



Ministero dell'Istruzione

Progetto Rete Locale cablate e wireless nelle scuole

“D.D. Leinì”



Progettista: Cosimo Esposito

PREMESSA

La necessità di connettività di rete, di banda larga, di stabilità di segnale, di sostegno alla densità di dispositivi connessi, cresce di giorno in giorno, nel mondo, in Italia, nella nostra scuola. La recente pandemia ha messo a dura prova i sistemi informatici dei nostri istituti scolastici. La DAD, la didattica a distanza, la didattica mista, hanno spesso causato disagio, per colpa di mancanza di dispositivi, per colpa di scarse conoscenze degli utenti, per bassa disponibilità di connessione Internet. Col tempo e con la volontà di tutti le conoscenze sono state colmate, i dispositivi sono stati donati, acquistati, noleggiati.

I fondi stanziati nel 2021 con questo PON FESR diventano l'occasione per un potenziamento globale della nostra infrastruttura, per colmare le grandi e piccole lacune di connettività, per poter garantire ad ogni utente, docente e studente, una costante disponibilità di connessione e banda larga.

Questo progetto illustra, attraverso spiegazioni, immagini, corredate dalle piante degli edifici scolastici, il miglior modo per raggiungere gli obiettivi prefissati.

A. Descrizione tecnologiche

1. Wi-Fi 6
2. VLAN 802.Q

B. Descrizione Dispositivi

1. Access Point
2. Switch
3. Cavo di rete
4. Armadio Rack
5. Ups
6. Firewall

1. Stato degli edifici, disponibilità di connettività e dispositivi esistenti nei plessi scolastici
 - a. Plesso 1
 - b. Plesso 2
 - c. Plesso 3
 - d. Plesso4
2. Problematiche rilevate nella connettività attuale dei plessi
3. Descrizione degli interventi per plesso
 - a. Access Point
 - b. Switch
 - c. Firewall
 - d. Accesso controllato: filtro e captive portal
4. Allegati: Piante degli edifici con segnalazioni

A.1 WiFi 6

L'ultimo decennio ha portato le nostre vite sempre più online e le connessioni Internet wireless hanno contribuito a rendere possibile questa transizione. L'ultima versione di questa tecnologia è il Wi-Fi 6, noto anche come 802.11ax.

Che cos'è il Wi-Fi?

Il termine "Wi-Fi" è stato creato dall'associazione no profit Wi-Fi Alliance e si riferisce a un gruppo di protocolli di rete wireless basati sullo standard di rete IEEE 802.11. Il Wi-Fi esiste dalla fine degli anni '90, ma è notevolmente migliorato nell'ultimo decennio.

Per rendere più evidenti le differenze tra ogni generazione, la Wi-Fi Alliance ha recentemente adottato una convenzione di denominazione più tradizionale, eliminando la designazione 802.XX in luogo di un suffisso numerico semplificato. Questa convenzione di etichettatura più semplice (Wi-Fi 6 rispetto a 802.11ax) consente di conoscere in che modo viene utilizzata la generazione della tecnologia e al fine di determinare la compatibilità con i dispositivi che supportano questa versione.

In cosa differisce il Wi-Fi 6 dal precedente standard?

Il Wi-Fi 6 rappresenta un aggiornamento sostanziale rispetto alle generazioni precedenti. Questi cambiamenti potrebbero non modificare drasticamente il modo in cui utilizziamo i router wireless o la connessione di rete wireless, ma consistono invece in diversi miglioramenti progressivi che confluiscono in un unico aggiornamento sostanziale.

Il primo cambiamento è rappresentato dal fatto che il Wi-Fi 6 consente velocità di connessione più elevate.

Velocità più elevate

Un Wi-Fi più veloce comporta maggiori velocità di upload e download (o throughput) grazie alla maggiore larghezza di banda offerta dal Wi-Fi 6. Questo fattore sta diventando sempre più importante man mano che le dimensioni dei file aumentano, oltre alle maggiori esigenze dello streaming video di alta qualità e dei giochi online sempre più pesanti.

Quindi, di quanto è più veloce il Wi-Fi 6?

- **9,6 Gbps è il throughput massimo del Wi-Fi 6 su più canali.** Al contrario, il Wi-Fi 5 offre un massimo di 3,5 Gbps. I dispositivi dotati di Wi-Fi 6 possono godere di velocità notevolmente più elevate.
- **Le velocità possono essere più elevate rispetto al Wi-Fi 5.** Si presuppone l'uso di un router Wi-Fi con un singolo dispositivo. Il Wi-Fi 6 può raggiungere maggiori velocità di trasferimento dei dati attraverso una varietà di tecniche, a partire da una codifica dei dati più efficiente e dall'uso intelligente dello spettro wireless, reso possibile da processori più potenti.
- **Il Wi-Fi 6 può portare a una riduzione della latenza fino al 75%.** Tale riduzione è ottenuta mediante la gestione di grandi quantità di traffico di rete in modo più efficiente.
- **Il Wi-Fi 6 avvicina le prestazioni delle reti wireless e cablate.** In tal modo permette potenzialmente a più utenti di liberarsi dai vincoli di una connessione cablata al modem. Il Wi-Fi 6 contribuisce a colmare ulteriormente il divario tra connettività cablata e wireless.

Cosa rende il Wi-Fi 6 più veloce?

La maggior parte delle case ospita oggi molti più dispositivi Wi-Fi rispetto a cinque anni fa. Il Wi-Fi 6 comunica meglio con più dispositivi connessi simultaneamente e gestisce in modo più efficiente le priorità del traffico generato da tali dispositivi.

