**RELAZIONE SULLA TOPOLOGIA E GESTIONE DELLA RETE**

In questa relazione verranno illustrate e motivate le scelte progettuali decise per lo sviluppo della rete necessaria per il lavoro e le necessità di Mr. Leet.   
Mr. Leet ha comunicato le sue necessità, che sono:  
Amministrare da casa sua in modo sicuro i sistemi aziendali e due Autonomous Systems che questa gestisce e gestire gli oggetti smart della sua abitazione.  
La rete che analizziamo si può trovare a questo link: www.github.com/Marco-Malanchin/Progetto-sistemi.  
Ora vediamo nel dettaglio le varie parti in cui è suddivisa la rete e come verranno gestite.

**La casa di Mr. Leet**All’interno della casa di Mr. Leet sono presenti vari dispositivi smart che possono essere gestiti e monitorati attraverso la rete di casa. Nello specifico sono stati richiesti dal cliente:  
- Sensori di movimento in giardino e al piano superiore  
- Sensori di fumo al piano terra (cucina e salotto)  
- Sistema di allarme nel capannone esterno  
- Sistema di videosorveglianza all’interno del capannone

Ma come decisione del gruppo di lavoro è stato deciso di integrare nella rete i seguenti sistemi:  
- Sistema di videosorveglianza al piano superiore e in giardino  
- Sensori di movimento al piano superiore e in giardino  
- Sistema antincendio al piano inferiore  
- Sistema di ventilazione al piano inferiore (costituito da ventole e finestre)  
- PC fisso per il controllo dei dispositivi  
- Server per la gestione dei dispositivi

A seguire la lista dei dispositivi utilizzati:  
- 1 Router PT  
- 6 Switch PT  
- 1 PC  
- 1 Laptop  
- 1 server  
- 3 rilevatori di movimento  
- 3 webcam  
- 2 rilevatori di fumo  
- 2 spruzzatori d’acqua  
- 2 ventole  
- 2 finestre  
- 1 sirena

Dopo aver visto il numero di dispositivi abbiamo deciso il piano di indirizzamento, cioè un indirizzo privato (192.168.10.0) con subnet-mask 255.255.255.224, con il quale possiamo collegare fino a 30 host.

Per ordinare i dispositivi li abbiamo dapprima divisi tra le aree individuate della proprietà di Mr. Leet, cioè l’abitazione, il capannone e il giardino.  
L’abitazione è stata ulteriormente suddivisa tra i dispositivi presenti nel piano superiore e quelli presenti nel piano inferiore.  
Per effettuare queste divisioni gli apparecchi sono stati collegati a switch diversi, per permettere il collegamento via cavo tutti i dispositivi sono stati opportunamente modificati, aggiungendo una porta ethernet.   
Di seguito un’immagine della topologia scelta per la rete:

IMMAGINE CASA MISTER LEET

Gli indirizzi IP dei dispositivi collegati alla rete personale di Mr. Leet sono assegnati attraverso il servizio DHCP fornito dal router.  
Al server è stato assegnato un IP fisso per far sì che i dispositivi IoT lo possano sempre trovare allo stesso indirizzo.  
Il PC fisso della casa di Mr. Leet può connettersi alla rete pubblica senza rivelare il suo indirizzo privato grazie alla NAT dinamica impostata sul router. Per configurare la NAT dinamica è sufficiente configurare all’interno del router il pool di indirizzi pubblici che può utilizzare, la rete privata in cui sono gli host e il numero di host che possono uscire.   
Il PC utilizza come server DNS quello presente nell’AS 1000.  
Al laptop sono stati affidati IP e DNS statici, per permettere di impostare come server DNS quello presente nell’AS 2000. L’indirizzo assegnato al laptop è nattato dal router in modo statico.  
Dopo aver creato un account per l’amministrazione dei dispositivi smart ed aver collegato gli stessi al server sono state create le routine (condizioni) necessarie per il loro corretto funzionamento e la loro interazione.  
Le routine si basano sul principio “If This Than That”, cioè se succedono uno o più eventi, o si avverano determinate condizioni vengono portate a termine una o più azioni.  
Le condizioni che sono state create si possono riassumere in 3 tipi:  
**1.** Rilevamento movimenti  
**2.** Antincendio  
**3.** Allarme

**1.** In caso venga rilevato un movimento viene attivata la webcam collegata a quel sensore, che poi si spegne quando il rilevatore di movimenti non rileva più nulla.

