ottica su almeno 4 porte oppure, in alternativa, aggiungere in CED1 e CED2, in cui fa capo la maggior parte delle dorsali in fibra, nuovi switch del tipo

già utilizzato dividendo così il carico dei link ridondati.
Oltre alle soluzioni già proposte sarebbe utile installare nuove dorsali in fibra ottica in modo tale da collegare i vari reparti anche tra loro e non solo verso i due CED così da garantire percorsi alternativi per connettersi alla rete e collegamenti ridondati più efficienti.
Lo switch 10.42.42.31 del laboratorio tecnologico, sebbene abbia entrambe le porte di uplink a 1000 Mbps libere, è raggiunto comunque da un collegamento ridondato a 100 Mbps con cavo in rame UTP cat5e perchè sprovvisto di allacciamento alla dorsale in fibra.
La topologia dei collegamenti ridondati è da considerarsi tuttavia solamente un'emergenza nel caso si manifesti un guasto e per questo si è valutato non essere necessaria al momento nessuna modifica.
Si è ritenuto intelligente inoltre privilegiare connessioni che potessero essere utili nel caso il guasto si verificasse su un dispositivo piuttosto di collegamenti che garantissero il funzionamento della rete nel caso il guasto si verificasse sui cavi, cosa assai più rara.

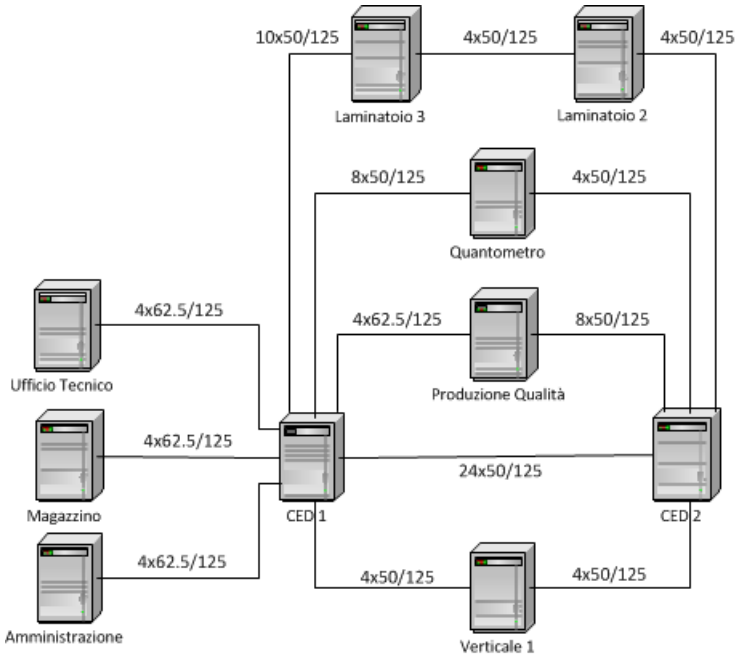


Figura 2.37: Dorsali fibra ottica
(su ogni collegamento è indicato il numero di fibre, il diametro del core/cladding)