L'**Orthogonal Frequency Division Multiple Access (OFDMA)** è uno dei modi in cui è possibile ottenerlo. L'OFDMA opera suddividendo i canali in portanti secondarie e consentendo la trasmissione a più endpoint (dispositivi) contemporaneamente. Un router Wi-Fi 6 può inviare segnali diversi nella stessa finestra di trasmissione. Ciò si traduce in una singola trasmissione dal router in grado di comunicare con più dispositivi, anziché costringere ogni dispositivo ad attendere il proprio turno mentre il router trasmette i dati in rete.

L'**Overlapping Basic Service Sets (OBSS)** è un'altra funzionalità Wi-Fi 6 che può contribuire a migliorare la congestione della rete. Con le precedenti versioni Wi-Fi, i dispositivi che cercavano di connettersi a una rete adottavano un approccio "ascolta prima di parlare", il che significava che dovevano "ascoltare" eventuali rumori su un canale prima di trasmettere.

Se sul canale fosse stato presente del rumore, anche proveniente da una rete distante, avrebbero dovuto attendere che il canale si liberasse prima di trasmettere, per evitare potenziali interferenze. L'OBSS consente al punto di accesso di utilizzare un "colore" per identificare in modo univoco la rete. Se viene rilevato altro traffico sul canale, ma non è dello stesso colore della rete locale, i dispositivi possono ignorarlo e continuare la trasmissione. Questo può contribuire ad aumentare l'affidabilità e ridurre la latenza.

Lavorando simultaneamente, OFDMA e OBSS assicurano una comunicazione più efficace su reti affollate. Poiché sempre più dispositivi utilizzano il Wi-Fi, questo contribuirà a preservare la velocità e la stabilità delle nostre connessioni.

Il **Beamforming** è un'ulteriore tecnologia migliorata dal Wi-Fi 6 al fine di ottenere velocità più elevate. Questo metodo di trasmissione dei dati dal nome futuristico è in realtà relativamente semplice. Invece di trasmettere dati in tutte le direzioni, il router rileva dove si trova il dispositivo che richiede i dati e trasmette un flusso di dati più focalizzato in quella direzione.

Il beamforming non è una novità del Wi-Fi 6, ma la sua efficacia è stata aumentata in questa generazione.

Vantaggi della rete oltre la velocità

La velocità è probabilmente la cosa più importante ma c'è di più in una rete wireless. Il Wi-Fi 6 promette anche una maggiore sicurezza.

WPA3

Il Wi-Fi Protected Access (WPA) è un protocollo di sicurezza Wi-Fi comune che utilizza le password per la crittografia. Ogni volta che è richiesta una password per accedere a una rete Wi-Fi, il WPA entra in azione. Il WPA 2 è considerato lo standard ormai da tempo, ma con il Wi-Fi 6 questa condizione cambierà.

Uno dei principali miglioramenti introdotti da questa tecnologia è l'implementazione di una maggiore sicurezza delle password tramite il sistema Dragonfly Key Exchange, chiamato anche SAE o Simultaneous Authentication of Equals. Questo metodo di autenticazione rende le password più difficili da decifrare, adottando un metodo più sofisticato per stabilire l'handshake con la rete Wi-Fi.

Questo ulteriore livello di sicurezza, unito a una crittografia più solida, consente al Wi-Fi di offrire opzioni di sicurezza più robuste che mai.

Questo ulteriore livello di sicurezza è un ottimo esempio di come il Wi-Fi 6 possa cambiare le cose in meglio, senza influire negativamente sull'esperienza dell'utente.

Durata della batteria e TWT

Un altro sviluppo rivolto al futuro introdotto dal Wi-Fi 6, è il Target Wake Time (TWT) che permette potenzialmente di aumentare l'autonomia della batteria di alcuni dispositivi.

Questa tecnologia consente una comunicazione più efficiente tra il router e il dispositivo per quanto riguarda attivazione e disattivazione. Comunicando efficacemente con la radio Wi-Fi del dispositivo e attivandola solo quando necessario, sono necessari molto meno tempo ed energia per cercare un segnale wireless.

Questo può contribuire ad aumentare la durata della batteria.

A.2 VLAN 802.q

Al giorno d'oggi una rete fisica si basa per lo più su uno o più switch, vale a dire dispositivi che regolano il traffico dati tra i partecipanti della rete. Allo **switch** vengono collegati tutti i cavi di rete che rendono possibile la comunicazione tra diversi computer. È possibile che tali switch colleghino addirittura centinaia di dispositivi tra loro, assicurando comunque un'ottima comunicazione. Tuttavia, potrebbe avere senso suddividere una rete così ampia senza dovervi apportare delle modifiche fisiche.

Una Virtual Local Area Network (VLAN) è un **piccolo segmento logico** all'interno di un'ampia rete fisica collegata tramite cavi. Il raggruppamento delle diverse stazioni in un'unica rete avviene indipendentemente dalla loro localizzazione: infatti, finché esse sono collegate ad una stessa LAN, possono essere raggruppate in un'unica VLAN. Non è un problema se la LAN si estende su più switch: la cosa importante è che lo switch sia adatto per la VLAN. Le VLAN possono basarsi solo sui managed switch.

I managed switch offrono infatti numerose possibilità di configurazione per l'uso professionale, al contrario degli unmanaged switch che vengono invece utilizzati per le reti domestiche e sono basati sull'idea del plug and play. Si possono ad esempio gestire specifici indirizzi IP, filtrare indirizzi MAC o impiantare VLAN.

Ogni singola VLAN riceve un proprio **dominio broadcast**: se un partecipante invia un broadcast all'interno della VLAN, tutti i partecipanti all'interno dello stesso segmento (e soltanto loro) ricevono il messaggio. Il broadcast non viene trasmesso oltre i confini della rete virtuale. La comunicazione tra le diverse VLAN avviene attraverso gli stessi cavi. I computer possono essere connessi a una stessa VLAN anche se non sono collegati allo stesso switch.

