# Capitolato Scuola Wi-Fi

## Introduzione

La realizzazione di un'idonea infrastruttura Wi-Fi nella scuola permette il contemporaneo accesso alla rete a tutti i partecipanti alla specifica azione didattica svolta all'interno di un determinato ambiente didattico wireless (garantendo accessi contemporanei da parte dei docenti e studenti all'interno del singolo ambiente didattico wireless). La configurazione nel seguito prevede una soluzione che permette l'abilitazione/riconoscimento degli accessi grazie all'integrazione nell'architettura della piattaforma hardware che funge da gateway di perimetro e da controllore degli accessi.

## Rete Wi-Fi

Il presente capitolato tecnico definisce le specifiche tecniche, funzionali e prestazionali per la realizzazione di una rete wireless indoor in tecnologia Wi-Fi IEEE 802.11 b/g/n nella banda di frequenza non licenziata 2,4 GHz presso l'Istituto Scolastico XXXnome istitutoXXX.

La rete ha lo scopo di garantire l'accesso in tecnologia Wi-Fi ai servizi messi a disposizione dalla scuola (Internet/Intranet) per gli utenti forniti di dispositivi dotati di connettività IEEE 802.11 b/g/n in banda 2,4 GHz (definiti in seguito "client"), quali computer portatili, smartphone, sistemi wireless o simili.

La rete Wi-Fi da realizzare sarà composta dai seguenti elementi:

1. Access Point (AP): è il dispositivo che permette al client di collegarsi ad una rete wireless. L'AP collegato fisicamente alla rete cablata della scuola (tramite Switch distribuiti) è l'elemento della rete che realizza la copertura radio Wi-Fi (in banda 2,4 GHz, standard 802.11 b/g/n). Il numero di AP da fornire è riportato nella tabella di computo metrico.
2. Switch distribuiti (a 4 o 8 porte di zona): operano come porte LAN remote del controllore (Gateway)
3. Gateway: è l'apparato che svolge la funzione di nodo centralizzato di governo e gestione del collegamento ad Internet e degli AP costituenti la rete Wi-Fi.

Oltre la fornitura dei materiali nelle quantità descritte nella tabella di computo metrico, devono essere forniti i seguenti servizi:

1. posa in opera, installazione e attivazione degli AP, degli switch e del gateway componenti la rete;
2. connessione degli AP, degli switch e del gateway alla rete cablata LAN della scuola;
3. configurazione, test e collaudo operativo della rete Wi-Fi fornita.

Nella seguente Tabella si riporta il computo metrico del sistema Wi-Fi da fornire.

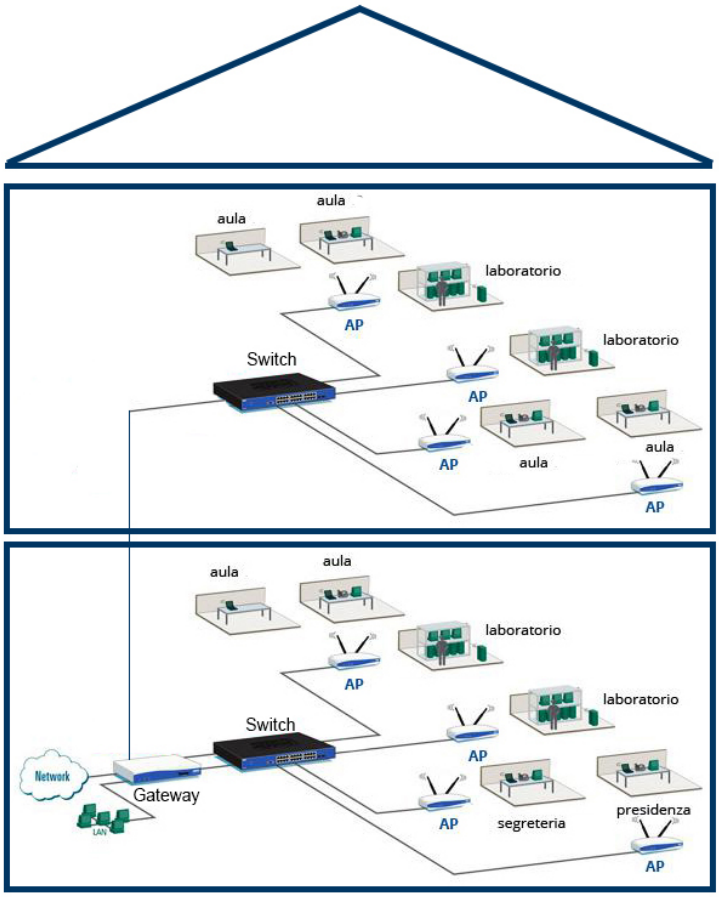
| Apparati | Quantità |
|---|---|
| Access Point (AP) | x |
| Switch distribuito di tipo A | x |
| Switch distribuito di tipo B | x |
| Gateway | 1 |