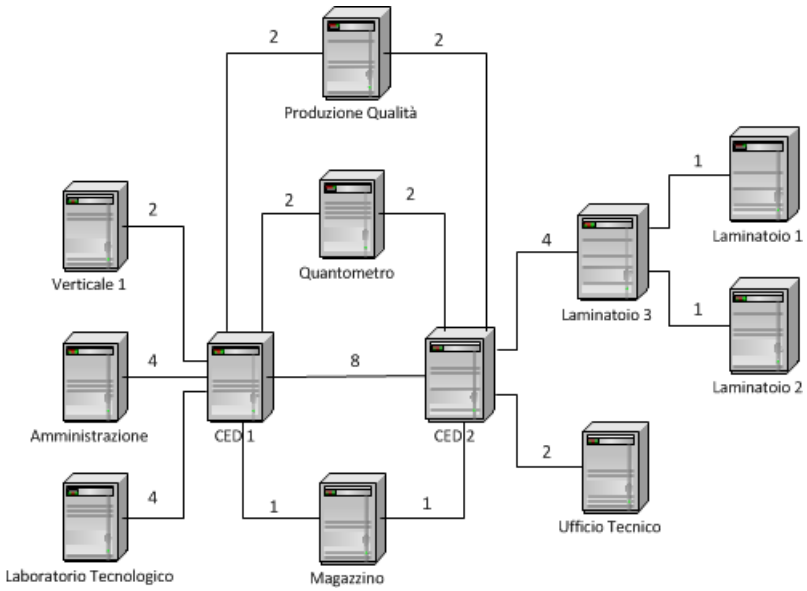


Figura 2.38: Dorsali cavi in rame UTP cat5e
(sopra ogni collegamento è indicato il numero di cavi stesi)

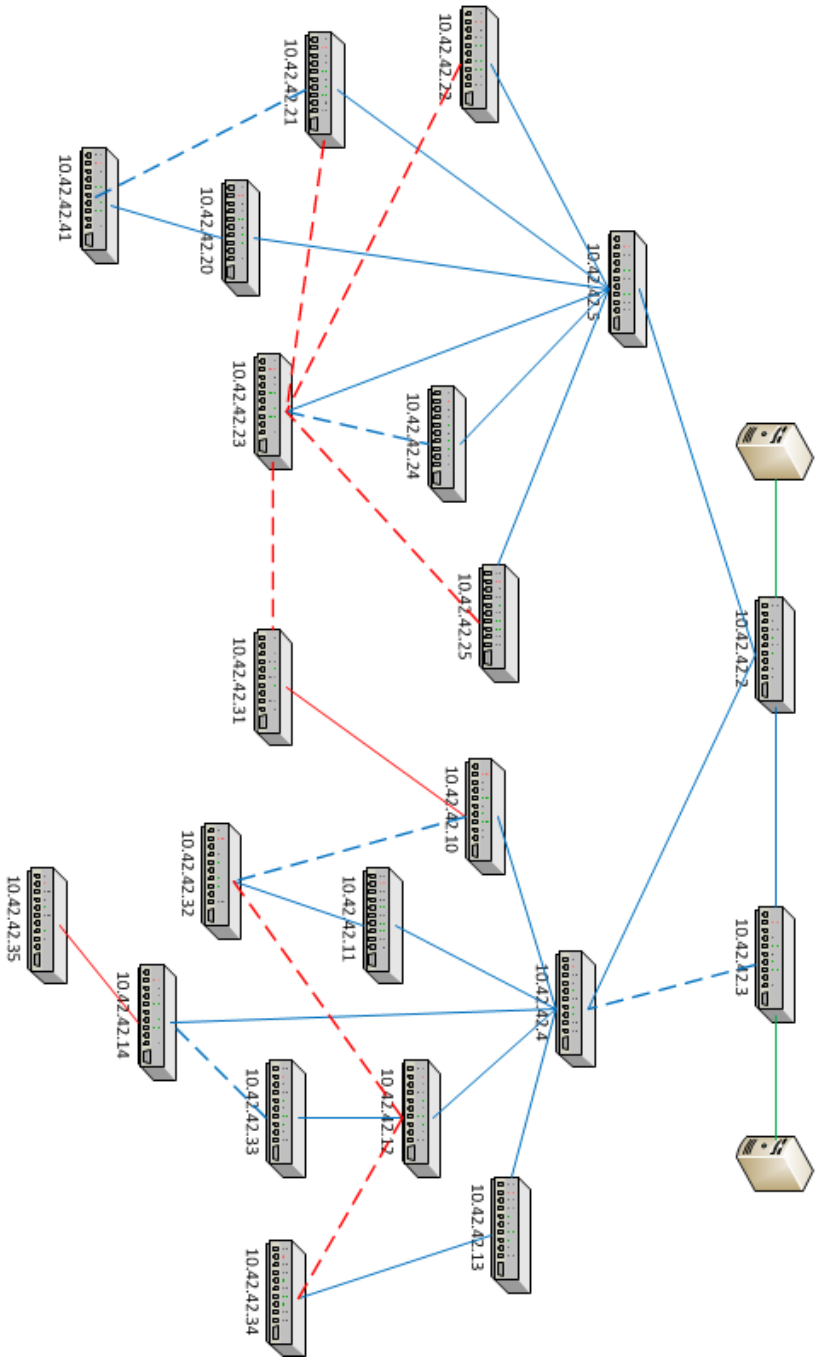


Figura 2.39: Schema resilient links
(collegamenti blu = fibra, verde = UTP cat6, rosso = UTP cat5e;
tratteggiati = ridondanti, non attivi in condizioni normali)

