

Infrastrutture e servizi per la connettività: due casi di studio

Introduzione

La disponibilità di linee **ADSL** (*Asymmetric Digital Subscriber Line*) a costi contenuti o a volte gratuitamente (nell'ambito di convenzioni ad hoc con alcuni fornitori del servizio), ha reso possibile anche per le scuole usufruire di connessioni a Internet che siano *always on* e a banda larga.

Le connessioni *always on* (sempre in linea) sono connessioni dedicate che non si attivano solo su richiesta (come le connessioni commutate) ma sono a disposizione 24 ore su 24. Questo tipo di linea è dunque adatta a trasformare la scuola da un soggetto che usufruisce dei servizi Internet a un soggetto che può offrire esso stesso servizi, al proprio personale, agli studenti, ai genitori e a terze parti interessate. Una connessione *always on* consente dunque, per esempio, di ospitare a scuola un *server Web* visibile dall'esterno, oppure di gestire un *server* di posta per fornire a tutti gli studenti un *account* di posta elettronica e gestire opportune *mailing list*.

Le connessioni **a larga banda** offrono larghezze di banda misurabili in Mbps e sono dunque adatte a fornire connettività Internet ad alcune decine di stazioni mantenendo un elevato grado di interattività. Questo tipo di connessione consente inoltre di fruire di servizi multimediali innovativi, quali per esempio i sistemi di *e-learning* e risulta quindi particolarmente interessante in ambiente scolastico.

Riprogettare la connettività

Questo approfondimento presenta due casi di studio, nei quali l'introduzione della tecnologia **ADSL** come supporto alla connettività Internet ha introdotto modifiche strutturali alle infrastrutture della rete locale. Per ciascuno dei due casi sono riportate le principali scelte progettuali, avendo cura di citare le tecnologie utilizzate e di motivare le decisioni prese. Maggiori informazioni sulle specifiche tecnologie verranno fornite nei moduli successivi. Non sono stati riportati i costi delle infrastrutture perché questo tipo di informazioni sono soggette a una fortissima obsolescenza.

In particolare nel **primo caso**, la relativa complessità delle esigenze della scuola e in particolare la scelta di utilizzare la connessione ADSL anche per collegare a Internet le macchine dell'amministrazione, ha portato all'introduzione nell'architettura della rete di un *firewall*. Il *firewall* viene utilizzato per raggiungere diversi scopi:

- aumentare la **sicurezza** perimetrale,
- aumentare la sicurezza interna,
- limitare le attività degli utenti a un insieme di operazioni consentite.

Il **secondo caso** integra l'innovazione apportata dall'introduzione di una connessione *always on*, con aspetti di mobilità introdotti attraverso l'uso di tecnologie **wireless**. La scelta della connessione ADSL e il conseguente ripensamento della struttura interna della LAN, ha infatti creato l'occasione per valutare l'opportunità di installare una rete *wireless* che offra supporto alla mobilità degli utenti e consenta di portare la rete nelle aule e negli uffici con interventi di cablaggio molto limitati.

Un primo caso di studio

In vista dello spostamento in una nuova struttura, un Istituto Tecnico Industriale imposta un nuovo progetto di connettività che ha come obiettivo finale quello di collegare a Internet stabilmente e a banda larga sia i laboratori didattici che le segreterie. Nel precedente edificio la connessione a Internet avveniva mediante due linee commutate ISDN, una per l'amministrazione e una per i laboratori.

L'istituto ha due laboratori didattici che sono composti da attrezzature recenti e che verranno spostati senza integrazioni. Nel primo laboratorio sono collocate 13 postazioni e nel secondo 15. La

segreteria opera invece su 4 postazioni. Sono presenti inoltre due *server* che fungono da *controller* di dominio (per l'**autenticazione** degli utenti), *file server* e *server* stampa rispettivamente per la segreteria e per i laboratori.

Il progetto deve considerare:

- la scelta del fornitore del servizio di accesso.
- Il cablaggio della rete locale.
- Le problematiche di **sicurezza** e la prevenzione degli **attacchi**, sia interni che esterni.
- Il progetto di nuovi servizi da offrire agli utenti, tra i quali la posta elettronica e la possibilità di consultare da casa la posizione personale degli studenti.

