

Esame di maturità 2026

ITT Informatica e Telecomunicazioni

Articolazione Informatica

Svolgimento della prova di SISTEMI E RETI

Prima parte

Il progetto e le attività richieste nella prima parte riguardano il contesto di una grande società di ingegneria che intende acquisire presso la propria sede centrale un sistema BIM, che dovrà interfacciarsi con apparecchiature digitali presenti sui cantieri, in particolare: tablet con scanner di vario tipo, fotocamere timelapse, sensori di sicurezza.

Ipotesi aggiuntive

Si fanno le seguenti ipotesi aggiuntive:

- la sede centrale è situata in un edificio composto da piano terra e due piani soprastanti, interamente dedicati ad uffici e sale riunioni per il personale dell'azienda, con anche, al piano terreno, un locale tecnico in cui possono essere collocati i dispositivi informatici di vario genere,
- non si prevede di consentire l'accesso alla rete a persone e/o dispositivi non appartenenti alla società,
- nei cantieri in cui si utilizza il sistema BIM è possibile avere a disposizione un locale 'protetto' in cui posizionare apparati e dispositivi di rete.

Eventuali altre ipotesi aggiuntive o note interpretative vengono fornite nel corso della trattazione.

Soluzione del punto 1

Nel primo punto si richiede un progetto generale dell'infrastruttura di rete relativa ad un cantiere.

Analizzando la situazione, i principali elementi che costituiscono l'ambito del progetto sono: i tablet con gli scanner, le fotocamere, i sensori, dei 'sistemi locali per l'attivazione di notifiche ed allarmi in tempo reale', tutta l'infrastruttura di rete per il collegamento di questi elementi in modo che sia garantito il passaggio dei dati verso la sede centrale e, almeno in parte, verso i sistemi del cantiere stesso.

Il contesto del cantiere è una realtà molto particolare su cui operare, che, seppure con variazioni legate alla dimensione e alle specificità del caso, è caratterizzata da:

- problematiche di sicurezza fisica e ambientale dei locali da utilizzare come possibili 'locale tecnico' in cui alloggiare dispositivi di rete e dotazioni informatiche,
- situazione molto dinamica, soggetta a frequenti cambiamenti fisici (demolizioni, costruzioni, modifiche, ...) e all'accesso continuo di molte persone e mezzi che lavorano nel cantiere con tempistiche, caratteristiche ed esigenze diverse,
- durata limitata nel tempo,
- possibilità di furti in tutta l'area di cantiere, nel caso di realtà piccole o poco presidiate.

Queste considerazioni hanno un impatto sulle scelte progettuali, che peraltro sono da adeguare allo specifico cantiere: per esempio, nel caso di un cantiere piccolo o poco presidiato, si opterà più possibile per tecnologie di tipo rete cellulare, facilmente spostabili e poco costose. Inoltre, si rileva la necessità di semplicità di installazione e manutenzione di qualsiasi sistema informatico, in modo da evitare interventi di tecnici specializzati

Al fine di fornire un esempio piuttosto complesso, si prende in considerazione un grosso cantiere, in cui sia possibile ricorrere a varie tecniche abbastanza complete ed esaustive per quanto riguarda il progetto da proporre, considerando che nella realtà difficilmente si riuscirà ad implementare soluzioni di questo tipo e si ricorrerà quasi sempre a tecnologie di tipo cellulare, molto flessibili, scalabili, economiche. che non necessitano di particolari infrastrutture: questo tipo di tecnologia è comunque prevista nel progetto qui presentato.

Si ipotizza di avere a disposizione almeno un box di cantiere, con una parte blindata in cui allocare i dispositivi di rete e le dotazioni informatiche necessarie, inoltre si ipotizza che tutta l'area sia presidiata e che sia possibile posizionare i vari dispositivi richiesti nel testo senza che questi debbano essere rimossi ogni volta che viene chiuso il cantiere per il rischio di furti.