Diversi tipi di VLAN

È possibile configurare le VLAN in diversi modi e, a seconda della tipologia, viene applicata una tecnologia diversa. Nella pratica ritroviamo due tipi di applicazione: VLAN basate su porta o tagged

VLAN ("VLAN taggate"). In molti casi gli amministratori di rete realizzano le installazioni e le assegnazioni implementando entrambe le tipologie.

VLAN basata su porta

All'interno di uno switch ogni partecipante di rete viene indirizzato verso una **porta**, ovvero una presa all'interno della quale viene inserito il relativo cavo di rete collegato al computer di turno. Tuttavia, le porte vengono utilizzate anche per collegare gli switch tra di loro. Se da un'unica rete fisica si vogliono ricavare due VLAN, si assegnano le relative porte alla rete virtuale desiderata.

La configurazione **attraverso diversi switch** è possibile anche quando l'installazione della VLAN basata su porta è attuata su piccole reti e viene realizzata all'interno di un solo switch. Così le porte da 1 a 3 sul primo switch e la porta 1 sul secondo switch possono essere collegate insieme a un'unica VLAN. Per fare ciò bisogna collegare tra di loro i due switch con due cavi, prevedendo una connessione per ogni VLAN.

Questo tipo di connessione viene definita **trunking**. Gli switch hanno una o più porte predisposte per tale scopo e attraverso le quali si possono definire le opzioni di impostazione. La tipologia di connessione è secondaria: non è rilevante se si usino cavi in rame o in fibra ottica o una connessione wireless.

La distribuzione dei pacchetti avviene tramite gli stessi switch. Gli amministratori di rete impostano e assegnano le porte alle rispettive VLAN. In questo caso la VLAN si definisce **statica**. Se le VLAN devono essere configurate in modo diverso, le porte devono essere ridistribuite in fase di configurazione dello switch. Inoltre, ogni porta, e quindi anche ogni dispositivo ad essa connesso, appartiene solo a un'unica VLAN. La comunicazione tra i dispositivi di una VLAN con quelli di un'altra deve avvenire attraverso un router che permette di inoltrare i messaggi, così come avviene per la comunicazione tra la rete domestica e Internet.

Tagged VLAN

Nel caso della tagged VLAN l'assegnazione alla VLAN è più dinamica: a garantire l'assegnazione è un tag nel frame del pacchetto, che sostituisce la permanente impostazione nello switch. Per questo motivo questa tecnologia viene denominata **basata su frame**, come avviene per le reti basate su porta. Nel tag è contenuta l'informazione che indica in quale VLAN ci si trova al momento. Uno switch riconosce in quale segmento avviene la comunicazione e in base a questo inoltra il messaggio.

Un tag VLAN è di 32 bit e compare direttamente dopo l'indirizzo MAC del mittente all'interno del **frame ethernet**. Il tag inizia con un ID di protocollo di due byte: il Tag Protocol Identifier (TPI) mostra se è stato stabilito un ID VLAN. Se nel frame si identifica una VLAN, questi blocchi hanno il valore di 0x8100. In seguito, il frame indica in tre bit la priorità del messaggio. Segue poi un bit per il Canonical Format Identifier (CFI). Questa posizione serve per garantire la compatibilità tra ethernet e token ring.

È solo negli ultimi dodici bit che il protocollo indica il vero ID VLAN (VID). Il campo frame può **ospitare 4.096 VLAN diverse**. Ogni VLAN ha il suo numero proprio. Le tagged VLAN possono essere implementate anche direttamente sulle schede di rete.

La struttura del frame segue lo standard **IEEE 802.1q**, che è la variante più usata. In realtà ci sarebbero ancora altre possibilità per inserire i tag VLAN nei pacchetti.

Il vantaggio di una tagged VLAN, in confronto a una VLAN con assegnazione su porta, è rappresentato dalla connessione tra diversi switch. Per le VLAN basate su porta devono essere

collocati almeno due cavi tra gli switch, in quanto ogni Virtual lan ha bisogno della propria connessione. Per le **trunking in tagged VLAN**, invece, basta un solo cavo, in quanto la distribuzione dei dati avviene attraverso le informazioni del frame. Lo switch riconosce la VLAN corretta e la inoltra al secondo switch. Qui il tag viene eliminato e il pacchetto viene inoltrato al corretto destinatario.

Rete virtuale

Perché si dovrebbe suddividere una LAN più grande in diverse VLAN più piccole?

Flessibilità

Se un nuovo partecipante vuole far parte di una LAN, il dispositivo deve essere connesso tramite cavo a uno switch. Nel caso in cui un dipendente cambi il suo team all'interno dell'azienda e debba quindi lavorare su un'altra rete, è necessario cambiare la postazione di lavoro oppure effettuare un nuovo cablaggio. **La configurazione di una VLAN avviene esclusivamente sulla base di un software** e quindi l'amministratore può assegnare lo stesso computer a un'altra VLAN.

Sicurezza

È una buona idea limitare i partecipanti della rete a un piccolo gruppo affinché le persone non autorizzate non abbiano accesso a dati sensibili. Nell'ambito della VLAN **si possono limitare i domini broadcast** solamente a poche stazioni. In questo modo il broadcast sarà reperibile solo per i destinatari delle informazioni.

Performance

Attraverso la riduzione dei domini broadcast si migliorano anche le prestazioni. I messaggi broadcast non dovranno più circolare per tutta la rete. I messaggi inviati a tutti i partecipanti della rete ma che in realtà sono destinati solo a un definito gruppo di persone creano solamente un inutile traffico di dati. Utilizzando una VLAN **il sovraccarico della larghezza di banda viene ridotto al minimo**.