Cablaggio

Il progetto dell'edificio prevedeva la realizzazione di un cablaggio strutturato molto esteso, messo in opera in fase di costruzione del plesso.

Il cablaggio disponibile è basato sulle seguenti scelte operative:

- connettere ogni aula dell'istituto con un centro stella, posto in un armadio di permutazione, attraverso due prese per aula;
- realizzare una sottorete per ciascuno dei due laboratori (per ospitare fino a 20 postazioni) e una per la segreteria (per ospitare fino a 8 postazioni).

Sono stati utilizzati doppini di tipo UTP (*Unshielded Twisted Pair*) categoria 5, che supportano *Fast Ethernet* (fino a 100 Mbit/sec).

Apparati attivi

Posto che la posa in opera dei cavi era già stata stabilita dal progetto di costruzione dell'edificio, la realizzazione della LAN deve essere completata attraverso la collocazione e connessione degli apparati attivi.

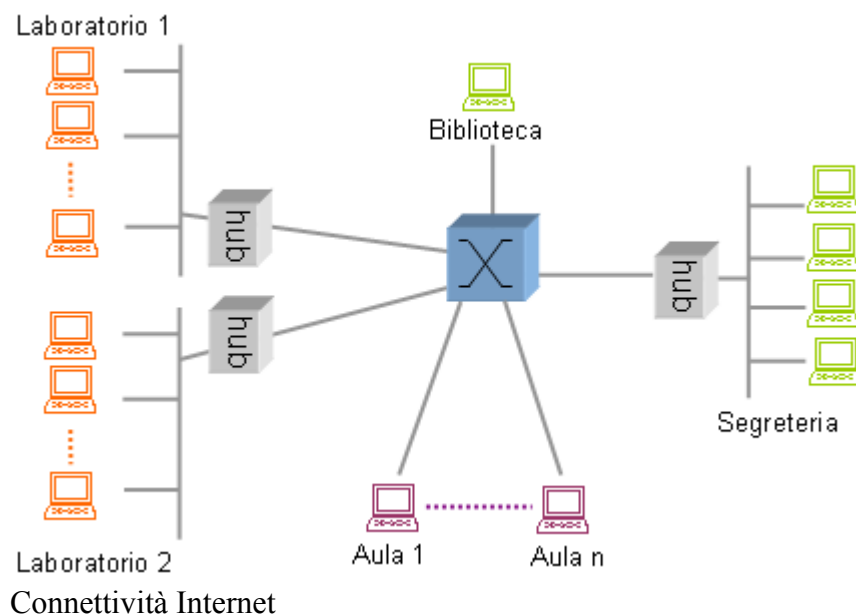
L'istituto è dotato di calcolatori per lo più recenti, equipaggiati con schede di rete a 10/100 Mbit/sec che nel vecchio edificio erano connessi tra loro tramite *hub* a 100 Mbit/sec. Sono dunque disponibili due *hub* a 100 Mbps da 16 porte che erano utilizzati nei laboratori e un *hub* a 100 Mbps a 8 porte utilizzato in segreteria.

Per la connessione delle portanti tra i vari laboratori e la segreteria è stato scelto uno *switch* di livello 2, con 24 porte, ovvero un apparato attivo in grado di instradare i pacchetti esclusivamente verso l'indirizzo (di livello 2) destinatario. Questa scelta va nella duplice direzione di migliorare le prestazioni e aumentare la **sicurezza** del sistema. Il numero di porte è sufficiente a coprire le esigenze iniziali dell'Istituto, ma l'apparato dovrà essere integrato se si vorrà installare un *computer* per aula.

Per i laboratori didattici e per la segreteria si opta per il riuso degli *hub* preesistenti e utilizzati già nel vecchio edificio, fatta salva l'opportunità di sostituirli in futuro con altri *switch*. Gli *hub* sono infatti apparati di livello 1 che hanno il solo compito di rimbalzare il segnale sulle porte a disposizione e quindi non effettuano uso selettivo delle risorse e, condividendo il canale, rendono possibili attacchi alla sicurezza dei dati. Gli *switch* sostitutivi consentirebbero di aumentare le prestazioni, la sicurezza e il numero di postazioni collegabili.

