Dispense di Sistemi e Reti per l'Esame di Stato

A.S. 2025/2026

Contents

Prerequisiti **5**

1 Cablaggio strutturato **7**
1.1 Il modello gerarchico ISO/IEC 11801 . . . 7
1.2 MDF e IDF . . . 7
1.3 Mezzi trasmissivi . . . 7
1.3.1 Fibra ottica: monomodale vs multimodale . . . 8
1.3.2 Rame: UTP cat. 6A . . . 8
1.3.3 PoE (Power over Ethernet) . . . 8

2 Topologia e apparati di rete **9**
2.1 Il modello a 3 livelli: core / distribution / access . . . 9
2.2 Switch L2 vs Switch L3 . . . 9
2.3 Firewall UTM . . . 9
2.4 DMZ . . . 10
2.5 ONT/CPE dell'ISP vs router di frontiera . . . 10
2.6 Access Point e Controller . . . 10

3 VLAN e segmentazione **11**
3.1 Cos'è una VLAN e perché segmentare . . . 11
3.2 Trunk 802.1Q . . . 11
3.3 Quante VLAN servono? . . . 11
3.4 La VLAN Management: cosa ci va dentro . . . 12
3.5 Policy inter-VLAN e default deny . . . 12

4 Piano di indirizzamento IPv4 **13**
4.1 Scelta del blocco privato . . . 13
4.2 FLSM vs VLSM . . . 13
4.3 Procedura VLSM in 3 passi . . . 13
4.4 Subnet punto-punto: /30 e /31 . . . 13
4.5 DMZ su blocco separato . . . 14
4.6 IP pubblici nella WAN . . . 14

5 WiFi e copertura wireless **15**
5.1 Standard WiFi 6 (802.11ax) . . . 15
5.2 Dimensionamento degli AP . . . 15
5.3 SSID multipli e autenticazione . . . 15
5.4 Roaming . . . 16

6 Servizi di rete **17**
6.1 DHCP . . . 17
6.2 DNS . . . 17

6.3 RADIUS e 802.1X . . . 17
6.4 Captive portal e tracciabilità . . . 18
6.5 VoIP e QoS . . . 18
6.6 NAS, backup e regola 3-2-1 . . . 18
6.7 Monitoraggio e logging . . . 18

7 Collegamento tra siti remoti **21**
7.1 Ponte radio P2P . . . 21
7.1.1 Caratteristiche operative . . . 21
7.1.2 Configurazione di rete . . . 21
7.1.3 Normativa italiana . . . 21
7.2 VPN: IPsec e WireGuard . . . 22

8 Sicurezza della rete **23**
8.1 La triade CIA . . . 23
8.2 Autenticazione: password, MFA, passkey . . . 23
8.3 Ransomware . . . 23
8.4 Phishing . . . 23
8.5 HTTPS e TLS . . . 24
8.6 MITM (Man in the Middle) . . . 24

9 Cloud e migrazione dei servizi **25**
9.1 IaaS, PaaS, SaaS . . . 25
9.2 Quando migrare e quando no . . . 25
9.3 Privacy e GDPR nel cloud . . . 25

10 Conformità normativa **27**
10.1 GDPR (Reg. UE 2016/679) . . . 27
10.2 Decreto Pisanu e tracciabilità WiFi . . . 27
10.3 NIS2 (Dir. UE 2022/2555) . . . 27
10.4 ISO/IEC 11801 e CEI 64-8 . . . 27

Prerequisiti

Questo capitolo richiama i concetti che dovresti già conoscere. Se qualcosa non è chiaro, fermati e ripassalo prima di procedere: tutto il resto si costruisce su queste basi.

Modello a strati: OSI e TCP/IP

Le reti si studiano a strati. Il modello OSI ha 7 livelli; nella pratica si usa il modello TCP/IP a 4 livelli. Per l'esame ti servono soprattutto i livelli 2 e 3:

OSI	Nome	TCP/IP	Cosa fa (in pratica)
7,6,5	Applicazione	Applicazione	HTTP, DNS, DHCP, SIP, SMTP
4	Trasporto	Trasporto	TCP (affidabile), UDP (veloce)
3	Rete	Internet	IP, routing, ICMP
2	Data-link	Accesso rete	Ethernet, WiFi, MAC address, VLAN
1	Fisico	Accesso rete	Cavi, fibre, segnali radio

Osservazione: uno switch L2 lavora al livello 2 (conosce i MAC address, non gli IP). Un router lavora al livello 3 (conosce gli IP, sa instradare tra reti diverse). Uno switch L3 fa entrambe le cose.

Indirizzo MAC e indirizzo IP

Ogni dispositivo di rete ha **due identità**:

L'**indirizzo MAC** è un identificativo hardware di 48 bit (6 byte), scritto in esadecimale, es. `A4:CF:12:8B:5E:01`. È "bruciato" nella scheda di rete dal fabbricante ed è unico al mondo. Serve al livello 2 per comunicare *nella stessa rete locale* (stesso dominio di broadcast).

L'**indirizzo IP** (IPv4) è un identificativo logico di 32 bit, scritto come 4 ottetti decimali separati da punti, es. `192.168.1.10`. Viene assegnato (staticamente o via DHCP) e può cambiare. Serve al livello 3 per comunicare *tra reti diverse* (attraverso router).

Analogia postale

L'indirizzo MAC è come il numero di serie stampato sulla cassetta delle lettere: identifica fisicamente l'oggetto. L'indirizzo IP è come l'indirizzo postale (via, numero, città): identifica una posizione nella rete, può essere riassegnato se il dispositivo "trasloca" in un'altra rete.

Il protocollo **ARP** (Address Resolution Protocol) traduce da IP a MAC: quando un dispositivo vuole comunicare con un IP nella sua stessa rete, fa un broadcast ARP chiedendo "chi ha l'IP X?" e il proprietario risponde con il proprio MAC.

Indirizzamento IPv4: struttura e maschere

Un indirizzo IPv4 ha 32 bit, divisi in due parti dalla **subnet mask**: la **parte di rete** (comune a tutti gli host della stessa rete) e la **parte di host** (unica per ciascun dispositivo).