Si considera inoltre di poter realizzare un cablaggio, seppur provvisorio, almeno in una piccola porzione di cantiere (in modo da analizzarne gli aspetti tecnologici principali), mentre per il resto si prevede una copertura wireless attraverso l'uso di access point con infrastruttura, cioè collegati alla parte cablata della rete: se questo non fosse possibile, si potrebbero utilizzare tecnologie diverse, per esempio Wi-Fi Mesh, in cui gli access point comunicano direttamente fra loro.

Scendendo nel dettaglio, il progetto comprende i seguenti elementi:

Per quanto riguarda l'infrastruttura complessiva, si prevede, a titolo esemplificativo, un cablaggio 'provvisorio' di tutta l'area adiacente alla zona dei box di cantiere: data la situazione di relativa precarietà, non si ritiene opportuno citare in questo caso gli standard del cablaggio strutturato, che verranno invece riportati nel punto 2, né si scende nel dettaglio dei vari livelli del cablaggio, limitandoci a considerare, come esempio, una struttura con due livelli ('centro stella'), che possono essere considerati con cablaggio orizzontale o verticale a seconda del tipo di cantiere su cui si lavora. Nel box blindato si posiziona il centro stella del cantiere, in cui sarà allocato uno switch che si può immaginare a 8 porte e il router che consente il collegamento alla rete WAN: data la quasi impossibilità di poter avere un collegamento in fibra in un'area di cantiere, si prevede di utilizzare la rete cellulare, pertanto il router dovrà essere con tecnologia 4G/5G e relativa scheda SIM attiva.

Si prevede di utilizzare cavi in fibra monomodale per i collegamenti fra gli switch e con il router, mentre per tutto il resto si utilizzano cavi UTP classe E (cat. 6, Gigabit Ethernet).

Allo switch del centro stella del cantiere si considera di collegarne altri, con almeno 20 porte, come centro stella di livello inferiore, al quale sono collegati in modalità infrastruttura i vari access point dislocati nei diversi punti del cantiere per fornire connettività wi-fi a vari dispositivi ed eventuali fotocamere, laddove il loro posizionamento ('punti strategici del cantiere') fosse raggiungibile da cablaggio.

Data la situazione, non si prevede di avere una copertura wi-fi totale dell'area di cantiere, infatti i BSS individuati dagli access point possono essere posizionati in modalità disgiunta, in quanto servono sostanzialmente per dare connettività a telecamere e sensori, che non necessitano di spostamenti che renderebbero indispensabile la modalità parzialmente sovrapposta. E' invece utile che gli access point siano di tipo POE in modo da non dover essere alimentati a parte e siano compatibili con diverse versioni dello standard IEEE802.11, almeno fino alla tecnologia Wi-Fi 6 (IEEE802.11ax), che prevede velocità, flessibilità e scalabilità sfruttando le bande dei 2,4 GHz e dei 5 GHz: la compatibilità è utile per consentire la connessione a diversi tipi di dispositivi, anche con tecnologie meno recenti.

Per quanto riguarda le apparecchiature digitali indicate nel testo, si prevedono le seguenti tipologie:

- Tablet – per la connettività utilizzano rete cellulare 4G/5G con scheda SIM, sono dotati di software per l'acquisizione dei dati dai diversi tipi di scanner ad essi collegati, come descritto nel testo. Si collegano attraverso il protocollo HTTP ai server della sede centrale in cui è installato il sistema BIM per il passaggio dei dati grezzi delle 'nuvole'.

- Fotocamere – utilizzano il protocollo FTP per inviare le foto ad un server repository posizionato presso la sede centrale; si prevedono con tre diverse tipologie di connettività, a seconda del tipo di cantiere e della posizione in cui verranno installate: connessione wired (da utilizzare nei punti raggiunti da cablaggio), connessione wi-fi con collegamento agli access point posizionati nei vari punti del cantiere, connessione a rete cellulare 4G/5G con SIM, laddove non sia possibile utilizzare gli altri tipi di connettività.

