Università degli Studi di Padova
Facoltà di Ingegneria

UNIVERSITÀ DEGLI STUDI DI PADOVA
FACOLTÀ DI INGEGNERIA

—

DIPARTIMENTO DI INGEGNERIA DELL'INFORMAZIONE

—

TESI DI LAUREA TRIENNALE IN INGEGNERIA INFORMATICA

GESTIONE DEL NETWORKING IN AZIENDE DI MEDIE DIMENSIONI

RELATORE: PROF. SERGIO CONGIU

LAUREANDO: JENNY SPAGNOL

ANNO ACCADEMICO 2011-2012

Alla mia famiglia...

“ L’apprendere molte cose non insegna l’intelligenza ”

Eraclito

Indice

Sommario

La tesi si propone di mostrare il lavoro svolto durante il periodo di tirocinio effettuato presso la ditta Gruppo Effeci SrL con sede a Musano di Trevignano. Tale tirocinio, svolto durante i mesi di aprile, maggio e giugno 2012, ha avuto come scopo l'avvicinamento al mondo del lavoro, in particolare nel settore delle reti informatiche.

In questa tesi verranno presentati alcuni dei principali compiti svolti nell'ambito delle reti di medie dimensioni. Una prima parte si occupa della programmazione di switch in una rete di medie dimensioni di un'azienda ospedaliera del territorio. Successivamente viene spiega come è stato sviluppato un server DHCP per la piattaforma linux, da utilizzarsi in azienda.

Nella parte centrale viene mostrato il lavoro di progettazione svolto per la creazione di una rete di un albergo a cinque stelle situato a Venezia. Tale progetto è però solo agli inizi, in quanto, per esigenze della ditta ospitante e del committente, l'impianto verrà installato solo a novembre dell'anno corrente.

Nella parte finale è mostrata una parte di altre attività svolte, magari marginali, ma comunque utili a fini della conoscienza del mondo delle reti informatiche. Viene mostrato in questa sezione, il lavoro svolto per la mappatura della rete informatica propria della ditta ospitante.

Buona lettura.

Introduzione

Un punto focale per la riuscita di un'azienda di piccole, medie o grandi dimensioni è la gestione efficiente delle informazioni tra i vari nuclei (o singole persone) che la compongono. Per il buon funzionamento e il coordinamento dei vari settori di un'azienda è necessario ci sia un buon mezzo di comunicazione. La gestione dei vari flussi di informazioni è gestito dal sistema informativo. Normalmente il sistema informativo è sinonimo di sistema informatico, a detta del fatto che ormai tutte le aziende si avvalgono di componenti tecnologiche per lo scambio e la memorizzazione di dati utili al perseguimento del core business. Tale sistema informatico è quindi costruito su una rete informatica, più o meno complessa a seconda delle dimensioni e delle esigenze. La rete informatica di un'azienda ha quindi un'importanza vitale talvolta, ed è quindi necessario sia affidabile ed efficiente.

In questa tesi si vogliono illustrare alcune delle peculiarità proprie delle reti di medie dimensioni che ne consentono un buon funzionamento. Verranno quindi esposti concetti tipici del mondo delle reti, quali VLAN, STP, ecc. Come riferimento, per la spiegazione di queste tecnologie, si è preso l'esempio di una rete a stella di medie dimensioni presso gli ospedali di Castelfranco Veneto e Montebelluna. La rete di Montebelluna è una sottorete più piccola, collegata direttamente al centro stella di quella di Castelfranco Veneto. Nella sede principale, oltre al router che fa da centro stella, sono collocati tutti i server che fornisco i vari servizi ai molteplici host collegati alle due reti. I vari dispositivi sono gestiti dal CED dell'ospedale, mentre il Gruppo Effeci SrL si occupa della gestione degli switch e del centro stella. Mi è stata offerta la possibilità di vedere come funzioni e come sia gestita una rete di tali dimensioni, avendo potuto anche accedere di perso-

na al CED e alla sala server dell'Ospedale. In questa occasione mi è stato ben chiaro che non è neccessaria solo una buona progettazione della rete, ma anche un costante controllo del buon funzionamento della stessa. In questa sezione vi è una parte che illustra l'importanza di un buon metodo di monitoraggio della rete, sfruttando un software che faciliti tale compito. Per l'amministratore di rete è necessario essere al corrente in modo tempestivo di ogni eventuale anomalia presente nella rete.

Nello stesso capitolo viene spiegato un dispositivo di rete molto importante: il DHCP server. Questo dispositivo gestisce gli indirizzi IP dei vari dispositivi collegati in una rete. Si tratta di un server di fondamentale importanza, in quanto ogni dispositivo in rete, per poter comunicare con gli altri, necessita di un indirizzo IP. Nel caso in cui non disponga di un indirizzo IP statico, dovrà fare richiesta per averne uno. Il server fornisce un indirizzo al dispositivo che gli permetta di entrare a far parte della rete, assicurandosi di non fornire un indirizzo doppio che potrebbe creare conflitti. La gestione degli indirizzi IP automatica è importante e fondamentale, soprattutto nelle reti di dimensioni maggiori.

Dopo aver visto come mantenere in funzione una rete informatica già esistente, mi è stato possibile assistere alla progettazione di una nuova rete con richieste specifiche da parte del committente. Nel secondo capitolo si parla di una rete informatica e telefonica che verrà installata nell'Hotel Gritti a Venezia. Questo progetto, oltre ad avermi mostrato come possa essere il rapporto con un reale committente, è stato utile per vedere la progettazione di una rete informatica dagli inizi. È stato necessario creare il tutto partendo dalle richieste e dalle informazioni, non sempre concordanti, fornite dal cliente. Partendo dalle piantine di ogni piano dell'hotel e dai documenti riservati contenenti le specifiche che la rete deve supportare, si sono create alcune possibilità di implementazione della rete da consegnare poi al cliente. Una parte dello stesso capitolo mostra invece come, con l'aiuto del tutor aziendale, sono stati scelti e collegati i vari dispositivi appartenenti al centro stella. Anch'essi sono stati pensati per rispettare alla perfezione le richieste del committente. Per esigenze della ditta ospitante e del cliente, non mi è stato possibile vedere la fine del progetto, in quanto sarà messo in opera verso fine anno.

Nell'ultimo capitolo sono illustrate altre attività svolte durante il periodo di tirocinio. La principale che verrà mostrata riguarda l'intera mappatura della rete dell'azienda ospitante. Essendo di dimensioni minori rispetto le reti precedentemente viste, è stato possibile vederne le funzionalità per intero, consentendo di vedere da sola come ogni dispositivo sia collegato alla rete ed, eventualmente, le funzioni dello stesso. Per svolgere questa attività oltre a ricorrere ad alcuni software disponibili, è stato necessario toccare con mano i dispositivi principali (switch in particolar modo) e vedere concretamente come sia una rete informatica fisicamente attiva e funzionante. Nello stesso capitolo, è presente un cenno all'implementazione di un server fax da utilizzarsi nella ditta ospitante.

Capitolo 1

Tecnologie di Networking

In questo primo capitolo saranno trattate le principali teconologie di networking. Nella prima parte verrà preso in considerazione l'esempio della rete degli ospedali di Castelfranco Veneto e Montebelluna. Si tratta di un'unica rete, dove la parte situata a montebelluna è collegata con la sottorete principale di Castelfranco. Qui è situato il centro stella con i vari server. Verranno spiegate le principali tecnologie utilizzate per la programmazione degli switch che fanno parte dell'intera rete.

Nella seconda parte verrà trattato l'esempio di un server DHCP creato per l'azienda stessa che mi ha offerto la possibilità di svolgere il tirocinio. Si tratta di un server prova creato per affiancarne uno già esistente, da utilizzare solo nel momento in cui il server principale dovesse avere dei problemi.

1.1 Programmazione Switch HP e CISCO

In questo capitolo è stato preso in considerazione l'esempio della rete informatica in uso presso gli ospedali di Castelfranco Veneto e Montebelluna. Si tratta di una rete a stella, dove sono stati usati principalmente switch HP per ricoprire posizioni intermedie quali switch di livello 2 (Data Link Layer), mentre per implementare il *centro stella* si è preferito utilizzare uno switch della CISCO di livello 3 (Network Layer). Quest'ultimo, di più difficile programmazione, è però più ricco di funzionalità e capace di gestire il traffico dati richiesto in una rete di medie dimensioni come questa.

Ci sono alcune peculiarità da tener conto in entrambi i tipi di switch, implementabili grazie a istruzioni diverse a seconda della casa produttrice anche se molto simili. Tutta la programmazione è stata vista, modificata o creata tramite un collegamento telnet presso lo switch stesso. In alcuni casi è stato possibile collegarsi direttamente all'apparato tramite un cavo seriale, o, come ultima opzione, consultarne l'interfaccia html.

Di seguito l'elenco delle prinicipali tecnologie tenute conto.

1.1.1 VLAN

Una VLAN (Virtual Local Area Network) è una LAN realizzata in modo astratto su dispositivi fisici. Questa tecnologia è definita nello standar IEEE 802.1Q Tagging Protocol. L'utilizzo delle VLAN permette a computer anche non vicini fisicamente, di comunicare tra loro come se siano nello stesso dominio di collisione; è possibilie implementare questa teconologia anche per restringere l'accesso a risorse senza dover modificare la topologia fisica della rete, consentendo un notevole risparmio in fatto di apparati necessari all'implementazione della rete stessa e di conseguenza un notevole risparmio economico. Durante l'esperienza di tirocinio, è stato visto come configurare le VLAN nel livello 2, è possibile però l'implementazione anche coinvolgendo il livello 3.

Nella pratica vengono a crearsi diversi *Domini di Broadcast*, uno per ogni VLAN creata, che si traduce nel fatto che ogni dispositivo appartenente alla VLAN 1, per esempio, invia dati in broadcast solo ed esclusivamente ad altri dispositivi appartenenti alla stessa VLAN 1.

Nella figura 1.1, un esempio di rete con l'implemento della teconologia 802.1Q.

È stato visto come implementare le VLAN mediante il *frame tagging*, tecnica che modifica il frame nel livello 2. Il dispositivo mittente aggiunge l'informazione della VLAN al pacchetto da inviare, informazione che verrà poi rimossa dallo switch una volta instradato il pacchetto verso il dispositivo destinatario. In pratica viene assegnato un ID VLAN ad ogni frame, in modo da capire a quale VLAN appartenga.