La subnet mask è una sequenza di 1 seguiti da una sequenza di 0. Si scrive in due modi equivalenti:

Notazione CIDR	Notazione decimale	Significato
`/24`	`255.255.255.0`	24 bit di rete, 8 bit di host
`/25`	`255.255.255.128`	25 bit di rete, 7 bit di host
`/26`	`255.255.255.192`	26 bit di rete, 6 bit di host
`/27`	`255.255.255.224`	27 bit di rete, 5 bit di host
`/28`	`255.255.255.240`	28 bit di rete, 4 bit di host
`/29`	`255.255.255.248`	29 bit di rete, 3 bit di host
`/30`	`255.255.255.252`	30 bit di rete, 2 bit di host

Con k bit di host si hanno 2^k indirizzi totali, di cui $2^k - 2$ **utilizzabili**: il primo (tutti zeri nella parte host) è il **network address**, l'ultimo (tutti uni) è il **broadcast address**.

Calcolo rapido

Rete `192.168.1.0/26`: maschera /26 $\rightarrow$ $32-26 = 6$ bit di host $\rightarrow$ $2^6 = 64$ indirizzi totali, $64 - 2 = 62$ host utili. Network address: `192.168.1.0`. Broadcast: `192.168.1.63`. Range utile: `.1` – `.62`.

Spazi di indirizzamento privati (RFC 1918)

Non tutti gli IP sono instradabili su Internet. Tre blocchi sono riservati per le reti private:

Blocco	Range	Uso tipico
`10.0.0.0/8`	`10.0.0.0` – `10.255.255.255`	Reti enterprise grandi
`172.16.0.0/12`	`172.16.0.0` – `172.31.255.255`	DMZ, reti medie
`192.168.0.0/16`	`192.168.0.0` – `192.168.255.255`	PMI, reti domestiche

Per uscire su Internet da una rete privata serve il **NAT** (Network Address Translation): il firewall/router sostituisce l'IP privato sorgente con il proprio IP pubblico nel pacchetto in uscita, e fa l'operazione inversa in risposta.

Potenze di 2 (da sapere a memoria)

2^1	2^2	2^3	2^4	2^5	2^6	2^7	2^8	2^9	2^{10}
2	4	8	16	32	64	128	256	512	1024

Queste ti servono per il subnetting: la maschera $/k$ ti dà 2^{32-k} indirizzi. Un `/25` ha $2^7 = 128$ indirizzi (126 host utili). Un `/28` ha $2^4 = 16$ indirizzi (14 host utili). Sapere queste potenze a memoria ti fa risparmiare minuti preziosi in sede d'esame.

Capitolo 1 Cablaggio strutturato

1.1 Il modello gerarchico ISO/IEC 11801

Il cablaggio strutturato è l'infrastruttura fisica permanente di una rete: cavi, connettori, prese, armadi rack, percorsi di canalizzazione. È progettato per durare 15–20 anni e deve supportare qualsiasi tecnologia futura senza essere rifatto. Lo standard internazionale di riferimento è **ISO/IEC 11801** (in Nord America si usa l'equivalente TIA-568).

L'idea fondamentale è organizzare il cablaggio in **sottosistemi gerarchici** con punti di distribuzione intermedi. In una struttura tipica per l'esame (albergo, azienda, scuola) si identificano:

Sottosistema	Funzione	Mezzo tipico
Campus backbone	Collegamento tra edifici distinti (es. hotel ↔ SPA esterna)	Fibra OS2 monomodale, armata e interrata
Building backbone	Collegamento verticale tra piani (MDF ↔ IDF)	Fibra OM4 multimodale
Cablaggio orizzontale	Dal pannello di permutazione alle prese utente (max 90 m)	UTP cat. 6A schermato
Area di lavoro	Dalla presa a muro al dispositivo (max 5 m)	Patch cord UTP cat. 6A

1.2 MDF e IDF

MDF (*Main Distribution Frame*) è il locale tecnico principale, solitamente al piano terra o in un seminterrato. Contiene il cuore della rete: firewall, switch core, server, UPS, patch panel principale, attestazione della fibra dell'ISP. È il punto dove convergono tutti i backbone verticali e i collegamenti verso l'esterno.

IDF (*Intermediate Distribution Frame*) è l'armadio di piano. Ogni piano (o ogni ala di un grande edificio) ha il proprio IDF, contenente uno switch di accesso PoE+ e un patch panel. L'IDF è collegato al MDF tramite il building backbone (fibra).

Quanti IDF servono?

La regola pratica è: **un IDF per ogni piano** (due per ridondanza) che ha prese utente. Se l'edificio ha un solo piano e meno di 100 prese, può bastare un unico locale tecnico (che funge da MDF e IDF insieme). Se la traccia d'esame parla di "struttura su un piano" con poche decine di utenti, non serve inventare IDF separati.

1.3 Mezzi trasmissivi

1.3.1 Fibra ottica: monomodale vs multimodale

Fibra monomodale (OS2, single-mode): core molto sottile (9 μm), un solo modo di propagazione. Raggiunge distanze di **decine di km** con bassissima attenuazione. Si usa per i campus backbone (collegamento tra edifici) e per le dorsali dei provider. Costa leggermente di più (soprattutto le ottiche SFP).

Fibra multimodale (OM3, OM4, multi-mode): core più largo (50 μm), diversi modi di propagazione. Distanza massima utile: **300–550 m** a 10 Gbps (OM4). Si usa per i building backbone (collegamento tra piani all'interno dello stesso edificio). Le ottiche SFP sono meno costose.

Regola per l'esame

Tra edifici (campus backbone) → fibra monomodale OS2.
Dentro un edificio (building backbone) → fibra multimodale OM4.
Se la distanza tra edifici è < 300 m e non servono prestazioni estreme, anche OM4 può andare.

1.3.2 Rame: UTP cat. 6A

Il cablaggio orizzontale (dal patch panel alle prese utente) usa cavo in rame **UTP cat. 6A schermato**, che supporta 10 Gbps fino a 100 m. In pratica lo standard prevede: max **90 m** di cavo fisso (da patch panel a presa a muro) + **5 m** di patch cord lato utente + **5 m** di patch cord lato armadio = 100 m totali.

