LONZI MARTINA
5BM 14/4/2025

Sommario

PROBLEMA O DESCRIZIONE SPECIFICHE

Un comune vuole introdurre il servizio **BiblioFun** come soluzione cloud, integrandolo con la gestione tradizionale della biblioteca. Questo servizio consente agli utenti di consultare e leggere libri online, prenotarli e ritirarli fisicamente in biblioteca. Dopo la registrazione sul portale, gli utenti possono accedere a vari servizi, inclusi la catalogazione dei libri, la gestione delle prenotazioni, dei prestiti, delle proroghe e delle restituzioni.

BiblioFun offre un catalogo aggiornato di libri cartacei e digitali, con una scheda per ogni libro che include informazioni come titolo, autore, genere, numero di pagine e trama. Gli utenti, una volta loggati, possono cercare libri, leggerli online, prenotarli per il ritiro, e controllare i propri prestiti. Il servizio è accessibile anche da dispositivi mobili.

La biblioteca è divisa in due piani: uno per il magazzino dei libri non esposti e uno per il pubblico. Gli utenti possono utilizzare 10 postazioni fisse o la rete Wi-Fi tramite le proprie credenziali. Ci sono anche due postazioni per i bibliotecari che gestiscono i lettori e i prestiti, oltre a postazioni nel magazzino per l'accesso al database e al sito web. L'accesso a Internet è libero per l'uso dei servizi web.

ANALISI QUALITATIVA DEL PROBLEMA E DESCRIZIONE LOGICA DEI MACROELEMENTI DEL SISTEMA

La rete da realizzare sarà composta da dei clienti, che possono essere fisicamente nella biblioteca o remoti tramite una connessione a internet e le opportune credenziali.

La biblioteca e la relativa struttura di cablaggio sarà divisa in due piani:

1. Il magazzino in cui saranno presenti 2 postazioni per i bibliotecari per accogliere i lettori e gestire i prestiti.
2. Sarà il piano pubblico per tutti coloro che verranno accolti in biblioteca in cui saranno inserite 10 postazioni fisse per accedere al servizio web.

In aggiunta nell'edificio è presente il servizio wi-fi a cui gli utenti si possono connettersi attraverso le stesse credenziali di registrazione per il sito.

Nella rete saranno installati due server , uno web e l'altro dns nella DMS in modo da essere pubblici e visibili anche dagli utenti non all'interno della struttura.

Saranno invece presenti e privati, nella rete intranet i server dhcp per assegnare in modo dinamico gli indirizzi all'interno della struttura e un database che si occupa della memorizzazione di tutti i file.

SCHEMA

BiblioFun è un sistema complesso che deve gestire molte funzionalità diverse: la consultazione del catalogo, la prenotazione e il prestito di libri, la lettura online e la gestione degli utenti. Per far funzionare tutto in modo fluido, sicuro e scalabile si è optato per un'architettura **3-tier**, che divide il sistema in tre livelli logici ben distinti:

1. Presentation-tier (web server)

Rappresenta l'interfaccia web che le persone utilizzano ogni giorno. Che accedano dal cellulare, dal tablet o da uno dei computer in biblioteca, troveranno sempre un'interfaccia chiara e reattiva.

