SCUOLA SEC. I°- "V. E. ORLANDO"-PALERMO
Prot. 0001999 del 21/02/2022
(Entrata)

PROGETTO RETE LAN E Wi-Fi

Scuola Secondaria di Primo Grado Vittorio Emanuele Orlando

AVVISO 20480 del 20/07/2021 - FESR REACT EU - Realizzazione di reti locali, cablate e wireless, nelle scuole.

IDENTIFICAZIONE LORO ESIGENZE

- Dismissione impianto rete lan e w-lan esistente sia didattica che amministrazione.
- Realizzazione centro stella principale comprensivo di armadio rack opportunamente dimensionato almeno 42 U, con all'interno patch panel in cat 6° e pannello ottico, realizzazione alimentazione elettrica con interruttore magnetotermico differenziale dedicato e presa industriale monofase interbloccata da parete, gruppo continuità con relativa realizzazione di pulsante di sgancio, switch management POE+ layer 3, ventole raffreddamento, installazione pulsante di sgancio.
- Realizzazione dorsali in fibra ottica tra il centro stella verso gli armadi secondari di piano.
- Realizzazione impianto rete lan area amministrazione OMNICOMPRENSIVO.
- Realizzazione impianto rete lan/ wifi 6 802.11ax area didattica OMNICOMPRENSIVO.
- Installazione Next Generation Firewall fascia alta.
- Installazione controller di rete.
- Creazione VPN "Site to Site".
- Creazione VPN "Client to Site".

ESIGENZE

L'esigenza principale della realizzazione è quella di dotare la nostra Amministrazione scolastica di un'infrastruttura di rete capace di coprire gli spazi didattici e amministrativi della scuola, nonché di consentire la connessione alla rete da parte del personale scolastico, delle studentesse e degli studenti, assicurando, altresì, il cablaggio di tutti gli ambienti, la sicurezza informatica dei dati, la gestione e autenticazione degli accessi.

Nonostante la complessità intrinseca di un impianto così tecnologicamente avanzato, si vuole mirare ad ottenere un sistema di semplice fruibilità, di facile di utilizzo da parte di tutti i soggetti che fanno parte del sistema scuola e non possiedono competenze informatiche estremamente avanzate.

OBIETTIVI

- Fornire ai Docenti e agli allievi accesso a risorse utili alla didattica (Internet, E-learning, ecc.);
- Facilitare la nuova didattica digitale collaborativa e co-costruttiva, mettendo a disposizione degli utenti le classi virtuali funzionanti anche in assenza di collegamento ad Internet;
- Fornire ai docenti l'accesso al Registro Elettronico, con priorità rispetto ad altre applicazioni che utilizzano Internet, per non rallentare la normale attività didattica;
- Fornire una infrastruttura affidabile e sicura che consenta a docenti ed allievi di utilizzare a scuola anche i dispositivi personali (tablet e PC), senza rischi di poter arrecare danni o manomissioni sulla rete;
- Vietare l'accesso a contenuti non adatti all'ambiente scolastico;
- Consentire priorità al traffico utile alla didattica, come il registro elettronico, all'accesso dei Docenti rispetto agli alunni, limitare il traffico pesante ed inutile (ad es. aggiornamenti automatici di tablet e PC) durante le lezioni;
- Tenere separati, dati sensibili e risorse condivise (stampanti, scanner, dischi di rete, totem

informativi) presenti nell'area amministrativa rispetto all'area didattica;

- Attivare i servizi in remoto della rete;
- Realizzare nell'area amministrazione del dominio active directory;
- Realizzare tutte le Opere civili accessorie alla fornitura di cablaggio;
- Garantire la gestione e manutenzione on site delle postazioni di lavoro;
- Implementare una Piattaforma hardware/software di repository (completa di tutto);
- Formare attraverso il personale con corso della durata non inferiore alle 20 ore da svolgersi on site;
- Attivare una piattaforma web contenete corsi di autoformazione, per docenti e personale ATA, relativi all'utilizzo del sistema di cablaggio strutturato.

- L'attivazione del servizio di garanzia, assistenza e manutenzione h 24 senza limiti di chiamata "**on site"** della rete e di tutti gli apparati attivi e passivi che compongono la stessa per almeno 3 anni dalla data di sottoscrizione del contratto. I numeri telefonici e di fax dei centri di manutenzione e assistenza devono essere numeri Verdi gratuiti per il chiamante o, in alternativa, numero/i telefonico/i di rete fissa. Non sono ammessi, pertanto, numeri telefonici del tipo 199.xxx.xxx.e simili. L 'installazione e gestione del software di gestione della rete "licenza illimitata";
- L'attivazione dei servizi di: manutenzione preventiva, manutenzione correttiva, manutenzione evolutiva;
- servizio di assistenza e manutenzione di tipo ***SHP*** Super High Profile da espletarsi, cosi come previsto dal documento di cui al precedente capoverso, ad opera di personale che abbia adeguate competenze professionali in termini di esperienza lavorativa almeno quadriennale in ambito manutenzione e gestione dei sistemi di reti locali. Pertanto si richiedono i nominativi ed relativi curriculum del personale che sarà dedicato allo svolgimento del servizio presso la Ns Istituzione scolastica, allegando, come di prassi, certificato CCIAA e dati anagrafici del responsabile nominato per l'assistenza e la manutenzione;
- L' installazione, la gestione e l'assistenza on site dei server sistemi di sicurezza "firewall" con l' attivazione dei servizi di tipo sicurezza alta uno per ogni sede sia centrale che succursale;
- L'installazione di un sistema di gestione NSA (Network Security Appliance) della rete sia lan che wlan;

Condizioni necessarie inerenti alla configurazione di Network Policy

Per ottenere una rete lan-vlan/wlan ben strutturata, dalla facile e semplice gestione, si rendono necessarie l'adozione di policy opportunamente configurate che avranno come obiettivo primario, la sicurezza informatica, la corretta distribuzione delle risorse ed il mantenimento delle misure di privacy.

Inoltre dovranno essere implementati tramite configurazione tutti gli strumenti necessari per la rilevazione di malfunzionamenti, intrusioni, con i relativi settaggi per l'invio di alert presso mail istituzionali. I report dovranno essere facilmente leggibili e contenere le informazioni per una veloce risoluzione dell'eventuale criticità.

In particolare devono essere implementate le seguenti funzionalità:

1. Creare VLAN rispettanti lo standard 802.1Q *IEEE Std. 802.1Q-2003, diverse per* destinazione d'uso secondo le esigenze (es. amministrazione, didattica, wi-fi, voip, laboratori ecc), ed implementare le policy per evitare che tra le diverse Vlan ci siano "attraversamenti" di rete non voluti, che possono mettere a rischio l'integrità della struttura.
2. Creare differenti Wlan con SSID diverse (es: scuola, docenti, alunni, ospiti), ogni rete WIFI deve avere delle policy specifiche, come ad esempio la possibilità di far navigare con il WIFI a servizio degli alunni solamente su una lista di siti specifici;
3. Creare delle blacklist personalizzate per il blocco di siti specifici o il blocco di utenti o dispositivi;
4. Attivare e configurare le tecnologie di trafficshaper e bandwidth su ogni vlan, fare un attento studio sul carico lavoro/traffico dati, creare degli alert e dei grafici sul traffico di ogni singola vlan da inviare via mail.
5. Attivare e configurare QoS (Quality of Service) per definire una politica di prioritizzazione del traffico.
6. Creare regola per la gestione degli SNMP per il monitoraggio del traffico di rete, i flussi di rete, le code. Garantire l'implementazione di MIB di primo e secondo livello per inviare trap al server SNMP eventi come lo stato del collegamento di rete, l'accesso a cartelle, lo stato dei dispositivi.

7. Creare regole per il controllo delle porte di trasmissione SMTP, per il monitoraggio di flussi dati riconducibili a virus che posso generare spam, generare alert ed invio mail al verificarsi dell'evento.