Ogni postazione di lavoro ha tipicamente una **presa doppia RJ-45**: una porta per il PC, una per il telefono VoIP o un dispositivo ausiliario. Nelle camere d'albergo la traccia potrebbe specificare 2 prese LAN (per SmartTV e PC ospite).

1.3.3 PoE (Power over Ethernet)

Il **PoE** (IEEE 802.3af/at/bt) permette di alimentare dispositivi tramite il cavo Ethernet, senza un alimentatore separato. È essenziale per gli **access point WiFi**, i **telefoni VoIP** e le **telecamere IP**: si cablano con un solo cavo che porta sia dati che alimentazione.

Gli switch di accesso negli IDF devono essere **PoE+** (802.3at, 30 W per porta) o **PoE++** (802.3bt, 60–90 W per porta). Il budget PoE totale dello switch deve coprire il consumo di tutti i dispositivi alimentati.

Capitolo 2 Topologia e apparati di rete

2.1 Il modello a 3 livelli: core / distribution / access

Le reti enterprise si progettano con una gerarchia a tre livelli funzionali. Non sempre corrispondono a tre apparati fisici distinti (in reti piccole, core e distribution possono coincidere), ma la separazione logica dei ruoli resta.

Core — è il cuore della rete: instrada velocemente il traffico tra le VLAN e verso Internet. In una rete di medie dimensioni (hotel, azienda, scuola) è uno **switch L3** nel MDF. Deve essere veloce (10G uplink), affidabile (alimentazione ridondante, STP/RSTP), e fare routing inter-VLAN in hardware (ASIC, wire-speed).

Distribution — aggrega il traffico degli switch di accesso e applica le prime policy (QoS, PoE). In molte architetture d'esame, la funzione di distribution è svolta dagli **switch di piano** (quelli negli IDF), collegati al core via fibra.

Access — è il livello dove si collegano fisicamente gli endpoint: PC, telefoni, AP, stampanti. Ogni switch di accesso PoE+ serve le prese di un piano o di un'area.

2.2 Switch L2 vs Switch L3

Uno **switch L2** conosce solo i MAC address: inoltra i frame in base alla sua tabella MAC. Supporta le VLAN (802.1Q) ma non sa instradare tra VLAN diverse. Due host su VLAN differenti collegati allo stesso switch L2 non possono comunicarsi senza un dispositivo L3.

Uno **switch L3** fa tutto quello che fa un L2, *più* il routing IP tra VLAN. Per ogni VLAN si configura una **SVI** (Switched Virtual Interface) con un IP che funge da gateway per quella VLAN. Il routing tra SVI avviene **in hardware**, a velocità di linea (wire-speed), senza impattare la CPU.

Perché il core è L3 e non L2

Se il routing inter-VLAN fosse sul firewall, ogni pacchetto tra due host su VLAN diverse dovrebbe attraversare il link core–firewall *due volte* (andata e ritorno). Il firewall diventa un collo di bottiglia e un single point of failure per il traffico interno. Con un core L3, il routing inter-VLAN avviene in hardware nello switch, e il firewall si occupa solo del traffico perimetrale (WAN ↔ LAN). Questo pattern si chiama **"firewall at the edge, L3 in the core"**.

2.3 Firewall UTM

Il firewall è l'apparato che separa la rete interna da Internet. Un **UTM** (Unified Threat Management) combina in un solo dispositivo: stateful firewall, NAT/PAT, IPS/IDS (intrusion prevention/detection), VPN (IPsec, OpenVPN), content filter, antimalware, logging.

Il firewall ha almeno tre interfacce (fisiche o logiche): **WAN** (verso l'ISP), **LAN** (verso il core switch), **DMZ** (verso i server esposti su Internet). Ogni pacchetto che attraversa il confine WAN↔LAN viene

ispezionato.

2.4 DMZ

La **DMZ** (Demilitarized Zone) è un segmento di rete separato che ospita i servizi esposti su Internet (web server, mail server). È collegata a un'interfaccia dedicata del firewall, *non* alla LAN interna.

La regola di progettazione è: un server in DMZ va considerato come **potenzialmente compromesso**. Se un attaccante ne prende il controllo, non deve poter raggiungere la rete interna. Per questo il firewall consente traffico Internet → DMZ (solo sulle porte dei servizi esposti, es. 443), ma **blocca** traffico DMZ → LAN.

Errore frequente negli esami

Mettere il web server in LAN con port forwarding generico, senza DMZ. Questo è sbagliato perché una compromissione del server darebbe accesso diretto a NAS, gestionale, e tutta la rete interna. La DMZ esiste per evitare esattamente questo.

2.5 ONT/CPE dell'ISP vs router di frontiera

Tra Internet e il firewall c'è sempre un apparato dell'ISP: l'**ONT** (Optical Network Terminal) per le connessioni FTTH, o un modem-router per xDSL. Questo apparato **non è aziendale**: l'azienda non lo configura, non ne ha il controllo.

In reti enterprise di grandi dimensioni si aggiunge talvolta un **router di frontiera aziendale** tra il CPE dell'ISP e il firewall, giustificato da esigenze specifiche: BGP (routing dinamico con l'ISP), multi-uplink (due ISP con failover), o AS proprio. Per le strutture tipiche dell'esame (hotel, PMI, scuola) **non serve**: il firewall UTM ingloba già le funzioni di routing verso Internet, NAT e gestione degli uplink. Aggiungere un router separato è complessità non giustificata.

Se la commissione chiede "perché non hai messo un router di frontiera?", la risposta è: "il firewall UTM svolge già le funzioni di routing, NAT e gestione uplink WAN. Un router dedicato sarebbe giustificato solo con BGP o multi-uplink, non necessari per una struttura di queste dimensioni."

2.6 Access Point e Controller

Gli **Access Point (AP)** WiFi 6 (802.11ax) dual-band sono i dispositivi che forniscono la copertura wireless. Operano in banda 2,4 GHz e 5 GHz con tecnologia MU-MIMO. Sono alimentati via PoE+.