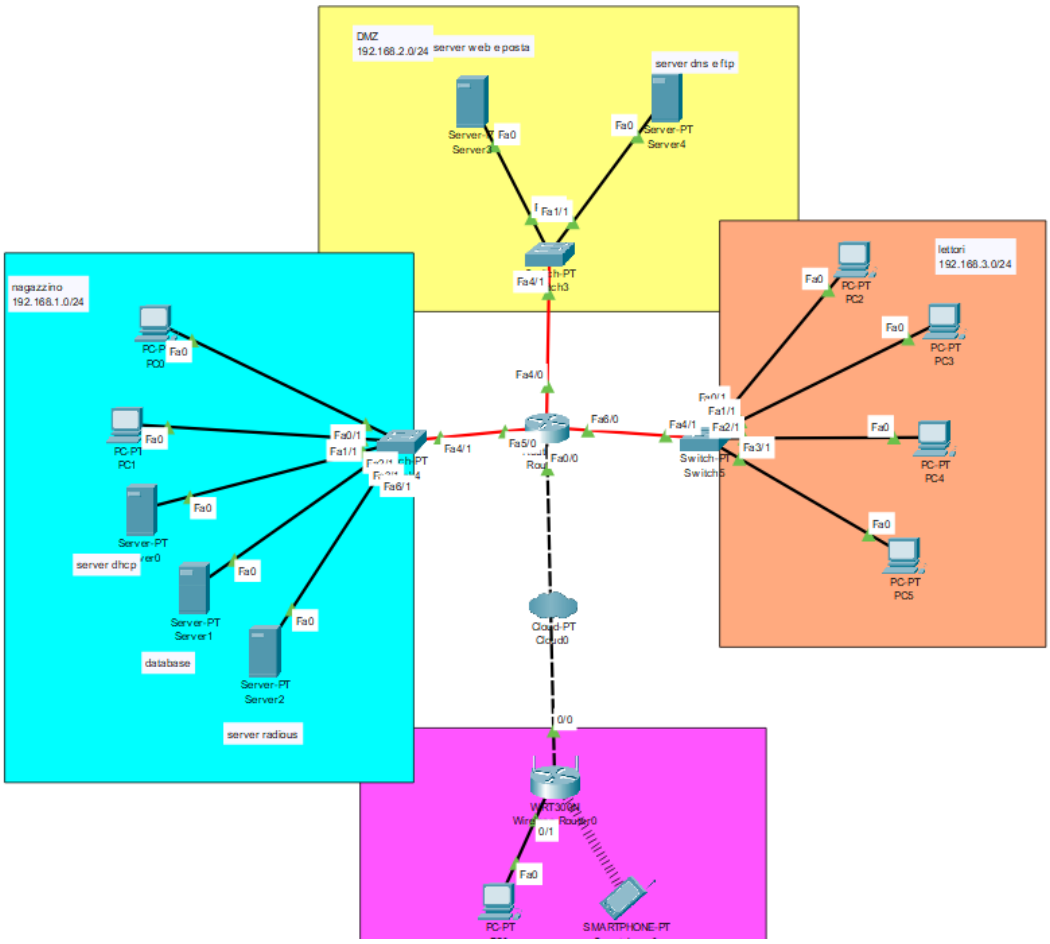
2. Business-tier (applications server)

Qui vengono elaborate tutte le richieste del cliente e produce i risultati da inoltrare come risposta.
Si è scelto di isolare questa parte perché:

→ Se il servizio diventa più popolare, possiamo potenziare solo questa sezione

→ Le regole (come il numero massimo di prestiti) possono essere modificate facilmente

3. **Data-tier (DBMS server)**
   Tutte le informazioni dai cataloghi ai dati personali sono custodite nel database in modo sicuro.



ANALISI E DESCRIZIONE COMPONENTI E DISPOSITIVI DI RETE

La rete è stata realizzata attraverso questi indirizzi:

NOME	INDIRIZZO RETE	MASCHERA	GATEWAY	BROADCAST
Magazzino	192.168.1.0/24	255.255.255.0	192.168.1.1	192.168.1.255
DMZ	192.168.2.0/24	255.255.255.0	192.168.2.1	192.168.2.255
Lettori	192.168.3.0/24	255.255.255.0	192.168.3.1	192.168.3.255

Sono state implementate tutte reti di classe in C in modo tale da rientrare in modo ampiamente all'interno delle richieste, ma così si avrà la possibilità di per esempio le postazioni lettori.

La configurazione del router è avvenuta tramite questi indirizzi:

INTERFACCIA	INDIRIZZO IPV4	MASCHERA
Fa5/0	192.168.1.1	255.255.255.0
Fa4/0	192.168.2.1	255.255.255.0
Fa6/0	192.168.3.1	255.255.255.0

La configurazione dei server è avvenuta tramite questi indirizzi:

NOME RETE APPARTENENZA	SERVIZI CHE OFFRE	INDIRIZZO IP	MASCHERA	GATEWAY	DNS SERVER
magazzino	DHCP	192.168.1.2	255.255.255.0	192.168.1.1	192.168.2.3
Magazzino	DATABASE	192.168.1.3	255.255.255.0	192.168.1.1	192.168.2.3
Magazzino	RADIUS	192.168.1.3	255.255.255.0	192.168.1.1	192.168.2.3
DMZ	http e POSTA	192.168.2.2	255.255.255.0	192.168.2.1	192.168.2.3
DMZ	DNS e FTP	192.168.2.3	255.255.255.0	192.168.2.1	192.168.2.3

In questa rete il server DNS del server che offre il servizio DNS è sé stesso, ma di consuetudine viene inserito il server DNS gerarchicamente più alto.

