SISTEMI DI ELABORAZIONE DELLE INFORMAZIONI

A.A. 2025-26

Ing. Paolo Querci

ING-INF-05

Lezione 4

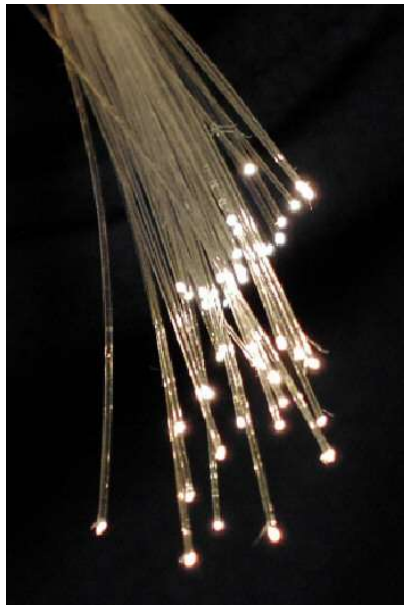
Introduzione alle reti di telecomunicazioni

In questa lezione analizziamo il ruolo delle **reti** e dei sistemi di comunicazione nei contesti informatici e sanitari moderni.

Vedremo come le informazioni (dati, voce, immagini, video) vengono trasportate in modo affidabile tra dispositivi diversi.

Collegheremo i concetti tecnici al funzionamento della sanità digitale: cartelle cliniche, referti, **telemedicina** e sistemi PACS/RIS.

Che cos’è una rete di telecomunicazioni



Una **rete di telecomunicazioni** è un sistema strutturato che permette la trasmissione di informazione tra punti geograficamente distinti.

L’informazione può essere rappresentata come voce, dati, immagini diagnostiche, segnali biometrici o video in streaming.

La comunicazione può avvenire tramite mezzi fisici (doppino, fibra ottica, cavo coassiale) oppure tramite mezzi wireless (onde radio, **Wi-Fi,** ponti microonde, satelliti).

Una **rete** moderna implementa livelli di **protocollo** che consentono instradamento, gestione degli errori, qualità del servizio e sicurezza.

Nella sanità, le **reti** sostengono l’intero ecosistema digitale: cartelle cliniche, referti, **telemedicina,** sistemi **PACS** e monitoraggio continuo dei pazienti.

Reti fisiche e reti logiche

La **rete fisica** rappresenta l'infrastruttura tangibile: cavi, fibre ottiche, apparati, armadi tecnici, data center.

La **rete logica** descrive come i dispositivi sono organizzati e comunicano dal punto di vista astratto: indirizzi **IP,** subnet, **VLAN,** tabelle di routing, regole di **firewall.**

È possibile avere più **reti logiche** che condividono la stessa infrastruttura fisica, ottenendo isolamento tra traffici differenti.

Negli ospedali è tipico separare il traffico amministrativo, clinico, diagnostico e quello degli ospiti tramite **VLAN** e regole di **firewall.**

Commutazione di circuito e commutazione di pacchetto

Le reti di telecomunicazioni possono funzionare secondo due modalità fondamentali: **Commutazione di circuito** e **Commutazione di pacchetto**.

Nella **commutazione di circuito**, tipica della telefonia tradizionale, prima della comunicazione **viene stabilito un canale fisso** e dedicato tra mittente e destinatario. Questo canale **resta riservato per tutta la durata della comunicazione**, anche quando non si trasmettono dati. Il percorso è costante, il ritardo è minimo e prevedibile, ma la rete risulta poco efficiente perché le risorse rimangono occupate anche nei momenti di inattività.

Commutazione di circuito

La **commutazione di circuito** è un sistema molto stabile, adatto alla trasmissione continua di voce o segnali in tempo reale, come una telefonata interna tra due reparti ospedalieri

Anche il **fax**, ancora usato in molte strutture sanitarie, si basa su questo tipo di collegamento: viene stabilita una linea fissa per il tempo necessario all'invio del documento, che poi si chiude.

Commutazione di circuito

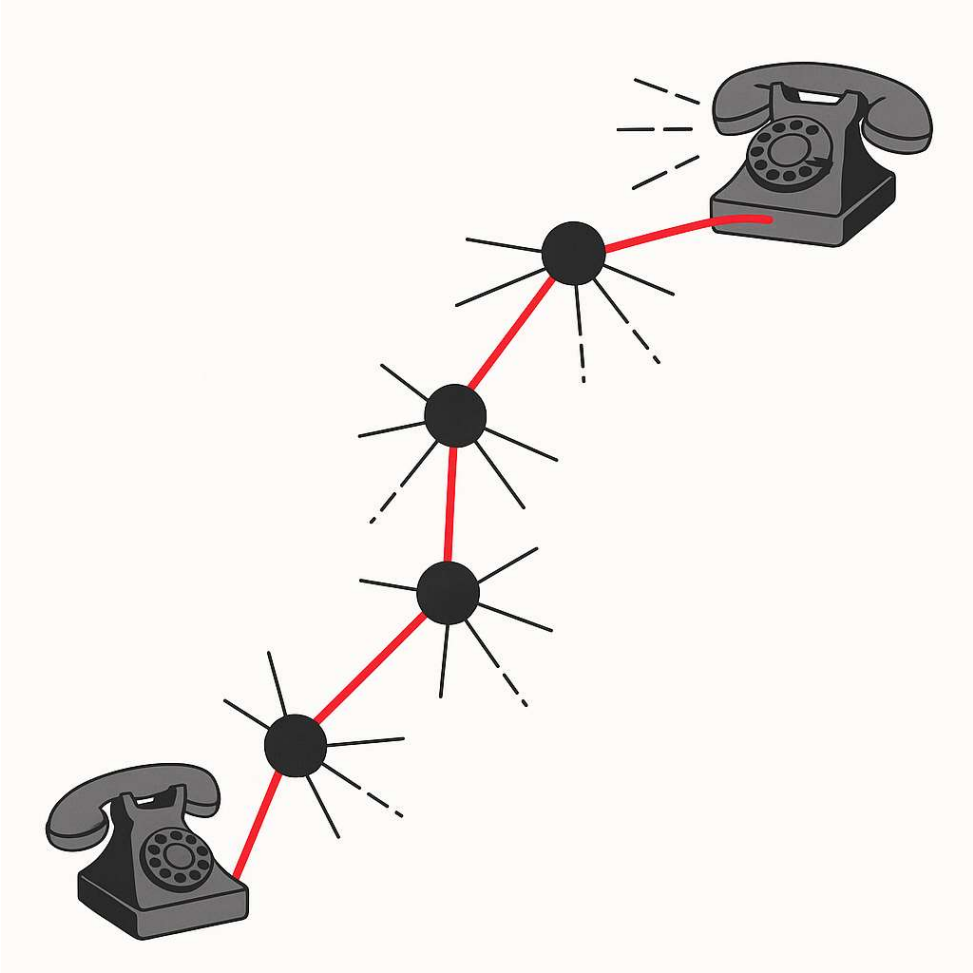


Immagine generata con AI – © 2025, P. Querci

Commutazione di circuito

Nella **commutazione** di **circuito** viene creato un percorso fisso e dedicato tra mittente e destinatario, prima di iniziare la comunicazione.

Le risorse di **rete** coinvolte rimangono riservate per tutta la durata del collegamento, anche se in certi momenti non vengono trasmessi dati.

Questo garantisce ritardo costante, jitter minimo e comportamento prevedibile, ma riduce l'efficienza complessiva dell'infrastruttura.

La **commutazione** di **circuito** è tipica della telefonia tradizionale e dei fax. In ambito sanitario alcuni collegamenti legacy utilizzano ancora questo modello.

Commutazione di circuito e commutazione di pacchetto

Nella **commutazione di pacchetto**, invece, **l'informazione viene suddivisa in piccoli blocchi, detti pacchetti**, ciascuno dei quali contiene l'indirizzo di destinazione e può seguire un percorso indipendente all'interno della rete.

I pacchetti vengono poi ricomposti all'arrivo per ricostruire il messaggio originale. In questo modo la rete può essere condivisa da molti utenti contemporaneamente, sfruttando le risorse solo quando servono.

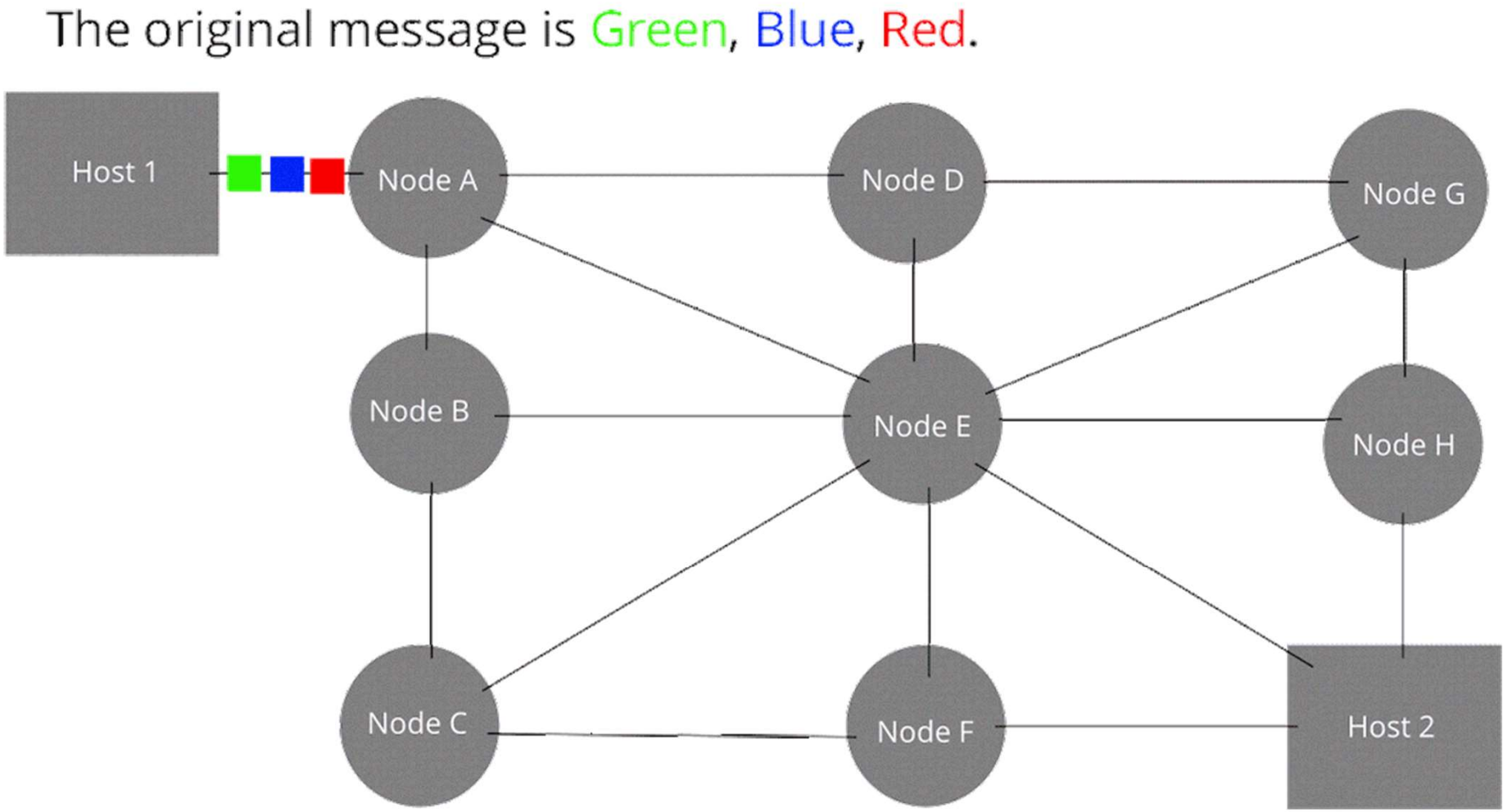
Il ritardo può variare leggermente, ma l'efficienza complessiva è molto più elevata.