**2.** Se un rilevatore di fumo registra una certa quantità di fumo nell’aria allora vengono attivati gli spruzzatori d’acqua e vengono attivate le misure per consentire un’adeguata ventilazione, cioè l’accensione delle ventole e l’apertura delle finestre. Tutto viene riportato allo stato iniziale quando la quantità di fumo rilevata raggiunge la quota di sicurezza.

**3.** Se il sensore del capannone rileva un movimento fa partire la sirena, che si spegne solo quando il rilevatore non nota alcun movimento.

**L’azienda di Mr. Leet (AS 3000)**L’azienda di Mr. Leet è uno dei tre Autonomous System per cui Mr. Leet ha necessità di una connessione sicura per la gestione dei sistemi informatici dell’azienda e per quelli gestiti dalla stessa.

All’interno della struttura aziendale sono presenti vari dispositivi che ne garantiscono la sicurezza e il corretto funzionamento dei sistemi, questi sono gli apparecchi da gestire presenti in azienda:  
- 3 router PT  
- 3 switch  
- 3 server  
- 2 webcam  
- 3 PC  
- 1 monitor della temperatura  
- 1 termostato  
- 1 condizionatore  
- 1 elemento riscaldante  
- 2 spruzzatori  
- 1 rilevatore di fumo  
- 1 rilevatore di fuoco  
- 2 porte  
- 1 sirena

L’azienda può essere vista in due parti separate, la sala server e la parte amministrativa composta dagli uffici e della reception.   
Dei dispositivi sopraelencati nella parte amministrativa troviamo:  
- 1 router   
- 1 switch  
- 2 PC  
- 1 webcam  
- 1 porta

Mentre tutti gli altri fanno parte della rete dedicata alla sala server, ad eccezione di un router che è necessario per far comunicare tra loro le due aree aziendali.  
All’interno di entrambe le zone aziendali è stato implementato l’OSPF, considerando tutta la rete aziendale come una singola area.   
Analizziamo ora nel dettaglio le due suddivisioni della rete aziendale.

**Sala server**Le reti utilizzate all’interno di quest’area sono due, l’indirizzo 192.168.0.196/30 per il collegamento tra il router interno e quello mediatore tra le due reti e l’indirizzo di rete 192.168.10.32/27 per il collegamento dei vari host che sono dispositivi smart e i server che ospitano i 2 siti aziendali, quello di vetrina e quello principale, e il server per la gestione dei dispositivi IoT.  
Ai server sono stati affidati degli indirizzi IP statici mentre per gli altri host è stato implementato all’interno del router il servizio DHCP dal quale sono stati esclusi gli indirizzi già assegnati. I server che comunicano all’esterno prima di entrare all’interno della rete pubblica vengono nattati dal router. Questi server hanno necessità di comunicare con la rete pubblica perché ospitano i due siti aziendali, quello di vetrina e quello utilizzabile dai dipendenti per lo svolgimento delle loro attività. I siti presenti nei server sono basati su dei template trovati in rete.  
Per la gestione dei dispositivi smart abbiamo scelto di utilizzare la stessa tecnica usata nella proprietà di Mr. Leet, ed abbiamo dunque creato le routine necessarie per soddisfare le necessità espresse dal cliente, queste routine sono:  
**1.** Antincendio  
**2.** Controllo temperatura

**1.** Nel caso in cui il rilevatore di fumo registri una certa quantità di fumo nell’aria, superiore o uguale a 1, allora viene azionato lo spruzzatore d’acqua e la sirena segnala l’emergenza con un segnale acustico.  
Tutto viene riportato allo stato iniziale quando la quantità di fumo rilevata raggiunge la quota di sicurezza.

**2.** Per un corretto dei sistemi informatici all’interno della sala server dovrebbe esserci una temperatura pari a 20°C, per consentire questo sono stati installati un termostato e un rilevatore della temperatura, che lavorano insieme per mantenere la temperatura costante.

Sono presenti anche altri dispositivi IoT non connessi alla rete, questi sono:  
Una webcam che consente di visualizzare il feed video della sala server per motivi di sicurezza ed una porta smart.