- Sensori per la sicurezza - possono essere di tipo analogico o digitale, a seconda della grandezza che devono rilevare; i sensori sono collegati in modalità wired o wi-fi a microcontrollori, che dovranno avere rispettivamente nei due casi opportuna scheda Ethernet o wi-fi per il collegamento. Il microcontrollore deve essere programmabile in un linguaggio di alto livello, per esempio C o Python, deve avere una interfaccia per il collegamento ad un pc per la programmazione e deve avere integrata un'area di memoria con una buona capacità di archiviazione per mantenere, oltre al codice del programma, anche i dati letti dai sensori in attesa di essere inviati ai sistemi locali e remoti. Infine, il microcontrollore deve avere le schede che gli permettano il collegamento alla rete: scheda Ethernet o Gigabit Ethernet da utilizzare nel caso di posizionamento in area coperta da cablaggio, scheda compatibile con le varie versioni del protocollo IEEE 802.11, nel caso di area coperta da connettività wi-fi, scheda 4G/5G altrimenti.

- Sistemi locali per l'attivazione di notifiche ed allarmi in tempo reale – si considera che i dati provenienti dai sensori, oltre che a sistemi remoti in sede, siano indirizzati ad un pc/server locale,

Per quanto riguarda il piano di indirizzamento, si utilizza l'indirizzo IPv4 privato 192.168.0.0, che consente un numero di host e di subnet sufficiente per le esigenze dei cantieri. Si sviluppa considerando di utilizzare il quarto ottetto per gli host, il terzo ottetto per individuare i diversi cantieri e le sottoreti della sede, dedicando ai primi il range 1-127 (primo bit del terzo ottetto a 0 in binario), alle seconde il range successivo (primo bit del terzo ottetto a 1 in binario). Per esempio, per un ipotetico cantiere n.10:

Di seguito si riporta uno schema di massima della rete, con indicazione solo di alcuni dispositivi:



Soluzione del punto 2

Nel secondo punto è richiesta una descrizione della rete pre-esistente della sede centrale e proposte di sviluppo per l'adozione del sistema BIM.

Per quanto riguarda la situazione pre-esistente, si può ipotizzare che la sede abbia già un'infrastruttura di rete adeguata con cablaggio in tutti i locali dell'edificio e connessione wi-fi disponibile per i dipendenti con copertura pressoché completa sull'edificio (non si ritiene necessario estenderne l'utilizzo a persone esterne, che si ipotizza siano presenti in sede solo occasionalmente). Per quanto riguarda il cablaggio, si prevede che sia già presente, adeguato allo standard ISO/IEC 11801 utilizzato in Europa. Si prevedono cavi in fibra monomodale per i collegamenti fra gli switch, fra questi e i server, fra il proxy e il router, mentre per tutto il resto si utilizzano cavi UTP almeno di classe E (cat. 6, Gigabit Ethernet). I vari dispositivi di rete descritti in seguito sono alloggiati in appositi armadi rack con permutatori, come da standard. Il locale tecnico, in cui sono posizionati i dispositivi di rete e i server, come da schema, è opportunamente protetto per garantire la sicurezza e l'affidabilità dell'intera rete: si considera per esempio che ci siano sistemi antintrusione, antincendio, di climatizzazione, di messa a terra, UPS.

E' presente una DMZ (Demilitarized Zone) separata dal resto della rete, in cui sono posizionati i server che devono essere raggiungibili dall'esterno (web server e mail server). La struttura è a vicolo cieco, con la DMZ collegata ad un server proxy sul quale sono attivate le funzionalità di firewall con opportune ACL.

Nel centro stella di edificio è presente uno switch con almeno 8 porte.