Commutazione di circuito e commutazione di pacchetto

La **commutazione di pacchetto** è il modello utilizzato da Internet e dalle reti informatiche moderne.

Nel contesto sanitario, la commutazione di circuito resta utile (sempre meno) per la fonia e i fax, mentre la commutazione di pacchetto è la base dei sistemi informativi contemporanei: trasmissione di immagini radiologiche (RIS/PACS), invio di referti, posta elettronica interna, telefonia VoIP e telemedicina.

Commutazione di pacchetto



Commutazione di pacchetto

Nella **commutazione** di **pacchetto** l'informazione viene suddivisa in **pacchetti** di dimensione limitata, ciascuno contenente indirizzo sorgente, indirizzo di destinazione e controlli di integrità.

I **pacchetti** possono seguire percorsi diversi attraverso i nodi di **rete,** grazie all'instradamento dinamico effettuato dai **router.**

All'arrivo, i **pacchetti** vengono ricomposti nell'ordine corretto per ricostruire il messaggio originale.

Questo modello massimizza l'utilizzo delle risorse, consente tolleranza ai guasti e scala facilmente con l'aumento del traffico.

L'intera **Internet** e i sistemi informativi sanitari moderni (referti web, **PACS, RIS, telemedicina)** si basano su **commutazione** di **pacchetto.**

Cos’è una Rete di Computer

Una **rete di computer**, in informatica e telecomunicazioni, è una tipologia di rete di telecomunicazioni a **commutazione di pacchetto** caratterizzata da un insieme di dispositivi hardware con software di commutazione, ossia nodi di commutazione collegati l'uno con l'altro da appositi canali di comunicazione (link), tali da fornire un servizio di comunicazione che permette lo **scambio e la condivisione di dati** e la comunicazione tra più utenti o dispositivi distribuiti o terminali (host)

Rete di computer

Una **rete** di computer è un insieme di dispositivi elettronici (PC, notebook, workstation, **server,** smartphone, tablet, apparecchiature mediche) collegati tramite una **rete** di comunicazione.

I dispositivi, chiamati spesso **host** o **nodi**, condividono risorse e servizi: archivi, stampanti, basi dati, applicazioni cliniche.

La comunicazione è regolata da **protocolli** standard, come il **TCP/IP,** che definiscono formati dei **pacchetti,** procedure di trasmissione e meccanismi di controllo degli errori.

In un ospedale, la **rete** di computer collega PC amministrativi, terminali di reparto, workstation di refertazione, **server** e dispositivi di imaging.

Il modello ISO OSI

Quando due dispositivi comunicano (PC, smartphone, sensori di uno studio dentistico, sistemi cartella clinica), lo fanno passando attraverso vari **passaggi logici**.

Il modello OSI è una **mappa che descrive questi passaggi in 7 livelli**, dal più “fisico” al più “astratto”.

Serve per capire **chi fa cosa** durante la comunicazione in rete, senza confondere i ruoli.

Il modello ISO OSI

Immagina di spedire un documento importante:

- **Qualcuno prepara il contenuto**
- **Qualcuno lo mette in una busta**
- **Qualcuno scrive l'indirizzo**
- **Qualcuno lo consegna ai corrieri**
- **I corrieri seguono strade e regole per recapitarlo**
- **Qualcuno dall'altra parte riceve, apre e ricostruisce il contenuto tutto come era all'inizio**

La comunicazione in rete funziona allo stesso modo: **ogni *livello OSI* svolge una parte del lavoro.**

I 7 livelli del modello ISO OSI

1. **Fisico** – i cavi, il Wi-Fi, i segnali elettrici.
2. **Collegamento dati** – come evitare errori nella trasmissione locale (rete dello studio).
3. **Rete** – trovare la strada giusta verso la destinazione (indirizzi IP).
4. **Trasporto** – consegnare correttamente i dati (es. TCP).
5. **Sessione** – gestire le “sessioni” tra due macchine.
6. **Presentazione** – tradurre i dati in un formato comprensibile (es. codifiche).
7. **Applicazione** – ciò che vede l’utente: browser, e-mail, software della cartella clinica.

Il modello ISO/OSI: perché esiste

Il modello ISO/OSI è una struttura teorica che descrive come avviene la comunicazione tra dispositivi di **rete.**

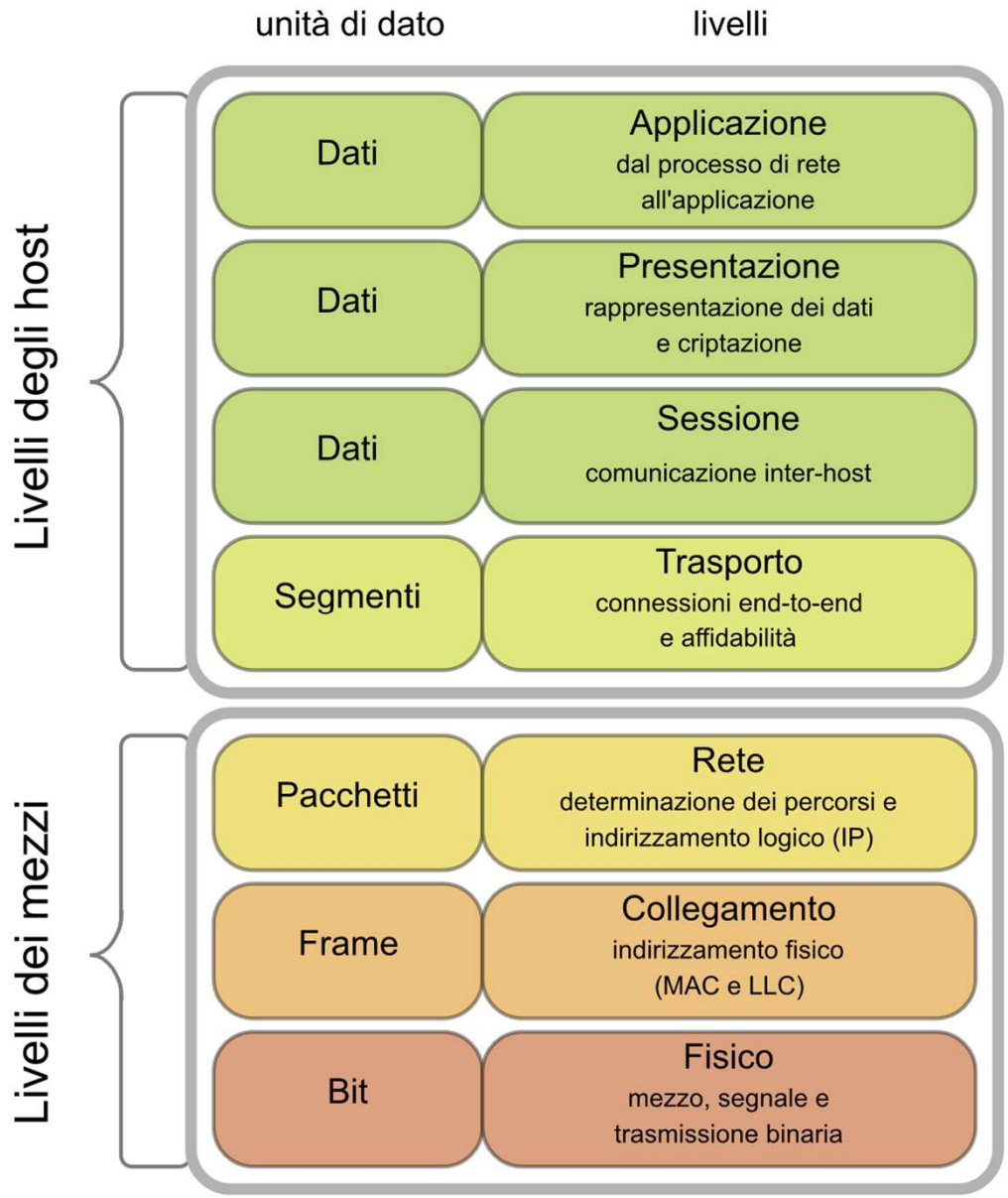
Non è un **protocollo,** ma un riferimento concettuale per comprendere, diagnosticare e progettare sistemi di comunicazione.

Divide la trasmissione dei dati in 7 livelli, ognuno con responsabilità specifiche e indipendenti.

Permette interoperabilità tra sistemi di produttori diversi e facilita l'analisi dei problemi di **rete.**

È utile per capire dove si verifica un'interruzione: **livello** fisico, indirizzamento, trasporto o applicazione.

I 7 livelli del modello ISO OSI



I sette livelli ISO/OSI

Livello 1 – Fisico: trasporta bit nel mezzo fisico (cavi, fibre, radio). Problemi comuni: assenza di segnale, cavo difettoso.

Livello 2 – Collegamento: gestisce frame e indirizzi **MAC.** Operano **switch, VLAN** e controllo errori locale.

Livello 3 – **Rete:** gestisce indirizzi **IP** e instradamento tramite **router.** Problemi di raggiungibilità tra subnet.

Livello 4 – Trasporto: gestisce porte applicative e affidabilità (TCP/UDP). Problemi tipici: porte bloccate, timeout.

Livello 5 – **Sessione:** mantiene attive le sessioni tra applicazioni, come nelle comunicazioni remote.

Livello 6 – **Presentazione:** converte formati, codifica, compressione e cifratura (TLS/SSL).

Livello 7 – Applicazione: **protocolli** come **HTTP, DNS,** SMTP, servizi **PACS, RIS** e portali clinici.

Cosa sono i pacchetti di rete

Le reti moderne usano la trasmissione a **pacchetti**: l'informazione viene suddivisa in unità più piccole dette pacchetti.

Ogni pacchetto contiene **dati di controllo** (indirizzi sorgente/destinazione, codici di errore, ordine dei frammenti) e un **payload** con i dati dell'utente.