8. Creare Vpn "Site to Site"tra i plessi distaccati e la sede centrale, tale Vpn deve essere a servizio delle Vlan opportunamente configurate, attivando le necessarie regole di protezione e privacy, consentire la gestione delle risorse dal plesso centrale secondo le aree di interesse e la possibilità di condividere le stesse dai vari plessi.

9. Creare Vpn "Client to Site" per client remoti e la sede centrale, tale Vpn deve essere a servizio dell'amministrazione e per tale motivo dovranno essere generati certificati di connessione "ad personam", da fornire al personale della segreteria su suggerimento del DS e del DSGA.

10. Configurazione Switch manageriali, per il corretto funzionamento delle vlan su tutti i plessi con struttura omogenea, garantendo accessi di tipologia LDAP-SSO

11. Manuali operativi in lingua italiana, oltre a quelli rilasciati dal costruttore delle apparecchiature, quelli relativi all' utilizzo dei dispositivi di rete redatti dalla azienda installatrice.

12. Rilascio relazione tecnica inerente alla certificazione del cablaggio.

13. Creazione portale di accesso alla connettività WIFI con autenticazione "ad personam" con tecnologia di tipo LDAP-SSO.

Esigenze Tecnologiche

Si intende realizzare un cablaggio strutturato che preveda le dorsali tra i vari armadi Rack principali e secondari in fibra ottica multi modale, e dai vari armadi di piano verso gli end point in rete lan (cat 6a). Per quanto concerne la rete Wireless dovrà essere realizzata tassativamente con apparati in tecnologia 802.11ax (wifi 6). Tale cablaggio strutturato dovrà permettere l'accesso a tutti i dispositivi sia in rete lan sia in modalità wifi senza fili, che includa tutti i plessi scolastici.
La rete che verrà realizzata deve garantire la massima protezione su tutti i fronti di accesso, sia Wireless che LAN.
Considerato che le frequenze wireless a 2,4 GHz sono ormai sature di dispositivi che operano su tali frequenze, tutti gli access point dovranno essere a doppia radio e supportare la doppia banda di frequenza 2,4 e 5 GHz contemporaneamente, per poter gestire un maggior numero di connessioni contemporanee e prive di interferenze.
Tutti gli access point dovranno essere di ultima generazione tipo 802.11AX, gestibili da interfaccia centralizzata, per velocizzare e semplificare la gestione, e per avere da un unico punto di accesso un quadro completo dell'andamento di tutta la infrastruttura di rete.
Tutti gli access point dovranno essere gestiti da un controller centralizzato, per avere funzioni avanzate quali l'handover degli utenti, l'assegnazione dei canali e la regolazione delle potenze di trasmissione automatica, per velocizzare e semplificare la gestione, e per avere da un unico punto di accesso un quadro completo dell'andamento di tutta la infrastruttura di rete. Il controller di gestione deve essere in grado di controllare gli access point e deve possedere una sua logica anche autonoma di funzionamento, per una maggiore affidabilità, e deve funzionare perfettamente anche in assenza di collegamento ad internet. Ogni access point dovrà essere collegato tramite cavo di rete allo switch di piano, e non si accetteranno installazioni con access point configurati come ripetitori wireless o mesh, perché tali soluzioni riducono notevolmente la banda disponibile.
Al fine di limitare l'esposizione ai campi elettromagnetici soltanto nelle ore di effettivo utilizzo, ed evitare abusi fuori dagli orari scolastici, l'accensione e lo spegnimento di ogni access point deve essere gestibile tramite una interfaccia grafica centralizzata, e deve essere possibile l'accensione e lo spegnimento del singolo access point in base alle necessità.
Per garantire adeguate performance attuali e future, si richiede che tutti gli apparati attivi e passivi (punti rete LAN, Switch, Access Point, Firewall, ecc.) siano certificati in categoria 6a e wifi 6.

SOLUZIONE PROGETTUALE La soluzione di Cablaggio strutturato, in relazione

Alle esigenze,si compone dei seguenti elementi:

Apparati Attivi

Col termine apparati attivi ci si riferisce comunemente ai dispositivi che gestiscono il traffico e la struttura del flusso dati nelle reti informatiche, come server, switch, router, firewall, access point ecc.

Nell' ambito di un progetto di rete, deve essere garantita l'installazione, configurazione ed amministrazione degli apparati attivi, definendo i componenti e configurando i dispositivi in base alle esigenze dell'utenza, consentendo una efficiente gestione dell'intera infrastruttura, un monitoraggio costante, nonché una accurata politica di sicurezza.

Gli apparati prescelti devono avere le massime potenzialità di espansione verso le future tecnologie, in modo da non causare una rapida obsolescenza del sistema. L'integrazione dei sistemi di comunicazione con il mondo VoIP e piu' in generale con il mondo della convergenza, richiede componenti mirati a risolvere le problematiche di convivenza dei pacchetti dati di diversa origine nella medesima rete.

L'utilizzo di componenti attivi con gestione del QoS (quality of service) permette di taggare i pacchetti dati, in base alla precedenza che essi devono avere, per una corretta distribuzione delle informazioni.

L'utilizzo di apparati di tipologia almeno layer 3 in grado di creare e gestire Virtual Lan, ciò consente di separare il traffico di gruppi di lavoro o dipartimenti di una rete, per applicare diverse policy di sicurezza e differenti criteri di gestione dei pacchetti.

L'utilizzo di VPN ad hoc per la crazione/gestione di connessione remote con un grado sicurezza e privacy maggiore rispetto a una "normale" connessione.

L'utilizzo di dispositivi Access point, permettono la configurazione di SSID (La sigla inglese sta per Service Set Identifier) differenti per destinazione d'uso o utente finale, ognuna assoggettata a policy di sicurezza opportunamente configurate.

SOLUZIONE PROGETTUALE

La soluzione di Cablaggio strutturato, in relazione Alle esigenze, si compone dei seguenti elementi:

Apparati e cablaggio passivo

Il sistema di cablaggio, in rame e fibra ottica, comprende la componentistica passiva necessaria a garantire la connettività di rete da ogni presa verso gli armadi rack di distribuzione (cablaggio orizzontale) e tra gli armadi di connessione delle dorsali dati e fonia (cablaggio verticale). Tutti i prodotti ed i sistemi di cablaggio devono essere conformi agli standard richiesti e alle diverse frequenze di lavoro, conformi alla normativa "Restriction of Hazardous Substances" (RoHS) certificati da enti/soggetti terzi indipendenti quali Delta, 3P Denmark, GhMT e dall' Istituto Superiore delle Comunicazioni e delle Tecnologie dell' Informazione del Ministero delle Comunicazioni Italiano ISCOM\ISCTI, dotati della "Marcatura CE".

Le caratteristiche di una rete passiva altamente performante, si possono riassumere in:

- Connettività fisica omogenea per tutta la rete cablata;

- Prestazioni adeguate alle esigenze attuali e possibilità di seguire le evoluzioni tecnologiche;
- Semplicità di gestione, manutenzione ed espansione della rete;
- Conformità alle raccomandazioni nazionali ed internazionali in relazione sia al materiale utilizzato sia alle procedure d'installazione, certificazione e collaudo adottate;
- Supporto di protocolli standard di comunicazione;
- Possibilità di far evolvere le applicazioni supportate senza modificare la struttura portante dell'infrastruttura.

I MEZZI DI TRASMISSIONE

Il mezzo trasmissivo è il supporto fisico su cui transitano i segnali e rappresenta uno degli elementi più critici in quanto condiziona le caratteristiche stesse dell'intero cablaggio strutturato.

La scelta del tipo di mezzo di trasmissione deve essere effettuata in modo da consentire di:

- raggiungere le prestazioni richieste;
- supportare le Normative vigenti;
- assicurare un'affidabilità costante nel tempo;
- garantire le opportune protezioni nell'ambiente d'installazione.