Una volta create le VLAN necessarie nello switch, è necessario definire per ogni porta la VLAN *untagged* e le eventuali VLAN *tagged*. La VLAN untagged,

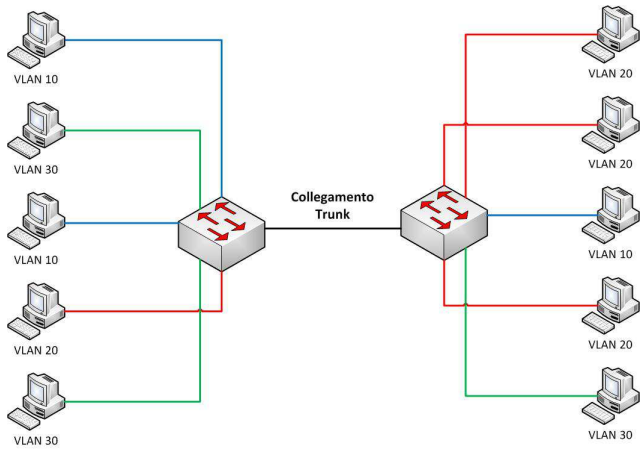

Figura 1.1: In figura si può vedere come i vari computer appartenenti a VLAN diverse, possano essere collegati allo stesso switch, senza interferire gli uni con gli altri e senza dover ricorrere a switch diversi per ogni VLAN. Il collegamento tra i due switch è invece di tipo trunk, in quanto in esso passano dati appartenenti alle 3 diverse VLAN.

ovvero la *native VLAN*, è quella di default e i pacchetti appartenenti ad essa, non subiranno modifiche. Quando sono presenti anche VLAN tagged in una porta dello switch, questa prende il nome di *Porta Trunk*, solitamente gli switch comunicano tra loro attraverso una porta di questo tipo.

1.1.1.1 VLAN su switch HP

Di seguito un esempio su come configurare due VLAN in uno switch HP.

```
10.20.10.42 - Piano 3 corpoQuin

vlan 1
        name "DEFAULT_VLAN"
        untagged 8-52
        ip address 10.20.10.42 255.255.0.0
        exit
vlan 2
        name "WIFI"
        untagged 1-7
        ip address 10.21.0.222 255.255.0.0
```

```
        tagged 52
        exit
```

In questo switch sono state create due VLAN, una di default per quanto riguarda la parte dati e una WiFi per il traffico wireless. Si può notare che le prime sette porte sono riservate a quest'ultima VLAN, ed essendo untagged, i vari frame non subiranno modifiche. Le porte dalla 8 alla 51 sono invece riservate alla VLAN di default. Nella porta 52 invece, appare evidente sia riservata al collegamento verso un altro switch, in quanto è l'unica porta in cui siano presenti entrambe le VLAN, rendendo tale porta una *Trunk Port*. [1]

1.1.1.2 VLAN su switch CISCO

Per quanto riguarda la programmazione del CISCO, usato in questo esempio come *Centro Stella*, la gestione delle VLAN è trattata diversamente, in quanto queste vanno prima create come nell'esempio qui sotto.

```
10.1.15.1 - c6509_cstella
!
vlan 2
name SERVER
!
vlan 3
name DMZ
!
vlan 4
name EXTRANET
!
vlan 10
name WIFI
!
vlan 200
name RADIOLOGIA
```

Successivamente, per ogni porta va indicata quale VLAN ne ha accesso, e nel caso siano più di una, va specificato che tale porta operi come una *trunk port*.

```
10.1.15.1 - c6509_cstella
!
interface GigabitEthernet4/1
        description verso switch primario centralino
        switchport
        switchport trunk encapsulation dot1q
        switchport trunk allowed vlan 1,4
        switchport mode trunk
!
interface GigabitEthernet4/2
        description verso RADIOLOGIA Vlan200 switch
        switchport
        switchport access vlan 200
        switchport mode access
!
```

Per completezza, si nomina il protocollo GVRP (Generic VLAN Registration Protocol), anch'esso definito nello standard IEEE 802.1Q, ma non utilizzato durante il periodo di tirocinio. Tale protocollo permette la negoziazione dell'insieme delle VLAN in modo automatico tra gli switch. Non appena una VLAN viene configurata in uno switch, questo protocollo permette la diffusione dell'informazione agli altri apparati coinvolti. [2]

1.1.2 Spanning Tree Protocol

Il protocollo Spanning Tree è definito nello standard IEEE 802.1D. È un protocollo di rete che assicura una topologia di rete priva di loop, lasciando attivo un solo percorso tra due nodi. I collegamenti ridondanti vengono così disabilitati, permettendone l'entrata in funzione solo quando uno dei bridge attivi cade. L'STP è fondamentale per la prevenzione da *broadcast storm*.

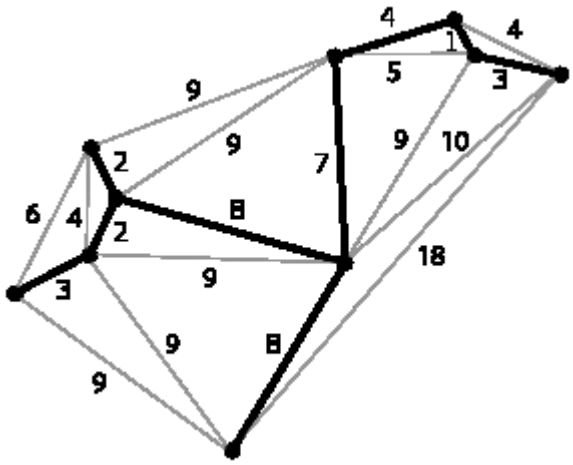

Figura 1.2: Un esempio di grafo di copertura aciclico in una rete di media complessità con ridondanze.[3]

L'algoritmo di Spanning Tree è un algoritmo distribuito, che opera quindi su tutti i bridge, permettendo che questi siano collegati tra loro tramite un albero di copertura (ossia un grafo senza cicli).

- Il primo passo sta nel trovare la radice, che è individuata dal nodo con l'ID più basso. Tale ID è solitamente definito in base al MAC Address, ma può esser forzato ad un valore diverso dall'amministratore di rete.

- Viene poi calcolato, per ogni nodo, il percorso con il costo minimo verso la radice. Vengono calcolati tutti i percorsi possibili dal nodo alla radice, e viene quindi scelto quello con il costo minore.

- La porta del nodo collegata alla radice, e che ha il percorso minimo verso di essa, viene chiamata *root port*. Ogni altra porta attiva, che non è una root port, viene chiamata *blocked port*, e viene quindi disabilitata per impedire loop all'interno della rete.

Nel caso in cui dallo stesso switch partano due collegamenti verso la radice, di eguale peso, passando per due switch diversi, verrà scelta la porta collegata allo switch con ID più basso. Il costo di un collegamento è dato dal tipo dello stesso, collegamenti più lenti avranno costo più alto, mentre collegamenti più veloci,

avranno ovviamente un costo minore, come in tabella 1.1. Anche in questo caso, l'amministratore di rete può forzare il costo di un link.

Data Rate	STP Cost
4 Mbit/s	250
10 Mbit/s	100
16 Mbit/s	62
100 Mbit/s	19
1 Gbit/s	4
2 Gbit/s	3
10 Gbit/s	2

Tabella 1.1: La tabella riporta valori standard di costo per i vari tipi di collegamento utilizzati tra due nodi: un collegamento molto veloce ha un costo molto basso, allo stesso modo, un collegamento a bassa velocità ha un costo più elevato. [3]

Ogni porta di uno switch in cui è implementato l'STP può avere uno stato diverso:

- Blocking: è una porta che potrebbe causare un loop, è pertanto bloccato ogni dato in ricezione o invio. L'unico tipo di dato accettato è il *Bridge Protocol Data Units* (BPDU) necessario per la comunicazione di dati riguardo lo stato dello Spanning Tree.
- Listening: lo switch processa BPDU e aspetta possibili informazioni che potrebbero indurre lo stato di blocking, non popola la tabella dei MAC Address e non invia frames.
- Learning: finchè la porta non invia frames, impara l'indirizzo del mittente dai frames ricevuti, e inizia così a popolare la tabella degli indirizzi MAC.
- Fowarding: la porta invia e ricevi dati, è in condizioni normali. Il protocollo monitora i BPDU in arrivo per l'evenutuale cambio di stato della porta a blocking.
- Disabled: la porta non fa parte dello Spanning Tree, operazione permessa all'amministratore di rete.

1.1.2.1 STP in switch HP

L'implementazione dello STP in switch HP è molto semplice, in quanto necessita di un'unica istruzione. Questa avrà tutti i parametri impostati in default, come per esempio costo del link, priorità dello switch e l'applicazione di tale regola all'intero switch (si può altrimenti selezionare solo le porte per le quali valga tale regola). È però possibile, tramite appositi comandi modificare tutti questi parametri.

```
10.20.10.42 - Piano 3 corpoQuin


spanning-tree
loop-protect 1-52
loop-protect trap loop-detected
loop-protect disable-timer 10
```

Negli switch HP è consigliabile inserire anche la protezione loop con l'apposita istruzione nelle relative porte. Tale protezione assicura la disabilitazione della porta per il tempo stabilito nel caso in cui venga riscontrato un probabile loop.

1.1.2.2 STP in switch CISCO

Per la parte CISCO, la programmazione è di più difficile lettura. Di seguito, un esempio:

```
10.1.15.1 - c6509_cstella
!
spanning-tree mode pvst
spanning-tree portfast bpduguard default
spanning-tree vlan 1-4,200 priority 0
```

La prima istruzione imposta la modalità PVST (Per-VLAN Spanning Tree), che fa in modo di mantenere un'istanza di STP per ogni VLAN configurata nella rete. Questo consente di trattare ogni VLAN come una rete separata, e permette un migliore bilanciamento del carico. Quando una porta viene disabilitata per mezzo di un frame BPDU, grazie alla seconda istruzione, è possibile abilitarla

solo manualmente. È altrimenti possibile configurare lo switch affinchè la porta si riabiliti automaticamente dopo un timeout prefissato. L'ultima istruzione imposta la priorità dello switch a zero per ogni VLAN esistente, in modo tale che questo sia considerato la radice dello spanning tree e ogni frame passi attraverso di esso e venga poi instradato nella giusta sottorete.

1.1.3 LACP

Per una futura implementazione per un migior collegamento tra le sedi di Castelfranco Veneto e Montebelluna, è stata vista la tecnologia denominata LACP (Link Aggregation Control Protocol) definita nello standard IEEE 802.3ad. Si tratta di particolari collegamenti tra due switch formati da più di un cavo fisico, ma visti come un unico collegamento logico. In questo modo è possibile aumentare la banda di un collegamento o permetterne la ridondanza dello stesso al fine di garantire una maggiore sicurezza contro danni al collegamento principale. Vengono di seguito riportate informazioni basilari e principali differenze tra HP e CISCO, senza riportare però la programazione alquanto varia per entrambi i casi.

1.1.3.1 HP

Nel mondo HP, ci sono alcune distinzioni da fare, in quanto la terminologia assume sfumature particolari. Si parla di LACP quando si vuole implementare un *trunk dinamico*, definito propriamente con lo standard 802.3ad sopra citato. HP offre però la possibilità di creare anche collegamenti di tipo *trunk statico*, quando si vogliono aggregare comunque più collegamenti, ma il dispositivo dall'altra parte del link non supporta la tecnologia LACP. In tutti i casi è comunque necessario che il collegamento sia di tipo point-to-point. Le possibilità implementabili sono:

- *Dynamic LACP*: È la configurazione standard, che risponde alle caratteristiche descritte sopra. Se le porte ad entrambi i capi del link sono compatibili in quanto hanno la stessa velocità ed entrambe configurate come full duplex, lo switch stablisce automaticamente un collegamento *dynamic LACP*. È necessario però che almeno uno dei due capi del link sia configurato

come attivo, come nell'immagine 1.3. Questa modalità consente di avere link in standby che vengono attivati automaticamente non appena uno dei collegamenti attivi va in down.