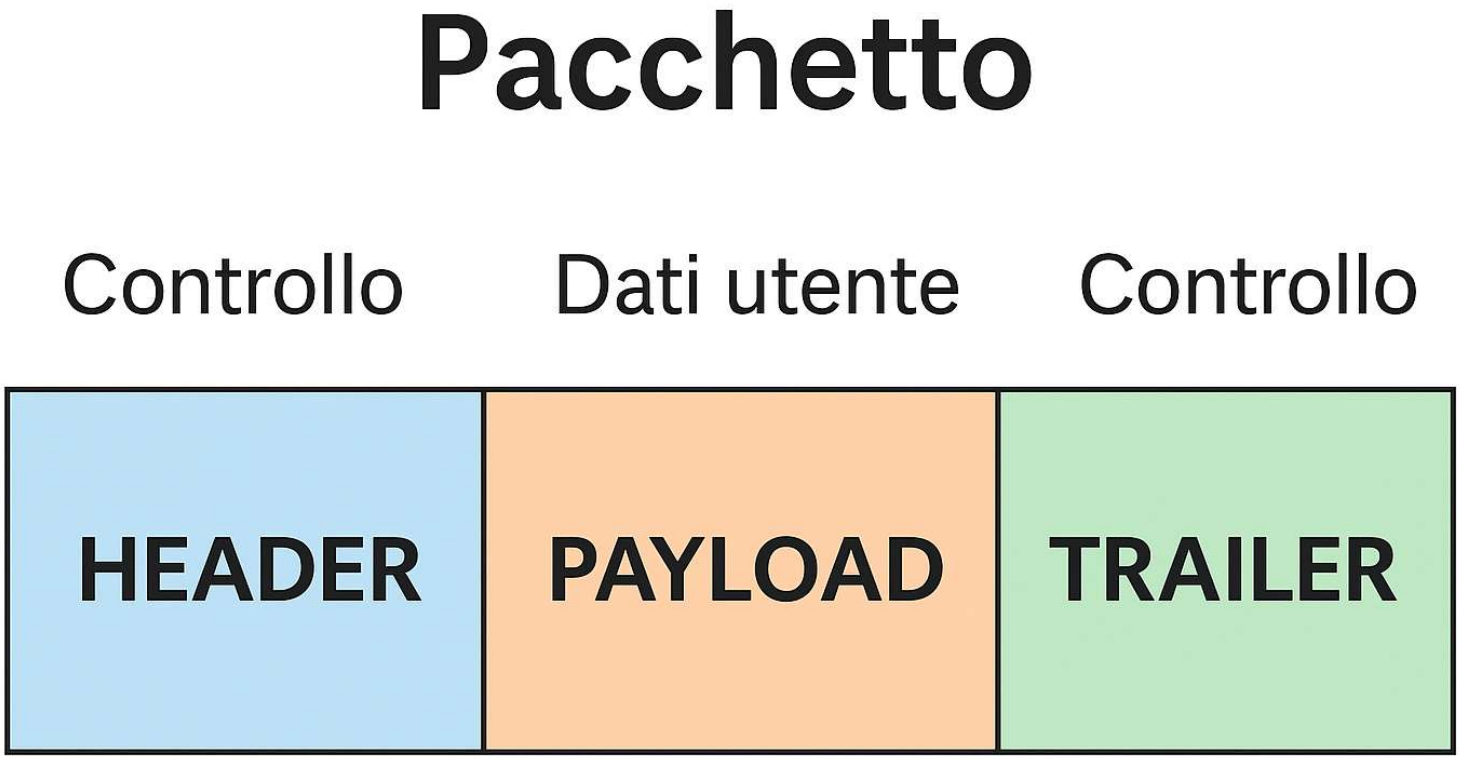
Il controllo è inserito in **header** e **trailer** (parte finale del pacchetto che contiene informazioni di controllo, in particolare il codice di verifica (CRC/FCS) usato per rilevare errori e garantire l'integrità dei dati durante la trasmissione), mentre il **payload** è al centro del pacchetto.

I pacchetti permettono di condividere efficientemente la banda: quando un utente non invia dati, altri possono utilizzare il collegamento.

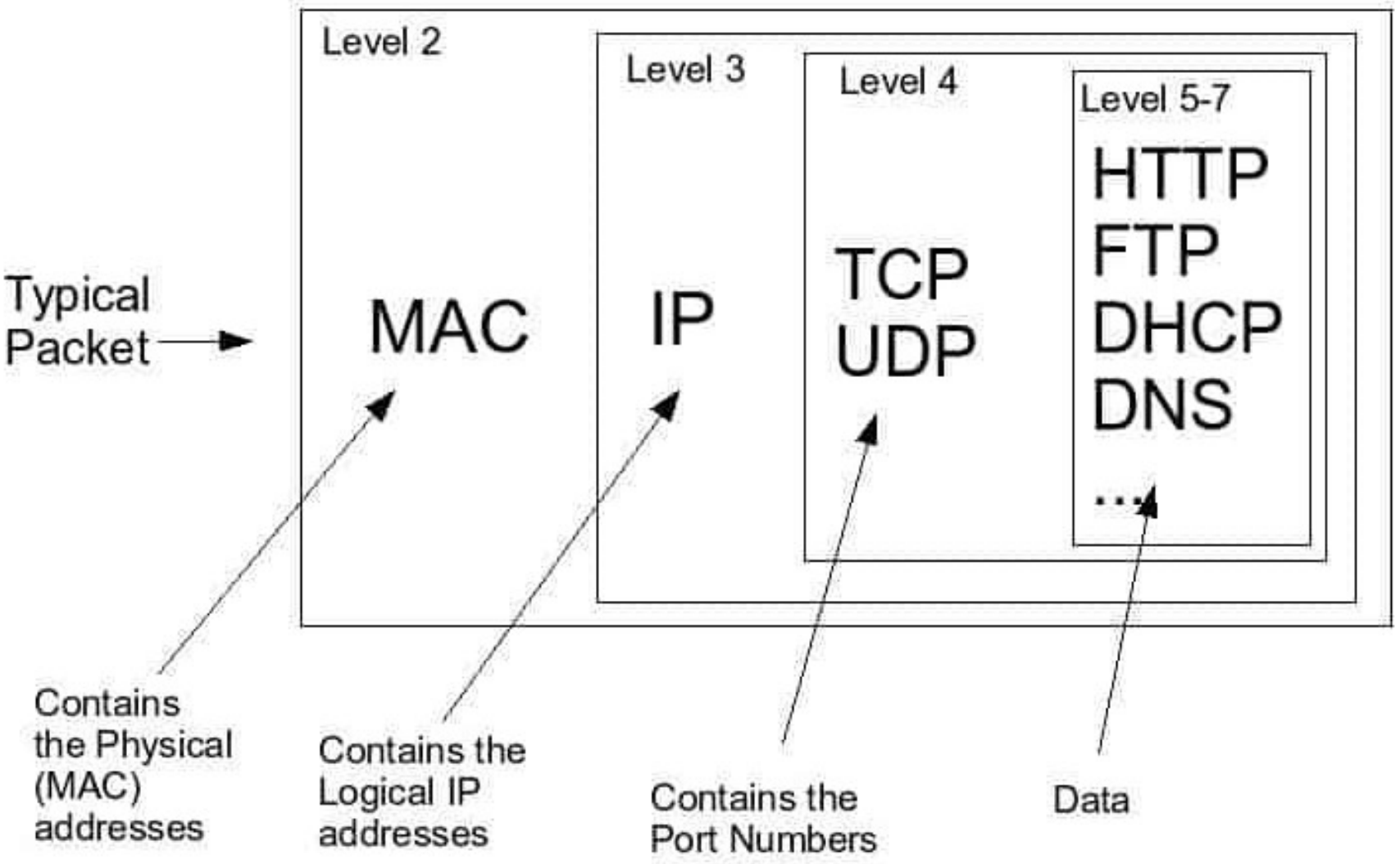
Se un percorso non è disponibile, i pacchetti attendono in coda finché il link si libera.

Le tecnologie di rete impongono un limite alla dimensione (MTU, Maximum Transmission Unit): messaggi più lunghi vengono frammentati e ricomposti all'arrivo.

Come è fatto un "pacchetto"



Come è fatto un "pacchetto"



IP, MAC e Porte: comportamento nella rete

- I MAC (Media Access Control) rimangono fissi solo all'interno della LAN locale: oltre un router vengono sostituiti.
- L'indirizzo IP rimane lo stesso nella LAN, ma può essere cambiato dal NAT quando si esce verso Internet.
- Il PC usa una porta sorgente temporanea (casuale) per ogni connessione.
- Il server usa sempre la porta del servizio (es. 80 per HTTP, 443 per HTTPS).
- Il server distingue le connessioni guardando IP sorgente e porta sorgente del client.

I 7 livelli del modello ISO OSI

Il modello OSI **permette di capire**, a grandi linee:

- come viaggiano le informazioni tra PC, radiografie digitali, sensori e server dello studio;
- come distinguere un problema **di rete** da un problema **del software**;
- come avere un linguaggio minimo per comunicare con tecnici e assistenza IT.

ISO/OSI: come usarlo per diagnosticare problemi

Se non c'è segnale o Wi-Fi assente → **Livello** 1 (Fisico).

Se due dispositivi locali non si vedono → **Livello** 2 (Collegamento).

Se un server remoto non risponde → **Livello** 3 **(IP** e routing).

Se un'app è raggiungibile ma "non carica" → **Livello** 4 (Trasporto).

Se la connessione cade dopo pochi secondi → **Livello** 5 **(Sessione).**

Se il sito segnala errori di certificato → **Livello** 6 **(Presentazione).**

Se il portale PACS/RIS non risponde → **Livello** 7 (Applicazione).

Il modello aiuta a ragionare "a strati" e a trovare rapidamente il punto di guasto.

Esempio 1 – La radiografia digitale non si apre

Scenario: L'igienista tenta di visualizzare una RX sul gestionale dello studio, ma l'immagine non arriva.

Come aiuta l'OSI:

- Se la rete Wi-Fi "non prende" → **Livello fisico**
- Se il PC vede il server ma dà errori di trasmissione → **Collegamento dati / Trasporto**
- Se il gestionale è aperto ma dà errore interno → **Applicazione**

Utilità: Capire subito *dove* potrebbe essere il problema, invece di andare a tentoni.

Esempio 2 – L'ortopantomografo invia immagini lentissime

Scenario: Il macchinario invia i file DICOM al server, ma l'upload è lento.

Come aiuta l'OSI:

- Cavo vecchio o switch saturi → **Livello fisico**
- Conflitti IP o errori di routing → **Livello rete**
- Software del macchinario che comprime male → **Presentazione / Applicazione**

Utilità: Distinguere subito se serve un tecnico *di rete* o un tecnico *dell'apparecchiatura*.