2.7.1 STP e RSTP

Una rete locale può essere costituita da diversi segmenti connessi tra loro tramite bridge[26] o switch, con il solo vincolo che la topologia di rete non contenga cicli, ovvero che tra ogni coppia di calcolatori esista un solo percorso. Se così non fosse, alcuni pacchetti verrebbero replicati all'infinito sulla rete, con risultati disastrosi. Il bridge così come lo switch conosce gli indirizzi MAC degli host connessi su ogni segmento, ma se riceve un pacchetto con destinazione sconosciuta, o un pacchetto broadcast, lo invia su tutti segmenti. Se esiste un ciclo nella rete, il pacchetto raggiungerà nuovamente il segmento da cui è partito, venendo nuovamente replicato. Questo porterebbe alla proliferazione di infinite copie dello stesso pacchetto sulla rete, e quindi alla saturazione della rete stessa. A livello di collegamento, dove bridge e switch lavorano, non esistono metodi che controllano la durata della vita del frame come invece succede a livello di rete nei router. I router infatti analizzano il campo Time To Live del pacchetto ip, e se raggiunto il valore zero lo eliminano dalla rete perchè attraversato tot elaboratori.
Una rete complessa priva di percorsi ridondanti è però estremamente fragile perché il guasto di un solo bridge o collegamento la partiziona in due reti che non comunicano tra di loro. In una rete locale è necessario dunque che ci siano dei collegamenti ridondanti, ma che alcuni di questi siano mantenuti fuori servizio fino a quando non si rendono necessari per sopperire a guasti di altri collegamenti o bridge. A questo prosito ci vine in aiuto lo Spanning Tree Protocol (IEEE 802.1d), un algoritmo per realizzare reti complesse a livello fisico con percorsi ridondati. L'algoritmo di spanning tree è un algoritmo distribuito che opera su tutti i bridge e gli switch coinvolti nei cicli della rete, facendo in modo che in ogni istante la rete sia connessa ma priva di percorsi chiusi, ovvero che il grafo dei collegamenti disponibili sia coperto da un albero (teoria dei grafi). Di seguito verrà descritto il principio di funzionamento dell'algoritmo STP e i termini bridge e switch verranno usati come sinonimi; anche se non sono propriamente la stessa cosa lavorano tutti e due a livello di collegamento e per quanto riguarda questo protocollo si comportano in modo identico.
Ogni switch della rete, dove attivo il protocollo, invia dei frames chiamati BPDU (Bridge Protocol Data Units) agli altri switch, opportunamente formattati per contenere delle informazioni utili a costituire lo spanning tree. Le più importanti informazioni inviate sono: il *BID* (Bridge ID), composto dalla priorità del bridge e dal MAC address e il *costo del percorso*, cioè la distanza dal root bridge, determinato dalla somma dei costi delle porte attraversate. Il costo di una porta è tipicamente determinato dalla velocità; maggiore è la velocità di una porta minore sarà il suo costo.

[26] Dispositivo di rete che si colloca al livello datalink del modello ISO/OSI, collega più segmenti di rete tra loro e dopo aver analizzato gli indirizzi dei pacchetti in arrivo decide su quale segmento inoltrarlo.