Il **Controller AP** è il software (on-premise o cloud) che gestisce tutti gli AP in modo unificato: configurazione degli SSID, assegnazione dei canali radio, potenza di trasmissione, roaming seamless tra AP (802.11r/k/v), aggiornamenti firmware. Senza controller, ogni AP andrebbe configurato individualmente.

Capitolo 3 VLAN e segmentazione

3.1 Cos'è una VLAN e perché segmentare

Una **VLAN** (Virtual Local Area Network) è una rete logica indipendente all'interno dello stesso switch fisico. Due porte dello stesso switch assegnate a VLAN diverse **non possono comunicare a livello 2**: è come se fossero collegati a due switch separati. Per comunicare tra VLAN serve un dispositivo L3 (switch L3 o router).

Perché segmentare? Tre motivi:

1. **Sicurezza**: un ospite nella VLAN Guest non può raggiungere i PC dell'amministrazione nella VLAN Staff. Un ransomware introdotto da un dispositivo nella VLAN Guest resta confinato.
2. **Prestazioni**: ogni VLAN è un dominio di broadcast separato. Meno broadcast = meno congestione.
3. **Gestione**: policy diverse per gruppi diversi (QoS per il VoIP, banda limitata per gli ospiti, isolamento per IoT).

3.2 Trunk 802.1Q

Un **trunk** è un collegamento tra due switch (o tra switch e firewall/router) che trasporta traffico di *più VLAN* sullo stesso cavo. Ogni frame Ethernet che attraversa il trunk viene "taggato" con un campo aggiuntivo di 4 byte (standard IEEE 802.1Q) che contiene il **VLAN ID** (un numero da 1 a 4094). Lo switch ricevente legge il tag e consegna il frame alla VLAN corretta.

Le porte utente (dove si collega un PC, un telefono, un AP) sono dette **porte di accesso**: appartengono a una sola VLAN, non taggano i frame. Il PC non sa di essere in una VLAN — per lui è una rete normale.

3.3 Quante VLAN servono?

La risposta giusta è: **proporzionate alla scala dell'organizzazione**. Per un hotel con 52 camere e sale convegni, 6–7 VLAN sono appropriate. Per una PMI con 10 utenti, 4–5 bastano. Il dimensionamento eccessivo (12 VLAN per 7 utenti) dimostra alla commissione che non sai calibrare.

Le VLAN "standard" che troverai in quasi tutte le tracce d'esame:

VLAN	Nome	Chi ci va
10	Management	Interfacce di gestione di switch, AP, firewall, server, UPS
20	Staff	PC del personale, stampanti ufficio
30	Guest	Dispositivi WiFi degli ospiti/clienti
40	VoIP	Telefoni IP (se richiesto dalla traccia)
50	Congress	Partecipanti a convegni/eventi (se richiesto)
60	Server	Interfacce di servizio dei server interni
70	IoT	Colonnine EV, sensori, telecamere, SmartTV (se richiesto)

Non usare tutte e 7 in ogni prova: scegli solo quelle che la traccia richiede o che sono ragionevolmente necessarie.

3.4 La VLAN Management: cosa ci va dentro

La VLAN Management è quella che tutti citano ma pochi sanno popolare. Ospita **l'interfaccia di gestione** di ogni apparato — non l'apparato intero. Uno switch serve traffico su 48 porte assegnate a VLAN diverse, ma la sua SVI di management ha un IP nella VLAN 10.

Inventario tipico di una rete alberghiera:

- **Apparati L2/L3**: firewall UTM, core L3, switch di piano (4–5 switch) → 5–6 IP
- **Access Point**: uno per AP → 10–15 IP
- **Server** (interfacce di management, non di servizio): hypervisor, PBX, RADIUS, NAS, controller AP, monitoring → 5–6 IP
- **Ausiliari**: UPS con scheda SNMP, IPMI/iDRAC dell'host server → 2–3 IP

Due regole importanti: **(1)** nella Management **non si usa DHCP** — tutti gli IP sono statici, perché un DHCP failure bloccherebbe la gestione della rete; **(2)** la Management ha accesso verso tutte le altre VLAN (l'admin deve poter raggiungere tutto), ma nessun'altra VLAN deve poter raggiungere la Management.

3.5 Policy inter-VLAN e default deny

Il routing inter-VLAN è implementato sullo switch L3 con **ACL (Access Control List)** applicate sulle SVI. L'approccio è **default deny**: tutto ciò che non è esplicitamente consentito è negato. Ogni ACL termina con una regola implicita `deny any any`.

In una soluzione d'esame, la matrice di policy inter-VLAN si presenta come una tabella con check-mark (✓) e crocette (✗). Il traffico permesso è sempre *specifico*: "Staff può raggiungere Server solo sulle porte del gestionale e del DNS", non "Staff accede a tutto".

La matrice inter-VLAN fa punteggio

Molti candidati propongono VLAN e piano IP perfetti, ma dimenticano di specificare *chi parla con chi*. La matrice di policy è il pezzo che in commissione fa la differenza tra una prova buona e una eccellente. Disegnala sempre, anche se la traccia non la chiede esplicitamente.

Capitolo 4 Piano di indirizzamento IPv4

4.1 Scelta del blocco privato

La prima decisione è quale spazio RFC 1918 usare. In pratica:

`10.0.0.0/8` è il più usato nelle reti enterprise perché offre oltre 16 milioni di indirizzi e consente un'organizzazione gerarchica (es. `10.0.VLAN.0/24`). Usalo quando la traccia parla di hotel, campus, strutture medio-grandi.

`192.168.0.0/16` è più familiare (è quello delle reti domestiche) e va bene per PMI con pochi utenti. Usalo per tracce tipo "piccola azienda con 10 dipendenti".

`172.16.0.0/12` si usa spesso per la DMZ, come blocco visivamente separato dal resto. Convenzione, non obbligo.

4.2 FLSM vs VLSM

FLSM (Fixed Length Subnet Mask): tutte le subnet hanno la stessa maschera. Semplice ma inefficiente quando le VLAN hanno dimensioni molto diverse (es. la Guest con 400 host e la Management con 25).