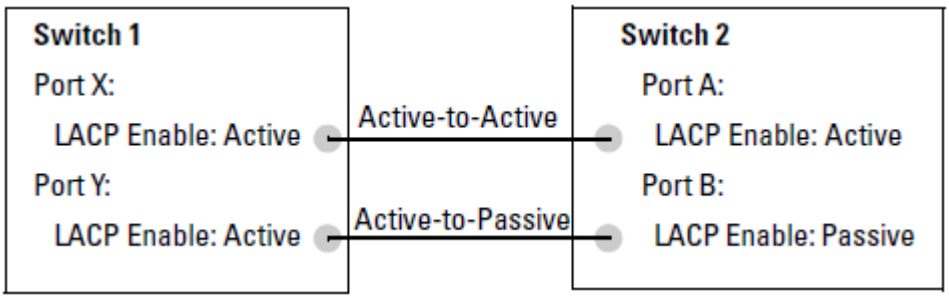

Figura 1.3: La figura mostra i tipi di collegamento in modalità dynamic LACP, che possono essere Attivo-Attivo o Attivo-Passivo. [1]

- *Static LACP*: Si utilizza quando la porta è configurata come LACP, ma non appartiene a nessun gruppo trunk esistente. Lo switch imposta automaticamente questa porta come *Static LACP*, che significa che entrambi i capi del link devono essere configurati manualmente per quanto riguarda STP e IGMP (Internet Group Management Protocol).

- *Trunk*: HP permette l'utilizzo di questa tecnologia per configurare un collegamento quando l'altro dispositivo all'altro capo del collegamento non implementa LACP protocol o non si conosce il protocollo che utilizza. Fornisce una configurazione manuale di trunking, che semplicemente bilancia il traffico dati tra un gruppo trunk tra due switch.

1.1.3.2 CISCO

CISCO consente la creazione di collegamenti LACP intesi come nello standard, senza le differenze che propone HP. CISCO permette di collegare in modalita LACP fino a 4 link fisici, a patto che tutte le porte siano identiche in quanto a velocità e impostazioni. Nel caso in cui uno dei link attivi, utilizzati per il canale LACP cada, il traffico sarà poi ripartito tra i rimanenti link attivi. Viene garantita una protezione per i pacchetti inviati in modalità broadcast, in quanto

se questi pacchetti arrivano ad un collegamento facente parte del canale logico, non verrà poi ritrasmesso negli altri link dello stesso canale, onde evitare una *broadcast storm*.

1.1.4 Gestione della rete

Durante la vita di una rete informatica è necessario un costante controllo sulla sua funzionalità e operatività. Per questa funzione, l'amministratore di rete fa uso di alcuni programmi di management dove è possibile vedere in tempo reale, o tramite dei report, il carico di lavoro e il reale funzionamento di tutti i dispositivi. È un software utile anche per venire a conoscenza della causa di eventuali danni o malfunzionamenti della rete stessa.

Il programma utilizzato dall'azienda per monitorare la rete di Castelfranco Veneto e Montebelluna è OpManager. Consente di vedere in tempo reale il carico di ogni porta di ogni switch collegato alla rete, tramite il semplice invio di messaggi SNMP. Si tratta di un protoccollo operante a livello 7 (Livello Applicazione) per la gestione e supervisione di apparati collegati ad una rete. Tramite questo programma, l'amministratore è in grado di venire a conoscienza tempestivamente di eventuali anomalie sul volume del traffico dati in quanto è presente un sistema di allert che invia una mail non appena alcuni parametri superano la soglia definita (per esempio il traffico dati non può superare un certo volume). Se l'allert non rientra entro un timeout stabilito, si può agire in modo tale da impedire un eventuale malfunzionamento.

Con tale software è anche possibile creare dei report che schematizzino l'andamento della rete (per esempio scegliendo una porta di uno specifico dispositivo) in un intervallo di tempo stabilito. Un esempio in figura 1.4 mostra l'andamento del traffico in una porta del router che fa da centro stella. Mostra un notevole aumento del carico dati verso le 14.30, ora appunto in cui è successa una broadcast storm.

Tramite questi report è possibile avere indizi utili sull'origine di malfunzionamenti venutisi a creare nella rete o prevenire problemi quando possibile.

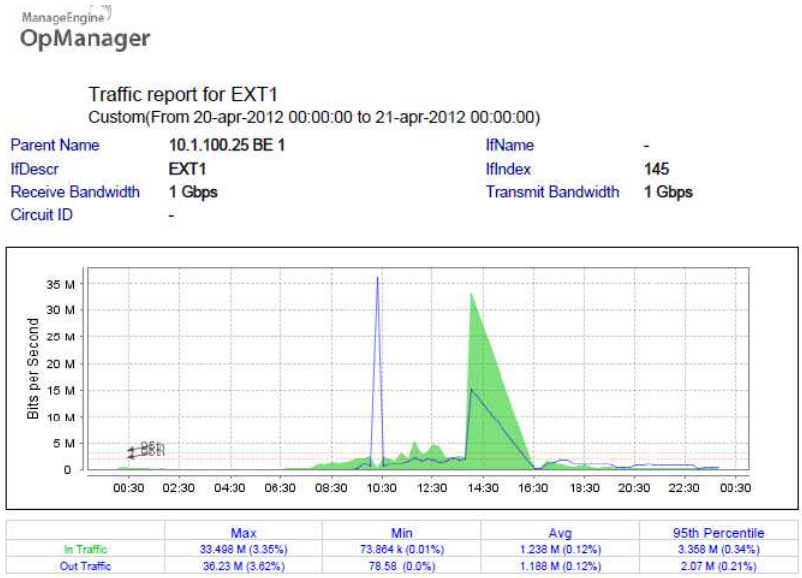

Figura 1.4: L'immagine mostra un report di una giornata durante la quale si è verificata una broadcast storm

1.2 DHCP Server

Durante il periodo di tirocinio, mi è stata richiesta la configurazione di un Server DHCP (Domain Host Control Protol) in un computer con sistema operativo Ubuntu 12.04. Tale server è stato pensato per la rete dell'azienda, con indirizzo di subnet 192.168.11.0 e maschera di rete 255.255.255.0. Lo schema di rete più dettagliato è disponibile al capitolo 3.

1.2.1 Cos'è

Il protocollo DHCP opera a livello 7, e gestisce le richieste di accesso ad una rete IP da parte di vari dispositivi. Ogni dispositivo di una rete IP ha bisogno di uno specifico indirizzo IP, e deve essere scelto tra una serie di indirizzi possibili assegnati alla sottorete in questione. Ogni dispositivo necessita di un indirizzo IP univoco, con il quale essere individuato e distinto dal resto dei componenti della rete. Una configurazione statica potrebbe non essere efficiente nel momento in cui sia presente un notevole numero di dispositivi, riducendo man mano il numero di indirizzi disponibili per nuove richieste. Quando un dispositivo si sconnette, sarebbe per tanto utile liberare l'indirizzo IP in suo possesso, permettendone

l'uso ad un altro che richiede la connessione. Per ovviare le problematiche date da una gestione manuale si utilizza il questo protocollo che svolge tutti questi compiti in maniera automatica. Quando un client richiede un indirizzo IP, gliene viene assegnato uno per un certo periodo di tempo e, allo scadere, tale richiesta deve essere rinnovata o l'indirizzo verrà liberato e reso disponibile per un altro host che ne faccia richiesta.

1.2.2 Come funziona

Il client che vuole fare richiesta di un indirizzo IP, invia una richiesta in broadcast: *DHCP DISCOVER 255.255.255.255*. Quando il server DHCP riceve la richiesta, risponde inviando il range di indirizzi IP disponibili con un messaggio *DHCP OFFER ip_proposto from ip_server*, dove ip_proposto è un IP libero e ip_server è l'indirizzo del server DHCP. Il client, una volta scelto un indirizzo all'interno di questo range, invia il pacchetto *DHCP REQUEST for ip_scelto (ip_server)* (ovviamente ip_scelto è quello proposto dal server), il server invia conferma con un *DHCP ACK from ip_server*.

Uno schema dello scambio di pacchetti all'immagine 1.5.

1.2.3 Installazione e configurazione

Come prima cosa, si è dovuto installare il pacchetto necessario al sistema operativo per operare come server DHCP, digitando in un terminale:

```
sudo apt-get install dhcp3-server
```

Nel file */etc/dhcp3/dhcpd.conf* sono contenute tutte le configurazioni di tale server, è necessario aprirlo ed editarlo per poterne modificare ogni singola impostazione. Di seguito viene riportato il file di configurazione utilizzato, al termine è presente una semplice spiegazione del codice. Si tratta comunque di un server DHCP da affiancare a quello già esistente, da utilizzarsi solo nel momento in cui questo abbia malfunzionamenti o non sia attivo.

```
ddns-update-style none;
one-lease-per-client;
```

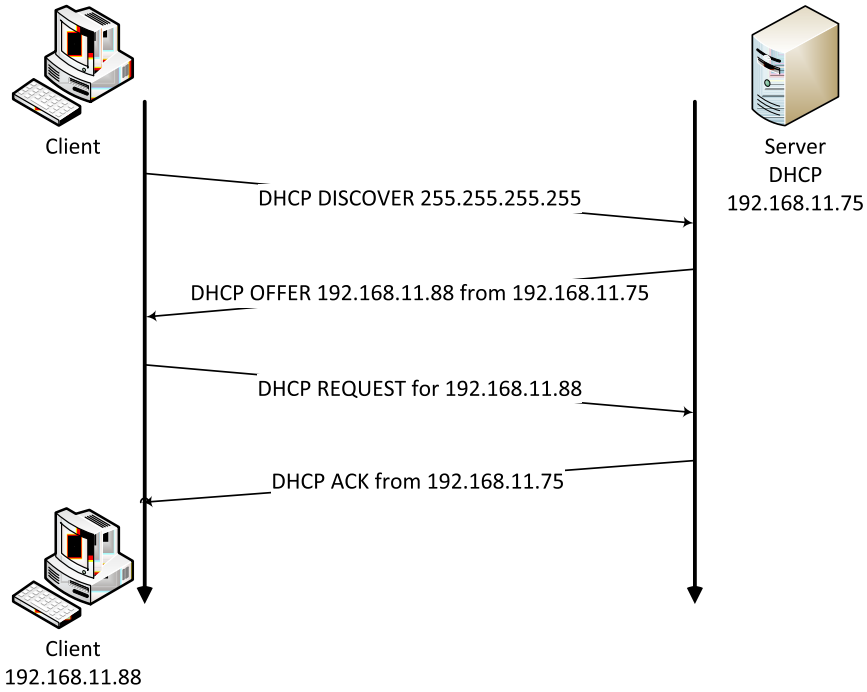

Figura 1.5: Lo schema mostra come avvengono gli scambi di messaggi tra un client che si connette alla rete e il server

```
deny duplicates;
failover peer "linux.dhcp_server"
{
   address 192.168.11.75;      #mio ip
   port 9264;
   peer address 192.168.11.250;  #dhcp primario
   peer port 9264;
   max-response-delay 60;      #secondi max prima del
      fail
   max-unacked-updates 10;
   mclt 3600;
}
subnet 192.168.11.0 netmask 255.255.255.0
{
   option domain-name "prv.effecitelefonica";
   option router 192.168.11.250;
```

```
    option subnet-mask 255.255.255.0;
19  option broadcast-address 192.168.11.255;
    option domain-name-server 192.168.11.1;
    option netbios-name-server 192.168.11.1;
    max-lease-time 3600;
    default-lease-time 3600;
24  pool
    {
       failover peer "linux.dhcp_server";
       range 192.168.11.80 192.168.11.99;
       host FabioFrassetto
29     {
          hardware ethernet 00:27:10:C8:23:AC;
          fixed-address 192.168.11.98;
       }
       host Silvio_Portatile
34     {
          hardware ethernet 88:AE:1D:B5:FE:E4;
          fixed address 192.168.11.96;
       }
    }
39 }
```

[4]

- Righe 1-4:

  Si è scelto di disattivare l'aggiornamento dinamico al server DNS con l'istruzione *ddns-update-style none*.