COMPONENTI:

ROUTER: Il router costituisce l'elemento centrale dell'infrastruttura di rete, svolgendo la funzione di instradamento del traffico tra le diverse sottoreti logiche: rete del magazzino, rete degli utenti lettori, rete DMZ e rete wireless. Tra le principali funzionalità configurabili figurano il routing statico o dinamico, il Network Address Translation (NAT) per l'accesso esterno, il relay DHCP per la distribuzione centralizzata degli indirizzi IP, nonché l'implementazione di ACL (Access Control Lists) per il controllo granulare del traffico in transito. Tali caratteristiche rendono il router un componente essenziale per la sicurezza, la segmentazione e l'efficienza della rete BiblioFun.

SWITCH: Lo switch è un dispositivo di rete di livello 2 del modello ISO/OSI, progettato per smistare i pacchetti di dati all'interno di una rete locale (LAN), indirizzandoli esclusivamente alla porta di destinazione corrispondente. A differenza dell'hub, che inoltra i dati a tutte le porte indistintamente, lo switch analizza l'indirizzo MAC di ciascun dispositivo per garantire una trasmissione efficiente e sicura.
Nell'architettura di rete BiblioFun, vengono utilizzati switch per la connessione fisica dei vari nodi all'interno delle seguenti aree funzionali: magazzino, sala lettori e DMZ. Ogni area dispone di uno switch dedicato, collegato centralmente al router principale tramite interfacce in fibra.

I dispositivi impiegati sono switch dotati di 10 porte, di cui almeno una o più porte in fibra ottica (tipicamente con moduli SFP), per garantire una connettività ad alta velocità e a bassa latenza verso il router principale. Le porte restanti, di tipo FastEthernet sono dedicate alla connessione dei dispositivi locali.

CABLAGGIO: La connettività fisica dell'infrastruttura di rete è realizzata attraverso una soluzione mista fibra-rame, in grado di garantire alte prestazioni, affidabilità e scalabilità.
I collegamenti tra il router principale e gli switch di accesso avvengono tramite fibra ottica monomodale, per supportare velocità di trasmissione fino a 10 Gbps, riducendo al minimo la latenza e il degrado del segnale anche su distanze medio-lunghe all'interno dell'edificio.
Per la distribuzione locale del segnale invece i collegamenti tra gli switch e i dispositivi sono realizzati mediante cavi in rame di categoria 7, con connettori RJ45 schermati (STP). Questa tipologia di cablaggio supporta velocità fino a 10 Gbps, mentre i cavi straight-through sono utilizzati per le connessioni standard tra switch e host.

SERVER**:** La rete dispone di diversi server, ciascuno con un ruolo specifico. Nella DMZ troviamo il server web, che ospita il portale BiblioFun accessibile via browser, e il server DNS, che gestisce la risoluzione dei nomi di dominio sia per gli utenti locali che per quelli che si connettono da remoto. Questo posizionamento nella DMZ è fondamentale per permettere l'accesso sicuro e pubblico ai servizi di risoluzione dei nomi, anche da parte degli utenti esterni alla rete aziendale.
All'interno dello stesso server DNS, oltre alla gestione DNS, è presente anche il servizio FTP, che consente all'amministratore di trasferire, inserire o modificare file all'interno del sistema in modo sicuro e efficiente.
Nella rete del magazzino sono presenti il server DHCP, responsabile dell'assegnazione automatica degli indirizzi IP ai client, e il server database, che conserva tutte le informazioni sul catalogo, utenti e prestiti.
Inoltre, all'interno della rete aziendale troviamo anche un server Radius per la gestione e l'autenticazione degli utenti, utilizzato per il controllo degli accessi alle risorse di rete.
Nel server web, oltre al portale BiblioFun, è attivo anche il servizio di posta, che gestisce l'invio di e-mail, ad esempio per inviare promozioni, notifiche di eventi o aggiornamenti ai clienti, migliorando la comunicazione con gli utenti.

ANALISI SERVIZI E PROTOCOLLI

SERVIZIO DHCP

Il **protocollo DHCP** è un protocollo di rete che consente agli host di ottenere automaticamente un indirizzo IP e altre informazioni di configurazione (come gateway e DNS) da un server DHCP, senza la necessità di configurazioni manuali.

Questo servizio può essere svolto da un server o dal router.