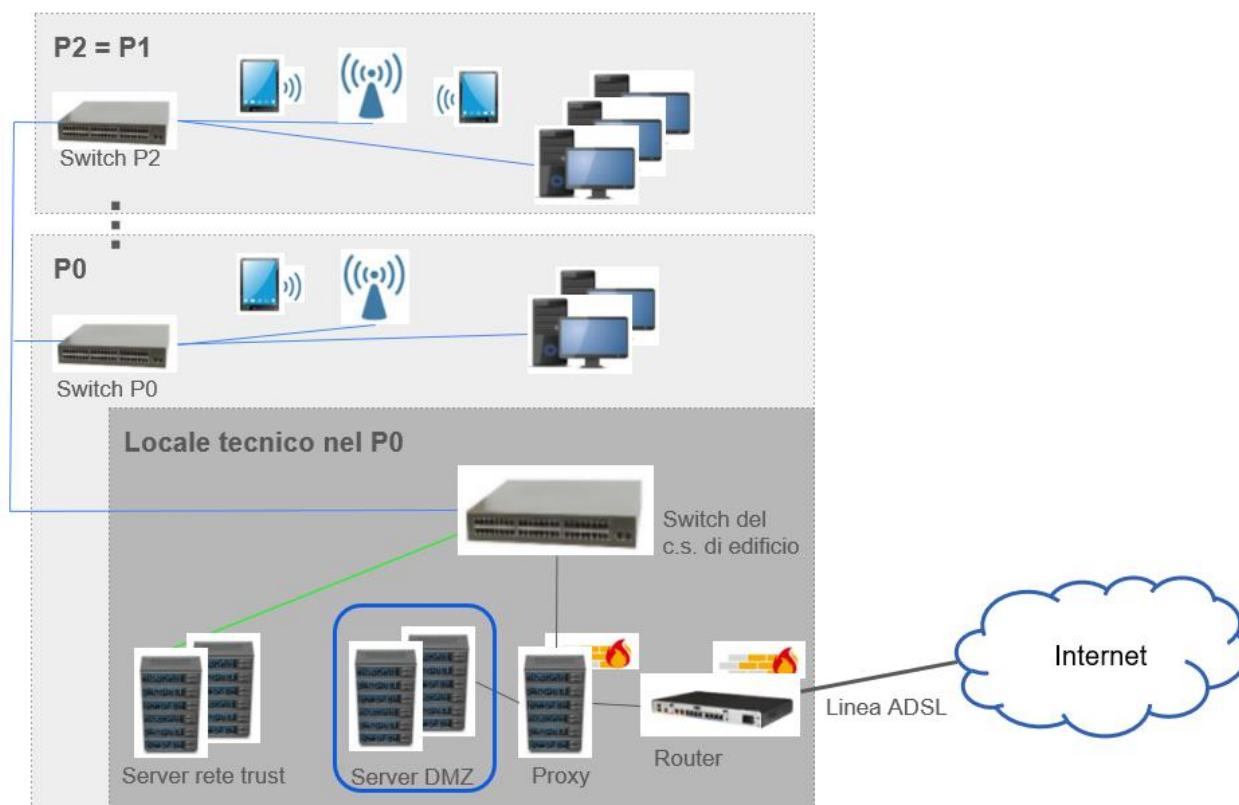
Nei centro stella di piano sono presenti switch con almeno 24 porte, mentre per quello di collegamento ai server sono sufficienti 8 porte. In ogni piano si trova anche un access point (o più di uno, nel caso di dimensioni elevate dei piani) con infrastruttura, collegato allo switch di piano per dare l'accesso alla rete ai dispositivi wireless la tecnologia è 802.11n con frequenze a 2,4 e 5 GHz, con compatibilità con precedenti versioni; il posizionamento degli AP è tale da creare BSS (Basic Service Set) parzialmente sovrapposti, così da avere una copertura continua, senza perdita di segnale su tutto l'edificio, inoltre si segue la regola del 5 per evitare interferenze. L'accesso alla rete Wi-Fi è ammesso solo per i dipendenti e limitato ai dispositivi della società, cosa che si ottiene attraverso ACL di tipo white list configurate negli AP in modo da bloccare tutti i MAC address tranne quelli ammessi e con utilizzo di credenziali di accesso alla rete per gli utenti validate attraverso server AAA: sugli AP è configurato il protocollo di sicurezza WPA2 enterprise, che si avvale di questo server per l'autenticazione.

