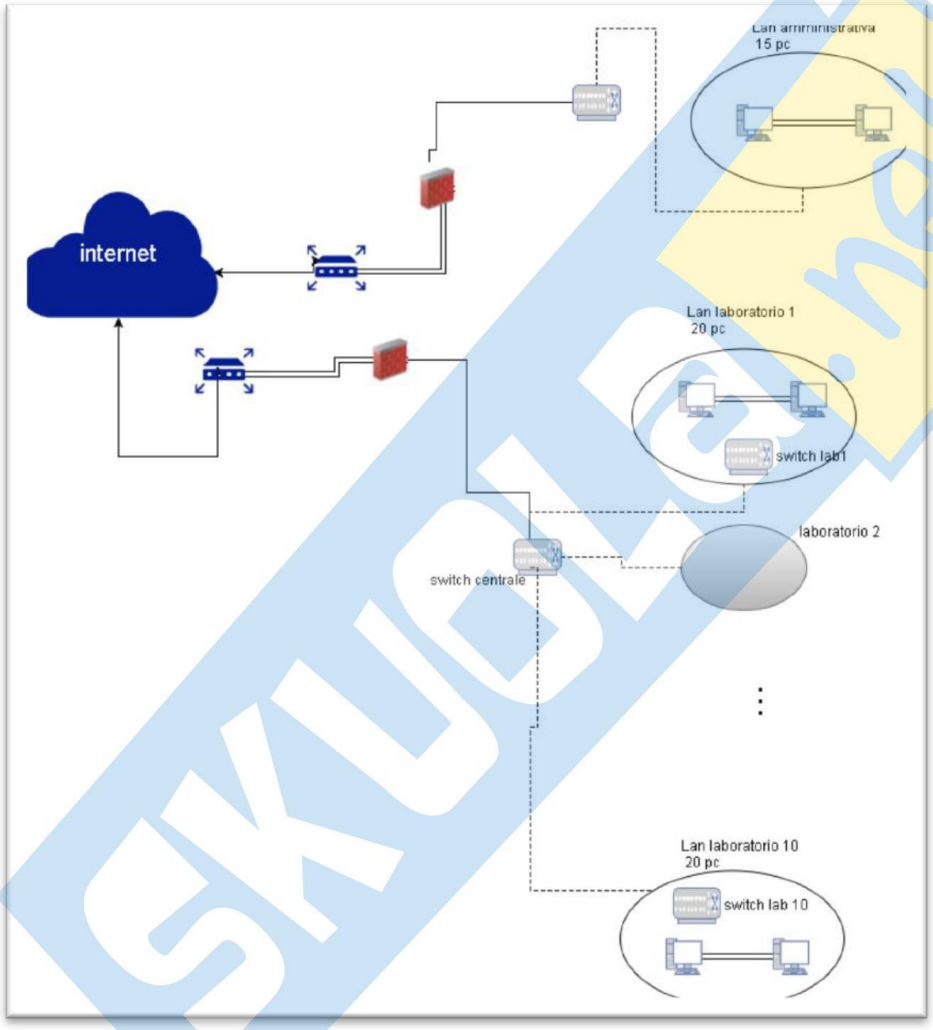
PROPOSTA DI SOLUZIONE PER LA SECONDA PROVA DI MATURITÀ 2016
TRACCIA: Sistemi e reti

Parte 1

Si ipotizza che tutti i laboratori didattici siano al piano superiore dell'edificio e quindi il cablaggio può avvenire tramite cavi non troppo lunghi.