Funzionamento di base:

1. **DHCP Discover**: Quando un dispositivo si connette a una rete, invia un messaggio in broadcast per trovare un server DHCP disponibile.
2. **DHCP Offer**: Il server DHCP risponde con un messaggio proponendo un indirizzo IP e altre informazioni di configurazione.
3. **DHCP Request**: Il dispositivo risponde con un messaggio confermando che accetta l'indirizzo IP offerto.

4. **DHCP Acknowledgment (ACK)**: Il server invia un messaggio per confermare l'assegnazione dell'indirizzo IP e completare la configurazione.

SERVIZIO WEB

Il **protocollo HTTP** è un protocollo di comunicazione utilizzato per il trasferimento di informazioni su una rete, in particolare tra un client e un server. È il protocollo principale utilizzato per la trasmissione di pagine web e di contenuti multimediali.

HTTP segue un modello client-server:

- **Client**: l'entità che effettua una richiesta, ad esempio, un browser che richiede una pagina web.
- **Server**: l'entità che risponde alla richiesta inviando le risorse richieste come pagine HTML, immagini, file.

Una richiesta HTTP è composta da:

1. **Metodo**: Indica l'azione da eseguire (GET, POST, ecc.).
2. **URL**: Specifica l'indirizzo della risorsa richiesta.
3. **Versione del protocollo**: (es. HTTP/1.1 o HTTP/2).
4. **Headers**: Informazioni aggiuntive come tipo di contenuto accettato, cookie, ecc.

Per impostazione predefinita, HTTP utilizza la **porta 80**. Nel caso di **HTTPS**, che è la versione sicura di HTTP con crittografia SSL/TLS, viene utilizzata la **porta 443**.

SERVIZIO DI POSTA

Il **servizio di posta elettronica** (E-mail) permette lo scambio di messaggi digitali tra utenti attraverso Internet o altre reti di comunicazione. Per inviare, ricevere e gestire le e-mail, si utilizzano dei protocolli standard che operano su specifiche porte di rete.

Esso utilizza due protocolli principali:

1. **SMTP (Simple Mail Transfer Protocol)**: per inviare e-mail.
    - **Porta 25** (non crittografata), **587** (con TLS), **465** (con SSL).
2. **POP3 (Post Office Protocol)**: per scaricare le e-mail sul dispositivo.
    - **Porta 110** (non crittografata), **995** (con SSL/TLS).

SERVIZIO DI TRASFERIMENTO FILE

Il **protocollo FTP** è un protocollo standard utilizzato per il trasferimento di file tra un client e un server. È uno dei metodi più datati e più comuni per caricare, scaricare e gestire file in remoto.

Caratteristiche principali:

1. **Architettura Client-Server**: il client si connette al server FTP per trasferire file.
2. **Modalità di trasferimento**: può operare in due modalità:
    - **Modalità attiva**: il client apre una porta per ricevere i dati e il server si connette a questa porta.

- **Modalità passiva**: il client richiede al server di aprire una porta per ricevere i dati, facilitando il superamento di firewall.

3. **Autenticazione**: può essere anonima o autenticata con username e password.

Porte utilizzate:

- **Porta 21**: utilizzata per il controllo della connessione (invio comandi e risposte).
- **Porta 20**: utilizzata per il trasferimento dati nella modalità attiva. Tuttavia, nella modalità passiva, la porta utilizzata per i dati è assegnata dinamicamente dal server.

SERVIZIO DI RISOLUZIONE DEI NOMI

Il protocollo **DNS** è un protocollo fondamentale di rete utilizzato per la risoluzione dei nomi di dominio in indirizzi IP, rendendo possibile la navigazione su Internet. Senza DNS, gli utenti sarebbero costretti a ricordare gli indirizzi IP numerici di ogni sito web, invece dei nomi di dominio leggibili.

Di solito le richieste DNS utilizzano **UDP** sulla porta **53**, perché il protocollo è veloce e la maggior parte delle query richiedono solo una singola risposta breve.

Fasi del funzionamento del DNS:

1. **Richiesta**: L'utente scrive un URL nel browser.
2. **Resolver**: Il dispositivo invia una richiesta a un server DNS per ottenere l'indirizzo IP.
3. **Root Server**: Se necessario, il server contatta i root server per trovare il server giusto.
4. **Server TLD**: Il server TLD indica il server autoritativo del dominio.
5. **Server Autoritativo**: Il server autoritativo restituisce l'indirizzo IP del dominio.
6. **Risposta**: Il resolver invia l'indirizzo IP al browser, che si connette al sito web.