Lo switch del centro stella di edificio è collegato attraverso il server proxy al router ADSL che fornisce connettività verso la WAN.

Sono previsti firewall per la protezione perimetrale e a diversi livelli della rete.

Di seguito si riporta uno schema di massima della rete pre-esistente:

Sede Società Ingegneria



Le principali modifiche da prevedere riguardano i seguenti aspetti:

- vista la quantità di dati che dovranno essere ricevuti dai cantieri e la necessità di continuità nella ricezione di questi per garantire almeno il controllo dei dati relativi alla sicurezza, è opportuno che l'accesso ad internet sia potenziato e ridondato con l'utilizzo di due linee in fibra FTTB con contratti fatti con due diversi provider in modo da avere garanzia di funzionamento anche nel caso di mancata connessione su una delle due linee;
- il router che consente l'accesso alla WAN dovrà essere sostituito con uno che abbia la possibilità di gestire quanto indicato al punto precedente (di tipo dual-WAN), da utilizzare normalmente in modalità load balancing (bilanciamento del carico di lavoro), salvo nel caso di malfunzionamenti;
- devono essere previsti server specifici per i software di gestione delle nuvole di punti con relativa modellazione 3D, per il repository dei fotogrammi, per l'elaborazione dei dati provenienti dai sensori di sicurezza;
- è opportuno separare il traffico proveniente dai cantieri da quello interno alla sede: per farlo, si prevede di sezionare la rete complessiva attraverso l'utilizzo di VLAN specifiche: se ne può prevedere una per gli uffici amministrativi, una per gli uffici tecnici che gestiscono BIM e i cantieri, una per i server interni alla sede centrale, una per i dati provenienti dai cantieri (individuabili attraverso il range di indirizzi IP e associabili alla VLAN attraverso opportune regole da impostare sugli apparati).

Per quanto riguarda i dispositivi di rete utilizzati, nel centro stella di di edificio va previsto uno switch Layer 3 con almeno 8 porte, necessario per la gestione delle VLAN (prima non c'erano): si sceglie questo invece di un router per minor costo, maggior semplicità di gestione, e migliori prestazioni per lo specifico ambito di utilizzo; questo switch deve avere porte tagged (standard IEEE 802.1q) e untagged: le prime per i collegamenti con gli altri switch sui quali transitano VLAN diverse e con il router, le altre per tutti gli altri collegamenti.

Il piano di indirizzamento deve essere coerente con quanto già indicato al punto precedente.

Soluzione del punto 3

Nel terzo punto è richiesto di analizzare i canali di comunicazione fra i cantieri e la sede centrale. La soluzione più indicata è una VPN site-to-site di tipo intranet, dal momento che i cantieri si possono considerare, seppure in via temporanea, come sedi distaccate della società di ingegneria. La VPN dovrà essere in modalità tunnel, realizzata con l'utilizzo di router VPN sia nella sede centrale che nei cantieri: per la prima si considera di utilizzare la connettività in fibra indicata al punto precedente, mentre per i cantieri, come indicato al punto 1, si opta per un collegamento 4G/5G, pertanto il router deve essere adeguato a tale tecnologia.

Per quanto riguarda gli aspetti di sicurezza, è necessario che presso la sede centrale sia presente un server AAA (es. Radius), che gestisce autenticazione, accesso e accounting per la rete, da utilizzare sia per chi accede da VPN che per gli altri, considerando anche che tale server è previsto per esempio anche in protocolli di crittografia delle reti wi-fi come WPA 2 e 3 enterprise.