Oltre alla corretta scelta del mezzo trasmissivo, è anche indispensabile prestare la massima attenzione alla posa dei cavi, poiché eventuali errori possono compromettere pesantemente le prestazioni dell'impianto.

NORMATIVA

Le norme di riferimento per il cablaggio strutturato riguardano sia il progetto e l'installazione del sistema nel suo complesso, sia le caratteristiche tecniche dei suoi componenti, specificando i requisiti di prestazione, sicurezza e idoneità d'installazione.

Le normative EIA/TIA, nate da una proposta congiunta dell'Associazione delle industrie elettroniche (EIA) e dell'Associazione delle industrie di telecomunicazione (TIA) sono state le prime normative riguardanti il cablaggio strutturato e per questo motivo, pur essendo Norme nazionali americane, sono state e continuano ad essere utilizzate anche in altri Paesi. In particolare, la serie TIA/EIA 568-C.2 specifica i requisiti minimi del cablaggio negli edifici commerciali singoli o di un comprensorio e indica, inoltre, i requisiti fisici, elettrici, trasmissivi, le lunghezze massime ottenibili, le caratteristiche dei componenti.

- La Norma ISO/IEC 11801 è, invece, lo standard internazionale per il cablaggio per telecomunicazioni, in cui si definisce un generico sistema di cablaggio che è indipendente dal tipo di applicazione e compatibile con i componenti di cablaggio (di differenti costruttori) rispondenti a tale Norma.
- Per quanto riguarda l'Europa, la serie EN 50173 definisce i requisiti di progetto dei sistemi di cablaggio strutturato in rame e in fibra ottica in diversi ambienti installativi:
- EN 50173-1: definizioni e caratteristiche generali;
- EN 50173-2: requisiti specifici per uffici e siti commerciali;
- EN 50173-3: requisiti specifici per ambienti industriali;

- EN 50173-4: requisiti specifici per ambienti residenziali;
- EN 50173-5: requisiti specifici per data center.
- La serie EN 50174 specifica i requisiti per la realizzazione pratica dei sistemi di cablaggio strutturato in rame e fibra ottica:
- EN 50174-1: pianificazione, amministrazione, manutenzione;
- EN 50174-2: installazione all'interno di edifici di tipo generico e indicazioni specifiche per edifici di tipo commerciale, residenziale, industriale, data center: dorsali e cablaggi orizzontali;
- EN 50174-3: installazione all'esterno di edifici.
- La Norma EN 50310 riporta i requisiti specifici per l'impianto di terra di un sistema di cablaggio strutturato.
- La Norma EN 50346 definisce i requisiti metodologici e strumentali per il collaudo del cablaggio strutturato in rame e in fibra ottica.

STRUTTURA DEL CABLAGGIO

Il sistema di cablaggio strutturato generalmente viene realizzato tramite la posa in opera di *dorsali di cablaggio* sia orizzontali che verticali. Tali dorsali vengono attestate verso gli armadi concentratori o RACK.

Cablaggio Orizzontale: si intendono i cavi che dalla "presa utente" nell'area di lavoro o dall' access point raggiungono il primo centro stella (ARMADIO RACK Distributore di Piano). È definito anche "cablaggio di piano" perché, in un edificio a più piani, normalmente collega tutti gli utenti di un piano.

La distribuzione orizzontale identifica quella parte di cablaggio spesso realizzata con cavo in rame.

Le norme prevedono l'impiego di cavi in rame composti da quattro coppie disposte all'interno di una guaina in base ad una particolare geometria al fine di ridurre i problemi di attenuazione e di diafonia. Le singole coppie, contraddistinte da colori standardizzati, sono, infatti, intrecciate (twistate) con un passo differente una dall'altra e a loro volta attorcigliate all'interno della guaina esterna in modo diverso.

In funzione dell'ambiente in cui viene installato il sistema, occorre valutare l'opportunità di utilizzare cavi con guaine differenti: quelle più comunemente usate sono in PVC o con guaina LSZH (Low Smoke Zero Halogen): in caso d'incendio, i cavi dotati di questo tipo di guaina sono caratterizzati da un basso livello di fumi emessi e dalla proprietà di non rilasciare nell'ambiente gas tossici. Secondo le Norme IEC e CEI.

La distribuzione orizzontale comprenderà l'allestimento dei locali tecnici di piano con pannelli di permutazione in Cat.6A, bretelle di connessione, cavi di distribuzione e posa di analoga

categoria, nella configurazione schermato o non schermato.

Tale architettura garantisce la possibilità di evoluzione del sistema acquisito in linea con gli standard emergenti e le nuove tecnologie.

La rete di distribuzione orizzontale tra l'armadio di permutazione di piano e gli end point sarà di tipo strutturato con topologia gerarchica a stella utilizzerà i seguenti componenti:

- Pannelli di permutazione
- Cavo di distribuzione orizzontale
- Patch cord (bretelle di permutazione lato armadio) e work area cable (bretelle lato postazione di lavoro)

Le guaine dei cavi UTP devono essere adatte per installazioni all'interno degli edifici giudicati:

- a medio rischio in caso d'incendio (cavi classificati secondo CPR come Cca aventi caratteristiche secondarie almeno pari a s1b, d1, a1)

supportano applicazioni ad elevata velocità di trasferimento dei dati poiché assicurano una larghezza di banda fino a 500MHz per i cavi di Cat.6a da 37m a 55m in accordo con gli standard di riferimento.

Tutti i cavi devono avere le caratteristiche di auto-estinguenza in caso d'incendio, di bassa emissione di fumi opachi e gas tossici corrosivi nel pieno rispetto delle normative vigenti (CEI 20-37, IEC 61034, NES 713, IEC60754,EN50265,EN50267) e di ritardo di propagazione della fiamma (FlameRetardant) conformemente alle normative IEC 60332-1-2 (CEI 20-35, EN 50265). I cavi devono avere caratteristiche rispondenti aglistandard:

- Cat.6A
- ANSI/TIA-568-C.2
- EN 50173 2nd edition;
- ISO/IEC 11801 2nd edition.

Pannelli di Permutazione Categoria 6A

I pannelli di permutazione (patch panel) per l'attestazione dei cavi in rame U/UTP (Categoria 6A Classe EA) saranno utilizzati all'interno degli armadi a rack per la distribuzione del cablaggio orizzontale.

I patch panel devono essere composti da un pannello dotato di una struttura metallica modulare a 24 fori atti a contenere permutazioni RJ45 Jack Cat. 6AU/UTP.

Il patch panel dovranno avere una struttura in acciaio satinato nero, con la parte frontale provvista di asole per montaggio su rack a 19", altezza 1U, scarico con 24 slot per prese RJ45 di Cat. 6A conformi alla normativa di riferimento ISO\IEC 11801 – 2nd Edition EIA/TIA 568-c.2 (per la Cat.6A), EN 50173-1 2nd Edition e testate in conformità alle IEC 60603-7.

I pannelli di permutazione devono avere la possibilità di "Identificare" frontalmente ogni singola connessione. Il pannello deve essere dotato di etichettatura anteriore prestampata da 1 a 24

per l'identificazione della postazione di lavoro connessa e dè inoltre dotato di spazio bianco per l'apposizione di etichette stampate. Posteriormente, il pannello deve essere equipaggiato con un supporto cavi removibile "clipon" al fine di garantire il corretto posizionamento e fissaggio dei cavi collegati e il rispetto dei raggi di curvatura richiesti dagli standard. Infine, ogni pannello deve essere dotato di punto di fissaggio per Kit di messa terra secondo le normeEN50310.