SERVER RADIOUS

Il **server RADIUS** è un componente fondamentale per la gestione dell'accesso alle risorse di rete aziendali, che opera attraverso tre principali funzionalità: autenticazione, autorizzazione e contabilizzazione.

1. **Autenticazione**: Il server RADIUS verifica l'identità degli utenti che tentano di accedere alla rete, confrontando le credenziali (tipicamente nome utente e password) con quelle memorizzate in un sistema di gestione centralizzato. Se le credenziali sono valide, l'utente viene autorizzato ad accedere alla rete.

2. **Autorizzazione**: Una volta autenticato, il server RADIUS determina quali risorse o servizi l'utente è autorizzato a utilizzare. Questa fase è regolata dalle politiche aziendali, che possono prendere in considerazione fattori come il ruolo dell'utente, l'orario di accesso o la posizione geografica.

3. **Contabilizzazione**: Il server tiene traccia di tutte le attività degli utenti all'interno della rete, come i dettagli delle sessioni di accesso (ad esempio, orari di inizio e fine), la quantità di dati trasferiti e altre informazioni rilevanti. Questo permette un monitoraggio accurato dell'utilizzo delle risorse di rete, utile sia per motivi di sicurezza che per eventuali attività di fatturazione.

CONFIGURAZIONE

Per configurare il router bisogna:

- Entrare nel router
- Andare nella sezione Config
- Nella sezione Interfacce, settare le interfacce interessate inserendo l'indirizzo IP e la sua rispettiva maschera

Per la configurazione dei vari server:

- PARTE COMUNE:
  - Entrare nel server
  - Andare nella sezione Desktop e poi IP Configuration
  - Inserire in modo statico l'indirizzo IP, la maschera, il gateway e il DNS server
- PER IL SERVER CHE SI OCCUPA DEL SERVIZIO DHCP:
  - Entrare nella sezione services
  - Selezionare il servizio DHCP
  - Inserimento di tutte le informazioni richieste
- PER IL SERVER CHE SI OCCUPA DEL SERVIZIO http
  - Entrare nella sezione services
  - Selezionare il servizio http
  - Creare il file html che poi potrà essere richiamato
- PER IL SERVER CHE SI OCCUPA DEL SERVIZIO DI POSTA
  - Entrare nella sezione services
  - Selezionare il servizio EMAIL
  - Inserimento del Dominio e creare user e password.
- PER IL SERVER CHE SI OCCUPA DEL SERVIZIO DI DNS
  - Entrare nella sezione services
  - Selezionare il servizio DNS
  - Inserimento del nome simbolico e dell'indirizzo ad esso associato
- PER IL SERVER CHE SI OCCUPA DEL SERVIZIO DI FTP
  - Entrare nella sezione services
  - Selezionare il servizio FTP
  - Inserimento dell'username e della password e delle relative autorizzazioni
- Per la configurazione degli host avviene tutto in modo dinamico grazie al server DHCP.

SICUREZZA

Sicurezza Perimetrale e Controllo degli Accessi

La protezione della rete della biblioteca deve partire dalla sicurezza perimetrale, per evitare accessi non autorizzati e proteggere i dati sensibili. La prima linea di difesa è rappresentata dai firewall, che devono essere configurati per controllare il traffico in entrata e in uscita, e per definire regole di accesso specifiche in modo che solo gli utenti legittimi possano interagire con i servizi online. Inoltre, è fondamentale implementare una DMZ (Demilitarized Zone), che funge da zona separata per i server che devono essere accessibili al pubblico, come i web server che ospitano il portale BiblioFun, e quelli interni, come i database server o i sistemi di gestione del catalogo e dei prestiti. La DMZ aiuta a isolare i servizi pubblici da quelli sensibili, riducendo il

rischio che un eventuale attacco a uno dei server esterni possa compromettere l'intera rete interna della biblioteca.

Un esempio pratico di Access Control List (ACL) da implementare potrebbe essere il seguente:

Permettere l'accesso HTTP(S) al Web Server dalla rete esterna (Internet):

access-list 100 permit tcp any host 192.168.1.10 eq 80

access-list 100 permit tcp any host 192.168.1.10 eq 443

PAT

Per proteggere gli indirizzi IP interni della biblioteca e consentire agli utenti di navigare su Internet, si utilizza PAT (Port Address Translation). Il PAT consente di mascherare gli indirizzi IP privati all'interno della rete, traducendoli in un unico indirizzo IP pubblico per tutte le connessioni in uscita. Questo processo è più veloce e semplice rispetto al NAT tradizionale, poiché utilizza un singolo indirizzo IP pubblico per molti dispositivi interni, migliorando l'efficienza nella gestione del traffico e riducendo il numero di indirizzi IP necessari. Inoltre, il PAT aumenta la sicurezza, poiché gli indirizzi IP interni non sono visibili su Internet.