Esempio 3 – WhatsApp Web funziona, ma il gestionale cloud no

Scenario: Connessione internet OK, ma il gestionale in cloud dello studio non si apre.

Come aiuta l'OSI:

- DNS che non risolve l'indirizzo del gestionale → **Livello rete**
- Problema di sessione sul server remoto → **Livello sessione**
- Aggiornamento del gestionale → **Livello applicazione**

Utilità: Capire che non sempre "internet funziona = tutto funziona".

Esempio 4 – Zoom o Teams si interrompe durante una call

Scenario: Il paziente a distanza non sente o la chiamata cade.

Come aiuta l'OSI:

- Wi-Fi disturbato → **Fisico**
- Congestione di rete → **Rete/Trasporto**
- Microfono non riconosciuto → **Applicazione**

Utilità: Saper dare una prima diagnosi rapida senza drammi.

LAN – Local Area Network

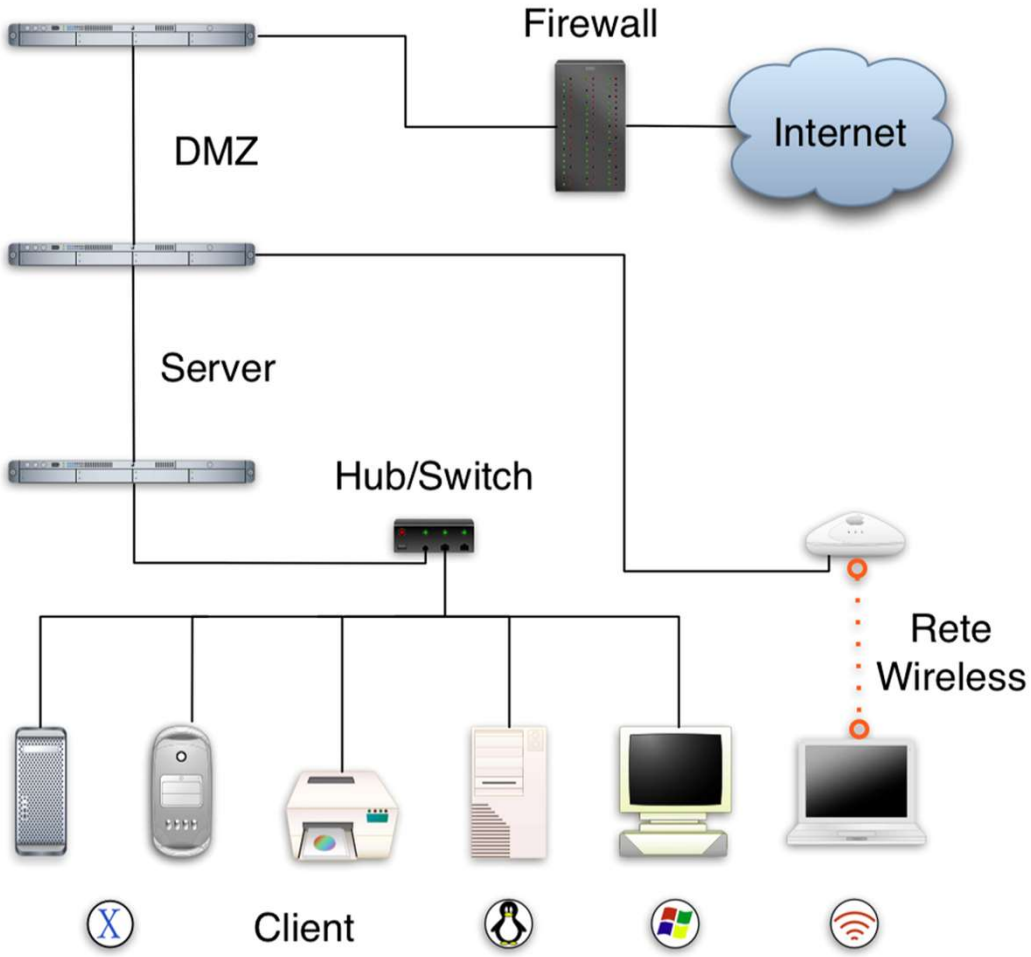
Una **LAN** è una **rete** locale che copre un'area geografica limitata, come un edificio, un campus ospedaliero o un laboratorio.

Le **LAN** utilizzano collegamenti ad alta velocità (ad esempio 1 Gbit/s o 10 Gbit/s) e forniscono latenza molto bassa e grande affidabilità.

All'interno di una **LAN** possono esistere migliaia di nodi, organizzati in **VLAN** per separare traffico clinico, amministrativo, guest, IoT medico.

Le **LAN** ospedaliere sono alla base della connettività di tutti i sistemi digitali: cartelle cliniche, gestione farmaci, **PACS, RIS** e sistemi di laboratorio.

LAN – Local Area Network



Cosa è una VLAN (Virtual LAN)

Una **VLAN** è una **rete logica** che separa gruppi di dispositivi sulla stessa infrastruttura fisica.

Permette di creare più **reti** indipendenti usando gli **switch,** senza cambiare cablaggio o apparati.

Le **VLAN** operano al **livello** 2 del modello ISO/OSI e utilizzano **tag 802.1Q** per identificare il traffico.

Ogni **VLAN** è un dominio di **broadcast** separato: i pacchetti restano confinati nel proprio segmento.

Questo aumenta **sicurezza, isolamento,** ordine e riduce traffico inutile sulla **rete.**

Negli ospedali si usano **VLAN** per separare: diagnostica (PACS/RIS), dispositivi medici, amministrazione, **Wi-Fi** ospiti.

WAN – Wide Area Network

Una **WAN** collega tra loro **LAN** situate in sedi geograficamente distanti: diversi ospedali, ambulatori territoriali, data center regionali.

Le **WAN** utilizzano collegamenti forniti da operatori di telecomunicazioni: fibre dedicate, collegamenti MPLS, ponti radio, collegamenti ridondati.

Nel contesto sanitario, la **WAN** permette di accedere a servizi centralizzati (anagrafe regionale, **FSE,** sistemi di prescrizione elettronica) da strutture periferiche.

Una **WAN** ben progettata assicura ridondanza, instradamento alternativo in caso di guasto e qualità del servizio per applicazioni critiche.

Internet e reti private

Internet è una **rete** globale pubblica che interconnette milioni di **reti** private e pubbliche tramite **router** e **protocolli** standard.

Una **LAN** ospedaliera è invece una **rete** privata, sotto il controllo dell'organizzazione, protetta da **firewall** e politiche di sicurezza.

Per consentire ai dispositivi interni di accedere a **Internet** si utilizzano **router,** sistemi di traduzione degli indirizzi **(NAT)** e **firewall.**

L'accesso verso l'esterno va regolato con attenzione per proteggere i dati sanitari e prevenire intrusioni.

Dispositivi di rete: switch

Lo **switch** è un dispositivo che collega più nodi all'interno di una **LAN.**

Lavora tipicamente a livello 2 del modello OSI, inoltrando i frame Ethernet in base agli indirizzi **MAC** dei dispositivi collegati.

Gli **switch** moderni supportano funzionalità avanzate: **VLAN,** qualità del servizio, Power over Ethernet per alimentare telefoni VoIP e access point **Wi-Fi.**

In un ospedale gli **switch** costituiscono la dorsale interna: ogni reparto, sala operatoria o laboratorio è connesso a uno o più **switch** di accesso, che a loro volta si collegano agli **switch** di distribuzione e di core.

Dispositivi di rete: router

Il **router** collega **reti** distinte e decide il percorso che i **pacchetti** devono seguire per raggiungere la destinazione. Lavora tipicamente a livello 3 del modello OSI

Utilizza tabelle di routing e, nelle **reti** complesse, **protocolli** dinamici (come OSPF o BGP) per aggiornare automaticamente le rotte disponibili.

In un contesto ospedaliero, i **router** permettono di collegare la **LAN** interna alla **WAN** regionale e a **Internet,** proteggendo al tempo stesso i segmenti più sensibili.

Spesso i **router** integrano funzionalità di **firewall, NAT** e **VPN,** diventando elementi chiave per la sicurezza e l'interconnessione.

Bridge e segmentazione della rete

Il bridge collega due segmenti di **rete** a livello 2, filtrando il traffico in base agli indirizzi **MAC** e riducendo il dominio di collisione.

Storicamente i bridge erano usati per segmentare le **LAN** e migliorare l'efficienza; oggi le stesse funzioni sono integrate negli **switch.**

Il concetto di segmentazione rimane fondamentale: suddividere una grande **rete** in più domini logici riduce traffico inutile e migliora sicurezza e isolamento dei guasti.

Nelle **reti** sanitarie questo approccio consente, ad esempio, di isolare i dispositivi medici rispetto alle postazioni di lavoro generiche.

Access Point Wi-Fi

L’Access Point **Wi-Fi** consente ai dispositivi wireless di collegarsi alla **LAN.**

Gestisce autenticazione, canali radio, potenza del segnale e roaming tra celle diverse.

In un ospedale, la **rete Wi-Fi** deve garantire copertura diffusa ma controllata, evitando interferenze con apparecchiature sensibili e garantendo la separazione del traffico (guest, staff, dispositivi medici).

L’uso di più SSID associati a differenti **VLAN** permette di implementare questa separazione in modo strutturato.

Wi-Fi: bande e standard

Il **Wi-Fi** opera su bande di frequenza licenza-free, principalmente 2.4 GHz, 5 GHz e, nelle versioni più recenti, 6 GHz.

La banda a 2.4 GHz offre maggiore copertura ma è più soggetta a interferenze e congestione.

La banda a 5 GHz offre maggiore capacità e velocità, a scapito di una copertura leggermente inferiore.

Standard come 802.11n, 802.11ac e 802.11ax **(Wi-Fi** 6) migliorano progressivamente capacità, efficienza spettrale e gestione di molti dispositivi contemporanei, scenario tipico delle strutture sanitarie.

Wi-Fi: sicurezza

I primi meccanismi di sicurezza come WEP sono oggi considerati insicuri e facilmente violabili.

Gli standard **WPA2** e **WPA3** introducono cifratura robusta e meccanismi di autenticazione più solidi.

Tuttavia, le **reti Wi-Fi** restano vulnerabili se vengono usate password deboli, se si espongono reti pubbliche non controllate o se vengono utilizzati access point non autorizzati.

In contesti sanitari è essenziale configurare correttamente le **reti Wi-Fi,** separare il traffico ospiti dal traffico clinico e monitorare continuamente eventuali anomalie.