Di seguito le caratteristiche tecniche e funzionali dei patch panel:

- struttura metallica a 1U con supporto rack 19" e 24 fori per RJ45;
- capacità di alloggiare 24 RJ45 sia U/UTP che S/FTP per pannelli di Cat.6a o 24 RJ45 sia U/UTP che S/FTP per pannelli Cat.6A;
- possibilità di fissaggio solidale alla struttura (ma removibile rapidamente "clipon");
- possibilità di identificare separatamente ciascuna porta mediante posizionamento di etichette;

Bretelle in rame (patch cord)

La connessione dei pannelli di permutazione agli apparati attivi e delle postazioni di lavoro alle prese delle PdL avviene attraverso rispettivamente patch cord costituite da un cavo a 4 coppie non schermate U/UTP rispondenti ai requisiti.

Le bretelle in rame fornite deve avere le seguenti caratteristiche tecniche e funzionali:

- prestazioni conformi alla norma ISO\IEC61935-2;
- protezione anti-annodamento sul plug;
- ingombro del serracavo minimo per l'inserzione in switch ad alta densità "Blade Patch Cord";
- vari colori disponibili;

Cablaggio Verticale dorsali

Il cablaggio verticale o dorsale di edificio, collega (sempre nella topologia a stella) i diversi rami di cablaggio orizzontale, connettendo i distributori di Piano (ARMADIO RACK Distributore).

In fibra ottica

Il cablaggio di dorsale realizzato con cavi in fibra ottica Multimodale, deve avere un numero di fibre ottiche adeguato a garantire tutti i collegamenti previsti dalle architetture logiche adottate, tenendo inoltre conto di possibili sviluppi futuri e delle eventuali fibre di scorta quale ridondanza o back-up per ogni singola tratta posata.

La fibra ottica è un mezzo trasmissivo che consente di disporre di maggiori ampiezze di banda rispetto ai cavi in rame. La trasmissione si basa sulla propagazione di impulsi luminosi, prodotti da un LED o da una sorgente laser nella banda infrarossa, lungo filamenti di materiale vetroso o polimerico.

Costruttivamente, la fibra ottica è formata da una parte interna (nucleo) e da una esterna (mantello); la differenza tra gli indici di rifrazione dei materiali con cui sono realizzati nucleo e

mantello permettono agli impulsi luminosi iniettati ad un capo della fibra di rimanere confinati tra i due strati di materiale e di propagarsi lungo il percorso della fibra.

In funzione della modalità di trasmissione esistono fibre di tipo monomodali e multimodali: nelle prime, la propagazione avviene seguendo un solo percorso o modo, mentre nelle seconde la luce si propaga seguendo diversi modi.

Le fibre vengono normalmente identificate da una sigla "n/m", dove "n" è il diametro del nucleo, mentre "m" è il diametro del mantello (ad esempio, 50/125 contraddistingue una fibra ottica con 50 µ di diametro del nucleo e con 125 µ di diametro del mantello).

Le fibre, molto delicate meccanicamente, vengono poi rivestite e raccolte in cavi ottici di diversa struttura per soddisfare le esigenze delle differenti applicazioni.

Vantaggi delle fibre ottiche

Rispetto ai cavi in rame, le fibre ottiche offrono rilevanti vantaggi:

- totale insensibilità alle interferenze elettromagnetiche;
- alta velocità di trasmissione;
- bassa attenuazione;
- dimensioni ridotte.

In Rame

Il cablaggio di dorsale realizzato tramite l'impiego di cavi in rame deve essere composto da quattro coppie disposte all'interno di una guaina in base ad una particolare geometria al fine di ridurre i problemi di attenuazione e di diafonia. Le singole coppie, contraddistinte da colori standardizzati, sono, infatti, intrecciate (twistate) con un passo differente una dall'altra e a loro volta attorcigliate all'interno della guaina esterna in modo diverso.

In funzione dell'ambiente in cui viene installato il sistema, occorre valutare l'opportunità di utilizzare cavi con guaine differenti: quelle più comunemente usate sono in PVC o con guaina LSZH (Low Smoke Zero Halogen): in caso d'incendio, i cavi dotati di questo tipo di guaina sono caratterizzati da un basso livello di fumi emessi e dalla proprietà di non rilasciare nell'ambiente gas tossici, secondo le Norme IEC e CEI.

Tale architettura garantisce la possibilità di evoluzione del sistema acquisito in linea con gli standard emergenti e le nuove tecnologie, tali dorsali supportano applicazioni ad elevata velocità di trasferimento dei dati poiché assicurano una larghezza di banda fino a 500 MHz per i cavi di Cat.6° in accordo con gli standard di riferimento.

Tutti i cavi devono avere le caratteristiche di auto-estinguenza in caso d'incendio, di bassa emissione di fumi opachi e gas tossici corrosivi nel pieno rispetto delle normative vigenti (CEI 20-37, IEC 61034, NES 713, IEC60754, EN50265, EN50267) e di ritardo di propagazione della fiamma (Flame Retardant) conformemente alle normative IEC 60332-1-2 (CEI 20-35, EN 50265). I cavi devono avere

caratteristiche rispondenti agli standard:

- Cat.6A
- ANSI/TIA-568-C.2
- EN 50173 2nd edition;
- ISO/IEC 11801 2nd edition.

Armadi Rack

Gli armadi rack devono essere attestati ai diversi piani dell'edificio in posizioni e con caratteristiche tali da soddisfare le esigenze della infrastruttura scolastica.

Gli armadi rack proposti devono avere tutti i requisiti conformità alle norme IEC297-2 e le DIN 41494 parte1 per il montaggio di apparati elettrici ed elettronici, e la DIN 41488 per le dimensioni esterne ed EIA31 0per le caratteristiche generali.

In base alle esigenze rilevate, saranno definiti numero e posizione degli armadi nei locali appositamente individuati. Per tali apparati deve essere previsto il montaggio, l'installazione e l'opera di allacciamento e di alimentazione, nonché la messa a terra, in rispondenza alle norme contenutene nel DM n.37del 22/01/2008 per quanto in esso riportato nello specifico.

LAVORI DI POSA IN OPERA DEL CABLAGGIO

Tra le attività relative ai lavori di posa in opera della fornitura dovranno prevedere:

- Attestazioni di qualsiasi tipo, includenti i connettori ottici o i connettori per cavo in rame;
- scatole di attestazione per cablaggio in fibra o rame;
- posa di canalizzazioni, sia verticali che per corridoi o per stanze incluso il relativo materiale (tubi, canaline ecc.). Questi lavori comprendono l'apertura e la chiusura di pannelli rimovibili per contro soffitti e pavimenti flottanti dopo aver introdotto le nuove canalizzazioni;
- fornitura e posa in opera di pannelli di permutazione;
- ripristino della qualità e dell'aspetto delle strutture alla situazione pre-lavori;
- quant' altro necessario per il completamento del cablaggio strutturato.

Installazione degli armadi rack

Il posizionamento dei vari armadi rack dovrà prevedere una distanza libera di circa 1metro davanti, dietro e ad un lato. Nel caso in cui uno dei montanti debba essere accostato al muro, sarà mantenuta una distanza minima di almeno 15 centimetri per consentire la gestione della salita di cavi.

Certificazione del sistema di cablaggio

A completamento del servizio di installazione del sistema di cablaggio devono essere effettuate le certificazioni di tutti i cavi e le terminazioni del nuovo sistema di cablaggio posto in opera, in accordo con le norme vigenti ed i parametri prestazionali degli standard normativi.
La certificazione deve essere eseguita con strumenti forniti di certificato di calibrazione e sarà rilasciata tutta la documentazione tecnica, inerente ai risultati dei test strumentali effettuati.

INSTALLAZIONE DEGLI APPARATI ATTIVI DELLA RETE LAN

Gli apparati attivi rack mount, devono essere installati nel seguente modo:

- Inserimento di eventuali moduli interni all'apparato;
- montaggio su rack: gli apparati devono essere ancorati ai montanti utilizzando le apposite staffe di sostegno. La posizione dell'apparato all'interno del rack e delle staffe relative (nella parte frontale, centrale o posteriore dell'apparato) sarà determinata dalla maggior convenienza in termini di accessibilità alle porte dell'apparato e di stabilità dello stesso;
- inserimento di eventuali moduli esterni all'apparato;
- connessione dei cavi di rete e di alimentazione. La connessione dei cavi di rete deve includere le operazioni di etichettatura degli stessi.