Inoltre, per la sicurezza della VPN si utilizza il protocollo IPSec, in particolare con i sottoprotocolli IKE e ESP, che garantisce crittografia, autenticazione e integrità, importante dal momento che sul canale transitano dati di vario genere, fra cui personali (per esempio, le immagini possono riprendere persone, ...)

Per quanto riguarda il dimensionamento, va considerato che nel collegamento sede - cantieri transitano i dati delle fotocamere e dei sensori, mentre quello degli scanner viaggia su rete cellulare attraverso i tablet, che, con tecnologia almeno 4G presentano già caratteristiche di larghezza di banda sufficiente per questo tipo di traffico. Per quanto riguarda invece il collegamento fra sede e cantieri appena citato, le esigenze in termini di larghezza di banda per i dati dei sensori è molto basso e costante, mentre per quelli delle fotocamere è elevato (le immagini sono in alta risoluzione, il testo indica come esempio 4K/8K), ma discontinuo. In considerazione di questo, in ogni cantiere, con utilizzo del router 4G si può garantire una banda di almeno 5Mbps in upload, che, considerando che ogni fotocamera utilizza tale banda solo per una frazione di tempo, è sufficiente per il traffico complessivo. Per quanto riguarda invece la sede centrale, il router qui dovrà gestire il traffico entrante dai diversi cantieri, ma la tecnologia utilizzata, fibra FTTB, offre prestazioni molto superiori a quelle della rete cellulare suddetta (si tratta di centinaia di Mbps, a seconda del tipo di fornitura) e garantisce la larghezza di banda sufficiente per il traffico complessivo proveniente dai vari cantieri.

Non sarebbe stato altrettanto con la precedente tecnologia ADSL, con larghezza di banda decisamente inferiore (al massimo 20 Mbps, ma difficilmente raggiungibili).

Soluzione del punto 4

In questo punto è richiesto di approfondire l'autenticazione ai vari sistemi, in sede e da remoto, questione in parte già affrontata nel punto precedente.

Come già indicato (si rimanda al punto precedente), la gestione dell'autenticazione è affidata al server AAA, utilizzato per autenticare gli utenti che accedono da remoto (attraverso VPN) e in locale, sia da rete cablata che wireless (in quest'ultimo caso, con protocolli di crittografia WPA 2 o 3 enterprise): i servizi offerti dal server AAA sono authentication, authorization, accounting.

Per quanto riguarda la modalità, si prevede l'autenticazione multifattore (MFA), in cui oltre alla password viene richiesto un ulteriore elemento, per esempio un codice OTP temporaneo inviato ad un dispositivo certificato o altri fattori: questa modalità è adatta in quanto nel testo si specifica che l'autenticazione riguarda gli operatori, non sarebbe stata valida per il passaggio di dati 'automatico'. Per quanto riguarda i protocolli, si prevede su utilizzare EAP (Extensible Authentication Protocol), che è in realtà una suite di protocolli, con caratteristiche che la rendono molto flessibile e adattabile sulle diverse tipologie di reti: lo stesso EAP può essere utilizzato su parte wired e wireless della rete e sulle VPN. Fa riferimento allo standard IEEE 802.1x.

Seconda parte

Soluzione del quesito 1

Il testo della prova prevede, nella prima parte, che l'archiviazione dei dati provenienti dai cantieri sia fatta presso i sistemi di repository della sede centrale: questa è la soluzione 'on premise', che vede l'alternativa di soluzioni cloud-based, in cui i dati vengono archiviati su server in cloud.

Per quest'ultimo, si sceglie un modello DaaS (Data as a Service), visto che il servizio richiesto riguarda solo l'archiviazione di dati. Alcune alternative al DaaS, non indicate nel caso in esame, possono essere: SaaS (Software as a Service) è indirizzato in modo più specifico all'utilizzo di software in cloud, IaaS (Infrastructure as a Service) in cui viene messa a disposizione un'intera infrastruttura IT in cloud, PaaS (Platform as a Service) in cui viene messa a disposizione una piattaforma completa per lo sviluppo di applicazioni.