VPN

La VPN (Virtual Private Network) è un altro strumento fondamentale per garantire che la comunicazione tra gli utenti e i servizi web avvenga in modo sicuro. Utilizzando una VPN, tutte le connessioni saranno criptate, proteggendo i dati sensibili degli utenti, come le credenziali di accesso e le informazioni relative ai prestiti, da eventuali intercettazioni o attacchi.

Crittografia

La crittografia è fondamentale per proteggere le comunicazioni all'interno della rete della biblioteca. Per garantire una protezione robusta, tutte le connessioni devono utilizzare il protocollo TLS (Transport Layer Security), che è più sicuro rispetto ai protocolli precedenti, come SSL. TLS assicura che i dati scambiati tra il client (ad esempio, il dispositivo dell'utente) e il server della biblioteca siano cifrati, prevenendo intercettazioni e manomissioni. Inoltre, per le connessioni VPN, è consigliabile utilizzare algoritmi di cifratura avanzati come DES, che assicura una protezione elevata dei dati durante il loro transito, mantenendo così la sicurezza delle informazioni sensibili.

Gestione Sicura degli Utenti

Poiché gli utenti devono registrarsi e accedere ai servizi della biblioteca, è cruciale implementare un sistema di autenticazione sicura. L'adozione di un sistema di autenticazione a più fattori aggiunge un ulteriore livello di protezione, riducendo il rischio di accessi non autorizzati. Inoltre, i privilegi di accesso devono essere gestiti in modo rigoroso, con accesso limitato per i bibliotecari e per gli amministratori in base al ruolo e alle necessità specifiche.

SIMULAZIONE E TEST

La verifica della rete è stata realizzata volta per volta quando si inserivano e configuravano ogni parte della rete attraverso dei ping.

1. Realizzato il collegamento degli switch al router si è mandato un ping da uno switch all'altro e viceversa in modo tale da verificare se riuscissero a comunicare.
2. Inseriti nella sottorete di sinistra tutti gli host e il server per il servizio DHCP configurato, per provare se esso funziona si entra in ogni host per costatare se l'assegnazione è andata a buon fine. Successivamente si controlla se gli host riescono a comunicare inviandosi ping a vicenda.
3. Inseriti e configurati tutti i server si controlla sempre attraverso dei ping se i computer riescono a comunicare con i vari server.
4. Quando si è costatato che tutti riescono a comunicare si comincia a configurare i vari servizi.
5. Configurato il servizio http per costatarne il funzionamento, dagli host si richiama quella determinata pagina web, che precedentemente è stata inserita nel server.
6. Configurato il servizio di posta, per verificarne il funzionamento, si assegnano a due host due indirizzi e-mail che sono inseriti nel server e attraverso lo scambio di un'e-mail si verifica se è stato configurato tutto bene.
7. Configurato il server FTP, attraverso il pront dei comandi di un host, entrando con le credenziali inserite nel server, verifico tutto ciò che posso fare se corrisponde alle autorizzazioni attribuite.
8. Configurato il servizio DNS per verificarne il funzionamento, si è attribuita la pagina web, precedentemente creata, a un indirizzo simbolico. Successivamente attraverso il browser dei computer si è verificato se inserendo quell'indirizzo simbolico portasse alla visualizzazione di quella pagina.
9. Infine si verificano se le ACL sono configurare in modo opportuno

CONCLUSIONE

L'infrastruttura proposta per BiblioFun garantisce sicurezza, efficienza e scalabilità per una gestione moderna e affidabile della biblioteca comunale. L'adozione delle tecnologie descritte permetterà di offrire un servizio digitale innovativo, accessibile e sicuro sia per gli utenti che per il personale bibliotecario.
Come possibile sviluppo futuro, si propone anche la realizzazione di una app mobile dedicata per dispositivi iOS e Android, che consenta un accesso più rapido e funzionale ai servizi offerti da BiblioFun, come la consultazione del catalogo, prenotazioni e lettura online, rendendo l'esperienza utente ancora più completa e intuitiva.