LAN

Una prima possibile configurazione della LAN è dunque la seguente:



Per la connettività Internet si è scelto un collegamento **ADSL**, di tipo permanente, che comprende l'utilizzo di un indirizzo IP statico, la registrazione e gestione di un dominio di secondo livello, la fornitura e installazione di un *router* ADSL. Il costo del contratto è di tipo *flat*, ovvero prevede un prezzo fisso mensile senza tenere conto del traffico.

La fornitura offre una velocità di 640 kbit/sec per la *download* e di 128 kbit/sec per l'*upload*, con una banda garantita verso qualunque destinazione di 20kbit/sec in *download* e 10 kbit/sec in *upload*. Infine il contratto prevede l'utilizzo di 50 MB di spazio disco e di 5 indirizzi di posta elettronica.

Si aprono dunque, rispetto alla configurazione della LAN appena prospettata due diverse tipologie di problema:

- la necessità di mascherare gli indirizzi della LAN dietro all'unico indirizzo IP routabile che è in possesso dell'istituto. Questo tipo di attività può essere realizzata mediante un sistema NAT/PAT che è integrato nel *router* ADSL fornito assieme al collegamento a Internet.
- La necessità di proteggere la rete locale e le sue risorse, poiché il collegamento stabile aumenta fortemente i rischi di attacco alla sicurezza del sistema. La rete può essere protetta mediante un **firewall**.

TIR

Nelle forniture **ADSL** il *router* viene anche indicato con l'acronimo TIR (Terminazione Intelligente di Rete) e tipicamente è in grado di fornire servizi aggiuntivi, rispetto al normale instradamento IP. In particolare le funzionalità aggiuntive più frequenti sono:

- il **NAT** (*Network Address Translation*), un servizio che offre la possibilità di collegare un numero qualunque di postazioni pur avendo un solo indirizzo IP pubblico. Il NAT è realizzato mappando le comunicazioni su indirizzi IP privati, visibili solo all'interno della rete.
- Il **PAT** (*Port Address Translation*) che consente a stazioni interne alla rete privata di fornire servizi a *client* della rete pubblica. Il PAT mappa le porte dei *server* della rete privata su porte logiche del TIR e reinstrada le comunicazioni di conseguenza.

Il TIR compreso nel contratto sottoscritto dall'istituto comprende funzionalità di NAT e PAT.

Sicurezza

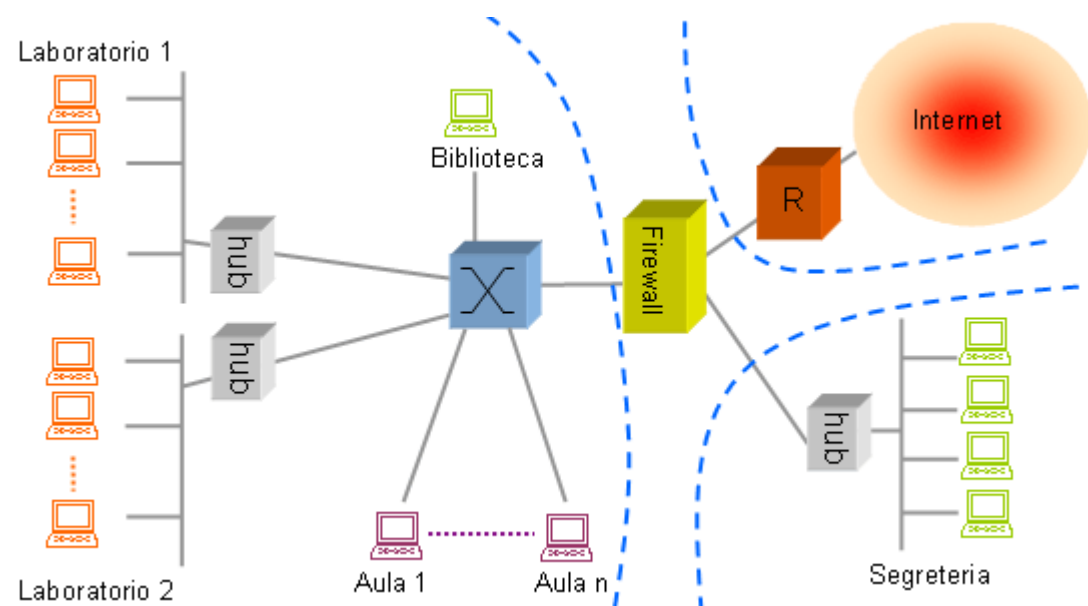
Due problematiche di **sicurezza** sostengono il progettista nella scelta di utilizzare un **firewall** per ridurre i rischi derivanti dall'architettura di rete finora prospettata:

- la connessione stabile rende maggiore il rischio d'attacco poiché le risorse sono sempre a disposizione di un eventuale intruso che miri a impossessarsene e/o a danneggiarle. A rischio sono sia le macchine dei laboratori che quelle dell'amministrazione e queste ultime devono essere protette con maggiore efficacia perché contengono dati sensibili.
- Gli studenti dell'istituto hanno, già in passato, dato prova di possedere abilità informatiche sufficienti a sferrare con successo attacchi alla sicurezza. In questo caso rispetto agli attacchi diretti verso l'esterno della rete, sono più critici gli attacchi interni che potrebbero essere rivolti alle macchine dell'amministrazione e ai dati (sensibili e non) in esse contenuti.

Per questo motivo è opportuno installare un *firewall* che effettui una sorveglianza non solo perimetrale ma anche interna. Il *firewall* dividerà dunque la LAN in tre sottoreti, una per i laboratori, una per l'amministrazione e, infine, una che include esclusivamente il *router* e diviene quindi la via di transito verso l'esterno del sistema.

Firewall

La configurazione completa della LAN è dunque la seguente:



I nuovi servizi

In fase di stesura del progetto vengono definiti alcuni nuovi servizi che si vogliono rendere disponibili agli studenti, al personale e alle famiglie. Vengono inoltre suggerite linee guida nella scelta delle risorse *hardware* e *software* di supporto ai nuovi servizi, rinviando a una futura analisi la scelta delle specifiche piattaforme e applicazioni e la fattibilità economica relativa.

In particolare, sentiti gli utenti finali (studenti, docenti e famiglie), risultano interessanti i seguenti servizi:

- un servizio di posta elettronica che assegna a ogni studente e a ogni docente una casella di posta in modo da incentivare le comunicazioni attraverso questo medium. Non sono evidentemente sufficienti le 5 caselle fornite dal *provider* d'accesso per cui per realizzare questo servizio si prevede di utilizzare un *server* di posta che fornisca supporto ai principali

protocolli (SMTP, POP e IMAP). Considerate le funzionalità del *server*, si consiglia di valutare la possibilità di basare il servizio su piattaforme *open source*.

- Un sistema basato su *Web* che consenta di utilizzare Internet per accedere ai dati sul rendimento scolastico degli allievi, sia in termini di valutazione dei risultati che in termini di presenze/assenze e ritardi. Il sistema dovrà prevedere una forma di autenticazione degli utenti in modo che solo persone autorizzate dall'Istituto (tipicamente i genitori) possano accedere alle informazioni e integrarsi con gli applicativi disponibili presso la segreteria.

Secondo caso

Un liceo classico è sito in un palazzo storico nel centro di una città e ha infrastrutture informatiche prevalentemente concentrate in due luoghi: il laboratorio multimediale e la segreteria. Il liceo ha recentemente sostituito la connessione commutata via ISDN del laboratorio con una connessione stabile a banda larga basata su tecnologia ADSL e vorrebbe utilizzare la nuova linea anche per garantire connettività a Internet a tutte le altre postazioni site nel palazzo.

Il progetto ha l'obiettivo di verificare la possibilità di cablare tutto l'edificio mediante una infrastruttura mista *wired* e *wireless* che integri il cablaggio basato su cavi con tecnologie senza fili. Attraverso questa infrastruttura la linea ADSL deve poter diventare il mezzo di accesso a Internet anche per gli elaboratori della segreteria e per le postazioni site nella biblioteca e nell'aula magna.

La connettività *wireless* deve essere realizzabile in due fasi: in una prima fase deve essere offerta copertura *wireless* alle aree dell'amministrazione, al laboratorio multimediale, all'aula magna e alle aree di studio e ricreazione di studenti e docenti. Una seconda fase deve rendere possibile la copertura di tutto il resto dell'edificio.