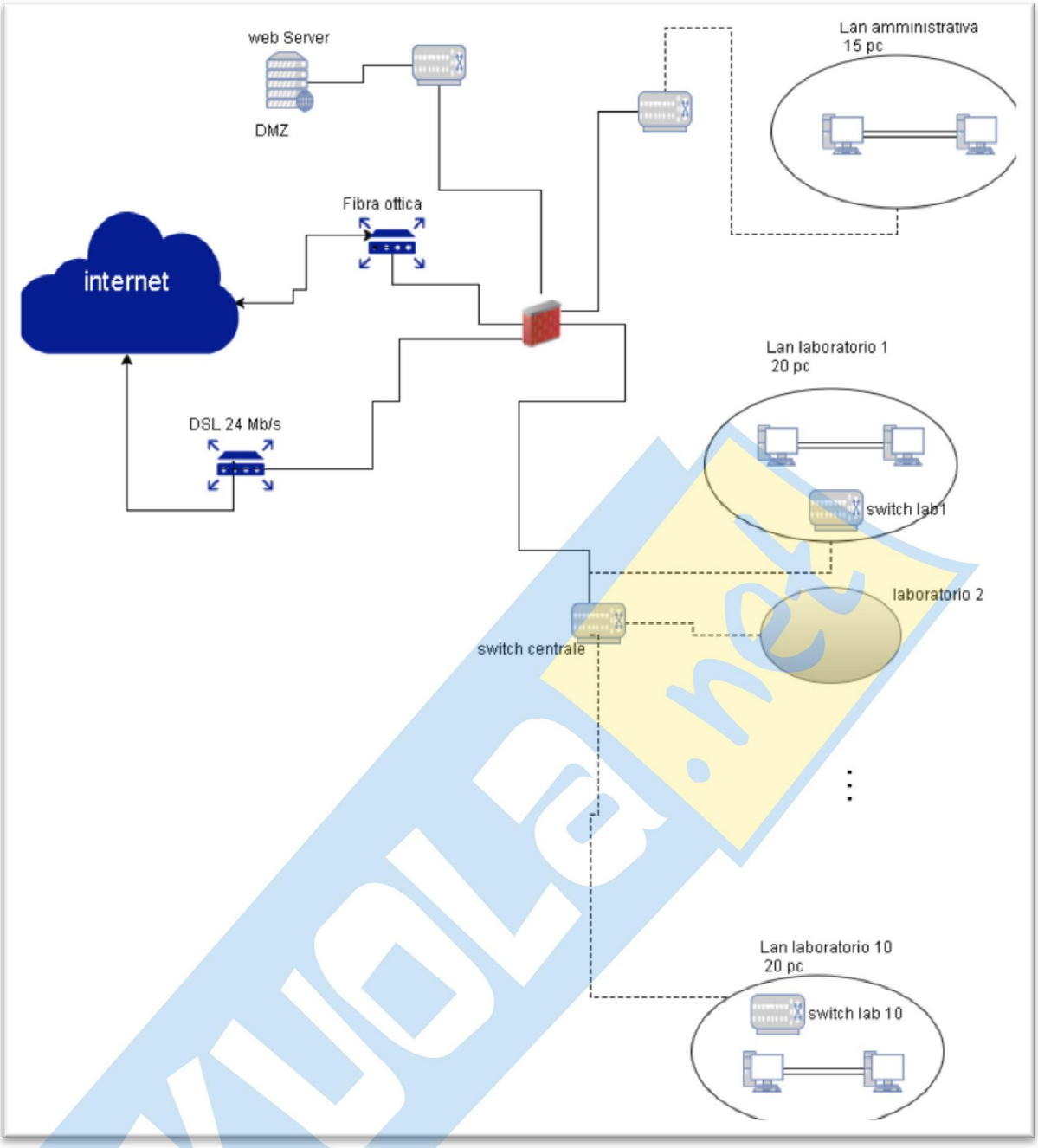
1. Lo schema logico dell` infrastruttura presente potrebbe essere il seguente:



Utilizzando cavi UTP di categoria 5 con rete Lan Ethernet e basata su protocollo TCP/IP.

Per l'estensione della rete, si deve provvedere ad un singolo accesso ad internet tramite collegamento con Fibra Ottica e per il collegamento nelle varie Lan si adottano invece cavi di categoria 5e che aumentano la velocità di connessione a 1000 Mbit/s.

Per l'implementazione della piattaforma didattica multimediale si ha bisogno di un server web e lo schema logico potrebbe risultare come:



Il firewall permette di lasciare separate le due sottoreti: quella amministrativa e quella relativa ai 10 laboratori, settando opportunamente le regole NAT per l'uscita verso internet degli Host delle lan e le regole ACL che definiscono i criteri di protezione e filtraggio.