Il costo di una porta, così come tutti gli altri parametri coinvolti in questo processo, può comunque essere sempre settato dall'amministratore di rete nel caso voglia influenzare il processo di elezione del percorso e non lasciarlo all'autoconfigurazione.
All'inizio del processo ogni switch, tramite l'invio del BPDU, dice agli altri di essere il root bridge ossia il bridge radice dell'albero coprente, impostando il costo del percorso al valore zero. Il Root Bridge viene scelto poi solo tra chi ha il BID più basso e dipende in pratica dalla priorità assegnabile dall'amministratore. Solo in caso di eguale priorità viene fatto il controllo sul MAC address "più basso" per decidere chi sarà eletto. Non appena uno switch riceve un BPDU contenente un BID più basso, smette di proclamarsi root, finchè ne resterà solo uno. Il perdente non smette di inviare BPDU, ma anzi continua, spammando in rete il BID del bridge vincitore. La radice dello Spanning Tree mette poi tutte le porte in FORWARDING e nel frattempo gli altri switch scelgono una porta root, quella che riceve BPDU al costo minore dal root bridge e le mette in FORWARDING. Infine vengono scelti i designated switch e le corrispondenti designated port nei segmenti con costo minore verso la radice; saranno quelli effettivamente attivi in rete e rappresentano il cammino principale. La designated port viene messa in stato FORWARDING e inoltrerà il traffico su quel segmento mentre tutte le porte rimanenti vanno in BLOCKING state.
Le informazioni che girano tra gli switch dello Spanning Tree sono ricevuti comunque da tutti gli switches e da tutte le porte in qualsiasi stato perchè è fondamentale che ognuno continui a ricevere costantemente informazioni fresche in modo da poter essere pronto e avere riferimenti attendibili quando ci sarà bisogno di cambiare lo Spanning Tree.
Ad intervalli di tempo regolare un BPDU viene inviato da un bridge verso quelli adiacenti che dopo averne aggiunto il costo, ne ripetono il procedimento. Quando un bridge non riceve più BPDU, pensa che qualcosa non stia andando per il verso giusto e inizia il processo di rielezione per ristabilire un path funzionante. I parametri che influiscono sulla velocità di reazione dell'algoritmo sono l'Hello Time, tempo di attesa che un bridge fa passare tra un BPDU e l'altro e il MaxAge, di solito multiplo dell'Hello time, che stabilisce quanto tempo uno switch deve stare in attesa senza ricevere BPDU prima di reagire e cercare di cambiare lo Spanning Tree.
Quando un link cade, e uno switch se ne accorge, prima di trasformare lo stato di una porta da BLOCKING a FORWARDING attraversa due stati transizionali. Questi stati sono LISTENING e LEARNING. Il primo stato mette il bridge in ascolto di BPDU contenenti soluzioni migliori mentre il secondo, successivo al primo, impara la nuova locazione dei MAC address per scrivere la nuova MAC table. Le porte di uno switch quindi, per compiere queste operazioni e passare dallo stato di BLOCKING a quello di FORWARDING, possono impiegare molto tempo (forward delay); fino ad un minuto. Troppo: nel frattempo possono venire perduti molti pacchetti.

L'algoritmo di Spanning Tree presenta dunque un limite importante: se la rete diventa estesa e complessa, il tempo di convergenza necessario al protocollo per reagire al guasto di un elemento o al suo ripristino, diventa enorme, danneggiando gravemente le prestazioni della rete. Bisogna stare attenti però a non farsi ingannare dal fatto che modificando i parametri Hello Time e MaxAge si riesca ad avere una convergenza più rapida. Nel caso di una rete estesa infatti i pacchetti impiegano molto tempo per navigarla tutta e se i parametri impostati non consentono di aspettare di ricevere tutte le adeguate informazioni ricevute dai BPDU, si rischia di configurare la rete in modo sbagliato o di calcolare uno spanning tree anche quando non necessario.
Per superare questo limite è stato sviluppato un protocollo compatibile con STP, chiamato Rapid Spanning Tree (RSTP-IEEE 802.1w), che provvede a ripristinare la topologia di rete nel nell'ordine di qualche secondo.

Nel protocollo RSTP il funzionamento dell'algoritmo rimane inalterato rispetto a STP ma presenta alcune evidenti differenze che permettono di migliorare il tempo di convergenza:

- Vengono identificate tre tipi di porte:

  Point-to-Point: Full-duplex, collegamenti verso dispositivi che implementano RSTP/STP.
  Edge: Half-duplex, collegamenti diretti a qualsiasi dispositivo end-users presente in rete.
  Point-to-Point/Edge: Full-duplex, verso dispositivi che non implementano STP/RSTP.

