

Relazione Lavoro Di Gruppo

Gruppo 2, Clown-Fiesta-ICT

Catone Mario,
Oglietti Riccardo,
Serena Thomas,
Volgarino Livio

June 26, 2021

Indice

1	Introduzione	2
1.1	La Sfida	2
1.2	Il Team	3
2	Organizzazione E Strumenti	4
2.1	Comunicazione	4
2.2	Strumenti Tecnici	4
2.3	Definizione Dei Ruoli	5
3	Diagramma Di Rete e Topologia	6
3.1	La Struttura In Generale	6
3.2	Il Diagramma	7
4	Sicurezza E Firewall	9
5	Microsoft Active Directory e Windows Licensing	10
5.1	Domain Controller	10
5.1.1	Server Di Autenticazione	11
5.1.2	Gestione Shared Directory	12
5.1.3	Gestione Roaming Profiles	13
6	Considerazioni Finali	14

Capitolo 1

Introduzione

1.1 La Sfida

Il progetto che mi accingo a descrivere e' nato come figlio del corso *Learning By Project* a opera dei docenti Bardi Laura Silvia e Blachietti Andrea. In esso ci e' stato richiesto di progettare una nuova infrastruttura di rete atta a rimpiazzare l'intera infrastruttura di una scuola superiore Piemontese. La scuola e' divisa in due gruppi di edifici, i quali contengono le sedi di tre differenti indirizzi: **Liceo Scientifico delle Scienze Applicate a Indirizzo Informatico**, **Istituto Tecnico Economico** e infine **Liceo Linguistico**.

Entrambi i gruppi di edifici sono composti da tre piani, il primo gruppo e' formato da tre edifici, in due dei quali sono concentrate aule, laboratori e locali amministrativi. Nella terza e' poi disposta la palestra e relativi locali.

Il seconodo gruppo, non contiguo al primo, e' invece formato da due edifici, nel quale sono dislocate le aule e i laboratori dell'Istituto Tecnico Economico, mentre nel seconodo e' presente la palestra e alcuni edifici amministrativi.

La progettazione e' stata portata avanti tenendo conto di alcuni punti fondamentali, quali la necessita' di fornire scalabilita' e facilita' di manutenzione da parte dei tecnici presenti all'interno dell'infrastruttura scolastica, e la necessita' di un controllo capillare della sicurezza tramite l'utilizzo di alcuni strumenti fondamentali quali l'infrastruttura MS Active Directory e l'utilizzo di firewall integrati con essa.

Un'altra sezione sicuramente fondamentale del progetto e' sicuramente quella legata all'organizzazione di un gruppo di lavoro il piu' efficiente e produttivo possibile, atto a risolvere un problema complesso nella sua struttura. Cio' ci ha permesso di venire in contatto con alcune delle piu' comuni difficolta' del lavoro di gruppo e di imparare molto su come gestirle, inoltre, trattandosi del primo vero progetto di gruppo per molti di noi l'entusiasmo si e' dimostrato molto fin dalla prima lezione.

1.2 Il Team

Il gruppo classe e' stata suddivisa in sette differenti gruppi, il nostro gruppo, il numero due, e' formato dai seguenti studenti:

- **Catone Mario**
- **Oglietti Riccardo**
- **Serena Thomas**
- **Volgarino Livio**

Durante l'organizzazione del progetto abbiamo optato per suddividere le mansioni principalmente in base agli interessi e alle passioni dei singoli componenti, in maniera da rendere lo sforzo collettivo quanto piu' produttivo possibile.

In merito all'organizzazione interna non possiamo dire di aver definito una gerarchia o un vero e proprio "Team Leader", bensì di esserci organizzati come pari, affidando un carico il piu' possibile uniforme in termini di importanza e impegno richiesto.

Capitolo 2

Organizzazione E Strumenti

2.1 Comunicazione

Come primo passo, durante il primo incontro abbiamo cercato di definire una selezione di strumenti atti a gestire una serie di aspetti fondamentali delle dinamiche insite nel teamwork, in primis la Comunicazione tra colleghi. La nostra scelta si è orientata verso alcuni strumenti chiave: innanzitutto abbiamo optato per la scelta della piattaforma *Telegram* per la messaggistica istantanea e le comunicazioni più rilevanti grazie alle ampie possibilità di gestione del gruppo, quale la possibilità di rendere un messaggio prioritario o evidenziato. Abbiamo poi deciso di usare lo strumento *GIT* per coordinare la gestione dei documenti prodotti da ogni membro del gruppo. Infine, abbiamo optato per lo strumento di conferenza *Discord* per gestire gli incontri in remoto al di fuori dell'orario scolastico.