Ovviamente oltre al firewall si adottano tutte le altre misure di sicurezza come:

- uso del protocollo TLS per l'accesso dall'esterno al server web (HTTPS)
- autenticazione degli accessi al servizio didattico web
- Il server ampiamente ridondante e collegato ad un gruppo di continuitá, collocato in un locale climatizzato opportunamente.
- Ogni pc delle reti è provvisto di antivirus, autenticazione tramite credenziali e soprattutto per i pc della rete amministrativa backup dei dati giornaliero.

Per proteggere la rete da attacchi esterni, si adotta il classico schema che utilizza una DMZ (DeMilitarized Zone) creata utilizzando un firewall con 5 interfacce ethernet. Questa soluzione viene adottata per consentire ai server collocati nella DMZ di fornire servizi all'esterno senza pregiudicare la sicurezza della rete interna. Nel nostro caso se il server Web, esposto verso Internet, subisse un attacco esterno, non ci sarebbero ripercussioni nella rete interna poiché il firewall la isola sia dalla DMZ che da Internet

Gli switch utilizzati sono di buona qualità con un collegamento di almeno 1Gbps con 24 porte

In ogni piano dell'edificio si colloca un armadio di piano IC = Intermediate Cross-connect che contiene router e switch per le reti di quel piano. Nello stesso piano ci possono anche essere diversi armadi per le singole reti in esso presenti, detti HC = Horizontal Cross-connect, che contengono lo switch relativo alla rete locale corrispondente.

Tutti i pc hanno indirizzi statici in un range che non crei conflitto.

Hardware

Server di fascia alta dotato di sistemi di fault tolerance.

Server web Apache completo dei modulo Php e Mysql

Database DBMS mysql.

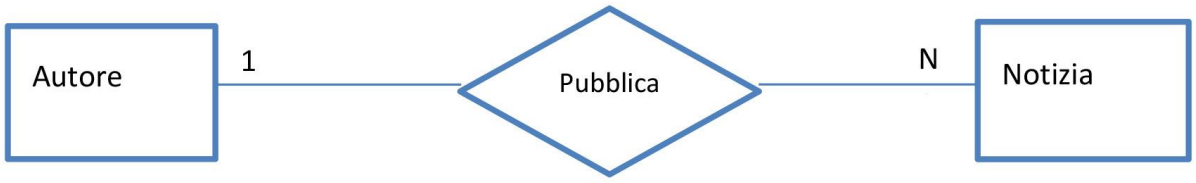
Parte 2

2. Dopo un'analisi del problema basterebbe una solo entità all'interno della base di dati che racchiuda tutte le informazioni che servono per descrivere le notizie riportate. Tuttavia sembra più realistico prevedere una ulteriore entità che descriva gli utenti abilitati ad inserire nuove notizie. Prima di poter inserire una notizia l autore dovrà autenticarsi al sito tramite email e password. Le notizie potrebbero essere anche caricate manualmente nel sito caricando il file opportuno tramite CMS, ma il funzionamento descritto rispecchia maggiormente la piattaforma Moodle (standard per l'e-learning in generale).

Si identificano quindi 2 entità:

- Autore
- Notizia

Si identifica quindi le seguente relazione fra le due entità riportata nel seguente schema concettuale:



Per realizzare lo schema logico che implementi il seguente schema concettuale non avendo relazioni molti a molti, basta inserire la chiave primaria della tabella Autore come chiave esterna di Notizia.

Quindi il modello che ne deriva è:

Autore

- ID_Autore (PK) codice univoco dell'autore
- Nome
- Cognome
- Email ()
- Password

Notizia

- ID_notizia (PK) codice univoco della notizia
- Titolo
- ID_autore (FK) chiave esterna della tabella Autore
- Testo
- Data
- Path (path dell'eventuale contenuto multimediale)

  La memorizzazione dell'eventuale contenuto multimediale è fatta tramite un campo che memorizzi il path di memorizzazione del contenuto all interno dello spazio del sito web. Si potrebbe optare per una memorizzazione diretta del contenuto come campo Blob, ma richiederebbe delle ipotesi aggiuntive sul DBMS utilizzato e risulterebbe comunque non performante.