  L'istruzione *one-lease-per-client* fa in modo che ogni client possa disporre di un unico indirizzo IP alla volta. Nel caso ne richieda un nuovo, quello vecchio viene rilasciato e tenuto libero per altre richieste.

  Con *deny duplicates* ci si vuole assicurare che se un client con un indirizzo IP già assegnato, faccia una nuova richiesta, gli venga assegnato lo stesso

indirizzo IP. La situazione si può presentare nel caso di un reboot da un computer con più sistemi operativi, dove cambiando OS dopo il riavvio, il server DHCP risponderà alla richiesta del client con lo stesso IP precedentemente utilizzato.

failover peer "linux.dhcp_server" indica il nome del gruppo di server DHCP (si vuole ricordare l'architettura a doppio server).

- Righe 5-12

  In questa parte del programma vengono definite le specifiche proprie del server, come ad esempio l'indirizzo IP, la porta tramite la quale comunica con l'altro server all'indirizzo *peer address*.

  Con *max-response-delay* si indica per quanti secondi al massimo si può interrompere la comunicazione tra i due server prima che quello rimasto attivo pensi che l'altro sia offline.

  Il parametro *mclt* indica il tempo massimo per cui uno dei due server, durante un fail, continuerà a rinnovare lease ai client.

- Righe 16-23

  Sono tutte istruzioni abbastanza autoesplicative, le uniche sulle quali ci soffemeremo sono quelle riguardo il time di lease. Indicano il tempo di possesso di un indirizzo IP da parte di un client.

- Righe 25-39

  Con la direttiva pool, si definisce il range di indirizzi IP che il server può offire ad un client. In questo caso gli indirizzi vanno da 192.168.11.80 a 192.168.11.99.

  Le due direttive host invece, definiscono due dispositivi che pur dovendo fare richiesta al server DHCP di un indirizzo, questo sarà sempre lo stesso. Per la distinzione del dispositivo, oltre al nome host, si fa riferimento al MAC Address, parametro diverso per ogni scheda di rete.

Gli indirizzi al di fuori del range, sono utilizzati dai dispositivi dell'azienda che hanno un IP statico, e non fanno per tanto richiesta di un indirizzo al server.

Capitolo 2

Hotel Gritti

Questo capitolo tratta di un progetto svolto per un hotel di Venezia. Era richiesta la creazione di una rete informatica, telefonica e di videosorveglianza per l'intera struttura, partendo dalle piantine dei vari piani dell'albergo e dalle specifiche dettate dalla catena di alberghi a cui questo fa riferimento. Ho avuto a che fare sostanzialmente con la parte della rete informatica e telefonica, tralasciando la parte di rete riservata alla videosorveglianza.

La prima parte del capitolo, oltre a presentare il progetto in modo più dettagliato, si occupa del calcolo e della verifica delle varie prese dati situate in tutti i piani dell'albergo, fornendo più soluzioni per la copertura di tutte le richieste.

La seconda parte è riservata alla progettazione del centro stella dell'albergo, la sua struttura e i dispositivi utilizzati, sempre seguendo le specifiche richieste.

2.1 Rete informatica

L'albergo è formato da sei livelli più la copertura, e per ogni livello è predisposta una stanza riservata ai vari armadi di piano, dove inserire gli switch a cui devono essere collegati tutti i dispositivi (telefoni IP, computer, access point, ecc) del piano stesso. Per tutto l'hotel è stata richiesta la presenza di 3 VLAN, una VLAN POS, una VLAN Ospiti e una VLAN Hotel.

La VLAN POS è situata unicamente al primo piano, e comprende tutte le postazioni POS, presso le quali i vari ospiti dell'albergo possono utilizzare le

proprie carte di credito.

Alla VLAN Ospiti, o VLAN Guest, appartengono i punti fonia/dati delle stanze e tutti quelli a disposizione degli ospiti. Access point, telecamere IP e tutte le prese dei locali tecnici appartengono a questa VLAN.

Le prese rimanenti appartengono alla VLAN Hotel, o VLAN Admin, a cui sono collegati i vari computer e telefoni IP utilizzati dal personale dell'Hotel.

Di seguito, la tabella 2.1 con le varie prese calcolate in ogni piano, suddivise in base alle VLAN di appartenenza. Ogni totale ha necessitato di un calcolo manuale di tutte le prese disegnate in ogni piantina di ogni piano, in quanto si sono riscontrate diverse anomalie tra i vari dati forniti dal cliente.

Descrizione	VLAN Ospiti	VLAN Hotel	VLAN POS	TOTALE
Totale livello A	134	103	9	246
Totale livello B	94	37	0	131
Totale livello C	39	53	0	92
Totale livello D	125	9	0	134
Totale livello E	134	1	0	135
Totale livello F	88	0	0	88
Totale livello G	5	0	0	5
TOTALE	619	203	9	831

Tabella 2.1: La tabella mostra il calcolo di prese telefonia/dati calcolate in ogni piano e suddivise in base alla VLAN di appartenenza.

Una possibilità richiesta dall'Hotel era quella di tener conto solo del 60% delle prese telefonia/dati (di seguito indicate con TD) riservate alla VLAN Hotel, in quanto non tutte sarebbero state utilizzate da subito. Un'altra possibilità richiesta, è stata quella di dividere le varie VLAN via hardware in modo da avere due sottoreti fisicamente divise (la VLAN POS, avendo un così ridotto numero di prese, può essere incorporata negli switch riservati ad una o all'altra VLAN).

Dal livello B, piano in cui è presente il centro stella di tutta la rete, dovranno partire dei cavi in fibra ottica per il collegamento con i vari switch di piano.

Nel livello A sono presenti 2 armadi di piano (A1 e A2), che si divideranno il fabbisogno di prese TD dell'hotel. Il committente non ha però ancora specificato il carico di lavoro assegnato a ciascun armadio.

2.1.1 Calcolo quantità switch

Prima di presentare i vari schemi proposti, di seguito un breve calcolo per la quantità di switch da utilizzare per le varie richieste. Essendo gli switch in commercio dotati di 24 o 48 porte, il metodo adottato per trovare il numero di switch necessari consiste nel dividere il numero di prese TD per 24. Nel caso in cui le VLAN vengano divise in hardware, è stato necessario applicare lo stesso procedimento una volta per la VLAN Guest e una volta per la VLAN Hotel, ovviamente il calcolo viene ripetuto per ogni piano. Nel caso più semplice, dove le VLAN sono divise in modalità software, il calcolo è stato fatto per la totalità di prese TD presenti in ogni piano.

Un altro fattore di cui tener conto, è il numero di porte libere negli switch. Se è nullo o troppo basso, si rischia che nel caso in cui in futuro siano necessarie ulteriori prese TD, sarà necessario l'acquisto nuovi switch. Tale parametro è stato evidenziato negli schemi proposti, fermo restando che spetterà al committente la scelta finale.

Di seguito le tabelle che mostrano il minor numero di switch possibili nelle due eventualità: divisione delle VLAN via software e via hardware. Il calcolo è stato fatto sul 60% delle TD appartenti alla VLAN Hotel, come richiesto. La tabella 2.2 mostra la modifica al calcolo delle TD Hotel:

Descrizione	VLAN Ospiti	VLAN Hotel 60%	VLAN POS	TOTALE
Totale livello A	134	62	9	205
Totale livello B	94	23	0	117
Totale livello C	39	32	0	71
Totale livello D	125	6	0	131
Totale livello E	134	1	0	135
Totale livello F	88	0	0	88
Totale livello G	5	0	0	5
TOTALE	619	203	9	752

Tabella 2.2: La tabella mostra i cambiamenti dovuti alla considerazione del solo 60% della totalità delle prese TD appartenenti alla VLAN Hotel

Ora è possibile calcolare il numero di switch necessari. Di seguito il calcolo effettuato nel caso della divisione delle VLAN via software. Si vuol far notare che il livello G è stato incorporato al livello F, trattandosi della sola copertura dell'albergo. Non vi sono quindi switch di piano.

Descrizione	N° pannelli da 24	N° switch da 24	N° switch da 48	TD libere
Totale livello A	9	1	4	11
Totale livello B	5	1	2	3
Totale livello C	3	1	1	1
Totale livello D	6		3	13
Totale livello E	6		3	9
Totale livello F-G	4		2	8
TOTALE	33	3	15	45

Tabella 2.3: Calcolo del minor numero di switch per una divisione delle VLAN via software

Secondo la richiesta fatta dal committente, è stato fatto il calcolo degli switch necessari per consentire la più dispendiosa divisione delle VLAN tramite delle sottoreti fisicamente distinte. Nella tabella 2.4, il calcolo fatto per la VLAN Guest; nella tabella 2.5, il calcolo per la VLAN Hotel.

Descrizione	N° pannelli da 24	N° switch da 48	TD libere
Totale livello A	6	3	10
Totale livello B	4	2	2
Totale livello C	2	1	9
Totale livello D	6	3	13
Totale livello E	6	3	9
Totale livello F-G	4	2	3
TOTALE	28	14	46

Tabella 2.4: Calcolo del minor numero di switch per la sola VLAN Ospiti

Si vuole far notare che non è necessario alcun switch da 24 porte, in quanto quelli da 48 sono sufficienti a coprire il fabbisogno richiesto.

Di seguito, lo stesso calcolo fatto per la sola VLAN Hotel. Viene tenuto conto solo del 60% delle prese effettivamente calcolate dalle varie piantine di livello come richiesto dal committente.