Indirizzi IP

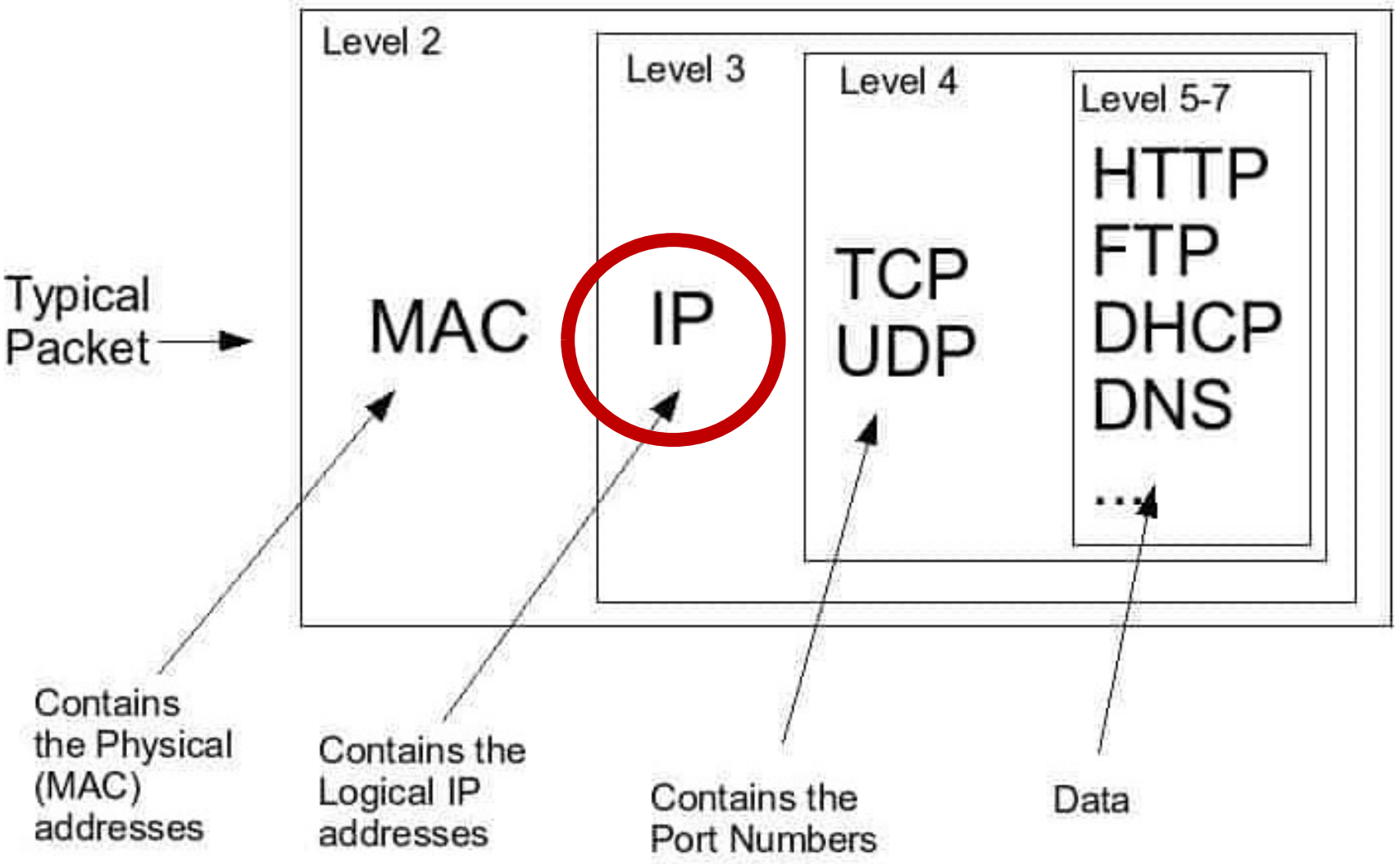
Un **datagramma IP** è un insieme di dati inviato attraverso Internet che contiene tutte le informazioni necessarie per il suo instradamento dall'origine alla destinazione.

Un **indirizzo IP** (dall'inglese **Internet Protocol address**) - in informatica e nelle telecomunicazioni - è un numero del datagramma IP che identifica univocamente un dispositivo detto host collegato a una rete informatica che utilizza l'Internet Protocol come protocollo di rete per l'instradamento/indirizzamento, inserito dunque nell'intestazione (header) del datagramma IP per l'indirizzamento tramite appunto il protocollo IP.

Esso equivale all'indirizzo stradale o al numero telefonico, infatti sono informazioni complete ed univoche a livello mondiale, similmente all'indirizzo IP.

L'indirizzo IP esiste in due versioni: **IPv4** (1981) e **IPv6** (1998).

Come è fatto un "pacchetto"



Indirizzi IP

Ogni dispositivo connesso in rete è identificato da un **indirizzo IP**.

Un **indirizzo IP statico**, è sempre lo stesso ogni volta che il computer (o altro dispositivo) si connette alla rete.

Un **indirizzo IP dinamico**, invece, deve essere assegnato ad un computer (o altro dispositivo) dinamicamente, cioè cambia sempre. Quando il computer è acceso, "cercherà" il server dinamico di IP (in Windows, questo può anche essere denominato **DHCP** o Dynamic Host Configuration Protocol). Una volta che questo indirizzo IP è assegnato, il dispositivo lo usa fino al suo spegnimento.

Indirizzi IP

Un indirizzo **IP** identifica univocamente un dispositivo in una **rete** basata sulla suite **TCP/IP.**

La versione **IPv4** utilizza indirizzi a 32 bit, consentendo circa 4.3 miliardi di indirizzi teorici.

La versione **IPv6** utilizza indirizzi a 128 bit, offrendo uno spazio enormemente più vasto, sufficiente per assegnare indirizzi univoci a miliardi di dispositivi.

Nelle **reti** ospedaliere, i dispositivi critici possono avere indirizzi **IP** statici, mentre il resto dei dispositivi usa assegnazione dinamica tramite **DHCP.**

Indirizzi IP

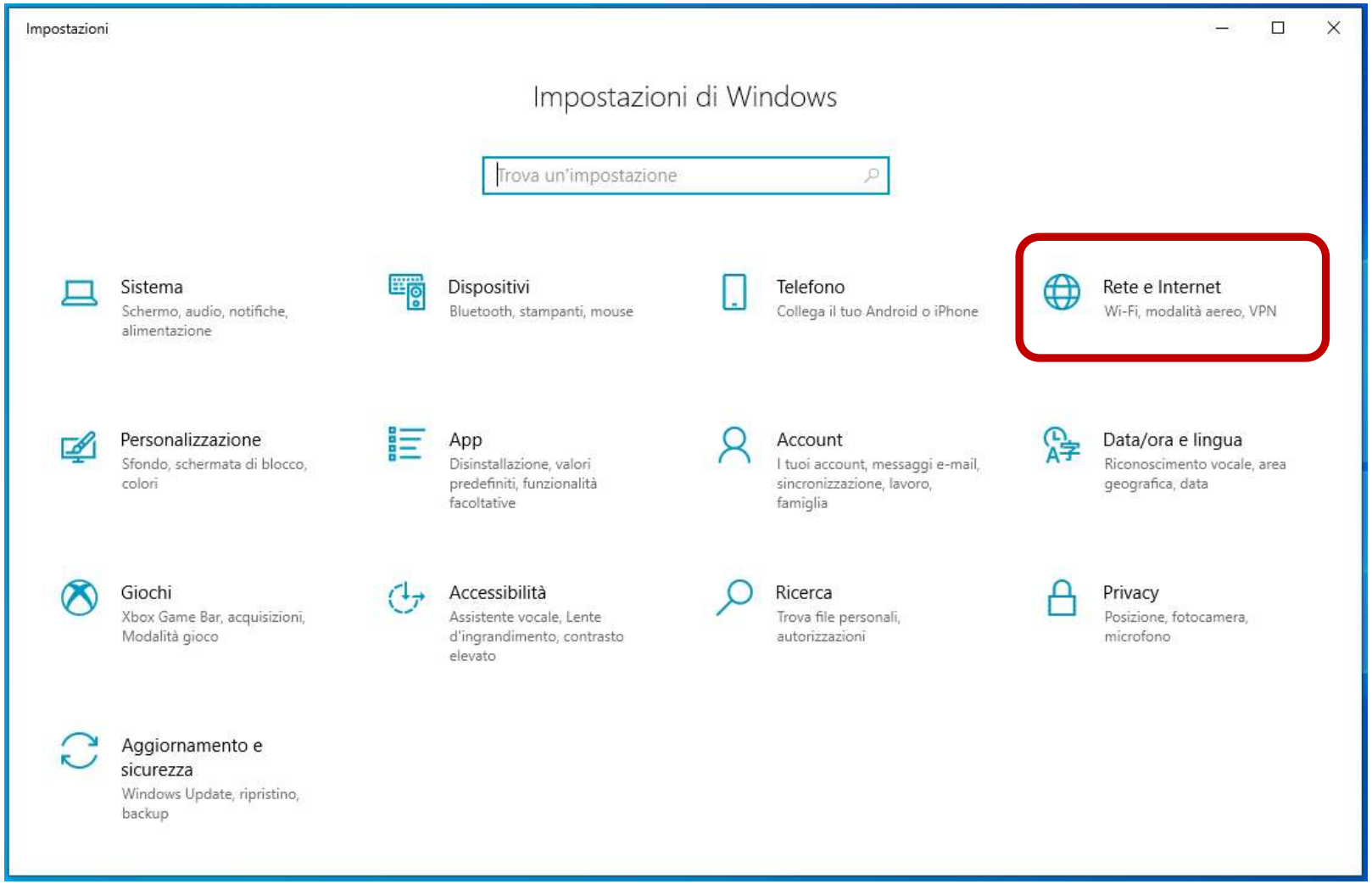
L'indirizzo IP esiste in due versioni: **IPv4** (1981) e **IPv6** (1998).