  I link di tipo Edge, lavorano ponendo la porta in modalità FORWARDING non appena il link diventa attivo mentre nei link Point-to-Point si attende solamente 3 BPDU non ricevuti per cominciare la convergenza.

- Per accelerare il processo di ricalcolo, RSTP riduce il numero di stati di una porta a tre: discarding, learning and forwarding. Lo stato di discarding racchiude in sé gli stati di blocking, disabled e listening dell'originale STP.

- L'algoritmo RSTP calcola un percorso alternativo definendo le porte che lo costituiscono ALTERNATE; eventuali porte formanti altri path con peggior costo rimangono in stato BLOCKING. Quando una porta in FORWARDING smette di ricevere BPDU e i timers scadono, viene subito attivato un path aprendo le porte ALTERNATE.

- Quando uno switch ha due porte in un stesso segmento, quella a costo più alto viene definita in un nuovo modo: BACKUP. Questa porta, lavora come DISCARDING, e resta in attesa; quando la gemella in FORWARDING va in panne, prende prontamente il suo posto.

C'è da ricordare infine che quando si utilizza STP/RSTP, collegamenti ridondati causati dalla presenza di VLAN[27] (802.1q) vengono trattati come cicli della rete e messi in stand-by, perdendo così connessioni che necessitano di restare attive. Per poter avere in ogni VLAN un proprio spanning tree è stato introdotto il protocollo MSTP, Multiple Spanning Tree (802.1s, dal 2003 incorporato in 802.1q). C'è da dire però che con qualche accorgimento, anche con STP o RSTP è possibile usufruire delle VLAN. Per evitare che rami necessari vengano disattivati, invece di utilizzare un collegamento tra switch per ogni VLAN creando percorsi ridondati, si effettua una sola connessione utilizzata poi da tutte.

I collegamenti tra dispositivi dove presenti le VLAN possono essere fatti in due modi diversi a seconda di come vengono configurate le porte degli switch:

Untagged: Le due porte attraverso cui viene fatto il collegamento appartengono alla stessa VLAN e non hanno bisogno di nessun identificativo. I pacchetti che transitano in questo collegamento non possono attraversare porte che non siano quelle appartenti a tale VLAN. E' necessario avere un collegamento tra gli switch per ogni VLAN.
Tagged: Viene effettuato un solo collegamento, detto *trunk*, anche se presenti più VLAN. I pacchetti che transitano attraverso questa porta vengono "marchiati" con un tag identificativo: il VLAN ID della rete di provenienza. Vengono aggiunti 2 byte all'header del frame ethernet per riconoscere la rete di appartenneza.

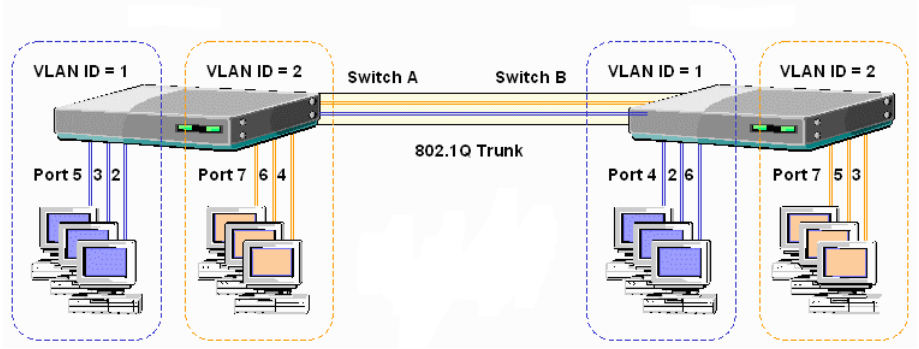


Figura 2.40: Connessione tra switch con più VLAN tramite un solo collegamento (trunking) in cui transitano tutti pacchetti "marchiati"

[27] Reti virtuali create per dividere i domini broadcast all'interno degli switch e unire sullo stesso dispositivo reti diverse. Si dividono logicamente le porte di uno switch assegnando a ciascuna un determinato ID che corrisponde all'identificativo della VLAN di appartenenza (VLAN ID) separando quindi il traffico in vari gruppi di lavoro.