## Architettura

La realizzazione di aree Wi-Fi all'interno dell'edificio avviene installando Access Point nelle aree desiderate. Gli Access Point saranno collegati agli switch distribuiti, e questi ultimi **direttamente** tra loro o al gateway.

Il collegamento ad Internet è affidato al gateway il quale governa la rete interna e funge da controllore di perimetro, isolando dall'esterno e proteggendo i nodi interni alla rete.

L'architettura realizzata dal progetto è sinteticamente descritta nello schema esemplificativo riportato in figura.




Di seguito è riportata una descrizione degli elementi funzionali del progetto. Le specifiche in dettaglio (requisiti minimi funzionali) sono riportate nell'allegato 1.

## Access point

La realizzazione di aree Wi-Fi all'interno dell'edificio avviene installando access point (AP) nelle aree desiderate (aule, aule multimediali, laboratori, segreteria, ecc.).

L'AP previsto nel presente capitolato è dotato di antenna integrata; l'alta sensibilità di ricezione ne estende il raggio di funzionamento, rendendo la connessione stabile e veloce. Conforme allo standard IEEE 802.11 b/g/n, ciascun AP crea una rete Wi-Fi fino a 54 Mbps, ideale per scambiare file e navigare in Internet. Il dispositivo deve poter essere alimentato utilizzando il cavo Ethernet che trasporta simultaneamente dati e corrente elettrica; questa caratteristica ne moltiplica le possibilità di installazione, svincolandola dalla presenza della rete elettrica. L'AP sarà montato a soffitto, per non creare significativo disturbo architettonico.

## Switch distribuiti

L'intero cablaggio di un edificio, anche se già esistente e dotato di switch, viene ristrutturato sulla base dei nuovi switch distribuiti che verranno installati e collegati tra loro o al controllore centrale. Ogni access point sarà collegato su una porta di uno degli switch distribuiti. L'intera architettura è concepita in modo da poter utilizzare anche access point pre-esistenti. Uno o più AP afferenti ad una porta di uno switch distribuito costituiscono una zona.

Le porte di tutti gli switch distribuiti devono costituire porte remote del gateway: devono essere singolarmente configurabili dal gateway rispetto agli indirizzi rilasciati in DHCP (dal gateway su quella porta) e nella possibilità o meno che dispositivi collegati (attraverso un AP) ad una porta siano raggiungibili da dispositivi collegati ad un'altra porta dello stesso o di un diverso switch distribuito (così da poter governare i rapporti *peer-to-peer* fra i dispositivi in rete Wi-Fi). Naturalmente, per gli AP di fornitura, devono essere impediti i rapporti *peer-to-peer* fra i dispositivi associati allo stesso AP (funzionalità di *client isolation*).

## Gateway

Al gateway di perimetro è affidato il collegamento con Internet e, tra le altre, la funzione di isolare dall'esterno e proteggere i nodi interni alla rete e di pubblicare servizi interni su Internet, a seconda delle necessità.

Il gateway fornisce anche il servizio DHCP; le sue specificità consentono di avere un unico dominio DHCP per tutte le zone realizzate oppure domini DHCP distinti per zone diverse. In questo secondo caso (domini DHCP distinti per zone diverse) deve essere possibile attribuire reti IP distinte a ciascuna zona e deve essere configurabile, in modo selettivo attraverso il gateway, il routing fra le diverse zone.

Il gateway consente di controllare e visualizzare quanti dispositivi hanno fatto richiesta DHCP e quanti hanno ottenuto l'indirizzo IP, zona per zona, in modo da poter controllare il numero di dispositivi associati agli AP della zona, anche in presenza di AP disomogenei.