La versione IPv4 permette di avere 2^{32} (circa 4,3 miliardi) indirizzi mondiali, mentre la versione IPv6 ne assicura 2^{128}, ovvero
340.282.366.920.938.463.463.374.607.431.768.211.456 indirizzi disponibili

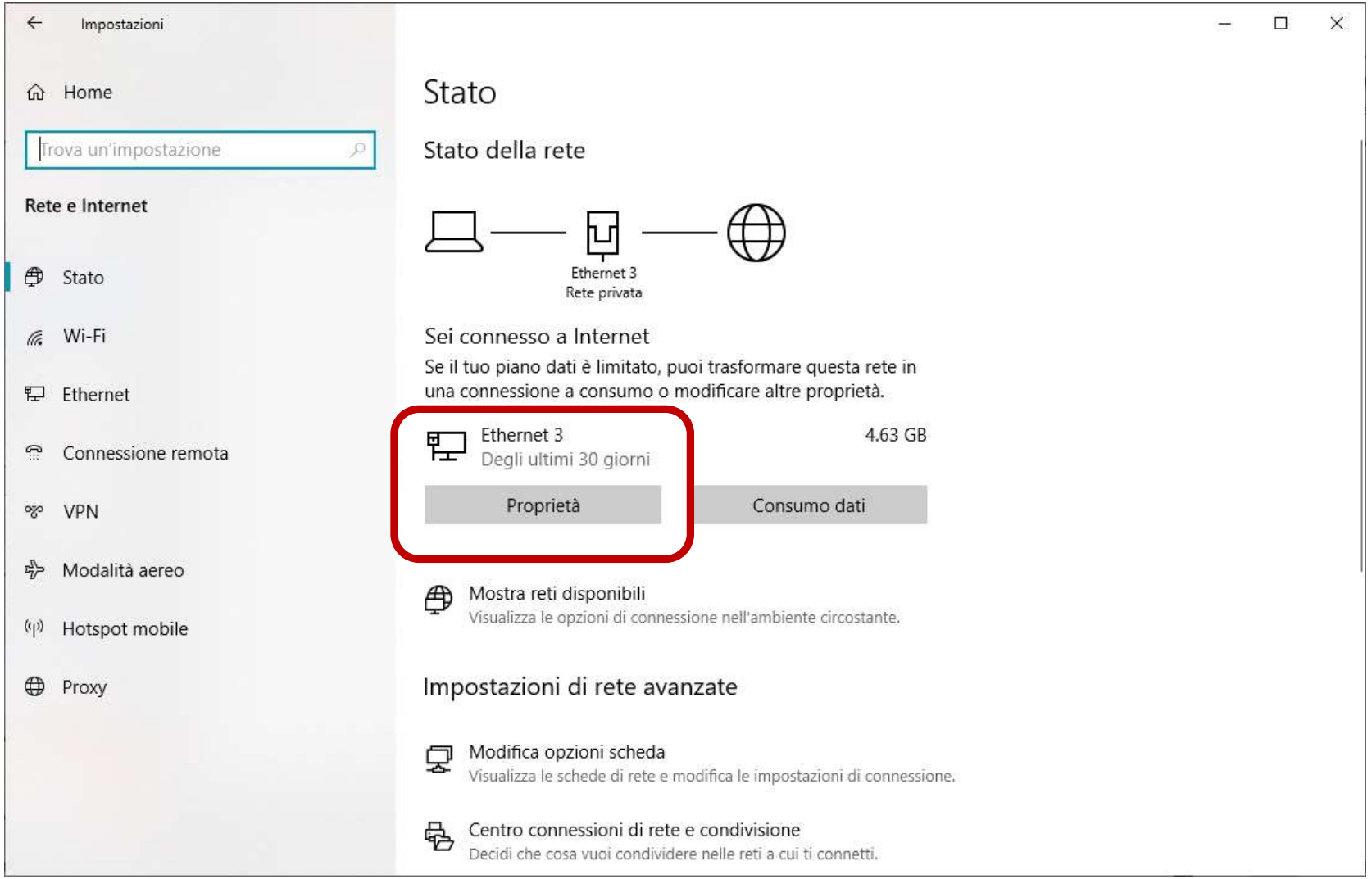
Attualmente gli indirizzi IPv4 sono terminati (tutti utilizzati), ma ciò non costituisce un problema grazie alla tecnica **NAT (Network Adress Translation)** che permette di utilizzare il medesimo IP per più computer.

Un indirizzo IPv4 ha il formato: 172.16.254.1
Un indirizzo IPv6 ha il formato: 2001:db8:0:1234:0:567:8:1

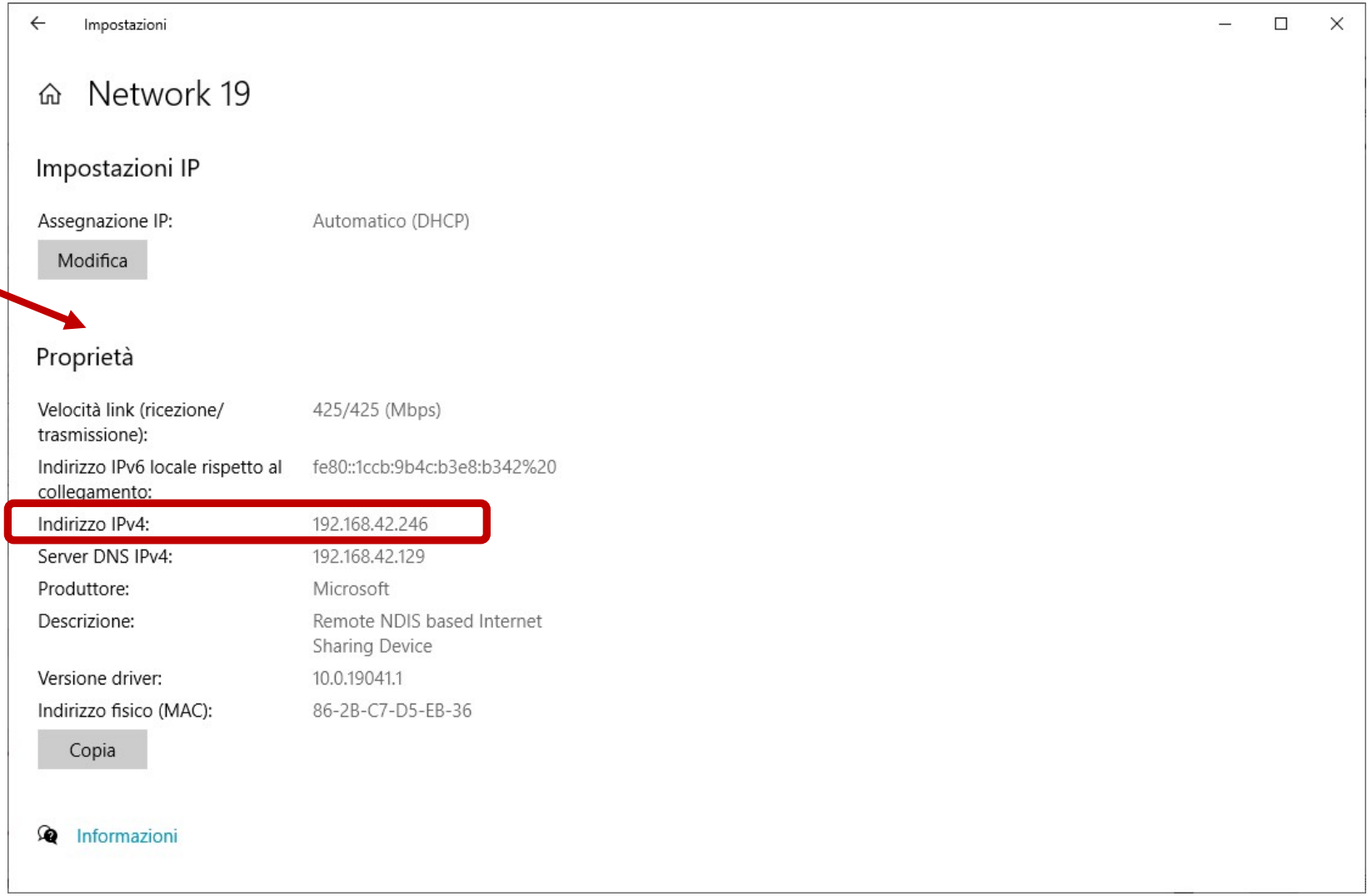
Indirizzi IP



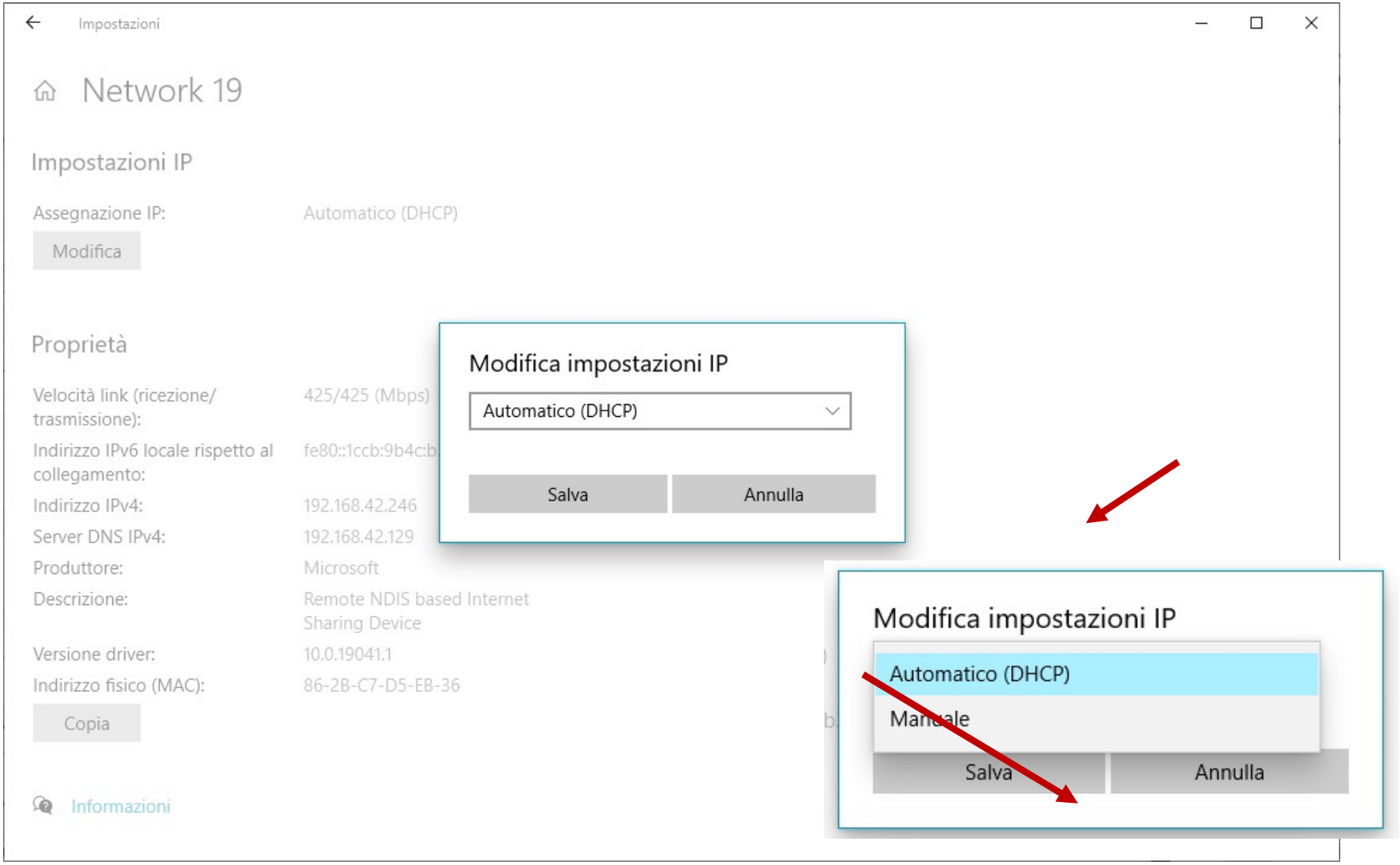
Indirizzi IP



Indirizzi IP



Indirizzi IP



Indirizzi IP privati e pubblici

Gli indirizzi **IP** pubblici sono instradabili su **Internet** e univoci a livello globale.