WLAN

Con il termine inglese *wireless* si indica una specifica tipologia di comunicazioni che utilizza come mezzo fisico per il trasporto dei dati l'etere. Un segmento del mercato *wireless* particolarmente significativo e stabile è costituito dalle *Wireless LAN (WLAN)* il cui obiettivo principale è quello di integrare, piuttosto che sostituire, le tradizionali LAN, fornendo connettività mobile agli utenti. In edifici in cui è complesso installare tradizionali reti via cavo, per particolari modelli strutturali o in edifici storici e soggetti a vincoli delle Belle Arti, le WLAN sono la soluzione ottimale per offrire connettività, sia dal punto di vista delle prestazioni che dal punto di vista economico.

In particolare nel settore delle applicazioni didattiche le WLAN hanno trovato un fertile terreno applicativo offrendo diverse tipologie di servizi, che risultano innovativi sia dal punto di vista della connettività che delle funzionalità. Sono ormai diverse le scuole che hanno affiancato al cablaggio via cavo con installazioni di reti con l'obiettivo di integrare meglio la presenza del personal *computer* all'interno delle classi e di favorire la mobilità dei docenti.

WiFi

IEEE **802.11** è il primo standard sviluppato per le WLAN e può essere comparato con lo standard 802.3 definito per le reti locali basate su *Ethernet*. Lo scopo di 802.11 è quello di definire un set di regole operative tali che apparati costruiti da differenti produttori possano operare tra di loro in maniera trasparente, proprio come avviene per tutti gli apparati basati sulla tradizionale tecnologia *Ethernet*.

Questo standard è basato sull'architettura cellulare, ovvero la LAN viene vista e definita come un insieme di più **celle**, in cui ogni cella è controllata da una stazione base chiamata punto di accesso o **Access Point**. Premesso questo, possiamo dire che una LAN può essere formata da una singola cella con un singolo punto di accesso oppure da un insieme di celle dove i vari punti di accesso sono

collegati tra loro attraverso un *backbone* che viene realizzato su una rete cablata *Ethernet* ma può essere anch'esso *wireless*.

La tipologia di WLAN più diffusa è nota come **WiFi** (*Wireless fidelity*) ed è definita dallo standard 802.11b (della famiglia 802.11) che opera a 2,4Ghz di frequenza e raggiunge un *transfer rate* di 11Mbps.

La struttura

Il liceo ha sede in due edifici: un palazzo principale, che ospita l'amministrazione, la biblioteca, la maggior parte delle aule e i laboratori, e un fabbricato separato in cui sono collocate le palestre. L'edificio principale è strutturato su due piani: al piano terra trovano ubicazione l'amministrazione, l'aula magna, la biblioteca, la sala di studio, il laboratorio multimediale e alcune aule. Il primo piano ospita le altre aule e il laboratorio di scienze. La linea ADSL arriva con un *router* nel laboratorio. I *computer* del laboratorio multimediale sono collegati tra di loro attraverso un *hub* a 100 Mbps. L'amministrazione ha un cablaggio interno a 100 Mbps attraverso un *hub* a 8 porte.

Il progetto deve prevedere l'acquisizione delle infrastrutture necessarie a:

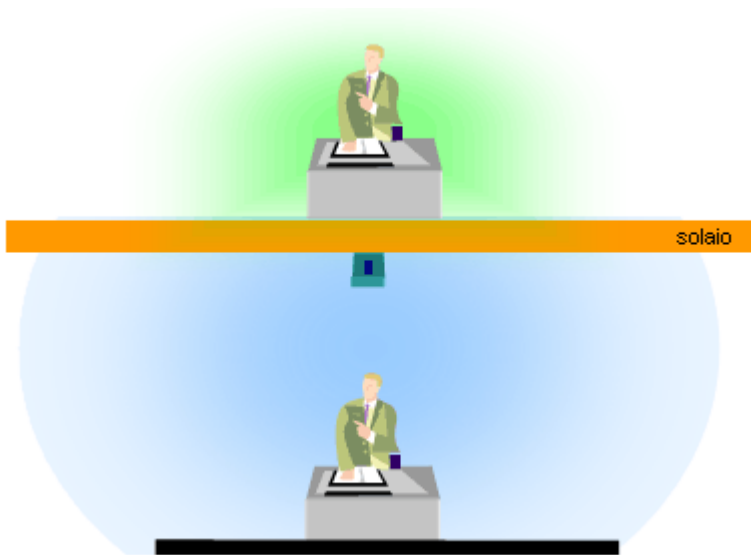
1. collegare (via cavo) l'amministrazione alla linea ADSL;
2. offrire copertura *wireless* alle aree indicate come primarie (tutte collocate al piano terra dell'edificio principale);
3. prevedere i lavori di ampliamento della copertura *wireless* a tutte le aule (piano terra e primo piano).