La scelta fra la soluzione on premise e cloud-based è legata a vantaggi e svantaggi offerti da ognuna delle due. In particolare, la prima soluzione, ossia l'archiviazione su server e aree di storage locali, ha come vantaggio principale la possibilità di controllo completo su tutto, dati e infrastruttura hardware e software, inoltre, considerando che i dati sono anche personali, è necessario essere ottemperanti alla normativa in vigore a livello europeo, ossia il GDPR (General Data Protection Regulation), che, fra le varie indicazioni che fornisce, è molto stringente per quanto riguarda il trasferimento dati in paesi extra-UE, cosa che risulta molto delicata in soluzioni in cloud, nelle quali va posta particolare attenzione proprio a questo aspetto: mantenere i dati internamente alla società da sicuramente maggiori garanzie in questo senso. Infine, l'accesso ai dati in locale è più veloce rispetto alla soluzione in cloud, consentendo maggiori performance dell'intero sistema, cosa che, visto il tipo di elaborazioni che si prevedono con il sistema BIM, può risultare vantaggiosa. Gli svantaggi della soluzione on premise riguardano principalmente l'investimento in termini di costi e di risorse, anche umane, necessari per l'avvio e la manutenzione della struttura (acquisto di hardware e software, necessità di personale interno o esterno qualificato e specializzato per la gestione dei sistemi, ...), inoltre può essere difficoltoso garantire scalabilità e flessibilità e anche tolleranza a guasti nelle varie parti dell'infrastruttura. La soluzione cloud-based si pone in modo esattamente contrapposto rispetto a quella on-premise.

Nel caso in esame, quest'ultima soluzione risulta effettivamente la più indicata in quanto la società ha intenzione di investire fortemente nel nuovo sistema e, da quello che emerge dal testo, dovrebbe avere le risorse disponibili per farlo, quindi i vantaggi di tale soluzione superano gli svantaggi.

Soluzione del quesito 2

Come ulteriori misure di sicurezza, oltre a quelle di autenticazione, nella soluzione della prima parte ne sono state individuate già varie, per esempio utilizzo di firewall a diversi livelli e server proxy (utili, fra i vari aspetti, per la sicurezza perimetrale della rete e per filtrare il traffico entrante/uscente dalla stessa), utilizzo di VLAN (che consentono di sezionare la rete in diversi domini di broadcast separando di fatto il traffico e limitando quindi le possibilità di eventuali accessi indesiderati), sicurezza fisica del locale tecnico, utilizzo di VPN con protocollo IPSec e modalità tunnel con crittografia, impostazione della crittografia WPA 2 o 3 enterprise sulle parti wireless della rete, ...

Per quanto riguarda la garanzia della continuità trasmissiva si è già considerato l'utilizzo per la sede centrale di due connessioni FTTB fatte con provider diversi, in modo che sia garantita la connettività anche nel caso di malfunzionamento di una delle due linee. Per quanto riguarda i cantieri, il collegamento avviene attraverso rete cellulare: si potrebbe prevedere, almeno per i cantieri più grandi o delicati, di ridondare le linee di connessione alla WAN, esattamente come fatto per la sede centrale, considerando solo la diversa tecnologia da utilizzare.

Infine, si può prevedere un sistema di backup di tutti i dati fatto a diversi livelli, sicuramente va implementato nei sistemi della sede centrale e, data la quantità e l'importanza dei dati, va schedato in più fasi durante la giornata e pianificato in modo preciso a livello giornaliero,

settimanale e mensile, prevedendo diversi tipi di backup, totale, incrementale, differenziale, in modo da bilanciare bene l'utilizzo delle risorse dell'infrastruttura e non ridurre le performance complessive. Non si ritiene necessario fare un backup dei dati presenti nei sistemi locali dei cantieri in quanto gli stessi sono già duplicati anche nel sistema in sede, mentre va previsto che i vari dispositivi abbiano una capacità di memoria sufficiente a mantenere al loro interno i dati finché questi non sono trasferiti verso i sistemi centrali (cosa già prevista per i microcontrollori a cui sono collegati i sensori).