Descrizione	N° pannelli da 24	N° switch da 24	N° switch da 48	TD libere
Totale livello A	3	1	1	10
Totale livello B	1	1		1
Totale livello C	2		1	16
Totale livello D	1	1		18
Totale livello E	1	1		23
TOTALE	8	4	2	68

Tabella 2.5: Calcolo del minor numero di switch per il 60% delle TD della VLAN Hotel

In questo caso sono stati omessi i livelli F e G in quanto non è presente alcuna presa TD riservata alla VLAN Hotel.

Per non annoiare ulteriormente il lettore, verrà risparmiata la tabella riportante lo stesso identico calcolo fatto per la quantità di prese TD per la VLAN Hotel al 100% e una suddivisione delle VLAN fatta in modo software.

2.1.2 Presentazione schemi proposti

In questo paragrafo verranno presentati i tre schemi proposti al committente. Le prime due possibilità presentate fanno uso di una divisione fisica delle VLAN. Il primo schema con l'utilizzo della rete Hotel al 60%, il secondo con la rete a pieno regime. Un terzo esempio, da utilizzarsi come confronto, è stato elaborato calcolando la totalità delle prese TD e la suddivisione delle VLAN via software. Quest'ultima opzione è stata riportata in quanto consente la creazione di una rete informatica capace di gestire il massimo carico di lavoro possibile con il minimo numero di dispositivi, e quindi ad un costo minore.

2.1.2.1 Schema 1

Il primo schema proposto è basato sul 60% della totalità delle prese TD appartenenti alla VLAN Hotel. La suddivisione delle VLAN è statta fatta in modo hardware, si ottengono quindi due sottoreti fisicamente distinte. Lo schema proposto è visibile nell'immagine 2.1.

Negli armadi E ed F è stato inserito uno switch apposito per la VLAN Hotel, pur avendo bisogno di un numero minimo di prese TD. È consigliabile, almeno per questi due piani, una divisione delle VLAN via software, per permettere un risparmio di 2 switch da 24 porte non obbligatoriamente necessari. In alternativa si propone la sostituzione dei due switch con altri con un minor numero di porte, in modo da poterne limitare il costo.

Per gli armadi A1 e A2 è stata ipotizzata una ripartizione sommaria degli switch, in quanto non in possesso di dati sufficienti. Per il calcolo di porte libere degli switch a questo piano, manca il calcolo delle porte riservate alla VLAN POS, che, se dovrà essere inserita negli switch riservati alla VLAN Ospiti (o dovrà anch'essa avere uno switch dedicato), richiederà uno switch supplementare.

Si vuol far notare che ai livelli B, F ed eventualmente A, il numero di prese libere, dopo gli effettivi collegamenti tra i vari switch appartenenti allo stesso armadio, è molto basso se non nullo. In caso di aumenti riguardo il numero di apparati da collegare (Access Point e IP cameras in primis o abilitazione di TD della VLAN Hotel), sarà doveroso rivedere il numero di switch necessari.

2.1.2.2 Schema 2

Come seconda opzione è stato richiesto di presentare lo stesso schema precedente, ma con la VLAN Hotel a pieno regime. La divisione delle VLAN sarà comunque fatta in via hardware. Lo schema è visibile nell'immagine 2.2.

Proponiamo qui uno schema che comprende il fabbisogno delle prese TD della VLAN Hotel al completo. Le considerazioni fatte per lo Schema1 sono valide anche per questa opzione, con l'eccezione del non dover preoccuparsi, a livello di numero di switch, di una futura ed eventuale abilitazione di prese appartenenti alla VLAN Hotel.

2.1.2.3 Schema 3

Come ultima opzione, viene proposto uno schema che tenga conto della totalità delle prese appartenenti alla VLAN Hotel. Per confronto ai metodi utilizzati precedentemente, in questo schema si divideranno le VLAN in modo software. L'immagine 2.3 mostra lo schema proposto.

Dagli switch Ospiti e Hotel partono 7 cavi ciascuno in fibra ottica multimodale verso gli armadi di piano. In ogni armadio di piano sono collegati tra loro gli switch necessari all'esigenza di prese TD, IP Cameras e Access Point conteggiati. Gli switch a livello F sono stati comunque collegati allo switch Hotel, per permettere una ridondanza che assicuri maggior sicurezza in caso di guasto. Per gli armadi A1 e A2 è stata ipotizzata una ripartizione sommaria degli switch, in quanto non in possesso di dati sufficienti. Vale anche in questa opzione quanto detto riguardo la bassa disponibilità di prese libere ai livelli C ed F.

2.2 Centro Stella

In questa sezione verrà presentata la struttura del centro stella per questa rete informatica. Ogni dispositivo è stato scelto tenendo ben presente le richieste del committente. Tali richieste sono state comunicate alla ditta presso cui ho svolto il tirocinio in un documento riservato, è quindi impossibile pubblicarlo per questioni

di privacy. Fanno riferimento a questo documento anche gli switch utilizzati per gli schemi proposti nella sezione 2.1.

Tutta questa parte è stata svolta con l'aiuto del tutor aziendale, in quanto necessita di una certa esperienza e conoscenza del mestiere e dei vari dispositivi attualmente in commercio.

2.2.1 Schema logico

Come visto negli schemi precedenti, il centro stella sarà ubicato nell'armadio di livello B. Qui ci sarà il cuore di tutta la rete informatica dell'hotel. Qui risiederanno i vari switch della rete interna, server, firewall, ecc.

Un primo lavoro è stato fatto scegliendo un opportuno schema logico per il centro stella che comprendesse tutti i dispositivi richiesti. Ci si è basati su uno schema precedentemente fornito dall'hotel, da usarsi come schema consigliato. Sono state poi apportate alcune modifiche a seconda delle esigenze della rete. L'immagine 2.4 mostra lo schema logico proposto.

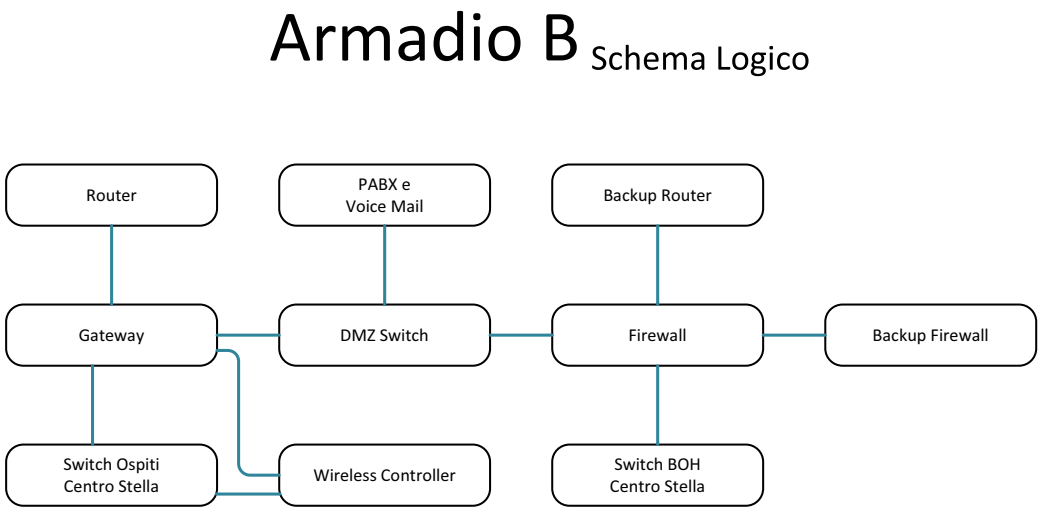

Figura 2.4: L'immagine mostra lo schema logico che mette in comunicazione i vari dispositivi del centro stella

Gli switch Ospiti e BOH sono collegati con gli switch situati nei vari livelli. Il primo è riservato alla VLAN Ospiti mentre il secondo alla VLAN Hotel. Come

nelle specifiche di VLAN, i dispositivi wireless sono collegati direttamente allo switch riservato alla VLAN Ospiti.

Router e firewall sono ridondanti, per consentire il miglior funzionamento anche in caso di guasto di uno dei due dispositivi.

Con PABX si indica la centralina telefonica, indicata per completezza. Lo switch DMZ mette in collegamento i vari server con il resto della rete.

2.2.2 Scelta dispositivi

Dopo aver impostato uno schema logico per il centro stella, si è potuto pensare a quali dispositivi adottare per ogni funzione.

Dopo aver firmato la sottoscrizione di dichiarazione di riservatezza, la mia ditta ospitante ha potuto venire a conoscenza delle caratteristiche tecniche richieste dal committente. In questo documento sono elencati, per ogni tipo di dispositivo, le caratteristiche tecniche da rispettare. Dopo un'attenta analisi, si è pervenuto alla scelta di tali dispositivi:

- HP ProCurve Switch 4204vl-48GS J9064A
  - ProCurve Mini-GBIC vl Module J8776A
  - GBIC - n. 13 Gateway server InnGate M200 (o E250)
- Cisco Router 2911/K9
  - HWIC 2A/S
  - HWIC ADSLI-B/ST
- Centrale Telefonica Alcatel
- HP ProCurve Switch 2510G-24 J9279A
- Cisco Firewall ASA 5510
- HP E2620-48-PoE+ J9627A
- HP ProCurve 2520-24-PoE J9138A

Per ogni dispositivo è stato trovato il data sheet, riportante tutte le caratteristiche tecniche. In alcuni casi, per esempio per il Cisco Firewall, è stato necessario esaminare anche il software abbinato al dispositivo stesso. È stato poi necessario un controllo incrociato tra i vari data sheet e il documento fornito dal committente con le caratteristiche richieste. Una volta confermata la conformità di ogni singolo dispositivo, è stato possibile procedere con lo schema fisico.

L'unico dispositivo mancante è il controller wifi, in quanto non ancora in possesso di adeguate informazioni sul carico di lavoro che avrebbe dovuto sostenere.

Gli ultimi due switch dell'elenco saranno utilizzati come switch di piano.

2.2.3 Schema Fisico

Una volta sviluppato lo schema logico e trovati i dipositivi necessari alle esigenze, si è potuti passare allo sviluppo dello schema fisico. Questo schema mostra come ogni dispositivo debba esser effettivamente collegato con gli altri, specificando la porta di ogni collegamento.