Il gateway deve offrire le funzioni di autenticazione degli utenti e, per ciascuno di essi, la possibilità di gestire l'accesso ad Internet, consentendolo o meno, e/o solo in certi momenti e/o per una predefinita durata e/o quantità. Deve essere anche possibile tracciare le attività Internet di ciascun utente, secondo le normative vigenti.

Il gateway previsto nel presente capitolato deve costituire una piattaforma di "*unified communication*" ed essere espandibile con le funzionalità di: Network Controller, SMS server, Cloud Storage, Mail server, Protocollo informatico, Fax server, Centralino telefonico VoIP, Wi-Fi Network Management, Hotspot Controller, VPN concentrator.

Le caratteristiche funzionali del gateway che dovranno essere implementate nel presente progetto sono di seguito elencate, si faccia riferimento all'allegato 1 per una completa descrizione delle funzionalità e di tutti i requisiti funzionali minimi richiesti.

### Hotspot Wi-fi

Il gateway deve consentire la realizzazione di distinti Hotspot Wi-Fi, differenziabili zona per zona con captive portal personalizzabili, con grafica e loghi della scuola. I diversi hotspot devono utilizzare un meccanismo di autenticazione unificato, basato sull'utente e sull'indirizzo IP del dispositivo (e non solo sul suo MAC address).

### Il governo dell'accesso ad Internet

In quanto apparato *intelligente* per accedere ad Internet, il gateway deve permettere, con facilità e sicurezza, di proteggere le reti interne, governandone l'uso *per utente*. Tra le caratteristiche principali:

- protezione completa della rete interna (*firewall*), con possibilità di pubblicare su Internet (*esporre*) servizi, in modo selettivo;
- separazione, su porte diverse, di reti interne diverse (rete uffici: Presidenza, Segreteria, . . . ; reti didattiche: Laboratori, LIM, . . . ), anche nel caso si utilizzi un unico accesso Internet (es. ADSL);
- governo delle attività Internet degli utenti interni, riconoscendoli *per nome utente* (e non solo per indirizzo IP);
- modalità di accesso ad Internet differenziate, ad es. per uffici, docenti, alunni. . . ;
- limitazione della navigazione per fasce orarie, per tempo massimo di navigazione e traffico massimo di navigazione.

### VPN

Il gateway include le funzionalità di concentratore VPN (Virtual Private Network) che consentono sia il collegamento di sedi (plessi) diverse fra loro in modo sicuro, sia l'accesso alle reti interne, in modo controllato e sicuro, di utenti esterni (docenti, personale esterno di assistenza, etc.) .

## Planimetrie

L'allegato 2 riporta le planimetrie delle aree della scuola che si desidera fornire di copertura wireless.

## Allegato 1. Specifiche funzionali

Di seguito sono riportati i requisiti minimi degli elementi funzionali previsti nel capitolato.

### Access Point (AP)

- Tecnologia di connessione: Wi-Fi
- Banda di frequenza: 2.4 Ghz
- Porta10/100 Ethernet
- Tecnologia di alimentazione: PoE
- Data Link Protocol: IEEE 802.11b/g/n

- Funzione di *client isolation*
- Indicatori LED di stato e funzionamento

## Switch

- Configurabile e controllabile dal gateway
- Alimentabile via cavo Ethernet (PoE) o con alimentatore
- Porte Ethernet:
  - Switch di tipo A: 10/100 se switch con AP
  - Switch di tipo B: 10/100/100 se switch di transito

## Gateway

### Descrizione apparato

Il gateway è l'apparato che svolge la funzione di nodo centralizzato di gestione per tutta la rete cablata e Wi-Fi e degli AP (access point); ad esso è affidato il collegamento ad Internet con l'obiettivo di isolare dall'esterno e proteggere i nodi interni alla rete. Il gateway, deve assolvere alle funzioni di autenticazione degli utenti e supportare avanzate funzioni di governo dell'accesso ad Internet e di gestione delle comunicazioni all'interno della scuola, nel seguito descritte.