2.2 Strumenti Tecnici

La selezione degli strumenti tecnici si è invece rivelata più ardua, l'ostacolo più grande è stato coordinare le necessità di ognuno all'interno di un set di strumenti congruo agli obiettivi del progetto. Per quanto riguarda la stesura di relazioni e documenti, abbiamo optato per l'utilizzo del linguaggio $\text{L}^{\text{A}}\text{T}_{\text{E}}\text{X}$: esso permette di strutturare documenti estremamente complessi mantenendo una relativa semplicità di utilizzo. Inoltre l'integrazione con lo strumento di sviluppo collaborativo *git* è ottima, e ha permesso di ottimizzare lo sforzo comune. Da notare poi la possibilità di gestire i documenti tramite il comodo sistema basato su commit sul quale si basa *git*, è stato largamente più semplice gestire le revisioni collaborative per qualsivoglia documento, e la scrittura collaborativa, indispensabile per la redazione delle relazioni. Per ciò che concerne invece la creazione di diagrammi di rete, è stato scelto lo strumento gratuito *Draw.io*: si tratta di una Webapp atta a creare rappresentazioni grafiche di qualsiasi genere. Il tool è stato scelto per via della sua semplicità d'uso e della

possibilita' di esportare liberamente i documenti creati.

2.3 Definizione Dei Ruoli

Infine, abbiamo deciso di operare alcune scelte organizzative a nostro avviso opportune per poter gestire il progetto nella sua interezza. Abbiamo optato per un organizzazione basata su una suddivisione in ruoli, con mansioni specifiche e mediamente lunghe, per poi coordinare gli sforzi durante meeting con cadenza settimanale. Per facilitare la nostra organizzazione interna abbiamo da subito deciso di assegnare un colore a ogni membro, tramite questo espediente ci e' stato piu' facile organizzare il lavoro e i compiti di ognuno in maniera chiara e visuale. La suddivisione e' quindi risultata come segue:

Nome Componente	Compito Assegnato
Catone Mario	Active Directory
Oglietti Riccardo	Reportistica e presentazione
Serena Thomas	Firewall e sicurezza
Volgarino Livio	Topologia di rete e routing

Questa particolare suddivisione dei ruoli e' nata dopo un confronto sulle nostre tematiche di interesse, e sui nostri punti di forza principali. Per citare un esempio, Catone Mario ha scelto la sua mansione dopo aver seguito con interesse il corso proposto per l'amministrazione di sistemi basati su *Windows e MS Active Directory* di Cristante Fabrizio e aver riscontrato un grande interesse sulla tematica. Invece, Serena Thomas, rimasto molto colpito dalle implicazioni legate alla sicurezza studiate e sperimentate durante il corso di *Firewall* a opera di Vedovato Alberto, ha deciso di intraprendere questa mansione.

Capitolo 3

Diagramma Di Rete e Topologia

Volgarino Livio

3.1 La Struttura In Generale

Come precedentemente specificato, la struttura di rete e' stata ideata principalmente da Volgarino Livio, ed e implementata dedicando particolare attenzione ad alcuni aspetti giudicati pilastri fondamentali del progetto:

- La separazione delle reti: e' stato scelto di progettare due reti separate e largamente indipendenti in modo da rendere piu' agevole l'installazione e il mantenimento, inoltre un eventuale fallimento dell'infrastruttura in uno dei due edifici non penalizzerebbe la didattica all'interno del secondo plesso.
- L'utilizzo di indirizzamento statico per i dispositivi fissi, propri dell'istituto (quali, per esempio, postazioni all'interno dei laboratori informatici in ambo i plessi), estremamente utile per mantenere un' estrema semplicita' di gestione e di troubleshooting.
- Filtraggio di tutto il traffico da parte di router/firewall che agiscono da endpoint per ognuno dei due plessi, cio' permette di innalzare lo standard di sicurezza, in quanto tutto il traffico nella sua interezza viene analizzato.
- Connessione dei due plessi tramite l'ausilio di una *VPN* gestita da due *New Generation Firewall*, che fungono anche da endpoint per entrambe le reti.