Ampliamento della LAN

Il cablaggio tradizionale deve assicurare la connessione della rete dell'amministrazione alla linea **ADSL**. Viene quindi prevista la posa di un cavo che realizzi questo collegamento e l'acquisto di uno *switch* a 100 Mbps con 16 porte. Allo *switch*, che fungerà da centro stella della LAN, andranno collegati: il *router* ADSL, l'*hub* del laboratorio multimediale e l'*hub* dell'amministrazione. La scelta di uno *switch* consente di aumentare il grado di sicurezza della rete, limitando le aree a mezzo condiviso. Questa scelta è particolarmente critica se si prevede l'integrazione con apparati *wireless*.

Il cablaggio tradizionale deve inoltre raggiungere tutti gli *access point*. Sono disponibili in commercio anche apparati che consentono di costruire il *backbone* tra gli *access point* utilizzando *link wireless*, ma hanno costi più elevati dei normali apparati WLAN. Per questo motivo viene scelta la stesura di cavi dallo *switch* centro stella (posto nel laboratorio multimediale) ai singoli **access point**. I punti di posa degli *access point* devono essere definiti dopo una attenta analisi della topologia della scuola e solo dopo aver effettuato opportune misurazioni. Il segnale radio si attenua infatti quando attraversa ostacoli fisici (quali i muri) e dunque per essere certi che il segnale copra tutta l'area indicata come primaria, occorre fare misure di ricezione. Una misura particolarmente utile risulta quella volta a comprendere il tipo di attenuazione prodotto dal solaio posto tra il piano terra e il primo piano.

Essendo l'edificio antico (e dunque il solaio realizzato senza cemento armato) è possibile che l'attenuazione prodotta dal solaio sia minima e dunque che gli apparati usati per coprire il piano terra, se posti sufficientemente vicini al soffitto, offrano copertura anche a parte del primo piano.

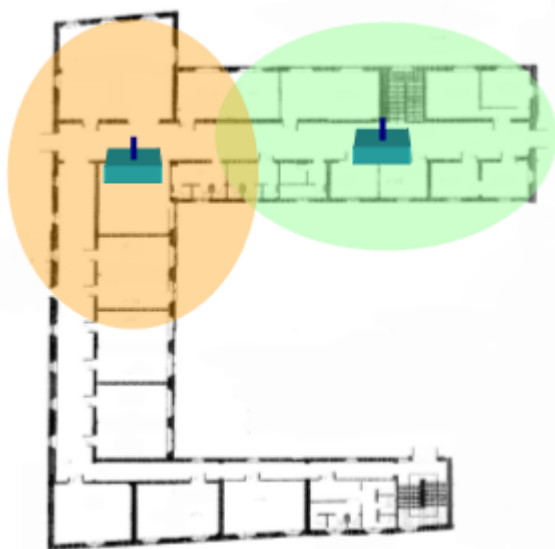


Il piano terra

Il piano terra del liceo è rappresentato dalla seguente piantina, dalla quale risulta evidente che le zone da coprire nella prima fase sono tutte attigue.