Gli indirizzi **IP** privati (come 10.x.x.x, 172.16.x.x, 192.168.x.x) sono utilizzati all'interno di **reti** locali e non vengono trasportati direttamente su **Internet.**

Le **LAN** ospedaliere utilizzano principalmente indirizzi privati, che vengono tradotti verso l'esterno tramite **NAT.**

Questo modello riduce il consumo di indirizzi pubblici e aggiunge un ulteriore livello di protezione.

NAT – Network Address Translation

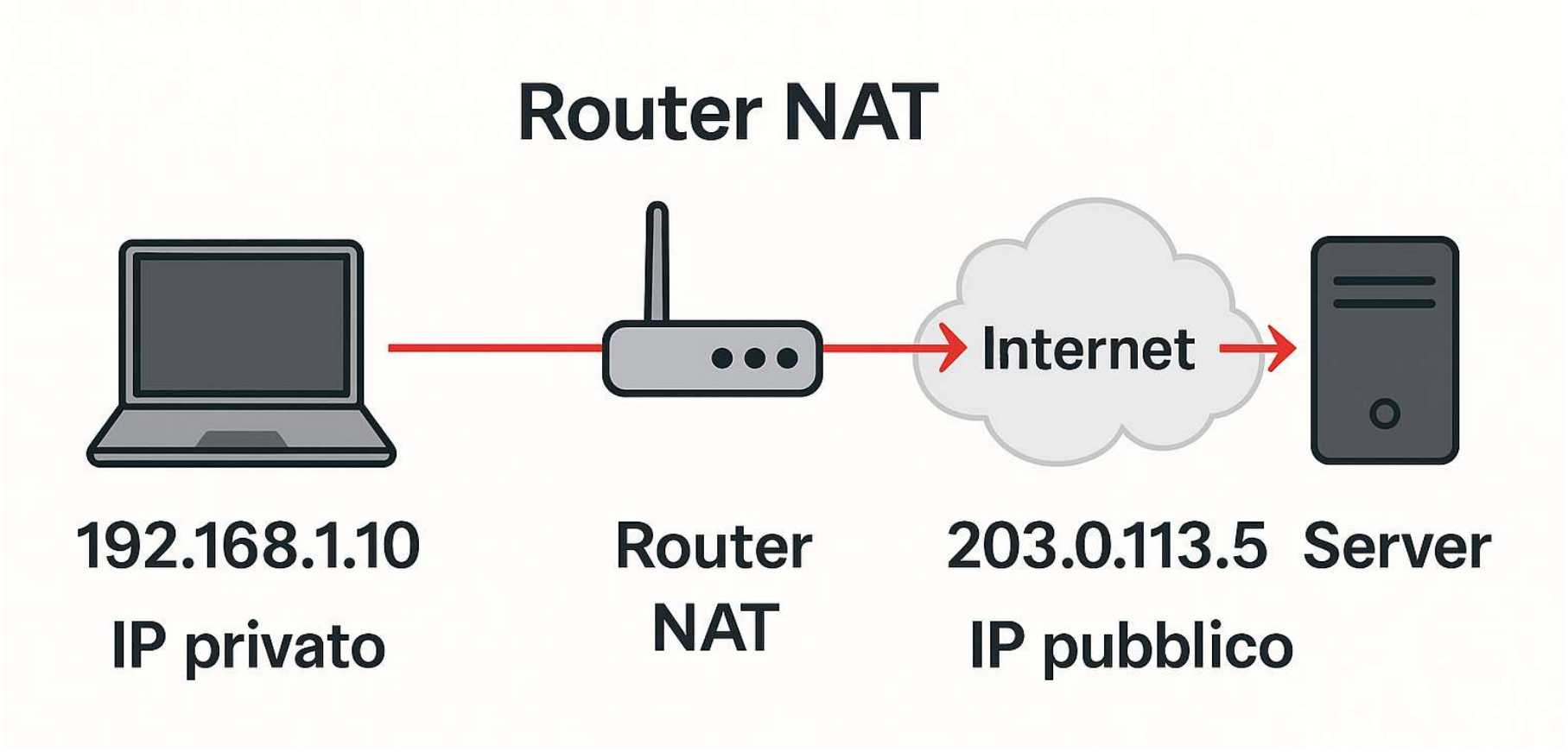
Il **NAT** è la funzione che permette a molti dispositivi con indirizzi **IP** privati di condividere uno o pochi indirizzi **IP** pubblici.

Quando un **client** interno contatta un servizio su **Internet,** il **router NAT** sostituisce l'indirizzo sorgente privato con un indirizzo pubblico e tiene traccia delle associazioni.

In questo modo, le risposte che tornano dall'esterno possono essere ricondotte al dispositivo interno corretto.

Nelle grandi organizzazioni sanitarie, il **NAT** è fondamentale per connettere migliaia di dispositivi verso **Internet** senza esporre direttamente la **rete** interna.

NAT – Network Address Translation



Indirizzi MAC

Un indirizzo **MAC** è un identificatore univoco assegnato dal produttore a ogni interfaccia di **rete** Ethernet o **Wi-Fi.**

Lavora a livello 2 del modello OSI ed è utilizzato dagli **switch** per decidere a quale porta inoltrare i frame.

La tabella **MAC** di uno **switch** associa indirizzi **MAC** alle porte fisiche, costruita dinamicamente osservando il traffico.

In un ospedale, conoscere gli indirizzi **MAC** può essere utile per tracciare dispositivi medici e controllare accessi non autorizzati.

Indirizzi MAC

In informatica e telecomunicazioni **l'indirizzo MAC** (in inglese MAC address, dove MAC sta per Media Access Control), detto anche indirizzo fisico, indirizzo ethernet o indirizzo LAN, è un codice di 48 bit (6 byte) **assegnato in modo univoco dal produttore ad ogni scheda di rete ethernet o wireless prodotta al mondo.**

Per visualizzare l'indirizzo MAC della propria scheda di rete i sistemi operativi forniscono in genere un comando specifico da digitare su shell testuale; tale comando su Windows è **ipconfig /all** (ifconfig -a su Linux) mentre il comando arp -a visualizza l'intera Arp cache dell'eventuale rete locale a cui il PC è connesso. La ARP cache è una tabella di memorizzazione temporanea usata dai dispositivi di rete per conservare le associazioni tra indirizzi IP (livello 3) e indirizzi MAC (livello 2)

Indirizzi MAC

Sebbene l'indirizzo MAC sia permanente di natura, esistono alcuni metodi che permettono di camuffarlo, operazione che in gergo tecnico viene detta **MAC spoofing**.

La modifica può essere utile per motivi di privacy, ad esempio collegandosi ad una rete Wi-Fi libera, o per motivi di interoperabilità. In ogni caso queste modifiche sono puramente software e non permanenti: al riavvio del sistema viene ripristinato l'indirizzo MAC originale memorizzato all'interno del dispositivo hardware.

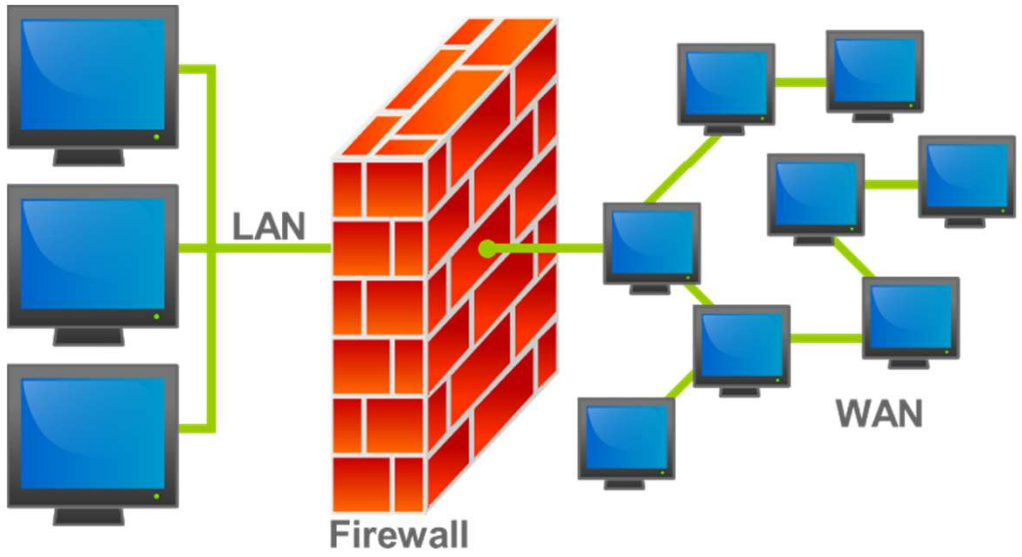
Firewall: concetti di base

Un **firewall** è un dispositivo o un software che controlla il traffico di **rete** in ingresso e in uscita in base a un insieme di regole.