Andremo ora a spiegare nel dettaglio l'architettura, aiutati dal diagramma di rete redatto tramite il precedentemente citato strumento di creazione grafici e diagrammi *Draw.io*.

3.2 Il Diagramma

La rete nel suo complesso puo' essere riassunta tramite l'ausilio del seguente diagramma:

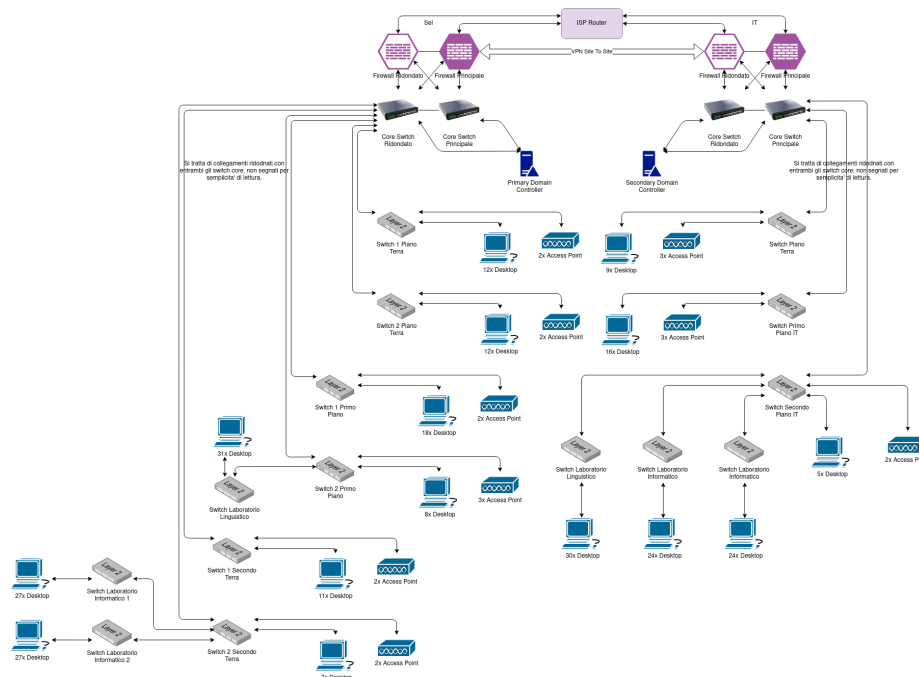


Immagine 3.1: Topologia di rete per ambo i plessi scolastici.

Partendo dall'alto, possiamo subito notare la disposizione e la configurazione dei *New Generation Firewall*, data l'enorme importanza che ricoprono all'interno della nostra infrastruttura, abbiamo deciso di optare per la ridondanza dell'intera macchina fisica, cio' permette di mitigare qualsiasi problema di compromissione anche fisica dell'apparato. Data la complessita' del soggetto, abbiamo deciso di dedicare una sezione a parte all' argomento *gestione New Generation Firewall e VPN* durante un successivo capitolo.

Un approccio simile e' stato adottato anche per quanto riguarda la gestione dei *Core Switch*, essendo il cardine della rete per quanto riguarda l'instradamento dei pacchetti, e' stato scelto di ridondarli fisicamente permettendo quindi una piu' elevata tolleranza ad eventuali guasti. In generale, l'intera struttura di rete e' gerarchica, composta da un massimo di tre livelli. Il primo e' rappresentato dai due *Core Switch* appena descritti, poi seguono un numero di apparati di "*Secondo Livello*" pari a sei nel primo plesso e a tre nel seconodo. Per terminare con alcuni *Switch* interni ai vari laboratori, denominati come di "*Terzo Livello*".

Continuando verso il basso, possiamo notare il posizionamento dei due *Do*-

main Controller, collegati direttamente con entrambi i *Core Switch* in maniera da poter mantenere la continuita' del servizio a prescindere dallo switch in uso in quel momento. Per via della necessita' di contenere i costi, abbiamo optato per non ridondare fisicamente tutte le macchine al di sotto del "*Secondo Livello*". Cio' ovviamente potrebbe compromettere l'accesso ad *Active Directory* a tutta l'area coperta da uno switch di "*Secondo*" o "*Terzo*" livello.

Sullo schema di rete e' poi illustrato il numero di postazioni *Desktop* collegati allo *Switch*, insieme al numero di *Access Point* atti a creare un uniforme copertura wireless per l'intera di entrambi i plessi.