In sintesi

Le VLAN sono una variante semplice ed efficiente per poter suddividere le grandi reti in piccoli gruppi logici.

B1. Access Point

Un access point, contraddistinto dall'acronimo AP e conosciuto anche come Access Point wireless, è un dispositivo hardware di rete che consente ad altri dispositivi Wi-Fi di connettersi a una rete cablata.

Un Access Point si collega direttamente a una rete locale cablata, generalmente Ethernet, per fornire connessioni Wi-Fi utilizzando la tecnologia LAN wireless. Questo garantisce di fatto un'estensione della rete Wi-Fi e permette quindi a ulteriori dispositivi rispetto al principale di collegarsi alla rete cablata per connettersi a Internet.

Access Point significa letteralmente "punto di accesso" e sta proprio in questa definizione la differenza tra AP e reti wireless ad hoc. Una rete wireless collega direttamente due o più dispositivi senza l'intermediazione di un Access Point.

La trasmissione del segnale avviene tramite **onde radio ad alta frequenza** (2,4 GHz e i più nuovi anche 5 GHz), che sono le stesse frequenze che utilizzano il comunissimo modem/router wireless ed altri apparecchi senza fili.

Un access point WiFi è in grado di operare in modalità **Bridge** (quando viene creata una connessione punto a punto tra due access point per connettere due reti cablate tra loro), in modalità **Repeater** (che consente di aumentare la copertura di una rete wireless senza dover usare altri cavi o modem/router) ed in modalità **Client** (che permette di far collegare alla rete senza fili anche i dispositivi senza scheda di rete wireless effettuando il collegamento via cavo di questi ultimi all'access point).

Altre modalità operative meno comuni ma comunque disponibili sono la **Universal Repeater** (quando l'accesso point si connette ad altri access point e client senza bisogno di particolari configurazioni) e quella **WDS** (quando un access point può collegarsi ad altri dispositivi della categoria in modalità wireless senza necessità di chiavi).

A scanso di equivoci, è poi bene sottolineare la differenza che intercorre tra gli access point WiFi ed i **ripetitori**, altrimenti definiti **range extender**, che spesso vengono confusi tra loro. I secondi, a differenza dei primi catturano il segnale WiFi di un modem/router dotato di connettività wireless e lo ripetono in un'altra zona dell'ambiente circostante. Alcuni range extender sono comunque dotati di funzione di access point ma nel caso dei dispositivi, per così dire, puri le funzioni sono quelle di cui sopra.

Caratteristiche tecniche

- **Classi WiFi e velocità di trasferimento dei dati** – Gli access point possono supportare diverse classi WiFi ed assicurare diverse velocità di trasferimento dati: classe b (802.11b) che arriva fino a 11 Mbps, classe g (802.11g) che arriva fino a 54 Mbps, classe n (802.11n) che arriva fino a 300 o 450 Mbps e ac (802.11ac) che arriva fino a 1.3Gbps o WiFi 6.
- **Antenne e porte** – Gli access point WiFi possono avere antenne e porte di rete di vario tipo ed in numero variabile. Le antenne possono essere interne o esterne, fisse o rimovibili ed il relativo livello di potenza che si misura dB, mentre le porte servono per connettere i dispositivi alla rete tramite cavo e possono essere Fast Ethernet, con una velocità di trasferimento dati fino a 100 Mbps, oppure Gigabit Ethernet, con una velocità di trasferimento dati fino a 1.000 Mbps.
- **Client contemporanei** – Ogni access point WiFi è in grado di supportare un certo numero di dispositivi connessi in simultanea. In ambito domestico la cosa non ha particolare importanza perché generalmente tale limite è molto elevato e difficilmente si arriva a superarlo, mentre in ambito aziendale occorre tener presente tale dato, considerando la gran quantità di dispositivi da connettere.
- **PoE (Power Over Ethernet)** – Gli access point con supporto PoE possono usare un cavo Ethernet per ricevere simultaneamente dati e corrente elettrica. Si possono dunque posizionare in punti lontani dal modem/router principale senza dover impiegare lunghissime prolunghe per la presa di corrente.
- **Crittografia** – La crittografia WPA/WPA2/WPA3 è quella attualmente più sicura in fatto di reti wireless nonché la più diffusa. Un access point che si rispetti dovrebbe dunque supportare tale sistema oltre ad eventuali altre soluzioni.
- **Multi-SSID** – Si tratta di una funzione grazie alla quale è possibile creare più punti d'accesso virtuali con nomi e password diverse.
- **WPS (Wi-Fi Protected Setup)** – Gli access point WiFi con supporto al WPS consentono ai dispositivi che andranno a far parte della rete di collegarsi a quest'ultima tramite la semplice pressione di un pulsante, senza dover digitare la password.
- **Beamforming** – Trattasi di una tecnologia che consente all'access point di indirizzare il segnale in maniera prioritaria nella direzione del dispositivo che ha richiesto la connessione.

B.2 Switch

Gli switch di rete utilizzati sulle reti Ethernet sono il tipo di dispositivi che garantiscono la connettività all'interno di una LAN. Il vantaggio di utilizzare uno switch di rete è quello di distribuire la banda disponibile in una modalità economicamente sostenibile. Tutti i pacchetti in eccesso sono bloccati da questo dispositivo che si occupa anche di ottimizzare l'utilizzo della rete, garantendo eventualmente anche la consegna di questi pacchetti non prima di aver dato la precedenza al traffico più importante.

Unmanaged Network Switch: Gli switch di rete non gestiti

Si tratta degli switch di rete più facili e semplici da configurare che permettono ai dispositivi della stessa rete di comunicare fra di loro senza doversi impegnare in alcuna configurazione. È una tecnologia completamente plugin play. Non essendo richiesto alcun tipo di conoscenza tecnica, sono lo strumento più indicato per i principianti.