Occorre che l'apparato:

- abbia due porte di rete fisicamente separate, una porta locale verso rete didattica (aule, laboratori, etc.) ed una verso rete uffici (presidenza, segreteria, etc.); il collegamento ad Internet deve avvenire attraverso una terza distinta porta;
- sia in grado di abilitare selettivamente delle comunicazioni fra la rete didattica e la rete amministrativa;
- sia in formato standard rack 19" ma all'occorrenza installabile in modalità desktop;
- includa una procedura di quickstart;
- includa il ripristino della configurazione di rete di fabbrica;
- preveda la possibilità di introduzione distinti profili di Amministrazione;
- sia facilmente gestibile e configurabile attraverso pagine web;
- preveda la funzionalità di importare ed esportare l'elenco degli utenti tramite file csv, xls;
- includa la possibilità di definire la password policy (lunghezza, caratteri speciali, ecc. . . )
- sia basato su un'architettura di Single Sign-On (SSO) integrata LDAP e Radius
- consenta una completa gestione dell'infrastruttura SSL con certificati localizzati e no standard

L'apparato costituisce una piattaforma di unifed communication in grado di integrare, in un unico hardware, funzionalità di:

- Network control;
- Mail server;

- Protocollo informatico;
- Fax server;
- Centralino VoIP;
- Wi-Fi Network management;
- Hotspot control;
- VPN concentrator;
- SMS server;
- Cloud Storage.

Di seguito si riportano le funzioni minime che l'apparato deve poter implementare, tramite l'acquisto di moduli aggiuntivi; le funzioni da fornire con questo progetto sono riportate nel capitolato.

Le caratteristiche tecniche dell'apparato dovranno essere documentate allegando, al progetto di gara, schede tecniche e manuale della piattaforma nel quale sono descritte le funzioni e le procedure di configurazione.

**Network control**

- Gateway di perimetro per la gestione dell'accesso contemporaneo ad Internet degli utenti della rete
- Possibilità di calmierare l'accesso di ogni utente per quantità di traffico e/o per tempo di connessione e di confinarlo in fasce orarie definite
- Il collegamento ad Internet deve essere attivato esplicitamente dall'utente
- Log degli accessi
- Log della navigazione
- Possibilità di impedire l'accesso a determinati siti (parental control) e domini o, in modo simmetrico, consentirlo solo per i siti e i domini d'interesse.I controlli devono essere esercitati non solo sulle attività di navigazione web, ma anche sulle apps degli smartphones e su determinati protocolli
- Possibilità, attraverso un firewall hardware integrato statefull inspection, di filtrare e bloccare indirizzi IP, protocolli, connessioni entranti ed uscenti, portando la protezione perimetrale al livello degli standard più evoluti
- Possibilità delle diverse reti (ad es: le reti per la didattica e quelle degli uffici) di poter condividere l'accesso ad Internet ed altre risorse comuni pur rimanendo reti distinte e separate fisicamente su interfacce diverse ed utilizzando un unico contratto di connessione
- Nel caso di organizzazione multisede, possibilità di consentire l'accesso diretto ad Internet per ciascuna sede (senza impegnare banda trasmissiva fra le sedi), pur mantenendone il governo centralizzato
- Nel caso di organizzazione multisede, gli utenti di ogni sede dovranno potersi muoverei fra le diverse sedi, conservando sempre le proprie credenziali (username e password) ed il proprio profilo di abilitazione.
- Ridondanza e back-up del collegamento ad Internet (funzione Auto ReRoute)
- Supporto SSL
- server DHCP
- servizio DHCP relay

- servizio DNS e alias DNS
- Funzionalità di NAT (Network Address Translation)
- Funzionalità di PAT (Permanent Address Translation)
- Funzionalità di certification authority, ovvero possibilità di auto-generare certificati per i propri servizi e per i servizi di altri server
- Configurazione Timeout (sec) e Soglia minima di traffico (Packets) che regolano l'interruzione automatica della connessione ad Internet, in assenza di traffico
- Supporto UMTS
- Supporto LTE
- Possibilità di effettuare connessioni di tipo PPPoE
- Supporto di tecniche di LOC bonding per aumentare la banda e garantire continuità del servizio in caso di caduta di uno o più link di comunicazione
- Utilizzo di regole di QoS con le quali sia possibile classificare il traffico e inviarlo su percorsi con bande limitate