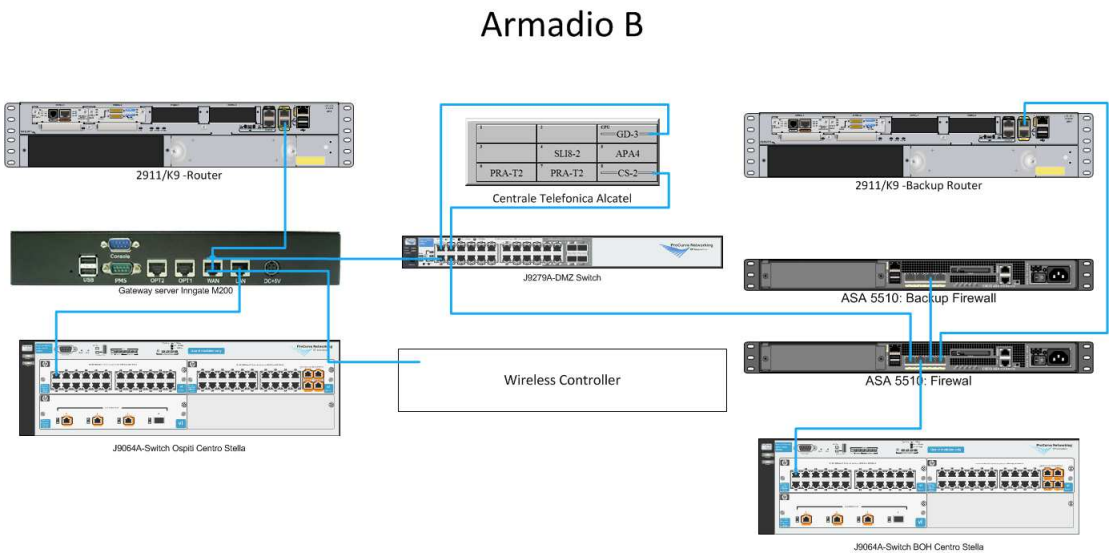

Figura 2.5: Lo schema presenta la struttura del centro stella con i dispositivi che verranno poi effettivamente montati

Per creare lo schema di figura 2.5 è stato semplicemente sostituito ogni dispositivo fisico con il corrispondente simbolo dello schema logico. La parte più impegna-

tiva dei vari collegamenti è accertarsi che le porte necessarie siano effettivamente presenti nel dispositivo, e che siano utilizzate per il giusto scopo.

Il gateway infatti, presenta una carenza di porte necessarie ai vari collegamenti. Non è stato ancora sostituito con uno adeguato in quanto è stato consigliato questo dispositivo dal committente, quindi prima di effettuare una sostituione del dispositivo o modifica dei collegamenti è necessario sentire il parere del cliente.

I due firewall sono collegati tra loro tramite un unico cavo, in quanto il secondo è puramente di backup, pronto ad entrare in funzione nel caso si riscontrasse un problema con il firewall normalmente attivo.

Quando i dispositivi verranno effettivamente installati, si dovranno riportare esattamente gli stessi collegamenti.

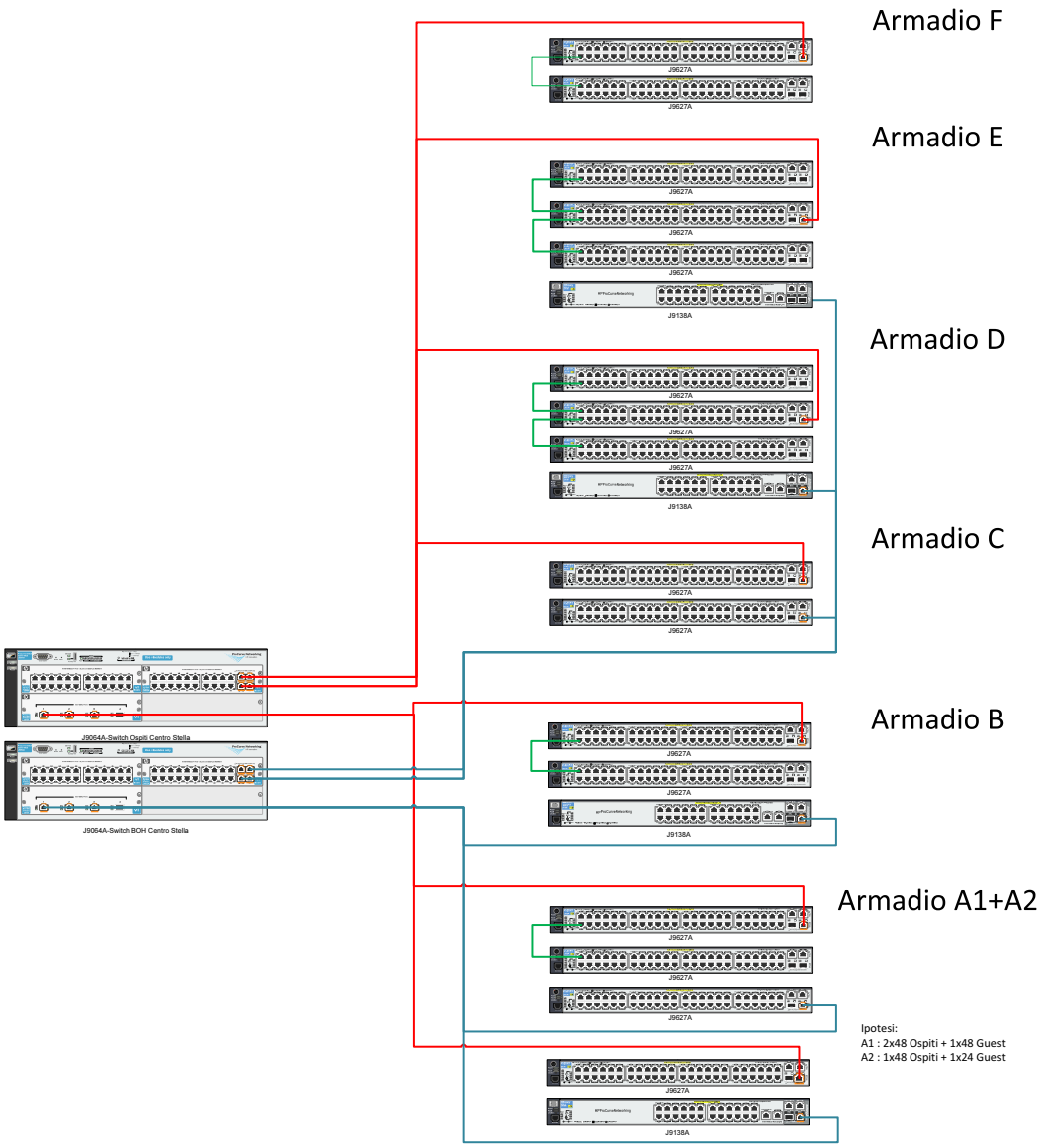

Figura 2.1: L'immagine mostra lo schema della rete ipotizzando la VLAN Hotel al 60% e la divisione delle VLAN fatta fisicamente

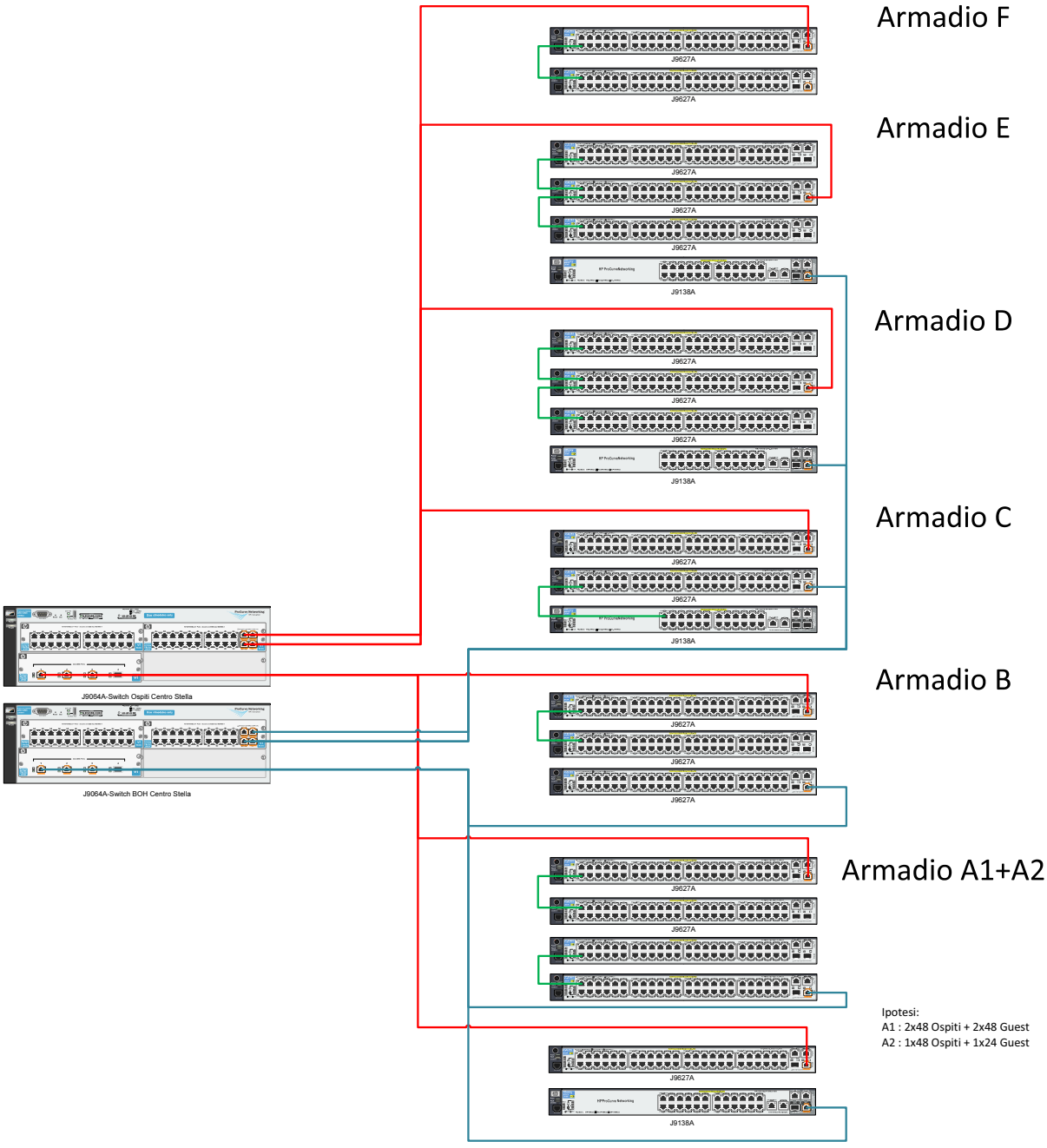

Figura 2.2: In questa immagine lo schema propone la divisione delle VLAN fatta sempre in modo hardware, e la VLAN Hotel è stata considerata con il 100% delle prese richieste.