Nel caso di apparati attivi che non consentano l'ancoraggio ai montanti del rack, essi devono essere alloggiati su appositi ripiani, mantenendo adeguato spazio libero per le operazioni di esercizio e manutenzione sugli stessi e per consentire un appropriato riflusso di aria.

Configurazioni degli apparati attivi della Rete LAN

I lavori di configurazione devono comprendere tutte le attività necessarie a garantire il corretto funzionamento dell'apparato in rete per ottenere un sistema "chiavi in mano" stabile e funzionante.
Le attività di configurazione che devono essere garantite al termine dell'installazione sono:

- aggiornamento all'ultima versione stabile di sistema operativo;
- configurazione di policy di sicurezza appropriate;
- configurazionedelleVLANnecessarieedinserimentodelleportenelleVLANrelative;
- Configurazione VPN di tipologia "SITE to SITE" e " Client to Site"
- configurazione dei protocolli di routing necessari;
- configurazione di eventuali indirizzi necessari al management (ad es: loopback di gestione);
- configurazione per l'invio delle trap SNMP appropriate al sistema di gestione;
- configurazione per l'invio delle trap SMTP appropriate al sistema di gestione;
- configurazione funzionalità e policy per dispositivi per la sicurezza delle reti.

La configurazione degli apparati attivi deve essere eseguita a seguito del buon esito dell'installazione

degli stessi.

Apparati attivi previsti

Di seguito sono elencati gli apparati attivi che devono essere installati e configurati a valle del router fornito dal gestore di connettività:

FIREWALL

Appliance indispensabile per la sicurezza del sistema informatico, le capacità di espansione devono permettere la scalabilità delle funzioni, partendo dal semplice accesso ad internet con controllo del traffico, per arrivare a servizi come filtro dei contenuti, VPN, vlan, gestione dell'allocazione di banda, funzioni IDS/IPS captive portal.

Il Firewall deve essere una distribuzione open source su base Hardware con supporto attivo .

La configurazione e la gestione devono poter avvenire tramite interfaccia web per un processo di configurazione e gestione semplice e intuitivo.

Le caratteristiche hardware devono essere tali da permettere l'esecuzione difunzionalità e servizinativi che richiedono molta potenza di calcolo, come VPN/firewall, antispam mail security, trap rules ,gestione servizio content and URL filtering, servizi sicurezza gateway, dual gateway, loadbalancing, fail over, DMZ, IDS/IPS IntrusionDetection System (IDS) e IntrusionPrevention System (IPS). Deve avere funzioni di Ispezione dei pacchetti di rete e bloccare quelli sospetti oltre ad avvisare gli amministratori riguardo ai tentativi di attacco. I registri di questi sistemi devono contenere informazioni relative alle minacce di rete riguardo il tipo di attacco, e i dispositivi presi di mira per aumentare la sicurezza della propria rete.

Deve essere prevista la funzionalità di Hot Spot True Identity con tecnologia ldap-sso per gestire e controllare gli accessi alla rete WI FI scolastica in tutta sicurezza tramite la gestione semplificata di credenziali ad persona nelle forme nome utente e password o voucher con la possibilità di creazione di gruppi e scadenze temporali fissate alla data prevista, la generazione di "Vouchers guest" che permettono ad utenti esterni non facenti parte della struttura di avere accesso alla connettività internet wifi senza compromettere la sicurezza dell'infrastruttura informatica. Deve supportare diverse tipologie di cifratura e di key generator, fornire indicazione sui tempi di connessione e Expired period. Deve essere possibile la personalizzazione della pagina portale hotspot, Stampa e personalizzazione dei Vouchers.

Deve avere un numero di interfacce di rete sufficiente (non inferiore a 4 lan gigabit) a garantire la possibilità di gestire più connessioni WAN per gestire al meglio le risorse di connettività e la banda a disposizione. Le interfacce devono poter essere impiegate per creare un cluster composto da due o più apparati, a scopo di failover e bilanciamento del carico.

Requisti tecnologici minimi:

tecnologia di costruzione industriale basta su architerttura Intel. La scheda madre integra non meno di 4 interfacce di rete. Funzioni native di network security, Hot Spot True Identity, support protocollo SSM, Router 4G redundancy con performance automatic startup, Firewall, Vlan, antispam e mail security, gestione servizio content and URL filtering, servizi sicurezza gateway, dual gateway , load balancing , fail over, DMZ , VPn(ipsec, pptp, l2tp, ovpn), trap alert, SNMP server. Throughput con stato 3,9 Gbps; Prestazioni DPI complete 850 Mbps; Throughput antivirus gateway 1,0 Gbps; Throughput prevenzioneintrusioni 2,0 Gbps; Gestione Wireless A. Point supportati 96; Failover 4G; Connettività Client VPN globali (max.) 500, Client VPN SSL (max.) 2, Connessioni non inferiori a 1500, Nuove connessioni/sec 15

SpecificheTecniche:

Gestione . Interfaccia web di gestione . Wizard per la prima configurazione . Console tramite Seriale . Console tramite SSH/SCP	Firewall e Routing . Supporto IPv4 e IPv6 . Stateful Packet Inspection . Filtro per sorgente e destinazione . Limiti per numero di sessioni/stati/nuove connessioni al secondo . Filtro per OS . Filtro per orario . Routing policy per rules . Alias per raggruppareporte, ip, network . Transparent layer 2 – 3 firewalling . Packet normalization . IDP/IDS (Snort) . Multiple IP Addresses . Supporto VLAN . Supporto Link Aggregation . Supporto Interface Groups . IGMP Proxy . Static Routing
Networ Address Translation . Port forwarding . 1:1 NAT	Autenticazione . Gestione Utenti, Gruppi e Diritti . Active Directory / LDAP

. Outbound NAT . NAT Reflection . IpSec NAT Traversal	. Radius . Local DB . Certification Authority Interna . Certification Authority Esterna
Interfacce . Supporto interfacce multiple per	WAN, LAN, DMZ, WLAN . SupportoWIFI . Supporto per UTMS/GPRS/3G USB Dongles . Supporto per connessioni ADSL/ISDN con Modem
High Availability . HW failower con CARP . Sincronizzazione degli stati e delle configurazioni con pfsync . Supporto di due o più firewall in failovergroup	Load Balancing . Outbound Load Balancing per la gestione multi wan e failover . InboundLoadBalancing per distribuire il carico su server multipli (web server, mail server ecc...)
Virtual Private Network . Ipsec (Client e Server) . OpenVPN (Client e Server) . OpenVPN client export . L2TP . PPTP Server Site to site Client to site	TrafficShaper . Supporto di HFSC, CBQ, FAIRQ, CODELQ, PRIQ . Supporto del limite di banda . Filtro layer 7 . Wizard di configurazione
Reporting e Monitoring . Dashboard personalizzabile . Grafici in tempo reale per il throughput di ogni interfaccia . Stato delle connessioni VPN . Stato delle code del trafficshaper . Grafici RRD per: Utilizzo CPU Throughput totale e per interfaccia	Diagnostics Tools . Packet Capture . Ping . Trace route . Test Port . DNS Lookup

Firewall State Pacchetti al secondo per interfaccia TrafficShaperqueues Tempo di risposta al pingsulleinterfacce WAN . Reporting via email (MailReport) . Supporto trap e daemon SNMP . Supporto SysLog	
DNS forwarder e server . DNS Forwarder . Host Overrides . Domain Overrides . DNS Server (TinyDNS)	Dynamic DNS . Custom . DNS Matic . DynDNS . DHS . DNSexit . DyNS . easyDNS . freeDNS . HE.net . Loopia . Namecheap . No-IP . ODS.org . OpenDNS . Route 53 . SelfHost . ZoneEdit
Captive Portal . Schermata HTTP/HTTPS personalizzabile . Limite per numero di connessioni . Idle timeout . Hard timeout . Logon pop -up window . Reindirizzamento URL . Filtro basato su MAC	DHCP Server e Relay . DHCP Server . DHCP Relay .PPPoE Server . PPPoE Server . Autenticazione con RADIUS . Autenticazione con DB Interno

. Autenticazione basata su Radius o DB Interno	

Switch Manageriale

Al fine di ottenere il controllo e la gestione peculiare del sistema informatico di rete è necessario l'adozione di apparati switch di tipologia manageriale per risolvere eventuali problemi di networking come loop, collisioni, mancato instradamento dei pacchetti e conseguente perdita di dati, tramite la configurazione e attivazione di policy di routing e policy di ispection.