**Mail server**

- Server di posta interno alla scuola, con mailbox fisicamente all'interno della rete della scuola
- Invio e ricezione delle email ad alta velocità, con garanzia di integrità dei dati e cifratura, nel rispetto delle normative in materia di tutela dei dati sensibili
- Gestione unificata delle caselle (interne ed esterne) del proprio dominio, delle caselle di altri domini, delle PEC
- Posta elettronica dovrà essere accessibile e sincronizzata tra PC, tablet e smartphone, tramite client di posta
- Uso tramite webmail
- Possibilità di gestire in automatico i flussi documentali delle pratiche, le richieste dei docenti, dei genitori e degli altri utenti, la corrispondenza interna ed esterna.
- Possibilità di condividere tra utenti o gruppi di utenti mailbox o solo alcune cartelle
- Possibilità di definire sofisticati filtri per lo smistamento automatico dei messaggi in base ai campi: from, to, subject
- Possibilità di inserire automaticamente per tutte le email in uscita un indirizzo email in bcc
- Antivirus e antispam integrati (con regole di apprendimento automatico)
- Gestione alias
- Funzione di stamping che consente di apporre una timbratura (stamping) alle email ricevute su specifici account
- Possibilità di apporre una firma di default della scuola
- Log delle email in transito
- Possibilità di definire un'identità esterna di deafult
- Possibilità di gestire le whitelist (da cui accettare sempre posta) e le blacklist (indirizzi da cui rifiutare posta)

**Protocollo Informatico**

- Sistema integrato di gestione informatica della corrispondenza e protocollo informatico, senza l'introduzione di software esterni dedicati allo scopo
- Numero di protocollo del documento generato automaticamente dal sistema e registrato in forma non modificabile;
- Data di registrazione di protocollo assegnata automaticamente dal sistema e registrata in forma non modificabile;
- Mittente per i documenti ricevuti e il destinatario o i destinatari per i documenti spediti, registrati in forma non modificabile;
- Data e protocollo del documento ricevuto;
- Segnatura del documento;
- Classificazione e titolario d'archivio;
- Completa registrazione di tutte le informazioni necessarie ad individuare il singolo documento ricevuto o spedito (entrata/uscita, oggetto, mittente/destinatario, titolo/classe/fascicolo, codice dossier, impronta, ufficio interno, n. di prot. e data del documento ricevuto in caso di corrispondenza in entrata, riferimento n. protocollo precedente).

**Fax server**

- Server fax con possibilità di gestire linee fax, collegandosi direttamente alla rete telefonica oppure ad un centralino telefonico
- Possibilità di trasmettere e ricevere fax tramite accesso a specifiche pagine web
- Reinvio automatico dei fax in caso di esito negativo di trasmissione
- Archiviazione dei fax trasmessi e ricevuti
- Possibilità di consultare gli archivi dei fax trasmessi e ricevuti tramite accesso a specifiche pagine web: l'archivio conserva la struttura delle corrispondenti pagine web per cui rende possibile una completa consultazione anche offline
- Possibilità di aggiungere ulteriori descrizioni ai fax trasmessi (il default è un unico campo "Commento")
- Possibilità di consultare dati statistici circa l'invio e la ricezione dei fax; tali dati sono accessibili ai soli utenti amministratori
- Cancellazione dei fax; tale funzionalità può essere disattivata in fase di installazione per impedire una cancellazione fortuita dei fax
- Invio tramite posta elettronica delle notifiche di ricezione fax, di avvenuta trasmissione (o errore di trasmissione) e di accodamento in attesa di trasmissione
- Possibilità di inserire, nel momento di trasmissione di un fax, un indirizzo email a cui far pervenire la notifica dell'invio e in allegato il fax.
- Possibilità di anteporre una cover page e di applicare filigrane di sfondo ad ogni fax trasmesso
- Possibilità di collegare il fax su porta analogica, ISDN o PRI
- Sistema multifax su primario
- Accesso da remoto al sistema per l'invio dei fax