Capitolo 4

Sicurezza E Firewall

Serena Thomas Come precedentemente specificato, per la gestione *Firewall* abbiamo optato per il depoloy di un totale di quattro macchine fisiche, ridondate due a due. Essendo esse gli endpoint di entrambe le reti semi-indipendenti presenti nei due plessi scolastici, assicurarne il corretto funzionamento e' essenziale per poter mantenere il servizio.

I firewall sono direttamente connessi all'provider tramite connessione a **Inserire Larghezza Della Banda**, come si puo' notare non sono presenti *Router* all'interno dell'infrastruttura, cio' perche' abbiamo scelto di accorpate gli apparati per poter contenere i costi e mantenere comunque alto lo standard qualitativo.

Capitolo 5

Microsoft Active Directory e Windows Licensing

Catone Mario

5.1 Domain Controller

L'ambiente *MS Active Directory* e' il cuore pulsante dell'intera infrastruttura di rete, in quanto tutta la gestione dell'autenticazione, e dei relativi permessi dedicati a ogni singolo utente, dagli amministratori di sistema agli studenti, viene gestita tramite quest'importante servizio. Abbiamo optato per una configurazione basata su due domain controller, uno per plesso, in modo da garantire la continuita' del servizio anche in caso di problemi hardware. Le macchine sono strutturate come segue:

- DC01:
 - Dell Smart Value PowerEdge R240
 - * Xeon E-2234 (4c/8t).
 - * 1x16GB UDIMM ECC 3200MT/s.
 - * 2x4TB HDD 7.2k RPM 512n.
 - * Dual Port 1Gb ethernet card.
 - Windows Server 2019 Standard Edition Desktop Experience.

- DC02:
 - Dell Smart Value PowerEdge R240
 - * Xeon E-2234 (4c/8t).
 - * 1x16GB UDIMM ECC 3200MT/s.
 - * 2x4TB HDD 7.2k RPM 512n.
 - * Dual Port 1Gb ethernet card.
 - Windows Server 2019 Standard Edition Desktop Experience.

Le macchine sopracitate, seppur dotate di perfomance modeste in relazione agli standard odierni, offrono un ottimo rapporto qualita' prezzo, inoltre, entrambi i *Domain Controller* non si troveranno a gestire mansioni particolarmente intensive dal punto di vista computazionale. Le funzioni principali di queste due macchine sono sintetizzabili come segue:

1. Server di autenticazione per l'intera infrastruttura.
2. Gestione Shared Directory.
3. Gestione Roaming Profiles.

5.1.1 Server Di Autenticazione

Il ruolo di **Server Di Autenticazione** da parte del *Domain Controller* e' di vitale importanza per il corretto funzionamento dell'infrastruttura nel suo complesso. Esso permette di gestire su base di gruppi o di singoli utenti molti aspetti dell'esperienza utente, che possono variare dalla configurazione dell'ambiente desktop e del menu' start, a eventuali permessi di scrittura, lettura e amministrazione di directory condivise, fino alla possibilita' di amministrare il sistema nella sua interezza.

In tutto cio' le *Organizational Unit*, anche dette **OU**, assumono un ruolo fondamentale. Si tratta di "Cartelle", atte a organizzare gli utenti in sottogruppi per renderne la gestione piu' agevole, nel nostro caso, abbiamo ritenuto opportuno suddividere gli utenti come segue:

- Liceo Scientifico delle Scienze Applicate a Indirizzo Informatico:
 - OU "*Studenti Liceo Scientifico*"
 - OU "*Docenti Liceo Scientifico*"
 - OU "*Personale Amministrativo Scientifico*"
- Liceo Linguistico:
 - OU "*Studenti Liceo Linguistico*"
 - OU "*Docenti Liceo Linguistico*"
 - OU "*Personale Amministrativo Linguistico*"

- Istituto Tecnico Economico:
 - OU "*Studenti Tecnico Economico*"
 - OU "*Docenti Tecnico Economico*"
 - OU "*Personale Amministrativo Tecnico Economico*"
- OU "*Sysadmin*"
- OU "*Personale ATA*"

I motivi di questa particolare suddivisione sono presto detti, innanzitutto la necessita' di dividere gli amministratori di sistema (*Sysadmin*) da qualunque altro utente in maniera tale da rendere semplice e intuitiva la gestione dei permessi per questi soggetti.