Le caratteristiche minime che deve avere uno switch manageriale sono:

Gestione centralizzata della rete e delle singole porte lan rame e fibra, attivazione/disattivazione di porzioni di rete, gestione vlan con routing di pacchetti layer 2 layer3, autodiagnostica per la rilevazione di loop nella rete,funzione spanning tree per velocizzare l'instradamento dei pacchetti nella rete, Quality Of Service, managed tecnology.

Deve essere gestibile e configurabile da qualsiasi luogo, locale e da remoto tramite applicazione web con interfaccia grafica (GUI) per un controllo accurato del sistema di gestione.

Deve essere dotato di touchscreen a colori LCM da 1,3" che visualizza in modo conciso informazioni chiave sul sistema e sulla connessione.

Il numero di porte on board del dispositivo è relativo alla destinazione d 'uso.

SpecificheTecniche:

Switch PoELayer 3 con porte RJ45 GbE e 2.5GbE, 802.3at PoE+, 802.3at PoE+ RJ45 e porte 10G SFP+
e un'alimentazione PoE totale di 400 W

Caratteristiche:

Touchscreen a colori LCM da 1,3" con gestione switch AR

Porte GbE, 802.3at PoE+ RJ45

Porte RJ45 da 2,5 GbE, 802.3at PoE+

porte 10G SFP+

Ingresso CC USP RPS

Alimentazione PoE totale da 400 W

Funzionalità di commutazione di livello 3

Layout della porta RJ45 a fila singola per una facile gestione dei cavi del pannello di permutazione.

SERVER LAN/WIFI CONTROLLER E DIAGNOSTICO NSA (Network Security Appliance)

È necessario prevedere un apparato di gestione centralizzata della struttura informatica, una console di rete all-in-one che esegue ogni applicazione dell'eco sistema rappresentato dall'infrastruttura di rete, nodo strategico di congiunzione tra Network e Protection, indispensabile intutte le strutture complesse da gestire in cui sono presenti diverse tipologie di architetture e endpoint, rappresentati da router, firewall access point, uplink bridge , switch, switch poe, pc smartphone, cam/nvr e IoT. Deve essere possibile configurare e gestire tramite una semplice interfaccia, organizzata su una piattaforma di classe

Enterprise una molteplicità di siti remoti (cluster-reti Wi-Fi come nel caso di sedi distaccate) ognuno costituito anche da centinaia di access point. Il Controller deve essere accessibile anche da remoto è tramite questo strumento deve essere possibile gestire l'intera rete wireless, aggiornare i firmware degli access point, aggiornare le password delle varie reti create, gestire i client che si connettono in rete.
Deve avere una console di semplice utilizzo nella gestione del routing dei pacchetti, riuscendo a monitorare fisicamente sulle porte degli apparati la tipologia di utenza e traffico. Devono essere previste le funzionalità di controllo sulle tabelle di protocollo layer 2 e layer 3. Deve avere funzionalità di server SNMP per il data collection delle informazioni degli apparati collegati alla rete e la configurazione delle corrispettive TRAP. Il dispositivo deve essere capace di rilevare e segnalare guasti o malfunzionamenti dei nodi principali che compongono la rete, e permettere il Controllo e il Monitoraggio dei flussi dati e del traffico delle aree lan /wlan e di eventuali Vlan,di monitorare in modo rapido il traffico del sistema. Tramite l'upload della mappa della struttura deve essere possibile ottenere una rappresentazione visiva della copertura rete wireless.

SpecificheTecniche:
Deve essere dotato di un gateway di sicurezza integrato, supporto 10G SFP+ WAN, uno switch Gigabit a 8 porte e un videoregistratore di rete che supporta unità disco rigido (HDD) da 3,5 pollici compatibili.
Switch a 8 porte con porte 1GbE RJ45 e 10G SFP+
Gateway di sicurezza integrato e videoregistratore di rete predisposto per dispositivi Protect che supporta HDD da 3,5" compatibili
Gestione delle minacce Internet di classe aziendale, ispezione approfondita dei pacchetti e funzionalità AI WiFi
Dotato di un processore minimoquad-core da 1,7 GHz
Console montabile su rack di dimensioni 1U
Deve consentire di scalare facilmente il suo deployment collegando dispositivi compatibili aggiuntivi
Sistema di ispezione di primo livello
Sistemadi verifica connettività apparati attivi in realtà aumentata con gestione delle connessioni e alert di primo livello

ACCESS POINT

Per consentire l'accesso alla connettività in qualsiasi luogo della struttura scolastica, è necessario prevedere l'installazione di punti di accesso WIFI (access point) che abbiano le seguenti caratteristiche minime:
tecnologia Wi-Fi 6 (802.11ax) con un sistema di antenne dual band 5 GHz (4x4 MU-MIMO and OFDMA) a 2.4 GHz (2x2MIMO) radios, 300 utenti connessi simultaneamente dovendo fornire connettività ad aule, laboratori e auditorium, rispettando la normativa e le leggi vigenti sulle emissioni radio, che in Italia impongono emissioni EIRP (potenza radio irradiata da un'antenna) di 20dbm sui 2.4Ghz e 30dbm sui 5ghz.

Deve essere alimentabile via PoE (802.3af), e disporre di 1 interfaccia Gigabit Ethernet. Protezione IP54.

Il dispositivo deve supportare Wireless bridging e Wireless Mesh, poiché tali tecnologie offrono un sostanziale aumento di stabilita ed aumento di throughput complessivo del sistema di accesso wireless, di cui ne beneficeranno indirettamente anche i client di vecchia generazione. In aggiunta alle tecnologie standard come VLAN SMA, Wireless Security, deve essere supportata tutta la gamma di funzionalità avanzate di Radio Calibration High Density, come:

band steering: tecnologia che si occupa di realizzare un utilizzo uniforme della rete Wi-Fi e di ottenere quindi una connessione stabile e veloce per tutti i dispositivi wireless nella rete locale;

push 5ghz performance optimization: che permette di forzare l'utilizzo della banda 5ghz più performante, per i dispositivi dotati di wireless 5ghz;

G.I.T.: Isolamento del traffico Guest, che migliora la sicurezza della rete wireless e riduce la congestione del traffico;

Load balancing: tecnologia concepita per distribuire il carico di lavoro tra gliAp installati il cui obiettivo è ottimizzare le prestazioni globali, il rendimento e la capacità dell'infrastruttura.