**Centralino VoIP – Voice over IP**

- Centralino telefonico VoIP
- Number portability: l'utente che digita il suo codice personale potrà portare con sé il proprio numero di telefono, spostandosi da una stanza (o da una sede) all'altra;
- Click2call: possibilità di accedere al proprio desktop web dal quale telefonerà cliccando sulla sua rubrica telefonica web
- Possibilità di accedere alla propria segreteria telefonica dal telefono (se le caratteristiche del telefono lo prevedono) e per mezzo della posta elettronica
- In caso di istituti comprensivi e circoli didattici, ciascun plesso potrà essere collegato agli altri, attraverso il suo centralino VoIP, senza particolari contratti per linee telefoniche dedicate, utilizzando numerazione abbreviata
- Possibilità di usare telefoni Wi-Fi come cordless
- Disponibilità di configurazione dell'interfaccia verso la rete PSTN con porta analogica, 2 o 4 porte BRI per ISDN, porta PRI
- Possibilità' di installazione di sistema IVR
- Possibilità di installazione di sistema voice-mail
- Connessione da remoto in L2TP dello smartphone

**Wi-Fi Network manager**

- Possibilità di supportare la realizzazione di reti Wi-Fi performanti ed economiche, attraverso dispositivi Switch (a 4 o 8 porte di zona), che operano come porte LAN remote del controllore
- Possibilità di integrazione di Access Point disomogenei
- Funzionalità L3
- Funzionalità L2: snooping IGMP, mirroring delle porte, protocollo Spanning Tree, protocollo LACP (Link Aggregation Control Protocol).
- Funzionalità di controllo di flusso 802.3x IEEE che consente ai server di connettersi direttamente allo switch per eseguire un trasferimento dei dati in modo rapido e affidabile
- Possibilità di controllare e visualizzare quanti dispositivi hanno fatto richiesta DHCP e quanti hanno ottenuto l'indirizzo IP

**Hotspot**

- Controllo delle connessioni ad Internet hotspot Wi-Fi
- Captive portal personalizzabile con grafica e loghi della scuola
- Registrazione manuale dell'utente, con la consegna di username e password
- Registrazione in self service dell'utente tramite SMS
  - Configurazione personalizzata dei testi di "Registrazione" e di "Recupera password"

- Possibilità di abilitare la navigazione sulla base di codici di autorizzazione che la scuola può stampare in autonomia e personalizzare nel formato grafico
  - Possibilità di associare distinti profili di navigazione ai codici di autorizzazione
- Meccanismo di autenticazione basato sull'indirizzo IP del dispositivo (e non solo sul suo MAC address)
- Possibilità di realizzare "federazioni" di hotspot in cui diversi accessi ad Internet condividono il database degli utenti: l'utente di un hotspot può navigare su tutti gli altri federati, con le medesime credenziali (username e password)
- Configurazione della cancellazione automatica degli utenti che non si collegano al sistema per lungo tempo
- Possibilità di configurare il collegamento diretto ad Internet, cioe' senza l'inserimento delle credenziali, verso siti internet o server specifici (come quello del registro elettronico)

**VPN**

- Concentratore VPN (Virtual Private Network) che consente di collegare sedi (plessi) diverse fra loro in modo sicuro
- Possibilità di consentire ad utenti esterni (road-warrior) l'accesso alle reti interne, in modo controllato e sicuro
- Supporto OpenVPN
- Supporto L2TP su Windows, Mac, Apple, Android

**SMS server**

- Server per la gestione e l'invio massivo di SMS, con trattamento sofisticato dei messaggi in-bound ed out-bound
  - gli SMS ricevuti vengono smistati via email agli utenti o agli alias di posta elettronica,, in base ad una serie di controlli che vengono effettuati sul testo e sul mittente dell'SMS
  - gli SMS ricevuti devono poter essere inoltrati anche via SMS, purché siano ricevuti da numeri di cellulare autorizzati a tale modalità di inoltro.
- Possibilità di invio degli SMS tramite email
- Possibilità di ricezione degli SMS tramite email
- Possibilità di utilizzo degli alias email nell'invio di SMS
- Visualizzazione delle statistiche degli SMS ricevuti ed inviati per mittente

**Cloud Storage**

- Piattaforma locale di archiviazione, sincronizzazione e condivisione di file e immagini
- Spazio di archiviazione configurabile per utente o gruppi di utenti.
- Possibilità di integrazione con servizi di storage esterni (Dropbox, WebDAV)
- Condivisione file e cartelle con account interni

- Statistiche delle attività utente e dello spazio di archiviazione
- File di log
- Accesso da remoto

## Allegato 2. Planimetrie

Allegare le planimetrie delle aree che si desidera fornire di copertura wifi

(Rev. 25281).