Managed Switch: gli switch di rete intelligente

Esattamente come gli switch non gestiti, questa tipologia di switch di rete ugualmente consente l'interconnessione di vari dispositivi all'interno di una rete ma offre una maggiore possibilità di personalizzazione e configurazione delle caratteristiche.

Gli switch di rete gestiti si suddividono essenzialmente in due categorie:

1. Smart Switch, limitate possibilità di configurazione e che consentono agli utenti di cambiare alcune funzionalità base utilizzando una semplice interfaccia Web.
2. Enterprise Switch, come il nome stesso suggerisce hanno una possibilità praticamente infinita di configurazione ma sono essenzialmente pensati per le reti più grandi. Oltre alla comune interfaccia Web, spesso sono dotati di veri propri sistemi operativi di configurazione che consentono di gestire

anche le configurazioni più complesse. Se ad esempio è necessario configurare molte VLAN un semplice switch non gestito non è sicuramente sufficiente. Oltre alla maggiore complessità, bisogna tenere presente anche il costo notevolmente superiore. La scelta di uno switch gestito quindi è molto legata anche al budget a propria disposizione.

B.3 Cavo di Rete

Eventuali nuove dorsali in fibra ottica saranno minimo in categoria OM3 con terminazioni LC.

Cos'è un cavo Cat 6?

Il cavo **di rete Cat 6**, ovvero di categoria 6, conosciuto anche col nome cavo di rete, LAN o cavo Ethernet, è un cavo in filo di rame a doppino intrecciato (ha 4 coppie di doppini) che può supportare **trasferimenti di dati fino a 1 GBit/s** (1000 megabits) di velocità. Questa ampia larghezza di banda permette trasferimenti veloci anche di file di grandi dimensioni.

È compatibile con **cavi Ethernet 10 BASE-T, 100 BASE-TX** e **reti Gigabit**, ed è retro-compatibile con gli standard di categoria precedenti come Cat5/5E e Cat3.

Solitamente le due estremità del cavo terminano con un connettore ad otto posizioni (riconoscibile dalla sigla 8P8C), il jack RJ45, usato per collegare due diversi dispositivi ed è molto importante utilizzare sempre jack compatibili con il Cat6 per ottenere le migliori performance possibili.

Come per tutti i cavi ethernet, può essere identificato dall'etichetta presente sulla guaina esterna. Acquista un cavo di rete cat. 6.

Quali utilizzi ha il Cat 6?

Nella maggior parte dei casi, il Cat 6 viene utilizzato per connettere il computer ad un dispositivo di rete come un router o uno switch, necessari per la connessione ad Internet o anche per lo scambio di file all'interno di una rete locale (LAN).

In circostanze più rare, il cavo di rete può anche essere utilizzato per **connettere i computer ad altri dispositivi**, come scanner o stampanti che operano con un modulo di rete anziché una interfaccia USB (o più obsolete porte LTP).

Cavi Cat 6: tipologie di frequenza e raggio di azione

A seconda dei segnali di frequenza supportati e del raggio d'azione che sono in grado di coprire i cavi di Cat 6 si distinguono in due tipologie:

- Cavo **Cat 6 standard**: permette segnali di frequenza più elevati di 250MHz e copre una distanza massima di 55m non schermati su 10 GBASE-T.
- Cavo **Cat6 enhanced**: questa tipologia viaggia su una frequenza di 500MHz e ha un raggio d'azione sino a 100m su 10 GBASE-T.

Qual è la differenza tra cavo schermato a doppino intrecciato e uno non schermato?

Le interferenze elettromagnetiche (EMI) sono disturbi derivanti dalla sovrapposizione di due segnali: uno che trasporta il contenuto informativo l'altro, indesiderato, solitamente causato da particolari sistemi di illuminazione, aria condizionata, stampanti e generatori vari. Specialmente nelle fabbriche, piuttosto che nei grandi uffici, questi tipi di interferenze sono molto frequenti e fastidiose.

Il cavo di Cat 6 utilizza un doppino intrecciato (STP Shielded Twisted Pair) che minimizza la diafonia causata dalle interferenze elettromagnetiche. Si parla di Cat 6 non schermato a doppino intrecciato (UTP) invece quando le interferenze non sono bloccate totalmente.

La protezione ulteriore che il cavo STP offre è data da una lamina in alluminio (la schermatura appunto) che avvolge i doppini, a sua volta la lamina è rivestita da una guaina in PVC o da una guaina senza alogeni a bassa emissione di fumi (LSZH Low Smoke Zero Halogen). Questa protezione aggiuntiva, rende **gli STP più costosi di natura**, ma anche più rigidi e conseguentemente meno flessibili durante l'installazione.

Altra considerazione va fatta per i jack RJ45 che devono essere collegati, i quali - al fine di sfruttare al meglio le caratteristiche di schermatura del cavo - dovranno a loro volta essere schermati.

Esiste un cavo Cat6 da esterni (e quindi impermeabile)?

Un cavo di rete, così come un cavo elettrico, offre un grado di protezione all'acqua piuttosto limitato. Tuttavia, esistono delle coperture specifiche per i cavi Cat 6 che permettono di impermeabilizzare i cavi adatti per un utilizzo all'esterno.

Queste guaine esterna ed impermeabilizzanti di contro rende i cavi più voluminosi e al tempo stesso rigidi. Questo di contro riduce il raggio di curvatura a causa dell'aumentato spessore, portando con sé delle limitazioni durante la stesura del cavo, un elemento che va tenuto in considerazione nel momento della progettazione dell'impianto.

B.4 UPS

La sigla UPS significa "**Uninterruptible Power Supply**" ed è tradotta in italiano come Gruppo di Continuità.

