

PROGETTO COMPLETAMENTO RETE WIFI SCUOLA

ISTITUTO ISTRUZIONE SUPERIORE "DI POPPA – ROZZI" TERAMO

RETE ESISTENTE

Le nostre sedi sono state opportunamente dotate di apparati access point Ubiquiti Unifi AP a copertura totale e gestiti da un pc con l'apposito software di Ubiquiti.

Il progetto mira a completare l'infrastruttura di rete esistente e consolidarla sulla base degli elementi tecnologici descritti (vedi allegato schema di rete). Il cablaggio esistente (inclusi gli eventuali switch di rete) verrà collegato ai nuovi switch distribuiti e, attraverso essi, monitorato e gestito pervenendo ad un completo governo della rete.

Il consolidamento dell'infrastruttura Wi-Fi esistente deve permettere il contemporaneo accesso alla rete a tutti gli attori della scuola definendo l'identità digitale di ognuno e consentendo ad essi di usufruire dei servizi digitali che la scuola offre: accesso ad internet, repository, mail, e-learning, messaggistica ecc.

La configurazione prevede l'introduzione di 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, in grado di erogare servizi IP di livello applicativo ed al tempo stesso in grado di governare le funzioni di rete cablata e Wi-Fi.

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 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.

Il gateway, nel caso di diversi apparati, dislocati in differenti aree e con connessioni ad Internet diverse, consente di realizzare una federazione di Hotspot, di modo che un utente che si registri in un'area Hotspot possa accedere, con le medesime credenziali, in tutte le altre aree Hotspot della federazione.

Il gateway deve svolgere le funzioni di:

1. Network control

- Gateway di perimetro per la gestione dell'accesso contemporaneo ad Internet degli utenti
- Possibilità di calmiere l'accesso di ogni utente per quantità di traffico e/o per tempo
- Il collegamento ad Internet deve essere attivato esplicitamente dall'utente
- Log degli accessi e 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
- 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 muovere 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
- Supporto SSL
- Server DHCP
- Servizio DHCP relay
- Servizio DNS e alias DNS
- Funzionalità di NAT (Network Address Translation) e 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/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

2. 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
- Possibilità di controllare e visualizzare quanti dispositivi hanno fatto richiesta DHCP e quanti hanno ottenuto l'indirizzo IP

3. 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, cioè senza l'inserimento delle credenziali, verso siti internet o server specifici (come quello del registro elettronico)

4. VPN concentrator

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

Il gateway deve costituire una piattaforma di "unified communication" ed essere espandibile con le funzionalità di: SMS server, Cloud Storage, Mail server, Protocollo informatico, Fax server, Centralino telefonico VoIP.

Il gateway, nel caso di diversi apparati, dislocati in differenti aree e con connessioni ad Internet diverse, consente di realizzare una federazione di Hotspot, di modo che un utente che si registri in un'area Hotspot possa accedere, con le medesime credenziali, in tutte le altre aree Hotspot della federazione.

Le caratteristiche funzionali del gateway che dovranno essere implementate nel presente progetto sono di seguito elencate:

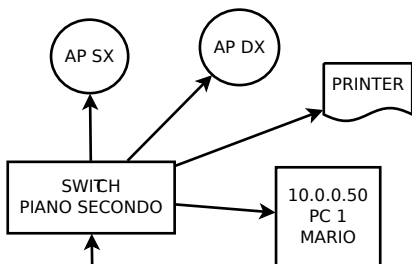
- deve consentire la realizzazione di distinti Hotspot Wi-Fi, differenziabili zona per zona con captive portal personalizzabili, con grafica e loghi della scuola. I diversi hotspot devono utilizzare un meccanismo di autenticazione unificato, basato sull'utente e sull'indirizzo IP del dispositivo (e non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

- controllo dei contenuti e blocco della navigazione per siti non idonei.
- gestione mail, in modo da gestire indirizzi di posta per docenti e studenti.