Soluzione del quesito 3

Il quesito richiede di bloccare l'uso delle piattaforme di intelligenza artificiale di sviluppo software. Si ipotizza che gli studenti non possano utilizzare i propri dispositivi personali e la propria rete dati (4G/5G), in considerazione anche dell'attuale normativa scolastica. Si considera pertanto la sola rete didattica per quanto riguarda le limitazioni da gestire.

Il modo più semplice per attuare il blocco suddetto è lavorare sui firewall e relative regole: per esempio, operando su quelli di livello applicativo, si possono bloccare specifiche categorie legate all'intelligenza artificiale semplicemente individuando parole chiave nei nomi dei domini che portano al blocco dei relativi messaggi in uscita e in entrata, oppure si possono bloccare direttamente i domini delle piattaforme note, per esempio `chatgpt.com` o `gemini.google.com`. Lavorare sugli indirizzi IP è più complesso nella situazione attuale: non è affatto detto che l'indirizzo della piattaforma resti sempre e solo lo stesso.

Per quanto riguarda la schedulazione, la maggior parte dei firewall prevede una funzione apposita che consente di specificare la regola da attivare e anche la fascia oraria in cui questa deve essere attiva. Infine, il blocco potrebbe essere attivato solo sui laboratori, come richiesto nel quesito, sezionando la rete in VLAN, assegnandone una specifica per i laboratori in questione e attivando poi le regole di blocco solo su tale VLAN. In effetti, è importante individuare la sezione della rete su cui i blocchi devono essere attivati in modo, per esempio, da impedire l'utilizzo delle suddette piattaforme agli studenti ma non ai docenti e al personale amministrativo e di dirigenza.

Soluzione del quesito 4

Il comando `ssh` viene utilizzato per avviare da un client una connessione remota verso un server con protezione crittografica.

Nel comando `ssh -p 25500 administrator@200.1.1.1`, la connessione avviene sulla porta 25500 del destinatario, che ha indirizzo IP 200.1.1.1 e viene fatta utilizzando l'utente `administrator`, al quale viene richiesta opportuna autenticazione: una volta fatto questo, l'utente avrà accesso al terminale del dispositivo remoto e potrà lavorarci come se fosse fisicamente lì.

Nel caso indicato nel quesito, sul dispositivo con indirizzo 200.1.1.1 è attiva la regola che reindirizza il traffico entrante dalla porta 25500 verso il dispositivo con indirizzo IP 172.16.1.100. Il risultato è che la connessione del client avverrà non con il destinatario richiesto nel comando, ma con il dispositivo di indirizzo 172.16.1.100, in modo del tutto trasparente: l'autenticazione di fatto avverrà su quest'ultimo, al quale pertanto il client dovrà essere autorizzato ad accedere.

Il comando indicato può essere utilizzato per vari motivi, primo fra tutti la sicurezza, infatti con il reindirizzamento viene mascherato l'indirizzo IP dell'effettivo destinatario della connessione: il client 'vede' solo il dispositivo con indirizzo IP 200.1.1.1, che funge da 'bastion host', esponendosi sulla rete esterna al posto dei dispositivi interni alla LAN, che risultano pertanto protetti. Inoltre, il reindirizzamento può essere utilizzato per gestire dispositivi 'nascosti' di una rete privata attraverso tecniche del tipo NAT o similari: si noti infatti che l'indirizzo IP effettivamente destinatario della connessione, 172.16.1.100, è privato di classe B, pertanto non utilizzabile all'esterno della rete.