VLSM (Variable Length Subnet Mask): ogni subnet ha la maschera più piccola che contiene i suoi host. È lo standard professionale e **quello che la commissione si aspetta**. In una prova d'esame mostra sempre il VLSM; se vuoi, menziona FLSM per spiegare perché non va bene.

4.3 Procedura VLSM in 3 passi

Metodo VLSM

Passo 1: Stimare il numero di host per ogni VLAN (contare i dispositivi, aggiungere margine).
Passo 2: Ordinare le VLAN per numero decrescente di host.
Passo 3: Per ciascuna, assegnare la maschera $/k$ più piccola tale che $2^{32-k} - 2 \geq n_{\text{host}}$. Allocare i blocchi in sequenza contigua a partire dall'indirizzo di base.

Calcolo della maschera

Servono 40 host. La potenza di 2 immediatamente $\geq 40 + 2 = 42$ è $2^6 = 64$. Quindi servono 6 bit di host $\rightarrow$ maschera /26 ($32 - 6 = 26$), con 62 host utili. Se servissero 65 host, si salirebbe a $2^7 = 128 \rightarrow$ /25, con 126 host utili.

4.4 Subnet punto-punto: /30 e /31

Quando due router (o un router e un firewall) sono collegati da un link dedicato, la subnet che li connette ha bisogno di soli 2 indirizzi host. Si usano:

Una /**30** (4 indirizzi totali: 1 network + 2 host + 1 broadcast) è la scelta classica. Esempio: `10.0.3.252/30` ha network `.252`, host utili `.253` e `.254`, broadcast `.255`.

Una /**31** (RFC 3021, 2 indirizzi totali, entrambi usabili come host) è la variante moderna che risparmia 2 IP. Usata nei grandi provider per risparmiare spazio su migliaia di link.

Quando serve la punto-punto nella prova?

Solo se nel diagramma c'è un **router aziendale dedicato** separato dal firewall. Se il firewall è direttamente collegato al CPE dell'ISP (caso normale per hotel/PMI), la punto-punto non va nel piano di indirizzamento: la subnet tra CPE e firewall è dell'ISP, non dell'azienda.

4.5 DMZ su blocco separato

La DMZ va su un blocco IP visivamente separato dalla LAN interna. Se la LAN usa `10.0.x.x`, la DMZ può stare su `172.16.0.0/29` (6 host utili: più che sufficienti per 1–2 server esposti). Questa separazione non è obbligatoria ma rende il piano IP più leggibile e le regole del firewall più chiare.

4.6 IP pubblici nella WAN

L'interfaccia WAN del firewall (o del router di frontiera, se presente) riceve un **IP pubblico statico** assegnato dall'ISP. In un compito d'esame **non si inventa un IP pubblico**: si scrive "IP pubblico statico fornito dall'ISP" e si lascia il campo aperto. Se proprio si vuole un esempio, usare il blocco `203.0.113.0/24` (RFC 5737, riservato per documentazione), mai un blocco privato.

Capitolo 5 WiFi e copertura wireless

5.1 Standard WiFi 6 (802.11ax)

Lo standard attuale per le installazioni professionali è **WiFi 6** (IEEE 802.11ax), operativo su entrambe le bande **2,4 GHz** e **5 GHz**. Le caratteristiche rilevanti per l'esame sono: throughput teorico fino a 9,6 Gbps (aggregato), tecnologia **MU-MIMO** (Multi-User, Multiple-Input Multiple-Output) che serve più client contemporaneamente, e **OFDMA** che divide il canale in sotto-portanti assegnabili a client diversi.

La banda **2,4 GHz** ha maggiore portata e penetrazione dei muri, ma solo 3 canali non sovrapposti (1, 6, 11) e molta interferenza. La banda **5 GHz** ha più canali, meno interferenza e throughput maggiore, ma portata inferiore. Gli AP moderni sono **dual-band**: servono entrambe le bande simultaneamente.

5.2 Dimensionamento degli AP

Regole pratiche per l'esame:

- **Corridoio con camere**: 1 AP ogni 4–6 camere (le pareti attenuano), montato nel corridoio.
- **Open space / sala convegni**: 1 AP ogni 200–300 m^2 (meno ostacoli, più client per AP).
- **Outdoor** (giardino, piscina, spiaggia): AP da esterno con grado IP65, montaggio su palo o parete.
- **Stima totale**: per un hotel da 52 camere + sale + spazi comuni → 12–15 AP.

5.3 SSID multipli e autenticazione

Un singolo AP fisico può trasmettere **più SSID** contemporanei, ciascuno associato a una VLAN diversa. Questo è il meccanismo che realizza l'"accesso differenziato" richiesto dalla traccia.

SSID	Utenti	Autenticazione	VLAN
`Staff`	Dipendenti	WPA3-Enterprise con 802.1X	Staff
`Guest`	Ospiti/clienti	Captive portal + codice check-in	Guest
`Congress`	Convegnisti	Captive portal + codice evento	Congress

WPA3-Enterprise con 802.1X: ogni dipendente ha credenziali personali (utente+password o certificato) verificate da un server RADIUS. Se un dipendente lascia l'azienda, si disabilita il suo account e immediatamente perde l'accesso WiFi senza dover cambiare la password di rete per tutti.

Captive portal: l'utente si associa alla rete aperta (o con una PSK semplice), ma il primo tentativo di navigazione viene rediretto a una pagina web di login dove inserisce un codice ricevuto al check-in. Il vantaggio è la **tracciabilità**: il sistema registra associazione utente ↔ dispositivo ↔ timestamp, come richiesto dalla normativa.

AP isolation: sugli SSID Guest e Congress si abilita il *client isolation*, che impedisce la comunicazione diretta tra i dispositivi collegati allo stesso AP. Un ospite non può "vedere" il portatile dell'ospite nella camera accanto.