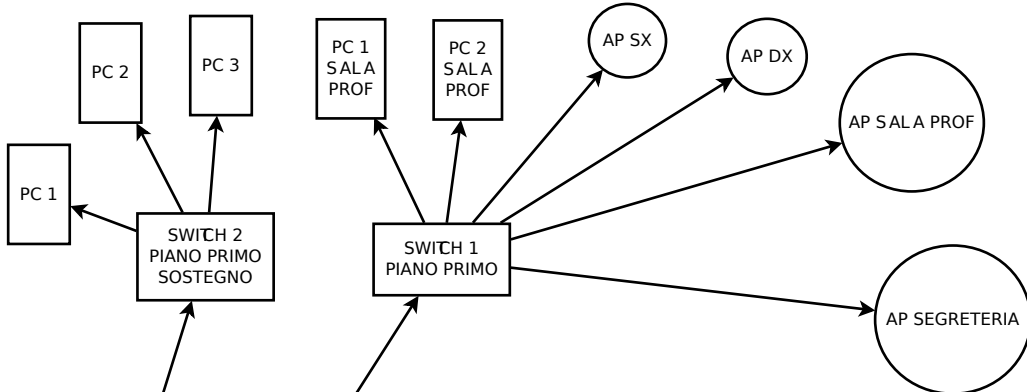
Il progettista

Prof. Giuseppe PIO

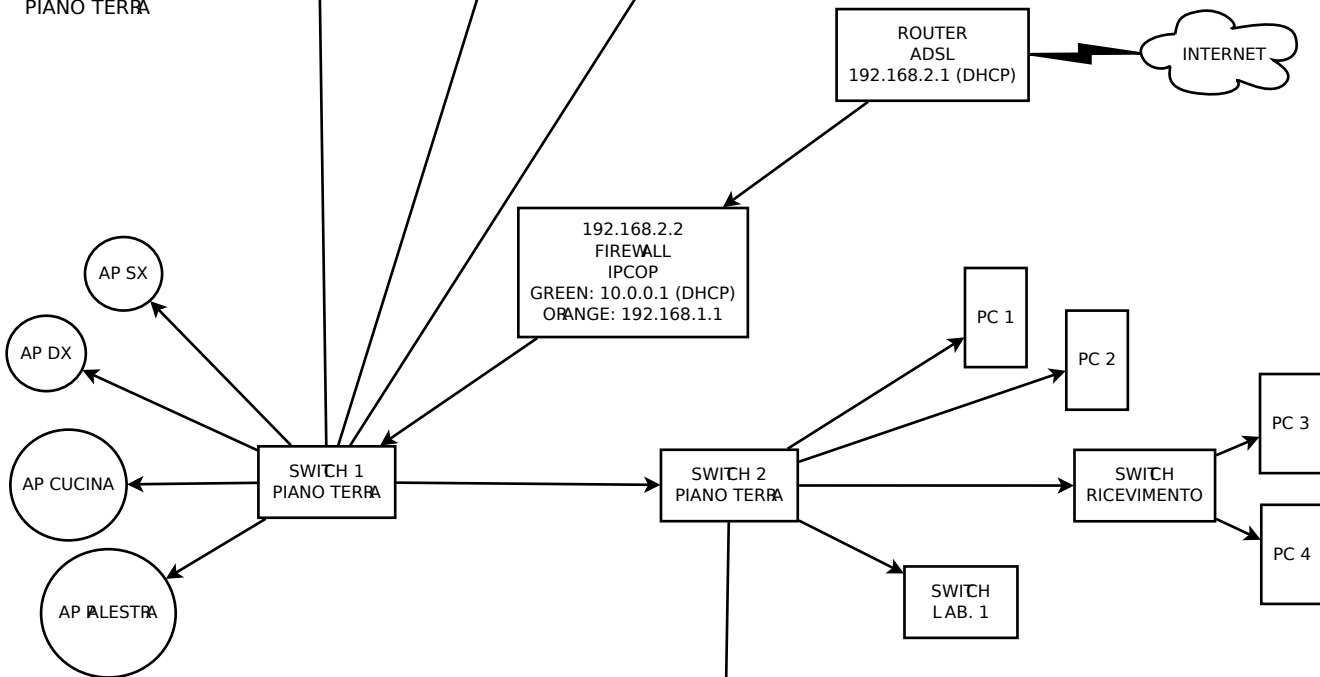
PIANO SECONDO



PIANO PRIMO



PIANO TERRA



PIANO SEMINTERNO