SpecificheTecniche:

Dual-band WiFi 6 (802.11ax)

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

Operates at full 4x4 MIMO with 160 MHz bandwidth

300+ concurrent client capacity

Guest Traffic Isolation, which enhances wireless network security and lowers traffic congestion

Included universal mounting plate, backing plate, and screw kit

Note aggiuntive:

- Realizzazione cablaggio rete wifi comprensiva di switch poe, gruppi di continuità (con relativo pulsante di sgancio) da rack, realizzazione delle dorsali in cavo UTP cat 6a
- Gestione degli access point centralizzata degli Access Point tramite server in Cloud senza alcun canone annuale di gestione per il funzionamento del sistema
- Installazione e gestione dei server sistemi di sicurezza "server firewall" con l'attivazione dei servizi di tipo sicurezza media/alta. Firewall Hardware di ultima generazione con autenticazione LDAPSSO, Filtro Contenuti, Filtro Applicativi. Almeno 300 Utenti contemporanei e funzioni di sicurezza e gestione integrata delle antenne AP.
- La realizzazione del cablaggio **deve essere testato per la categoria 6 a Gigabit.**
- L'intervento di posa in opera e realizzazione della rete deve essere reso "chiavi in mano" comprendendo anche eventuali opere murarie.

Capitolato tecnico

Descrizione dettagliata	Q.ta

Armadi di rete - rack	
Armadio Rack INTELLINET da pavimento, costituito da armadio in lamiera con struttura protetta per raggruppare server, apparati attivi e di pannelli di permutazione con larghezza standard da 19", con capienza di 42 unità, completo di portello frontale in lamiera e policarbonato con serratura a chiave, n. 2 ripiani prof. 40cm, barra di alimentazione da rack con prese universali, pannello di permutazione precaricato cat 6a 24 posti rame, pannello di permutazione completo di 12 connettori in fibra ottica LC, n. 24 bretelle cat. 6A e n. 12 bretelle fibra	1
Armadio Rack INTELLINET costituito da armadio in lamiera con struttura protetta per raggruppare server, apparati attivi e di pannelli di permutazione con larghezza standard da 19", con capienza di 6 unità, completo di portello frontale in lamiera e policarbonato con serratura a chiave, barra di alimentazione da rack con prese universali, pannello di permutazione precaricato cat 6a 24 posti rame, n. 12 bretelle cat. 6A	2
accessori armadi di rack	
Scatola Terminazione Ottica per Armadio Rack INTELLINET secondario	2
monitor 19" samsung LCD per L'Armadio Rack	1
KVM HDMI 4 dispositivi per Armadio Rack INTELLINET	1
Dispositivo networking controller APPLE Soluzione di ispezione rapida in realtà aumentata per il monitoraggio degli apparati di rete connessi Schermo 10” – 3 gb ram – 32 gb Rom	1
Quadro elettrico dedicato per Armadio Rack INTELLINET completo di interruttore magnetotermico differenziale da 30A , presa industriale monofase, spia alimentazione e fusibile	1
Centralino Stagno Per Emergenza Con Pulsante Illuminabile e Due Contatti	1
Gruppo di ventilazione a 4 ventole completo di termostato	1
Gruppo di continuità	
Gruppo di Continuità RIELLO rack mount CARATTERISTICHE GENERALI:Protezione Pc, Rack / Tower, Interruttore automatico, Line Interactive (VI); USCITA:1980 WATT, 2200 Va, Spine elettriche connettibili : 9 , IEC C13 - IEC C19, Frequenza d'uscita Minima : 45 Hz, Frequenza d'uscita Massima : 65 Hz, Bypass no; BATTERIE E TEMPI DI FUNZIONAMENTO:Ermetiche al piombo, 4 Min; INGRESSO:1 Numero Connettori in ingresso; CONNETTIVITÀ:Usb	1
Gruppo di Continuità RIELLO rack mount CARATTERISTICHE GENERALI:Protezione Pc, Rack / Tower, Interruttore automatico, sinusoidale; USCITA: 360 WATT, 600 Va, Spine elettriche connettibili : 5 , IEC C320 Schuko, Frequenza d'uscita Minima : 45 Hz, Frequenza d'uscita Massima : 65 Hz, Bypass no; BATTERIE E TEMPI DI FUNZIONAMENTO:Ermetiche al piombo, 4 Min; INGRESSO:1 Numero Connettori in ingresso; CONNETTIVITÀ:Usb	2
CABLAGGIO RAME	
Realizzazione punto rete lan con cavo tipo UTP CAT. 6A - comprensivo di cavo cassetta tipo 503, placca portafrutto e frutto femmina Rj45 : Cavo per trasmissione dati ad elevate velocita' di trasmissione, costituito da 4 coppie twistate di conduttori in rame ritorto a formazione rigida da 23 AWG con protezione interna in poliestere, isolante in polietilene, costruzione twistata con guaina di protezione antiincendio ed a bassa emissione di gas tossici (L.S.O.H) oppure in p.v.c., compreso installazione all'interno di cunicoli, tubazioni e/o canalette, completo di accessori vari e siglatura alfanumerica ai terminali ed incluso testatura da effettuarsi con tester certificatore dotato di certificato di calibrazione; frutto connettore RJ 45 Connettore femmina RJ45 rispondente alla normativa ISO/IEC 11801, TIA/EIA 568 standard cat 6a, compatibile con il sistema ed apparecchiature di trasmissione dati, completo di connessione delle coppie del cavo sulla presa RJ45, etichettatura su prese posto di lavoro o su pannello di cablaggio. Esecuzione di prove di conformità alla categoria 6a da condurre sulle prese RJ45 inserite nei vari posti lavoro o nei pannelli di permutazione, rilascio di documento attestante l'esito della certificazione con i valori misurati secondo quanto specificato nelle specifiche tecniche allegate, compreso l'infilaggio di tutte le attrezzature e apparecchiature idonee occorrenti, l'assistenza dei tecnici specialisti ed ogni e qualsiasi altro onere e prestazione che si rendessero necessari.	2

Realizzazione punto rete per Access Point con cavo tipo UTP CAT. 6A - comprensivo di cavo cassetta tipo 503, placca portafrutto e frutto femmina Rj45 : Cavo per trasmissione dati ad elevate velocita' di trasmissione, costituito da 4 coppie twistate di conduttori in rame ritorto a formazione rigida da 23 AWG con protezione interna in poliestere, isolante in polietilene, costruzione twistata con guaina di protezione antiincendio ed a bassa emissione di gas tossici (L.S.O.H) oppure in p.v.c., compreso installazione all'interno di cunicoli, tubazioni e/o canalette, completo di accessori vari e siglatura alfanumerica ai terminali ed incluso testatura da effettuarsi con tester certificatore dotato di certificato di calibrazione; frutto connettore RJ 45 Connettore femmina RJ45 rispondente alla normativa ISO/IEC 11801, TIA/EIA 568 standard cat 6a, compatibile con il sistema ed apparecchiature di trasmissione dati, completo di connessione delle coppie del cavo sulla presa RJ45, etichettatura su prese AP o su pannello di cablaggio. Esecuzione di prove di conformità alla categoria 6a da condurre sulle prese RJ45 in prossimità dell'AP con testatura della compatibilità Poe+ IEEE 802.3at e nei pannelli di permutazione, rilascio di documento attestante l'esito della certificazione con i valori misurati secondo quanto specificato nelle specifiche tecniche allegate, compreso l'infilaggio di tutte le attrezzature e apparecchiature idonee occorrenti, l'assistenza dei tecnici specialisti ed ogni e qualsiasi altro onere e prestazione che si rendessero necessari.	22
CABLAGGIO FIBRA OTTICA	
Realizzazione dorsale con cavo tipo Fibra Ottica - comprensivo di cavo Multimodale 50/125 OM4 e attestazione pannello permutazione in fibra ottica: Cavo per trasmissione dati ad elevate velocita' di trasmissione, costituito 4 fibre dielettrico, Conforme CPR (UE 305/2011) classe Dca - s2, d2, a1 - EN 50575:2014+A1:2016, compreso installazione all'interno di cunicoli, tubazioni e/o canalette, completo di accessori vari e siglatura alfanumerica ai terminali ed incluso testatura da effettuarsi con tester certificatore dotato di certificato di calibrazione. Esecuzione di prove di conformità, rilascio di documento attestante l'esito della certificazione con i valori misurati secondo quanto specificato nelle specifiche tecniche allegate, compreso l'infilaggio di tutte le attrezzature e apparecchiature idonee occorrenti, l'assistenza dei tecnici specialisti ed ogni e qualsiasi altro onere e prestazione che si rendessero necessari.	2
SWITCH apparecchiature per collegamenti alla rete	
UBIQUITI Port Switch 8 PoE Switch Gigabit PoE+ gestito con SFP switch senza ventola offre prestazioni silenziose ma potenti con le sue 10 porte di commutazione indipendenti. Condividendo un totale di 150 W PoE, otto porte Gigabit Ethernet offrono 802.3af/at PoE+ o 24 V PoE passivo e due porte SFP offrono connettività FIBRA. Configurazione versatile della porta Otto porte RJ45 Gigabit offrono diverse opzioni di potenza in uscita: IEEE 802.3af/at PoE/PoE+ con rilevamento automatico e PoE passivo a 24 V e due porte SFP forniscono opzioni di connettività in fibra ottica per supportare uplink fino a 1 Gbps. Commutazione aziendale avanzata Lo switch UniFi supporta il tagging VLAN, l'isolamento delle porte, il controllo storm e il controllo guest.ower consumption (typical) 20 W Power consumption (max) 150 W AC input voltage 100 - 240 V AC input frequency 50 - 60 Hz Data transmission Switching capacity 20 Gbit/s Jumbo frames support True Throughput 14.88 Mpps	3