Il Gruppo di Continuità è una apparecchiatura che viene posta fra la rete di alimentazione ed i dispositivi da proteggere, allo scopo di fornire energia alle apparecchiature anche in mancanza di energia elettrica.

Esistono diversi tipi di Gruppi di Continuità ma quelli che assicurano una alimentazione priva da qualsiasi tipo di disturbo sono quelli definiti On-Line.

Il Gruppo di Continuità non deve essere confuso con altri dispositivi quali, ad esempio, stabilizzatori di tensione, trasformatori di isolamento, surge suppressor, ecc.

L'UPS garantisce la protezione per gli apparati attivi (switch, firewall e Access Point) e inoltre protegge da oscillazioni di tensione.

B.5 Armadio Rack

Gli armadi rack sono ampiamente usati nel campo industriale, delle telecomunicazioni e informatico, e servono a contenere in modo ordinato, flessibile e facilmente accessibile apparati di rete quali server, switch, router, strumenti di misura ecc. In questo modo in caso di guasto o al momento in cui si decide di aggiornare un componente, la sostituzione del pezzo o la sua manutenzione può essere effettuata velocemente ed in modo pulito e sicuro, cosa ben più problematica, onerosa e con interruzione sulla disponibilità di servizio offerto nel caso di apparato unico monoblocco. L'armadio è predisposto con porta dotata di serratura per effettuare sia manutenzione da personale autorizzato sia per la sicurezza dei dati.

B.6 Firewall

Un **firewall** è una specie di filtro che controlla il traffico di dati e blocca le trasmissioni pericolose o indesiderate in base a una serie di **regole** specifiche. La maggior parte dei firewall dispone di norme standard a cui l'utente finale può aggiungere altre personalizzate, in base alle proprie necessità.

Il firewall si interpone tra la **rete esterna**, che comprende Internet, e la **rete interna** dell'azienda, di casa o semplicemente il computer dell'utente finale. Da un punto di vista teorico, la rete interna è considerata conosciuta, sicura, attendibile e protetta, mentre quella esterna è la presunta fonte di potenziali minacce, in quanto nel complesso è sconosciuta, insicura e non attendibile.

Il firewall deve essere basato su un Appliance Open Source che gestisce:

- Filtro contenuti
- Safe Search
- Servizio DNS
- Servizio DHCP
- Sistema di Autenticazione

Problematiche rilevate

I problemi descritti di seguito vengono riportati successivamente a un sopralluogo e tengono conto di fattori oggettivi e soggettivi, come rilevazioni tecniche, ma anche segnalazioni soggettive di utenti

L'infrastruttura di rete per quanto inadeguata ed obsoleta in alcuni plessi è stata gestita fino ad ora in maniera disomogenea e "raffazzonata" cercando di dare priorità ed importanza alla sicurezza installando firewall basati su distribuzioni valide e professionali, purtroppo si riscontra la necessità di rendere più omogenea la struttura di rete installando i firewall in maniera equilibrata e a monte della rete principale in modo da gestire tutto la scuola con un solo dispositivo che verrà sostituito con uno di nuova generazione bastato comunque sulla stessa distribuzione Open source che come accennato in precedenza sono valide e professionali.

Nei plessi in cui il cablaggio in aula è già presente in categoria 5e si riscontra la necessità di aggiornarli alla cat6 in modo da garantire il 1000mb/s in tutta la rete locale della scuola. In successione al cambio dei cavi è necessario cambiare gli apparati di rete attivi in modo da garantirne la stabilità e il traffico continuo all'interno della rete.