Per cio' che riguarda Studenti e Docenti si e' invece scelto di operare una macro suddivisione a livello di istituto, esso permette ad esempio agli studenti afferenti alla **OU** *Studenti Liceo Scientifico* di essere facilmente separabili rispetto a quelli presenti in *Studenti Tecnico Economico*. Sono poi previste unita' organizzative figlie per effettuare divisioni successive delle unita' *Studenti* raggruppando i soggetti per sezione e per anno, in modo da rendere agile la creazione e la condivisione di cartelle e documenti tra studenti e professori.

Come per gli studenti e i docenti, il personale amministrativo e' suddiviso per istituto e successivamente per mansione, cio' si e' reso necessario data l'estrema confidenzialita' di alcuni dati trattati dalla segreteria didattica.

Infine, e' stata creata una **OU** per gestire gli account del personale che necessita' di un accesso minimale all'infrastruttura, come ad esempio il personale in reception.

Da notare come gli account utente di Preside e Vicepreside sono stati lasciati al di fuori della classificazione, data la particolarita' e unicità dei loro ruoli.

5.1.2 Gestione Shared Directory

Durante l'analisi portata avanti, abbiamo riscontrato la necessita' di creare tre **Shared Directory** principali per ognuno dei tre differenti indirizzi che compongono il nostro caso di studio, che vanno poi a coniugarsi in ulteriori suddivisioni per assicurare la granularita' richiesta. Esse sono configurate come segue:

- Shared Directory "*Studenti*":
 - Ulteriormente suddivisa per rispecchiare materie, sezioni e anni scolastici.
 - *Studenti* hanno permessi di scrittura all'interno delle sottocartelle relative alla loro sezione, anno e materia.
 - *Studenti* hanno in ogni caso permessi limitati esclusivamente ai documenti prodotti da loro stessi. Limitando quindi azioni su documenti di colleghi o *Docenti*.

- *Docenti* hanno permessi di controllo completo sulla **Directory** padre e su tutte le derivate, ad eccezione della possibilità di modificarne la struttura in se (suddivisione in anno, sezione ecc.).
- *Docenti* hanno permessi di lettura verso i documenti creati da altri soggetti all'interno della stessa **OU** tuttavia non di modifica.
- Shared Directory "*Docenti*":
 - Ulteriormente suddivisa in un numero di cartelle pari al numero di *Docenti*.
 - *Studenti* hanno permessi in sola lettura sull'intera **Directory**.
 - *Docenti* hanno "*Full Control*" sull'intera directory, come sopra l'unica limitazione riguarda la possibilità di modificarne la struttura.
- Shared Directory "*Amministrativo*"
 - Date le particolari necessità dal punto di vista della privacy, *Docenti* e *Studenti* non avranno nessun accesso alla **Directory**.
 - *Sysadmin*, *Personale Amministrativo* e gli account singoli di *Presidente* e *Vicepresidente* avranno permessi di controllo totale sulla **Directory**, compresa la possibilità di modificarne la struttura in caso di necessità.

Da segnalare come *Presidente*, *Vicepresidente* e l'intera **OU Sysadmin** siano muniti di "*Full Control*" su l'intera **Directory** *Docenti* e *Studenti*, come di consueto ad eccezione della possibilità di modificarne la struttura.

5.1.3 Gestione Roaming Profiles

La gestione dei **Roaming Profiles** è sicuramente una sezione fondamentale dell'infrastruttura *Active Directory* da noi proposta. Tramite opportune configurazioni è possibile associare a ciascun account un differente profilo, in questo modo un utente può effettuare il log-in da un qualsiasi computer collegato all'infrastruttura e mantenere tutti i suoi file e permessi. Ciò permette un duplice beneficio, mobilità e sicurezza. Innanzitutto è da considerare come un qualsiasi studente o professore possa accedere ai suoi progetti e dati da qualsiasi macchina all'interno di entrambi i gruppi di edifici facenti parte del complesso scolastico. Dal punto di vista della sicurezza invece possiamo notare come la gestione dei permessi è relativa al login dell'utente, non alla macchina in se. Ciò rende l'infrastruttura più sicura, in quanto la condizione di accesso si sposta dal semplice accesso fisico alla macchina, all'ottenimento dei dati di accesso di un account con privilegi elevati.

Capitolo 6

Considerazioni Finali