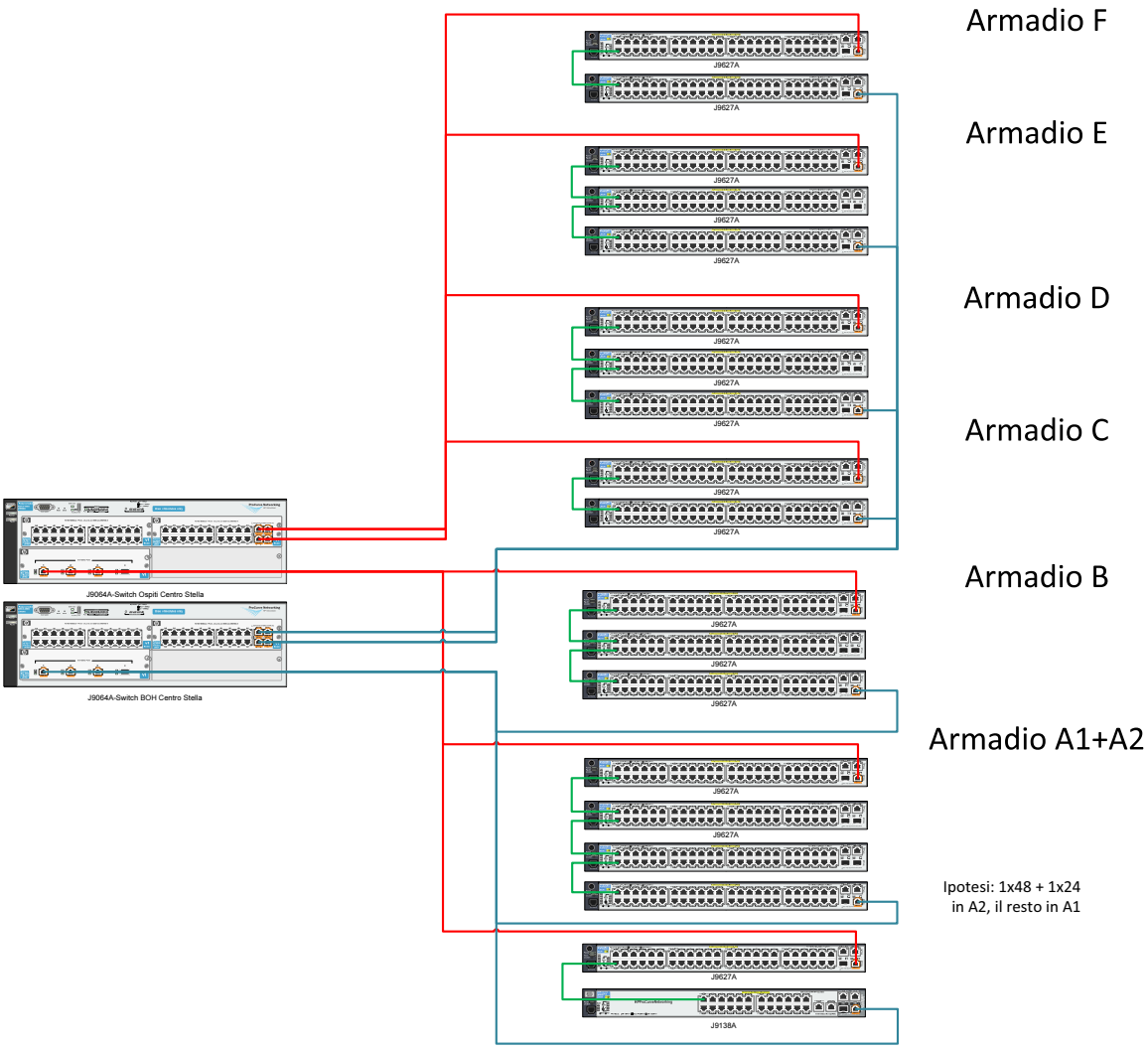

Figura 2.3: L'immagine mostra una rete capace di gestire tutti i dispositivi richiesti dall'hotel, consentendo una divisione via software delle VLAN

Capitolo 3

Altre attivittà

In questo capitolo verranno spiegate altre attività svolte durante il periodo di tirocinio. Si tratta di attività comunque inerenti al mondo delle reti informatiche, ma che hanno avuto un peso minore rispetto alle altre attività. Mi è stata offerta la possibilità di conoscere cenni sulla telefonia e sulla videosorveglianza. Ho avuto la possibilità di conoscere il software che la mia ditta ospitante usa quotidianamente. Ho potuto vedere come lavorano gli addetti al CED di una rete di medie dimensioni, ecc. Tra tutte le altre varie attività che ho potuto svolgere, ne riporto due. La prima è la mappatura di rete dell'azienda stessa, che mi ha fatto comprendere meglio la struttura di una rete informatica, almeno a livello pratico. La seconda è stata una prova per un computer che funzionasse da fax-server.

3.1 Mappatura di rete

Ogni volta che si va ad operare in una rete informatica, il requisito base è conoscere come questa sia progettata. Sapere appunto quanti dispositivi vi siano collegati, come e dove. Conoscere i servizi che la rete può offrire, i server, e tutto ciò che ad essa è collegato.

Per prendere familiarità con la rete dell'azienda ospitante, ed in seguito ad una recente modifica della rete, mi è stato chiesto di farne la mappatura. Si tratta quindi di creare uno schema logico che comprenda tutti i collegamenti principali tra i vari dispositivi e indicare dove ogni dispositivo sia collegato.

3.1.1 Verifica collegamenti

Come prima cosa è stato necessario controllare tutti i cavi degli switch presenti nell'ufficio CED. Ad uno ad uno è stato necessario verificare i collegamenti ad entrambi i capi del cavo. Per ogni porta di ogni switch è stato svolto lo stesso lavoro. Una volta segnati i vari percorsi a partire dagli 3 switch presenti, è stato possibile avere un'idea della struttura della rete dell'azienda (Immagine 3.1).

In un primo momento sono stati raggruppati tutti i vari computer presenti in azienda. I dispositivi indicati con *Brand Rex*, *CED* e *Patch Master* sono dispositivi necessari per portare il cavo ethernet dalla sala CED al resto dell'azienda. In particolare il dispositivo *CED*, forniva la sala CED di prese ethernet lungo tutto il perimetro. In altre parole, sono dei prolungamenti del cavo ethernet.

È stato poi inserito nello schema l'indirizzo IP dei dispositivi più importanti come server e firewall, che era noto prima dell'analisi.

L'*Encoder*, il *VioStor* e L'*Evision* sono tutti dispositivi necessari a monitorare il sistema di videosorveglianza pesente in azienda.

3.1.2 Indirizzi IP

Dopo aver trovato uno schema di rete sufficientemente chiaro, si è proseguiti con la ricerca dell'indirizzo IP di tutti i dispositivi della rete. Utilizzando un programma apposito (IPScan) è stata fatta la scansione dell'intera rete, e per ogni dispositivo è stato reso noto il nome, il MAC Address e l'indirizzo IP. Facendo un controllo incrociato con i dati appena ottenuti e quelli di cui sopra, è stato possibile creare delle tabelle, una per switch, indicando per ogni porta l'eventuale dispositivo collegato.

3.2 Fax Server

Un'altra attività svolta durante il periodo di tirocinio, riguardava l'implementazione di un fax server in un computer con sistema operativo Ubuntu 12.04. Si tratta di far in modo che tutti i fax dell'azienda, sia in ricezione sia in invio, invece che passare per un comune fax, fossero ricevuti tramite un pc, e reindirizzati ad

un indirizzo mail. Per rendere tutto ciò funzionante, è necessario conoscere bene i vari programmi che si andranno ad utilizzare e conoscere bene le tecnologie che si utilizzeranno. Essendo questi programmi di non facile configurazione, verrà di seguito spiegato in linea generale il funzionamento e lo scopo dei vari programmi necessari.

Tutte le informazioni utilizzate sono state reperite tramite diverse guide trovate in internet, spesso non aggiornate.

3.2.1 Panoramica

Per rendere possibile la ricezione di fax in un computer, è necessario un programma in grado di leggere il flusso di dati in entrata, una specie di centrale telefonica software da installare nel server. Tale funzione è svolta da *Asterisk*, un programma free per il mondo linux che permette di svolgere tutte le funzioni che potrebbe fare un comune software proprietario.

Una volta creata la centrale telefonica, è necessario creare un dispositivo in grado di interpretare il flusso di dati, e che appaia come un dispositivo fax virtuale. Un programma che consente questo è *IAXmodem*. Si tratta di un programma free per la piattaforma linux, in grado di creare e gestire uno o più fax virtuali e di metterli in comunicazione con la centralina telefonica creata con Asterisk.

Come parte finale, c'è il vero e proprio programma che consente al computer di diventare un fax server. È stato utilizzato *Hylafax* per questo scopo. È in grado di recuperare i fax ricevuti da un fax virtuale creato con IAXmodem, e tradurli nel formato scelto (per esempio pdf), e inviarlo come allegato ad un indirizzo mail scelto.

Allo stesso modo, per l'invio di un fax, sarà necessario il processo contrario, ossia inviare una mail con allegato il fax da spedire e passando prima per Hylafax, poi per IAXmodem ed infine per Asterisk, il fax potrà esser finalmente recapitato al destinatario.

3.2.2 Asterisk

Il primo programma necessario è Asterisk, si tratta di un software PBX libero. Può essere utilizzato come cuore di una PBX basata sul protocollo IP, gestendo le chiamate, facendo da router, connettere il dispositivo con la rete esterna, ecc. È un programma flessibile e supporta il VoIP in diversi protocolli ed è compatibile con la maggior parte degli apparecchi telefonici standard.

L'installazione è stata fatta manualmente, scaricando e compilando i file in binario.

Per avviare il servizio, è necessario digitare in un terminale il classico comando

```
sudo /etc/init.d/asterisk start
```

Per accedere e modificare le impostazioni sono disponibili due possibilità: la prima si tratta di digitare manualmente:

```
sudo asterisk -rvvvvvvvvvvvvvvvvv
```

che però non consente di modifichare ogni singolo parametro. L'altra opzione che lascia più possibilità di modifica, per una programmazione più specifica, sta nell'editare il file di configurazione in posizione /etc/asterisk/. Ogni file di configurazione ha estensione .conf, e la modifica va fatta con privilegi di amministratore tramite un editor di testo.

3.2.3 IAXmodem

Dopo aver configurato la centrale telefonica con Asterisk, è necessario un programma che riesca a leggere il flusso dati che questo fornisce. Il programma che legge questo flusso di dati (IAX Channel) è IAXmodem. Si sostituisce ad un modem fisico in grado di leggere una tradizionale linea telefonica offrendo la possibilità di creare uno o più modem virtuail.

Anche in questo caso sono stati scaricati i file binari dal sito ufficiale e poi compilati manualmente.

Dopo l'installazione, è necessario modificare il file di configurazione situato nella cartella /etc/iaxmodem a seconda delle proprie esigenze. Per poter modifica-

re i file .conf, è necessario aprire un editor di testo con privilegi di ammnistratore, come per Asterisk.

Il file /etc/iaxmodem/ttyIAX contiene tutte le configurazini del modem virtuale ttyIAX. Per avere più modem, è sufficiente creare più file di questo tipo.

3.2.4 HylaFax

Una volta stabilito il collegamento tra IAXmodem con Asterisk, si può passare alla fase successiva: il fax server vero e proprio. È un software progettato secondo l'architettura client-server dove i modem fax possono risiedere in una singola macchina in rete, mentre i client possono inviare il loro lavoro in uscita da ogni altro host presente in rete. Supporta più modem e un buon carico di lavoro.