La pagina di visualizzazione delle notizie deve comprendere tutte le informazioni riguardanti la notizia selezionata. Quindi apparirà nel seguente modo:

Un aspetto di interazione interessante può essere l'inserimento di una nuovo notizia. Il seguente codice PHP implementa tale funzionalità.

```
<?php session_start();
$id_autore=$_SESSION["author"]; ?>
<html>
<head>Inserimento nuova Notizia</head>
<body>
<?php
$titolo=$_POST[titolo]
$data=$_POST[data]
$testo=$_POST[testo]
$path=$_POST[path]
$db=mysql_connect("localhost","root","")
If ($db){
     Mysql_select_db("scuola")

    $sql="INSERT INTO notizie VALUES ( null,$id_autore,titolo,testo.....)
    if (mysql_query($sql))
          Echo "INSERITO"
    Else
         echo "Errore".myslq_error($db)
    mysql_close($db)
}
?>
</body>
</html>
```

3. la **crittografia simmetrica** è nota come la crittografia classica, cioè l'utilizzo di algoritmi in cui mittente e destinatario utilizzano la stessa chiave per criptare e decriptare un messaggio. Nella crittografia a chiave simmetrica è utilizzata quindi una sola chiave segreta, la quale è un parametro di una funzione invertibile. Il principio di funzionamento è il seguente.

- Il mittente cifra il messaggio con la chiave segreta
- Si trasmette il messaggio cifrato attraverso il canale (sicuro o insicuro)
- Il destinatario riceve il messaggio cifrato e lo decifra con la chiave segreta

I vantaggi sono la velocità di funzionamento, il che permette di poter utilizzare chiavi molto lunghe, tuttavia l`aumento delle prestazioni degli elaboratori rende meno sicuro questo sistema crittografico visto che molti algoritmi simmetrici sfruttano operazioni semplici come trasposizioni e sostituzioni e le ricerche esaustive diventano possibili in tempi sempre minori. Inoltre l'uso ripetuto della stessa chiave rende più facile la sua scoperta da parte di terzi. Infine, lo svantaggio maggiore è che serve un canale sicuro con il quale condividere la chiave segreta fra mittente e destinatario, ed il problema si amplifica quando la chiave deve essere condivisa fra un numero elevato di persone

L' algoritmo più utilizzato è il Data Encryption Standard (DES)

La **crittografia asimmetrica** si basa su coppie di chiavi: l` una capace di cifrare e l`altra di decifrare l informazione e viceversa. L'idea alla base dei sistemi a chiave asimmetrica è che la chiave di cifrazione sia diversa da quella di decrittazione: così facendo è possibile distribuire la propria chiave di decrittazione e mantenere segreta la chiave di crittazione. Questo tipo di crittografia nasce per risolvere i problemi della cifratura simmetrica, poiché lo scambio delle chiavi non è più critico ed il problema dell'autenticità del mittente viene immediatamente risolto, in quanto solo il titolare della chiave privata può aver generato il messaggio. Infine ogni soggetto dovrà mantenere una sola coppia di chiavi: le chiavi pubbliche verranno iscritte in appositi registri pubblici.
Il principio matematico alla base della cifratura asimmetrica è che è matematicamente improbabile ricavare una chiave dall'altra, ovvero le chiavi devono essere indipendenti; la conoscenza di una non deve concedere alcuna informazione utile alla ricostruzione dell'altra.
Uno dei grossi limiti nell` utilizzo di questa crittografia consiste nel fatto che i complessi calcoli rendono la loro implementazione poco efficiente soprattutto quando occorre garantire una lunghezza minima della chiave almeno superiore a 1024 bit.
È utilizzata per la firma digitale, cioè prendere un messaggio e crittografarlo con la chiave privata del mittente tramite l'utilizzo di funzioni hash come MD5, SHA1 ed il più recente RIPEMD-160.

SKUOLA.net