5.4 Roaming

Quando un utente si sposta (es. dalla camera alla hall), il suo dispositivo deve cambiare AP senza perdere la connessione. Gli standard **802.11r** (fast transition), **802.11k** (report sui vicini) e **802.11v** (gestione della transizione) consentono un roaming *seamless*. Il controller AP coordina il processo.

Capitolo 6 Servizi di rete

6.1 DHCP

Il **DHCP** (Dynamic Host Configuration Protocol) assegna automaticamente IP, subnet mask, gateway e DNS ai dispositivi che si collegano alla rete. In una rete segmentata con VLAN, il server DHCP ha **scope separati** per ogni VLAN (un pool di indirizzi diverso per Staff, Guest, VoIP, ecc.).

Se il server DHCP non è nella stessa VLAN del client (tipicamente è nella VLAN Server), gli switch di accesso e il core L3 devono avere la funzione di **DHCP relay agent** (chiamata anche `ip helper-address` in Cisco) che inoltra le richieste DHCP broadcast verso il server.

La VLAN Management è l'eccezione: **non usa DHCP**. Tutti gli IP degli apparati di rete sono statici.

6.2 DNS

Il **DNS** (Domain Name System) traduce i nomi di dominio (es. `www.example.com`) in indirizzi IP. Il server DNS interno dell'azienda fa due cose: **(1)** risolve i nomi interni (es. `gestionale.hotel.local` → `10.0.2.225`), **(2)** inoltra (*forward*) le query per nomi esterni verso DNS pubblici (Cloudflare `1.1.1.1`, Quad9 `9.9.9.9`).

Il DNS è un bersaglio di attacco. Le minacce principali sono: **DNS spoofing/cache poisoning** (iniezione di risposte false), **DNS amplification** (uso come amplificatore per DDoS), **DNS tunneling** (esfiltrazione dati via query DNS). Le difese: **DNSSEC** (firma crittografica delle risposte), **DoT/DoH** (cifratura delle query), disabilitazione della ricorsione aperta.

6.3 RADIUS e 802.1X

RADIUS (Remote Authentication Dial-In User Service) è un protocollo AAA (Authentication, Authorization, Accounting) usato dagli apparati di rete per autenticare gli utenti prima di dar loro accesso alla rete.

Il flusso 802.1X è:

1. Il **supplicant** (laptop/smartphone) si associa all'AP e chiede accesso.
2. L'**authenticator** (AP o switch) blocca tutto il traffico tranne il protocollo EAP e inoltra la richiesta al server RADIUS.
3. Il **server RADIUS** (FreeRADIUS, o NPS in Windows) verifica le credenziali contro una directory utenti (Active Directory, LDAP).
4. Se l'autenticazione ha successo, RADIUS risponde all'AP con "accesso consentito + VLAN da assegnare".

RADIUS non è Active Directory

Active Directory è la directory di identità (database di utenti, password, gruppi, policy). Parla LDAP e Kerberos. **RADIUS** è il protocollo che gli AP e gli switch 802.1X sanno parlare — e che AD non parla. RADIUS è il **traduttore** tra il linguaggio dei network device e il backend di identità. Non contiene password: le chiede ad AD.
L'architettura corretta è: AP $\xrightarrow{\text{RADIUS}}$ FreeRADIUS/NPS $\xrightarrow{\text{LDAP}}$ Active Directory.

6.4 Captive portal e tracciabilità

Il **captive portal** è il meccanismo di autenticazione per le reti WiFi Guest: quando l'ospite si connette e apre il browser, viene rediretto a una pagina di login dove inserisce un codice ricevuto al check-in. Il sistema registra: identità utente ↔ MAC address ↔ IP assegnato ↔ timestamp di login/logout.

Questa tracciabilità soddisfa le buone pratiche derivanti dal **D.L. 144/2005 (decreto Pisanu)** e s.m.i.: sebbene l'obbligo formale di identificazione sia stato alleggerito, resta buona pratica conservare i log per almeno 6 mesi.

Implementazioni tipiche: pfSense integrato, UniFi HotSpot, CoovaChilli, o il captive portal nativo del controller AP.

6.5 VoIP e QoS

Se la traccia richiede la **telefonia VoIP**, la rete deve ospitare un **PBX software** (FreePBX/Asterisk o 3CX) che gestisce gli interni SIP, l'instradamento delle chiamate, l'interfaccia con il trunk SIP del provider telefonico.

Il traffico VoIP è sensibile a **ritardo** (< 150 ms one-way) e **jitter** (< 30 ms). Per garantire la qualità del servizio si configura la **QoS** (Quality of Service) a più livelli:

- **Marcatura DSCP**: il traffico RTP (voce) viene marcato con **DSCP EF (46)**, il traffico SIP (segnalazione) con **CS3 (24)**.
- **Code di priorità**: sugli switch, i frame con CoS 5 (VoIP) vengono serviti prima degli altri.
- **Traffic shaping**: sul firewall, si riserva banda per il VoIP sull'uplink WAN.
- **VLAN dedicata**: il traffico VoIP sta in una VLAN separata per isolare il jitter da quello dati.

6.6 NAS, backup e regola 3-2-1

Il **NAS** (Network Attached Storage) è un dispositivo di storage in rete (Synology, QNAP) con dischi in **RAID** (tipicamente RAID 5: un disco può guastarsi senza perdita di dati). Serve per il backup centralizzato di server, configurazioni apparati, dati amministrativi.

Regola 3-2-1

3 copie dei dati (originale + 2 backup), su **2** media diversi (NAS + cloud, oppure NAS + disco esterno), di cui **1** offsite (cloud storage cifrato, oppure disco trasportato in un'altra sede). Il backup offsite protegge da incendi, furti e ransomware che cifra tutto ciò che è raggiungibile in LAN.

6.7 Monitoraggio e logging

Syslog centralizzato: tutti gli apparati (switch, AP, firewall, server) inviano i loro log a un server centrale. Serve per la correlazione degli eventi ("un AP è andato giù 2 minuti prima che il firewall

registrasse un tentativo di intrusione") e per requisiti legali (conservazione log ≥ 6 mesi).

NTP (Network Time Protocol): tempo unificato su tutti gli apparati. Senza NTP i timestamp dei log non sono comparabili.