UBIQUITI Switch PoE di layer 3 con (12) porte RJ45 2.5GbE, 802.3at PoE+, (12) porte GbE, porte RJ45 802.3at PoE+ e (2) porte 10G SFP+. Completamente gestito con (12) porte 2.5GbE, 802.3at PoE+ RJ45, (12) GbE, porte 802.3at PoE+ RJ45, (2) porte 10G SFP+, e un'alimentazione PoE totale di 400 W. Touchscreen a colori LCM da 1,3" che visualizza in modo conciso informazioni chiave sul sistema e sulla connessione. Questo switch può essere monitorato o configurato da qualsiasi luogo con la potente e intuitiva applicazione web e l'app mobile. (1) 1.3" LCM color touchscreen with AR switch management (12) GbE, 802.3at PoE+ RJ45 ports (12) 2.5GbE, 802.3at PoE+ RJ45 ports (2) 10G SFP+ ports (inclusi moduli SFP Fibra) (1) USP RPS DC input 400W total PoE supply Layer 3 switching features Single-row RJ45 port layout for easy patch panel cable management	1
Access point	
UBIQUITI AP Wi-Fi 6 Access point ad alte prestazioni che sfrutta la tecnologia WiFi 6 avanzata per fornire una potente copertura wireless agli ambienti aziendali. Offre una velocità radio aggregata fino a 5,3 Gbps con radio 5 GHz (4x4 MU-MIMO e OFDMA) e 2,4 GHz 2x2 MIMO. Si integra perfettamente in qualsiasi ambiente ed è in grado di essere montato in ambienti interni e semi-esterni (classificazione IP54)	22
DISPOSITIVO DI GESTIONE ACCESS POINT	
UBIQUITI DREAM MACHINE PRO Controller centralizzato di Rete Console di livello aziendale che offre un'esperienza di rete scalabile e una piattaforma completa per l'uso multi-applicazione. Console di rete all-in-one che esegue ogni applicazione come Network e Protect. È dotato di un gateway di sicurezza integrato, supporto 10G SFP+ WAN, uno switch Gigabit a 8 porte e un videoregistratore di rete che supporta unità disco rigido (HDD) da 3,5 pollici compatibili. DS/IPS Throughput: 3.5 Gbps - Processor: Quad ARM Cortex-A57 Core at 1.7 GHz - System Memory: 4 GB DDR4 - On-Board Flash Storage: 16 GB eMMC Switch a 8 porte con porte 1GbE RJ45 e 2 porte 10G SFP+ (inclusi moduli SFP Fibra) Gateway di sicurezza integrato e videoregistratore di rete predisposto che supporta HDD da 3,5" compatibili Gestione delle minacce Internet di classe aziendale, ispezione approfondita dei pacchetti e funzionalità AI WiFi Console montabile su rack di dimensioni 1U Consente di scalare facilmente il suo deployment collegando dispositivi aggiuntivi	1
FIREWALL Next Generation Firewall fascia alta	

NETGATE Server rack firewall fascia alta 19” UTM piastra madre con tecnologia di costruzione industriale basta su architerttura Intel processore Intel ; ddr3 ssd 64 GB. La scheda madre con almeno 4 interfacce rete Intel Con funzioni native di network security, Hot Spot True Identity, supporto protocollo SSM, Router 4G redundancy performance automatic startup, Firewall VPN/firewall, antispam e mail security, gestione servizio content and URL filtering, servizi sicurezza gateway, dual gateway , load balancing , fail over, DMZ , VPn. Throughput con stato 3,9 Gbps; Prestazioni DPI complete 850 Mbps; Throughput antivirus gateway 1,0 Gbps; Throughput prevenzione intrusioni 2,0 Gbps; Gestione Wireless A. Point supportati 96; Failover 4G; Connettività Client VPN globali (max.) 500, Client VPN SSL (max.) 2, Connessioni massime 1500, Nuove connessioni/sec 15 Deve essere prevista la funzionalità di Hot Spot True Identity per gestire e controllare gli accessi alla rete WI FI scolastica in tutta sicurezza tramite la gestione semplificata di credenziali ad personam nelle forme nome utente e password o voucher con la possibilità di creazione di gruppi e scadenze temporali fissate alla data prevista, la generazione di "Vouchers guest" che permettono ad utenti esterni non facenti parte della struttura di avere accesso alla connettività internet wifi senza compromettere la sicurezza dell’infrastruttura informatica. Deve supportare diverse tipologie di cifratura e di key generator, fornire indicazione sui tempi di connessione e Expired period. Deve essere possibile la personalizzazione della pagina portale hotspot, Stampa e personalizzazione dei Vouchers.	1
Software per la sicurezza	
HOT SPOT Modulo aggiuntivo di licenza per firewall: Pagina di accesso personalizzata per l'Istituto, Gestione Controllata degli utenti per l'accesso alla rete Wifi dell'Istituto, creazione di ticket temporali, gestione centralizzata Access point, Monitoring in modalità real time UTM della utenze. Licenza Elettronica	1
SERVIZI PER DISPOSITIVI SICUREZZA	
Configurazione- ATTIVAZIONE SERVIZI apparati rete locale lan assegnazione parametri IP , impostazione criteri di sicurezza così come richiesto nei paragrafi precedenti	1
Attività configurazione apparati	
Configurazione apparati rete locale lan assegnazione parametri IP, impostazione criteri di sicurezza così come richiesto nei paragrafi precedenti	1
SERVIZIO DI ASSISTENZA E MANUTENZIONE E GESTIONE DELLA RETE	
servizio di garanzia, assistenza e manutenzione h 24 senza limiti di chiamata “on site“ della rete e di tutti gli apparati attivi e passivi di tipo SHP Super High Profile "PREVENTIVA, CORRETIVA, EVOLUTIVA" da espletarsi, ad opera di personale che abbia adeguate competenze professionali in termini di esperienza lavorativa almeno quadriennale in ambito manutenzione e gestione dei sistemi di reti locali - 3 anni dalla data di collaudo	1
SERVIZIO DI MONITORAGGIO E GESTIONE DELLA RETE	
SW di monitoraggio, configurazione e gestione della rete	1
SERVIZIO DI ADDESTRAMENTO	
Servizio di Addestramento - Addestramento sulla fornitura 24 ore on site	12
SERVIZIO DI CERTIFICAZIONE DEL CABLAGGIO	
Servizio di certificazione del cablaggio	1