Plesso 1: Frank

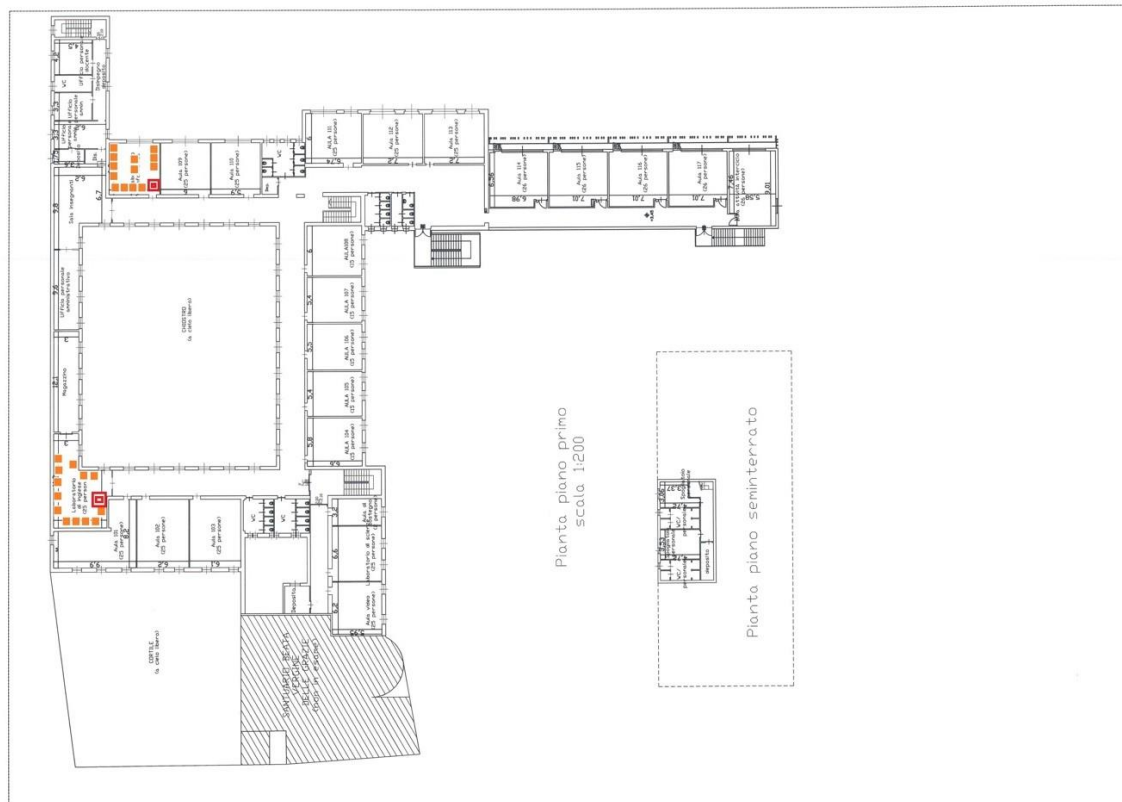
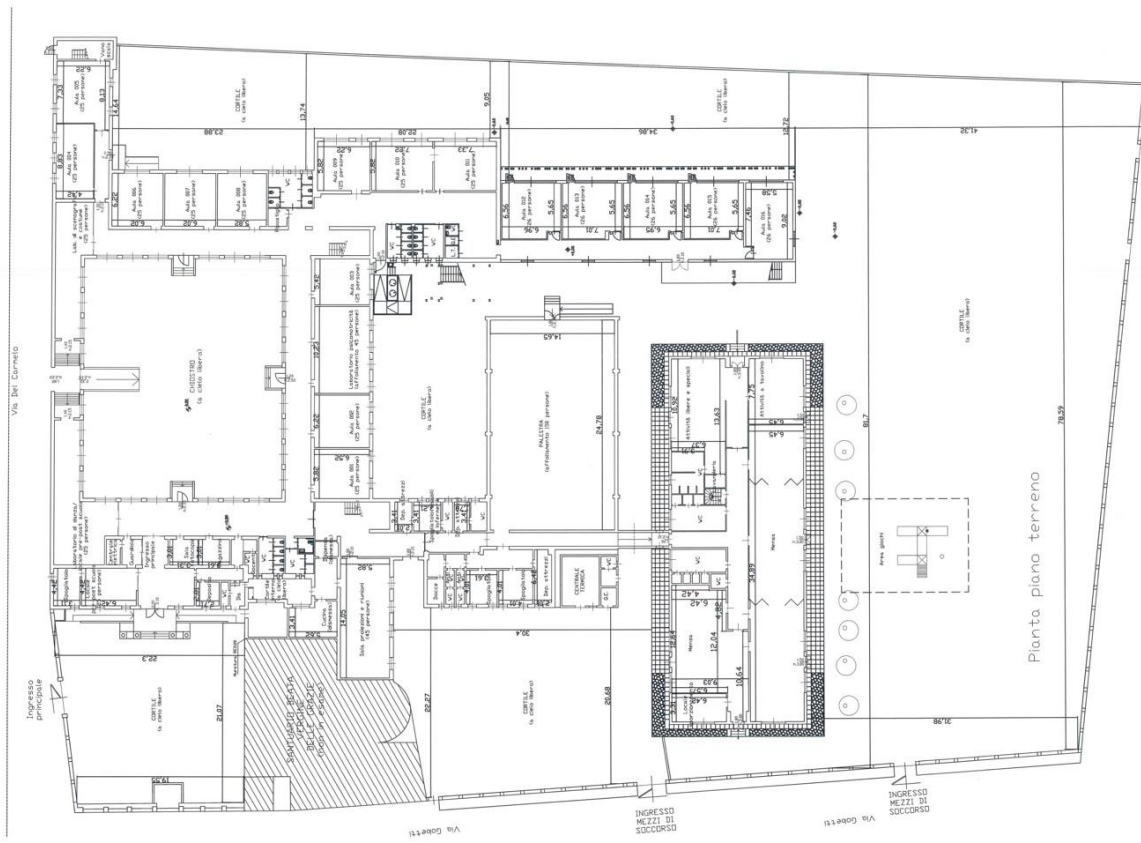
<i>Tipo</i>	<i>Caratteristiche di base</i>	<i>Numero di interventi / dispositivi</i>
<i>Access Point</i>	- Wi-Fi 6 - 5 GHz (4x4 MU-MIMO) band with a 4.8 Gbps throughput rate - 2.4 GHz (2x2 MIMO) band with a 573.5 Mbps throughput rate - 802.3at PoE+ - 300+ concurrent client capacity -IP54	0
<i>Switch</i>	- 802.3at PoE+ - 1000 mb/s - Opsione porta SFP - In dimensione 8/16/24/48 porte - Gestione vlan (802.1Q)	3
<i>Firewall</i>	- OpenSoure - Gestione filtro contenuti - Filtro dns - Servizio DHCP - Assistenza da remoto - All'occorrenza gestione VPN	0
<i>Punto di rete (inclusi quelli per le dorsali, per gli access point)</i>	<i>Cavo CAT6 schermato con terminazioni femmina in scatola 503 o su pannello Patch</i>	57
<i>UPS</i>	<i>Gruppo di continuita da 700w per Switch con stabilizzatore di tensione e protezione da cortocircuiti</i>	1
<i>Armadio rack</i>	<i>configurabile in 6/12/24/48 U</i> <i>Con Chiusura di sicurezza e vetro temperato</i>	3