Monitoraggio: strumenti come Zabbix, Prometheus+Grafana, o Nagios monitorano lo stato della rete (CPU switch, banda uplink, temperatura server) e inviano alert via email/SMS in caso di anomalia.

Capitolo 7 Collegamento tra siti remoti

7.1 Ponte radio P2P

Quando due siti sono **a vista** (Line of Sight, LOS) e distano poche centinaia di metri o qualche km, il ponte radio punto-punto è la soluzione più economica e rapida. Due antenne direzionali puntate l'una verso l'altra creano un link Ethernet wireless trasparente.

7.1.1 Caratteristiche operative

Frequenza: 5 GHz (banda ISM, non licenziata in Italia per uso outdoor P2P con EIRP $\leq$ 1 W e obbligo di DFS). Canali a 40 o 80 MHz per throughput reali di 300–450 Mbps.

LOS e zona di Fresnel: non basta la visibilità ottica tra le due antenne. Serve anche che la **prima zona di Fresnel** sia sostanzialmente libera da ostacoli: un ellissoide il cui raggio a metà percorso è circa $r = 17{,}3\sqrt{d/(4f)}$ (con d in km e f in GHz). Per 500 m a 5 GHz: $r \approx 2{,}5$ m. Le antenne vanno montate in alto (tetti, pali) per liberare questa zona.

Link budget: il calcolo che verifica se il link funziona è un bilancio di potenze in dB. La perdita in spazio libero (FSPL) è:

$$L_{fs} = 20\log_{10}(d) + 20\log_{10}(f) + 32{,}44 \quad \text{[dB]}$$

con d in km e f in MHz. Il segnale ricevuto è $P_{RX} = P_{TX} + G_{TX} - L_{fs} + G_{RX}$. Deve essere superiore alla sensibilità del ricevitore (~ -70 dBm) con un margine di almeno 10–15 dB per pioggia e attenuazioni aggiuntive.

7.1.2 Configurazione di rete

Il ponte radio opera come **bridge Layer 2 trasparente**: è equivalente a un cavo Ethernet virtuale. Lo si collega a porte **trunk** sugli switch di entrambi i lati. Le VLAN dell'edificio principale vengono estese al sito remoto via 802.1Q sul link radio. Non serve un secondo firewall, non serve un secondo DHCP, non serve una VPN: è trasparenza totale.

La cifratura del link radio si abilita a livello dell'apparato (WPA3 o AES-256 proprietario), impedendo l'intercettazione del traffico.

7.1.3 Normativa italiana

In Italia la banda 5 GHz (sottobande 5470–5725 MHz) è utilizzabile senza licenza per collegamenti P2P outdoor con EIRP $\leq$ 1 W (30 dBm) e obbligo di **DFS** (Dynamic Frequency Selection) per evitare interferenze con radar. Gli apparati commerciali (Ubiquiti, MikroTik) sono già conformi se configurati nella regione "Italy/EU".

7.2 VPN: IPsec e WireGuard

Una **VPN** (Virtual Private Network) crea un tunnel cifrato su Internet tra due siti o tra un utente remoto e la rete aziendale. Due tipologie:

Site-to-site: connessione permanente tra due firewall (es. sede principale e filiale). Tutto il traffico tra le due reti passa nel tunnel. Utile come alternativa al ponte radio quando la LOS non è disponibile: entrambi i siti hanno una FTTH propria e il firewall di ciascun sito stabilisce un tunnel verso l'altro. Le VLAN vengono incapsulate nel tunnel.

Client-to-site (*remote access*): un dipendente in smart working si collega alla rete aziendale con un client VPN. Riceve un IP della VLAN Staff e lavora come se fosse in ufficio.

Protocolli principali: **IPsec** (standard, compatibilità universale), **OpenVPN** (open source, TLS-based, facile da configurare), **WireGuard** (moderno, molto performante, configurazione minimale).

Capitolo 8 Sicurezza della rete

8.1 La triade CIA

Ogni sistema di sicurezza si costruisce su tre proprietà:

Confidenzialità (i dati sono accessibili solo a chi è autorizzato): cifratura a riposo (LUKS, BitLocker), cifratura in transito (TLS 1.3, WPA3, SRTP), controllo degli accessi.

Integrità (i dati non vengono alterati senza autorizzazione): hash crittografici (SHA-256), firma digitale, versionamento snapshot su NAS (Btrfs/ZFS), DNSSEC.

Disponibilità (i servizi sono accessibili quando serve): UPS, RAID, backup 3-2-1, ridondanza di rete, monitoraggio, piano di disaster recovery.

8.2 Autenticazione: password, MFA, passkey

Le **password** restano il meccanismo più diffuso ma hanno criticità strutturali: scelta di password deboli, riuso su più servizi (credential stuffing), attacchi brute-force e dictionary. Sul server le password vanno memorizzate come hash con *salt* usando funzioni lente: `bcrypt`, `scrypt`, `Argon2` (mai MD5 o SHA-1).

Contromisure: **MFA** (Multi-Factor Authentication) con OTP, token hardware o app authenticator. L'evoluzione sono le **passkey** (FIDO2/WebAuthn): coppie di chiavi asimmetriche memorizzate nel dispositivo che eliminano le password alla radice.

8.3 Ransomware

Un **ransomware** cifra i file e chiede un riscatto in criptovaluta per la chiave. Nella variante *double extortion* i dati vengono anche esfiltrati con minaccia di pubblicazione. Il ciclo di vita tipico è: intrusione (phishing, exploit, RDP brute-force) → escalation dei privilegi → lateral movement → esfiltrazione → cifratura di massa → riscatto.

Difese: patch management rigoroso, principio del privilegio minimo, segmentazione VLAN (blocca il lateral movement), EDR per il rilevamento comportamentale, backup 3-2-1 con almeno una copia *offline* o *immutable*. Il pagamento del riscatto è istituzionalmente sconsigliato. In caso di incidente: isolamento, analisi forense, ripristino, notifica al Garante entro 72 ore (GDPR art. 33).