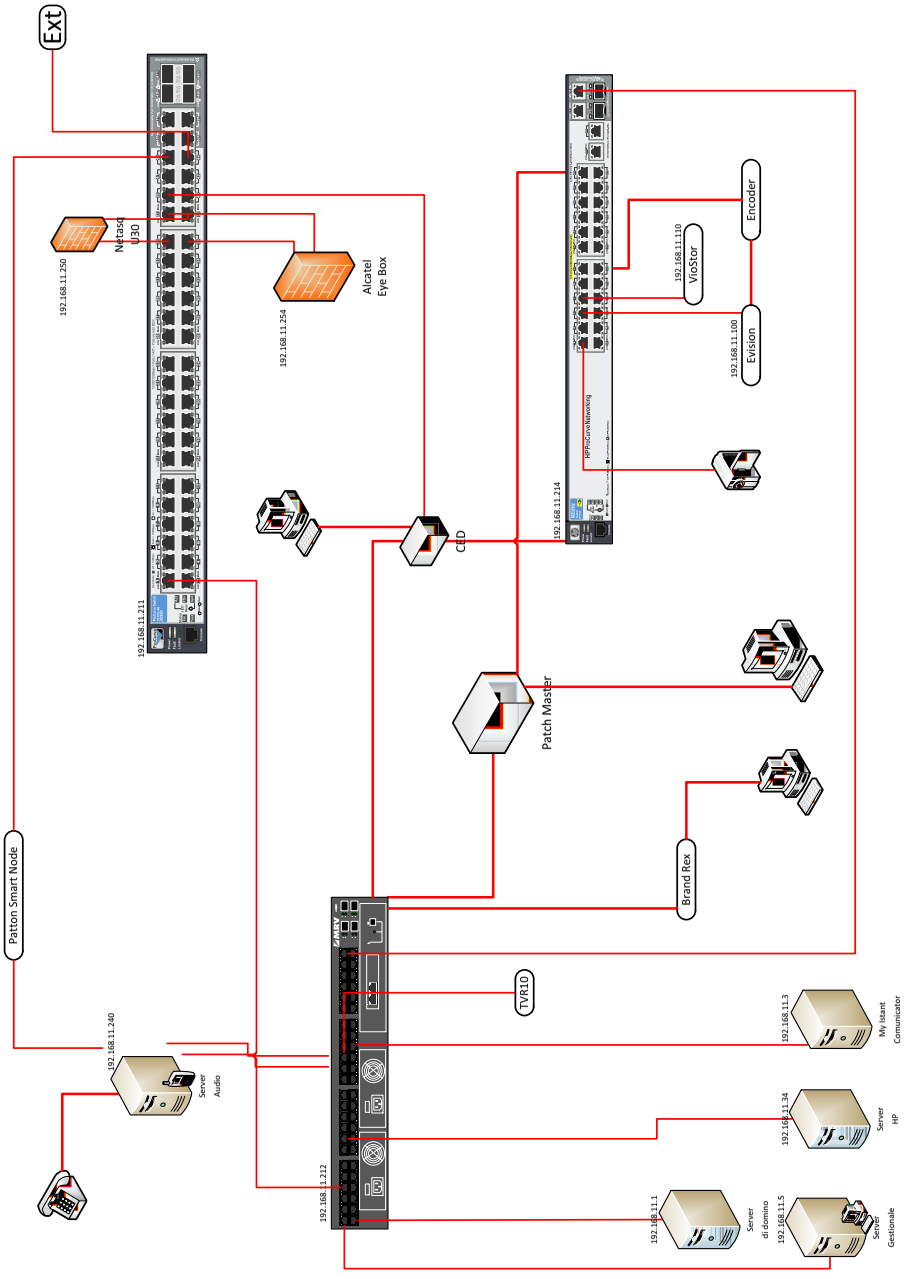

Figura 3.1: L'immagine mostra lo schema di rete della ditta ospitante

Switch HP 192.168.11.211

Led rosso
Led verde
Led spento

Porta	IP	Nome Host	MAC Address	Collegamento
1	192.168.11.214			Switch HP
2				
34				
35	192.168.11.250		000DB4-0665BF	Firewall Netasq
36	192.168.11.254	SMBSERVER	004063-DDDEBD	Firewall EyeBox
37			004063-DDDE6D	Firewall EyeBox
38			000DB4-0665BD	Firewall Netasq
39				CED 3
40				
41				
42				
43	80.86.155.100\24		00A0BA-01E84A	Patton Smart Node
44	FIBRA OTTICA			Esterno
45				
46				
47				
48				

Figura 3.2: Elenco dei dispositivi connessi allo switch 192.168.11.211. Sono state omesse le porte dalla 3 alla 33 in quanto prive di collegamenti.

MRV Switch				192.168.11.212	
Porta	**IP**	**Nome Host**	**Collegamento**		**Note**
1	192.168.11.5	GESTIONALE	Server Gestionale		
2	192.168.11.87	PC-MAURO	Brand Rex	14	
3	192.168.11.1	DELL400	Server di Dominio		
4			CED	11	
5	verso laboratorio		Patch Master	131	Switch Laboratorio
6					
7	192.168.11.136	CED2	Patch Master	123	
8			CED		
9			Patch Master	118	
10			CED	16	
11	192.168.11.17	SGATTO	Patch Master	49	
12	192.168.11.12	LISAGRESPAN	Patch Master	142	IC Network BLU
13	192.168.11.14	ANDREA F.	Patch Master	63	
14	192.168.11.10	RECEPTION	Patch Master	21	
15	192.168.11.34	CED1	Server HP		
16			Patch Master	30	
17					
18			Patch Master	26	
19	192.168.11.68	KMBT6AE56B D	Patch Master	57	
20			Patch Master	60	IC Network ROSSO
21			Patch Master	136	IC Network BLU
22			Patch Master	127	
23	192.168.11.15	ACQUISTI	Brand Rex	13	
24	192.168.11.151		Patch Master	85	
25	192.168.11.240		Server Audio		
26	192.168.11.66	PLOTTER	Patch Master	50	
27	192.168.11.241		Server Audio		
28					
29			TVR10		
30	192.168.11.3	ADMIN	Server Test		
31			Patch Master	135	
32	192.168.11.138	CEDSEVENPRO	Patch Master	56	
33			Patch Master	113	
34	192.168.11.19	MARIKAGROPPO	Patch Master	142	IC Network ROSSO
35			Patch Master	101	
36			Patch Master	120	
37			Patch Master	121	
38			Patch Master	128	
39	192.168.11.67	RNPB6CE3A	Brand Rex	17	
40			Patch Master	54	
41			Patch Master	70	
42			Patch Master	60	IC Network BLU
43	192.168.11.11	GIULIOFASSINA	Patch Master	68	
44			Patch Master	17	
45					
46			Brand Rex	9	
47	192.168.11.214		Switch HP		
48	192.168.11.211		Switch HP		

Led rosso
Led verde
Led spento

Figura 3.3: Elenco dei dispositivi connessi allo switch 192.168.11.212

Switch HP 2520 PoE				192.168.11.214	
Porta	**IP**	**Nome Host**	**MAC Address**	**Collegamento**	
1			001A07-02DE26	Telecamere IP	
2	192.168.11.45			CED	6
	192.168.11.139	SEVENPRO64BIT			
3	192.168.11.125			Patch Master	83
4	192.168.11.40			Patch Master	125
5	192.168.11.100			Evision	Lan
6				CED	10
7				VioStor	Basso
8	192.168.11.110	EFFECIQNAP		VioStor	Alto
9	192.168.11.114			Encoder	114
10	192.168.11.111				111
11	192.168.11.113				113
12	192.168.11.112				112
13	192.168.11.116				116
14	192.168.11.115				115
15	192.168.11.118				118
16	192.168.11.121				121
17	192.168.11.119				119
18	192.168.11.117				117
19	192.168.11.120				120
20	192.168.11.122				122
21	192.168.11.16	UFFTECNICOALESS		Patch Master	51
	192.168.11.44				
22	192.168.11.41			Patch Master	97
23	192.168.11.93	ROBERTOFASSINA		Patch Master	44
	192.168.11.85				
	192.168.11.96				
	192.168.11.199				
			4860BC-96156E		
	192.168.11.94				
			C8BCC8-3A0C17		
24	192.168.11.198			Patch Master	98
25					
26					
27					
28	192.168.11.212			Switch MRV	

Led rosso
Led verde
Led spento

Figura 3.4: Elenco dei dispositivi connessi allo switch 192.168.11.214

Conclusioni

Scopo dell'elaborato sono state le reti informatiche, il conoscere le principali tecnologie sulle quali esse si basino e come funzionino. È stato possibile conoscerne l'implementazione attraverso due tipi di switch abbastanza diffusi nel mercato odierno. Si è visto il problema della gestione degli indiririzzi IP di una rete e come viene normalmente eseguita. Come una rete nasce e viene effettivamente progettata a seconda delle esigenze del cliente. Come è possibile conoscerne topologia e dispositivi che compongono una rete di medie dimensioni.

Tutto il periodo di tirocinio è stato utile al fine di conoscere il mondo delle reti informatiche, come funzionino e come vengano progettate. È stato essenziale poter avere un riscontro pratico delle varie nozioni apprese durante il periodo di studi, cosa da non sottovalutare. Poter vedere le potenzialità e i limiti delle varie tecnologie utilizzate e conosciute durante il periodo di tirocinio è stato molto interessante.

Glossario

- Broadcast storm: è una situazione della rete che si verifica quando ogni host manda in broadcast alcuni messaggi ricevuti. Si verifica quindi un grande aumento del traffico dati con un conseguente rallentamento dell'intera rete o peggio. Si verifica nello switching di secondo livello a causa di collegamenti ridondanti.
- IGMP: è un protocollo che si usa per la gestione del multicast. Viene utilizzato quando un'applicazione in funzione in un particolare host collegato ad un router richiede di far parte di un particolare gruppo multicast.
- DMZ: Demilitarized Zone è una sottorete isolata da tutto il resto, raggiungibile sia dalla rete interna sia da quella esterna. La caratteristica principale è quella di poter limitare la connessione da parte di alcuni host della rete interna.
- CED: Centro Elaborazione Dati è la parte di un'azienda che si occupa della manutenzione e coordinazione dei dispositivi e dei servizi informatici della rete in uso dall'azienda stessa.
- PBX: Private Branch eXchange è una centrale telefonica per uso privato.
- VoIP: Voice over IP è una tecnologia che consente telefonate attraverso una rete a commutazione di paccheto. Si contrappone alla classica connessione.

Bibliografia

[1] http://www8.hp.com/it/it/home.html.

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

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

[4] http://wiki.ubuntu it.org.

Ringraziamenti

Ringrazio tutto il personale del Gruppo Effeci SRL, per la possibilità datami e per avermi offerto un ottimo ambiente di lavoro. In particolare ringrazio il mio tutor aziendale, Fabio Frassetto, per la grande pazienza avuta. Vorrei ringraziare il prof. Sergio Congiu per la grande disponibilità e gentilezza. Un ringraziamento particolare va alla mia famiglia che mi ha permesso di percorrere questo cammino di studi. Un sentito grazie a chi mi è stato vicino.