**Parte amministrativa**La seconda parte della rete aziendale è quella che comprende gli uffici e la reception all’ingresso. Per questa rete è stato scelto l’indirizzo di rete 192.168.10.64 con subnet-mask 255.255.255.224.   
Per l’affidamento degli indirizzi IP agli host viene utilizzato il servizio DHCP fornito dal router, eccetto che per il server di gestione IoT a cui è stato assegnato un IP statico.  
All’interno della di questa rete sono presenti due PC dai quali è possibile monitorare i due feed video delle webcam, una posta all’ingresso e l’altra all’interno degli uffici.  
All’ingresso è presente una porta automatica, che si apre quando il sensore di movimento a lei vicina si attiva.

**Autonomous System ALFA (AS 2000)**Questo è uno dei due Autonomous System che l’azienda per cui lavora Mr. Leet deve gestire, è costituito da:  
- 6 Router PT  
- 1 Server

Per il piano di indirizzamento è stato scelto di utilizzare indirizzi privati per collegare tra loro i router le reti presenti sono quelle che partono dalla rete 192.168.0.16 con subnet-mask 255.255.255.240 fino alla rete 192.168.0.96.  
Per popolare le routing table dei router abbiamo scelto di utilizzare il protocollo OSPF, nella sua variante single area.  
Di questo AS fa parte un server che offre servizio DNS ed è in grado di risolvere i nomi dei domini dei due siti aziendali.  
L’indirizzo del server, quando questo deve comunicare con qualcosa di esterno al suo AS, viene nattato dal router più esterno.



**Autonomous System OMEGA (AS 1000)**Questo è il secondo degli AS che l’azienda è chiamata a gestire, all’interno di questo AS sono presenti:  
- 5 Router  
- 1 Server

Come piano di indirizzamento all’interno di questo AS abbiamo scelto di utilizzare indirizzi privati, a partire dalla rete 192.168.0.112.  
Data la decisione di utilizzare il protocollo RIPv2 per la popolazione delle tabelle di routing non è stato necessario specificare le classi, visto che questo protocollo è definibile classless.  
Anche il server presente all’interno di questo AS offre il servizio DNS per i siti aziendali.  
In caso di malfunzionamento di uno dei due server negli host che lo richiedo è possibile impostare come indirizzo DNS quello del server funzionante, cioè permette di non causare disservizi prolungati nel tempo.  
Anche qui, come nell’altro AS, il server è sottoposto a NAT.

**Collegamento tra gli AS**Per collegare tra loro i vari AS abbiamo collegato i router esterni utilizzando dei cavi seriali ed abbiamo deciso di utilizzare reti pubbliche, a partire dalla rete 11.0.0.0 con subnet-mask 255.255.255.240 fino alla rete 11.0.0.160 con la stessa subnet-mask. La rete 11.0.0.48 che originariamente era di collegamento tra l’AS 2000 e l’AS 3000 è stata scarta perché causava dei malfunzionamenti, ed è stata sostituita con quella 11.0.0.160.  
I router connessi sono 8 e sono: i 3 router esterni degli AS aziendali, il router situato a Nizza (AS 4000), quello di confine della Francia (AS 5000), il router di confine con l’Italia (AS 6000), il router di Rovigo (AS 7000) e quello dell’abitazione di Mr. Leet (AS 8000).  
Come protocollo di routing abbiamo scelto di utilizzare il BGP, che essendo di tipologia EGP è adatto per la nostra situazione.  
Oltre che ai router esterni sono collegati tra loro grazie a delle reti pubbliche anche gli ultimi e i penultimi router degli AS, questo per consentire un facile supernetting utile al BGP.

**Gestione dei sistemi da remoto e sicurezza dei sistemi**Data la richiesta di Mr. Leet di poter svolgere il suo lavoro da amministratore di rete dalla sua abitazione è stato implementato all’interno dei sistemi aziendali il protocollo SSH per permettere lo svolgimento del lavoro in sicurezza.  
La sicurezza viene garantita anche grazie alla password necessaria per accedere alla modalità “EXEC”, che viene criptata con l’utilizzo del servizio disponibile all’interno dei router Cisco.