8.4 Phishing

Il **phishing** è un attacco di ingegneria sociale: l'attaccante si finge un'entità fidata per ottenere credenziali o far eseguire malware. Tipologie: phishing di massa, *spear phishing* (mirato), *whaling* (verso dirigenti), *smishing* (SMS), *vishing* (telefonata). Tecniche: spoofing del mittente, typosquatting di domini, URL shortener, form di login falsi.

Difese tecniche: **SPF/DKIM/DMARC** sul dominio aziendale, email filtering con sandbox, MFA, filtri DNS. Difesa culturale: formazione continua degli utenti, simulazioni periodiche.

8.5 HTTPS e TLS

HTTPS è HTTP cifrato con **TLS** (Transport Layer Security). Il browser e il server stabiliscono una sessione cifrata attraverso un *handshake* che coinvolge: scambio di chiavi asimmetriche (Diffie-Hellman), verifica del certificato del server (firmato da una **CA** — Certificate Authority), generazione di chiavi simmetriche di sessione (AES-256).

Per l'utente HTTPS garantisce: **(1)** cifratura (nessuno può leggere il traffico), **(2)** autenticazione (il sito è chi dice di essere), **(3)** integrità (i dati non vengono alterati in transito).

Per i server in DMZ: certificato TLS gratuito da **Let's Encrypt**, rinnovato automaticamente. Non ci sono scuse per restare in HTTP nel 2024.

8.6 MITM (Man in the Middle)

In un attacco **MITM** l'attaccante si interpone tra due parti comunicanti, intercettando e potenzialmente alterando il traffico. Esempi: *ARP spoofing* (l'attaccante risponde alle richieste ARP con il proprio MAC, dirottando il traffico), rogue AP (AP falso con lo stesso SSID).

Difese: HTTPS (il certificato rivela la manomissione), 802.1X (impedisce la connessione di dispositivi non autenticati), *Dynamic ARP Inspection* sugli switch, VPN per connessioni sensibili su reti non fidate.

Capitolo 9 Cloud e migrazione dei servizi

9.1 IaaS, PaaS, SaaS

IaaS (Infrastructure as a Service): il provider fornisce macchine virtuali, storage, rete. Tu gestisci il sistema operativo in su. Esempio: AWS EC2, Azure VM.

PaaS (Platform as a Service): il provider gestisce anche il sistema operativo e il runtime. Tu fornisci solo l'applicazione. Esempio: Heroku, AWS Elastic Beanstalk.

SaaS (Software as a Service): il provider gestisce tutto, tu usi l'applicazione. Esempio: Gmail, Microsoft 365, Google Workspace.

9.2 Quando migrare e quando no

La regola per l'esame è: **analisi servizio per servizio**, non "tutto in cloud" né "tutto on-premise".

Servizio	Scelta	Motivazione
Gestionale/PBX	On-premise	Mission-critical: deve funzionare anche senza Internet
Web server (sito)	Cloud	Scalabilità, CDN, protezione DDoS, uptime da SLA
Email	Cloud (SaaS)	Gestire un mail server è proibitivo per una PMI
Storage	Ibrido	NAS locale per le prestazioni + cloud come copia offsite
Backup	Ibrido	NAS locale + copia cifrata su cloud storage EU

La strategia complessiva è un'**architettura cloud ibrida**: cloud dove aggiunge valore (web, email, backup offsite), on-premise dove la continuità operativa è prioritaria (gestionale, PBX).

9.3 Privacy e GDPR nel cloud

Se i dati degli ospiti/clienti vanno in cloud, il GDPR impone: **(1)** localizzazione dei dati nell'UE (art. 44–49), **(2)** un **DPA** (Data Processing Agreement) con il provider (art. 28) che definisce ruoli (titolare = azienda, responsabile = provider), **(3)** cifratura a riposo e in transito. Rischio: **vendor lock-in** (dipendenza da un provider), mitigabile con backup locali e formati aperti.

Capitolo 10 Conformità normativa

10.1 GDPR (Reg. UE 2016/679)

Il GDPR si applica a qualsiasi trattamento di dati personali. Per una struttura alberghiera i dati rilevanti sono: identità degli ospiti, dati di pagamento, dati di navigazione WiFi, immagini di videosorveglianza. Obblighi principali:

- **Registro dei trattamenti**: documento che elenca tutti i trattamenti, le finalità, le basi giuridiche, i tempi di conservazione.
- **Privacy policy**: informativa pubblica (sul sito, alla reception) che spiega quali dati vengono raccolti e perché.
- **Minimizzazione**: raccogliere solo i dati strettamente necessari, conservarli solo per il tempo necessario.
- **Cifratura**: misura tecnica obbligatoria per i dati sensibili (a riposo e in transito).
- **Notifica breach**: in caso di violazione dei dati, notifica al Garante entro 72 ore (art. 33).
- **DPO**: Data Protection Officer, obbligatorio per trattamenti su larga scala.

10.2 Decreto Pisanu e tracciabilità WiFi

Il D.L. 144/2005 imponeva l'identificazione degli utenti dei servizi WiFi pubblici. L'obbligo formale è stato alleggerito, ma resta **buona pratica** (e spesso richiesta dalla traccia d'esame) tracciare l'associazione utente $\leftrightarrow$ dispositivo $\leftrightarrow$ timestamp tramite il captive portal, conservando i log per almeno 6 mesi.

10.3 NIS2 (Dir. UE 2022/2555)

La direttiva NIS2 riguarda la sicurezza delle reti e dei sistemi informativi dei "soggetti essenziali e importanti". Una struttura alberghiera singola probabilmente non è soggetta, ma una **catena alberghiera** come gruppo potrebbe rientrare tra i soggetti importanti. Misure richieste: gestione del rischio, incident response, continuità operativa, sicurezza della supply chain.

10.4 ISO/IEC 11801 e CEI 64-8

Lo standard **ISO/IEC 11801** (e il corrispondente TIA-568) regola il cablaggio strutturato: categorie dei cavi, lunghezze massime, connettori, test di conformità. La norma **CEI 64-8** regola gli impianti elettrici nei locali tecnici (MDF, IDF): messa a terra, protezioni, ventilazione.