CAPITOLO 3

Risultati e conclusioni

Con questo documento 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'hardaware al software passando per i server, le macchine di fabbrica e i dispositivi di rete, senza dimenticare i mezzi tramissivi e molto altro. Tutto questo questo a prescindere se si dispone o meno della documentazione riguardante le tecnologie adottate. È indubbio però che questo documento, così come altre guide/manuali, sia una valido aiuto per gli amministratori di rete in grado di guidarli in precisi interventi di manutenzione e in scelte consapevoli ogniqualvolta sia necessario.
A causa della continua crescita ed evoluzione delle tecnologie di rete non sarà però utile ancora per molto perchè a distanza di pochi anni se non adirittura mesi i dispositivi, i software e i protocolli diventeranno obsoleti e questa tesi perderà la sua utilita primaria restando solo un libro consultabile in caso di nostalgia. Una cosa resta però assolutamente indispensabile: mantenere uno storico aggiornato di tutti gli interventi eseguiti sulla rete aziendale e un database delle tecnologie adottate; cosicchè, anche nel caso di un passaggio di consegne tra responsabili incaricati di amministrare il sistema informatico, si possa sempre disporre di tecnici informati e preparati, con un conseguente beneficio per l'azienda.
Riguardo la situazione del sistema informatico aziendale, all'inizio, dopo un primo processo di analisi, non si può dire si fosse disastrosa ma di certo non era nemmeno delle migliori.
Scorrendo questo documento si è visto come si sono operate alcune modifiche mirate con l'obiettivo di aumentare le prestazioni ma soprattutto l'affidabilità e la sicurezza, concetti fondamentali che stanno alla base di ogni azienda seria e competitiva. Il poco tempo a dispozione 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.
La situazione attuale dunque, a seguito del lavoro svolto, è migliorata molto rispetto a quella iniziale e al momento non presenta nessun tipo di criticità, anzi, per le esigenze richieste è più che sufficiente sotto molti aspetti. Accontentarsi però non rientra nello spirito ICT che invece impone di ricercare sempre soluzioni innovative che permettano di incrementare la produzione aziendale ed espandersi nel mercato di riferimento.

Bibliografia

[1] Bruce S. Dave e Larry L. Peterson, *Reti di calcolatori*, Terza Edizione (2004), Apogeo Editore

[2] Tim Parker e Karanjit S. Siyan, *TCP/IP Tutto&Oltre*, Terza Edizione (2002), Apogeo Editore

[3] Dave Kearns e Peter Norton, *La guida di Peter Norton a Le reti*, Prima Edizione (2000), Apogeo Editore

[4] Curt M. White, *Reti di communicazione per l'aziend*a, Prima Edizione (2001), Apogeo Editore

[5] Tom Knott e Wendell Odom, *Fondamenti di networking*, Prima Edizione (2006), Pearson Education

[6] Andrew S. Tanenbaum, *Reti di calcolatori*, Quarta Edizione (2002), Pearson Education

[7] Douglas E. Comer, *Internet e reti di calcolatori*, Terza Edizione (2003), Pearson Education

[8] http://it.wikipedia.org

[9] http://www.areanetworking.it

[10] http://www.rhyshaden.com

[11] http://www.sprg.uniroma2.it

[12] http://www.acmeisud.it

[13] http://www.andreabeggi.net

[14] http://www.ieee.org

[15] http://www.cisco.com

[16] http://it.kioskea.net

[17] http://searchnetworking.techtarget.it

[18] http://en.wikipedia.org

[19] http://www.netsetup.it

[20] http://www.picosearch.com

[21] http://www.comptechdoc.org

[22] http://infocom.uniroma1.it

[23] Documentazione I.L.N.O.R. spa

[24] Documentazione Skytek srl