Plesso 2

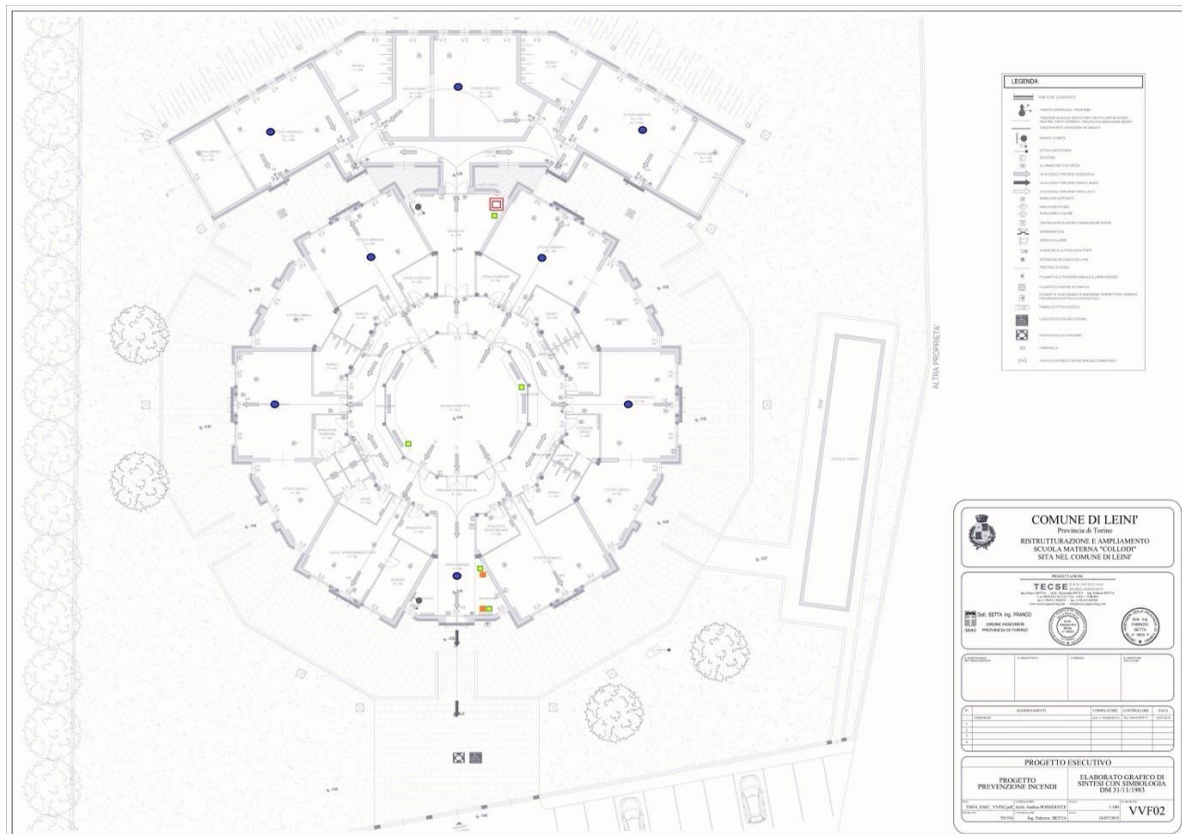
<i>Tipo</i>	<i>Caratteristiche di base</i>	<i>Numero di interventi / dispositivi</i>
<i>Access Point</i>	- Wi-Fi 6 - 5 GHz (4x4 MU-MIMO) band with a 4.8 Gbps throughput rate - 2.4 GHz (2x2 MIMO) band with a 573.5 Mbps throughput rate - 802.3at PoE+ - 300+ concurrent client capacity -IP54	8
<i>Switch</i>	- 802.3at PoE+ - 1000 mb/s - Opsione porta SFP - In dimensione 8/16/24/48 porte - Gestione vlan (802.1Q)	1
<i>Firewall</i>	- OpenSoure - Gestione filtro contenuti - Filtro dns - Servizio DHCP - Assistenza da remoto - All'occorrenza gestione VPN	1
<i>Punto di rete (inclusi quelli per le dorsali, per gli access point)</i>	Cavo CAT6 schermato con terminazioni femmina in scatola 503 o su pannello Patch	10
<i>UPS</i>	Gruppo di continuita da 700w per Switch con stabilizzatore di tensione e protezione da cortocircuiti	1
<i>Armadio rack</i>	configurabile in 6/12/24/48 U Con Chiusura di sicurezza e vetro temperato	1

Il posizionamento del singolo apparato o del punto di rete viene indicato sulle piante allegate

Plesso 1



Plesso 2



3. Riepilogo

<i>Tipo</i>	<i>Caratteristiche di base</i>	<i>Numero di interventi / dispositivi</i>
<i>Access Point</i>	- Wi-Fi 6 - 5 GHz (4x4 MU-MIMO) band with a 4.8 Gbps throughput rate - 2.4 GHz (2x2 MIMO) band with a 573.5 Mbps throughput rate - 802.3at PoE+ - 300+ concurrent client capacity -IP54	8
<i>Switch</i>	- 802.3at PoE+ - 1000 mb/s - Opzione porta SFP - In dimensione 8/16/24/48 porte - Gestione vlan (802.1Q)	4 in TOTALE: 1 Switch 8 POE+ 2 Switch 24 1 Switch 24 POE+
<i>Firewall</i>	- OpenSoure - Gestione filtro contenuti - Filtro dns - Servizio DHCP - Assistenza da remoto - All'occorrenza gestione VPN	1
<i>Punto di rete (inclusi quelli per le dorsali, per gli access point)</i>	Cavo CAT6 schermato con terminazioni femmina in scatola 503 o su pannello Patch	57 Punti laboratorio (rame) 10 Punti Access Point (rame) 02 Dorsali (fibra)
<i>UPS</i>	Gruppo di continuita da 700w per Switch con stabilizzatore di tensione e protezione da cortocircuiti	4
<i>Armadio rack</i>	- configurabile in 6/12/24/48 U - Con Chiusura di sicurezza e vetro temperato	4