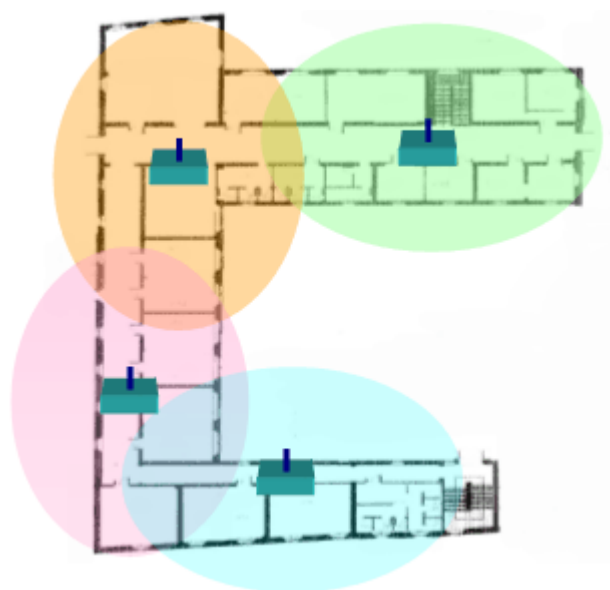


Copertura del piano terra



Dalle misurazioni effettuate risultano sufficienti due *access point* (collocati rispettivamente di fronte all'aula magna e sopra alla segreteria per coprire tutta l'area richiesta nella prima fase. Il segnale supera il solaio con un'attenuazione accettabile, per cui al primo piano arriva nitido oltre il metro da terra (distanza a cui verranno tenute le tipicamente schede di rete). Le misure sono state fatte da uno dei potenziali fornitori con AP identici a quelli che verranno installati nella scuola.

Copertura delle aule



Per offrire connettività *wireless* a tutte le aule (piano terra e primo piano) sono dunque sufficienti 4 apparati, i due previsti per la fase iniziale più altri due che possono essere acquisiti e collegati al centro stella in una fase successiva.

Scelta degli apparati

Gli apparati *WiFi* disponibili sono innumerevoli e hanno costi molto variabili a seconda delle funzionalità che offrono. In particolare sono offerti alcuni servizi aggiuntivi che possono essere interessanti in casi specifici:

- apparati **access point** con *backbone wireless*: sono AP dotati di più schede *wireless*.

Tipicamente una scheda è utilizzata per l'accesso dei terminali mobili e una per il *backbone*. Hanno il vantaggio di non richiedere il cablaggio LAN tradizionale.

- Appareti *access point* alimentati attraverso il cavo di rete: sono AP che ricevono alimentazione attraverso il doppino che li collega alla rete. Per utilizzarli occorre che lo *switch* sia in grado di alimentarli o che esista un altro apparato che viene aggiunto alla rete al solo scopo di fornire l'alimentazione agli *access point*.
- Appareti con funzionalità aggiuntive per la **sicurezza** e la gestione della rete. Le reti *wireless* sono infrastrutture poco sicure: il loro raggio d'azione esce a volte dalle aree per le quali sono impiantate e l'algoritmo di crittografia utilizzato ha diverse falle note da tempo. Sono in commercio apparati che offrono supporto a funzionalità per il miglioramento della sicurezza che implementano a questo scopo diverse strategie. Altre funzionalità di supporto alla gestione realizzano per esempio politiche di assegnazione dinamica degli indirizzi IP (**DHCP** e **NAT**).

Nel progetto del Liceo trovano applicazione semplici apparati di accesso senza funzionalità aggiuntive, che possono essere reperiti a costi molto limitati.

Conclusioni

I due casi mostrati hanno avuto lo scopo di presentare due diverse situazioni in cui la connettività *always on* a banda larga messa a disposizione dalle linee ADSL ha offerto lo spunto per ripensare alla rete locale della scuola e ridefinirne i servizi.

L'esposizione ha, in entrambi i casi, mirato a illustrare gli aspetti più innovativi delle scelte progettuali, tralasciando volutamente gli aspetti più tecnici e quelli più consueti.

Entrambi i progetti sono stati realizzati seguendo criteri di scalabilità, ovvero sono state acquisite infrastrutture che consentono la messa in opera di un primo nucleo di nuovi servizi, delineando già un insieme di possibili migliorie da realizzare nel breve periodo. Per questo motivo le trattazioni non sono esaustive e lasciano aperte ampie possibilità di miglioramento dell'infrastruttura in termini di servizi, sicurezza, prestazioni. I possibili potenziamenti sono individuati dai rispettivi progetti, ma rimandati a successivi interventi di finanziamento.