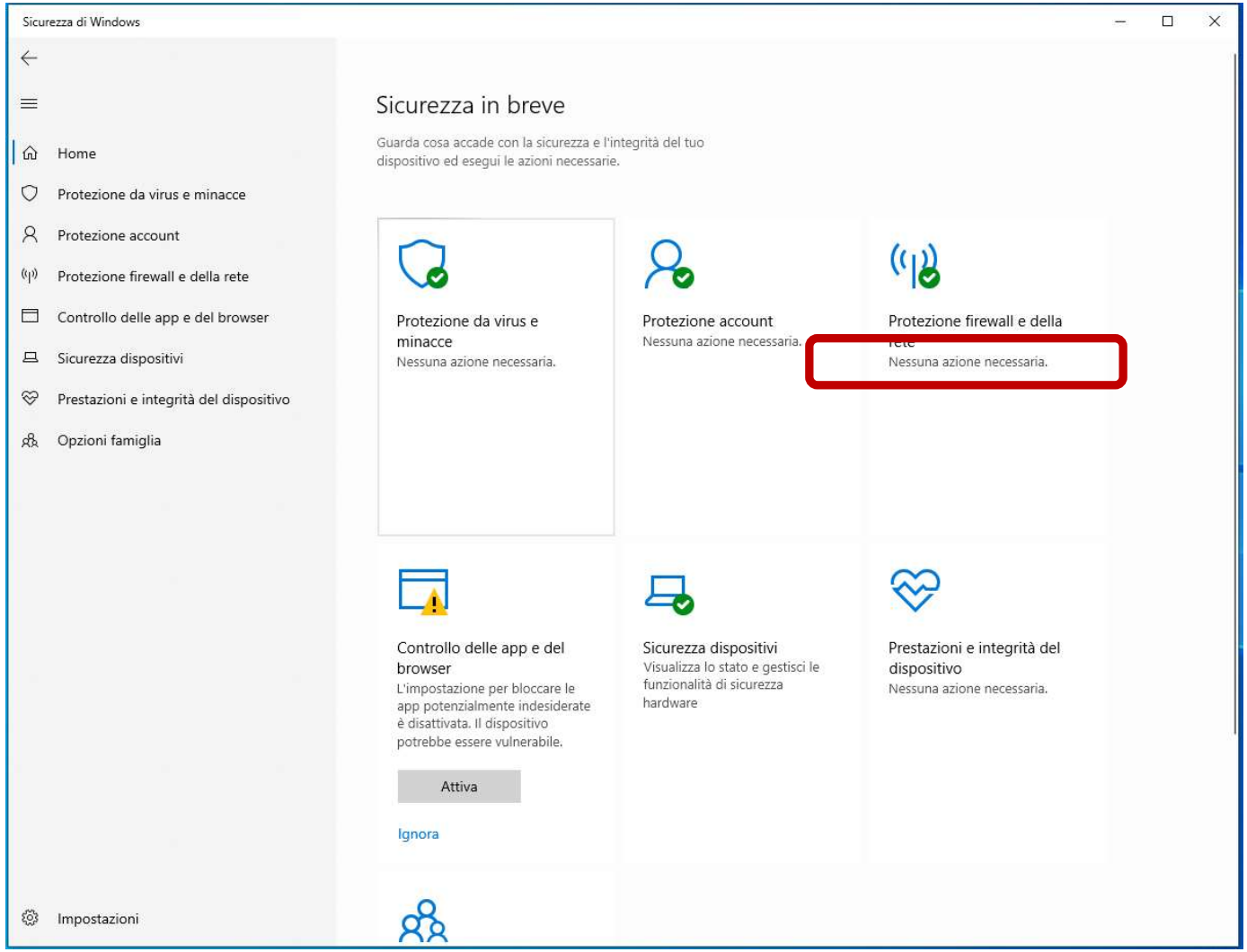
Può operare su vari livelli: filtraggio per indirizzo **IP,** porta, **protocollo,** stato della connessione, contenuto applicativo.

L'obiettivo principale è impedire accessi non autorizzati e limitare la superficie di attacco della **rete.**

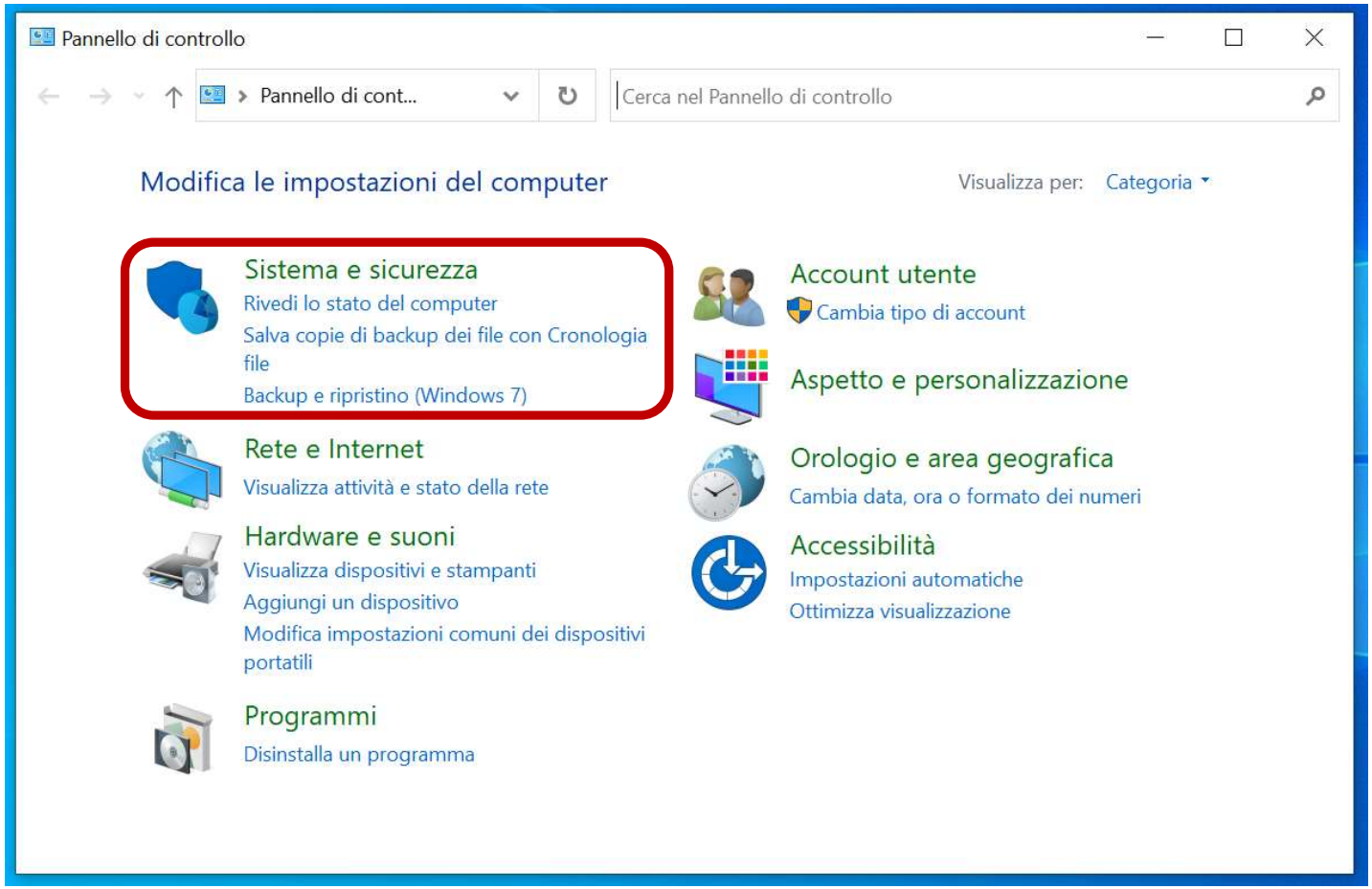
Negli ospedali, i **firewall** proteggono **server PACS,** database clinici, sistemi amministrativi e accessi remoti di **telemedicina.**



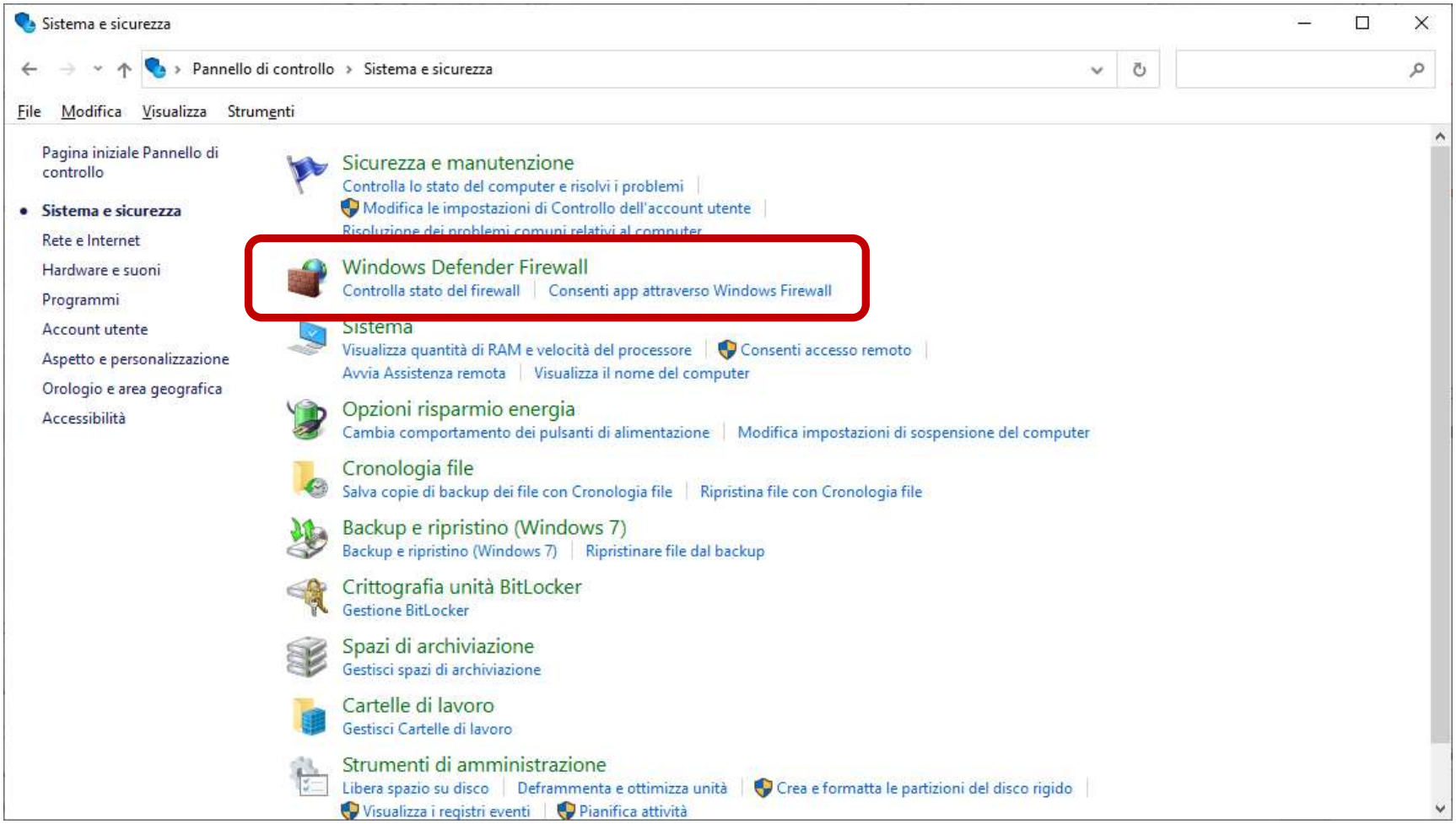
Firewall


Sicurezza di Windows
Home
Protezione da virus e minacce
Protezione account
Protezione firewall e della rete
Controllo delle app e del browser
Sicurezza dispositivi
Prestazioni e integrità del dispositivo
Opzioni famiglia
Impostazioni
Sicurezza in breve
Guarda cosa accade con la sicurezza e l'integrità del tuo dispositivo ed esegui le azioni necessarie.
Protezione da virus e minacce
Nessuna azione necessaria.
Protezione account
Nessuna azione necessaria.
Protezione firewall e della
Nessuna azione necessaria.
Controllo delle app e del browser
L'impostazione per bloccare le app potenzialmente indesiderate è disattivata. Il dispositivo potrebbe essere vulnerabile.
Attiva
Ignora
Sicurezza dispositivi
Visualizza lo stato e gestisci le funzionalità di sicurezza hardware
Prestazioni e integrità del dispositivo
Nessuna azione necessaria.

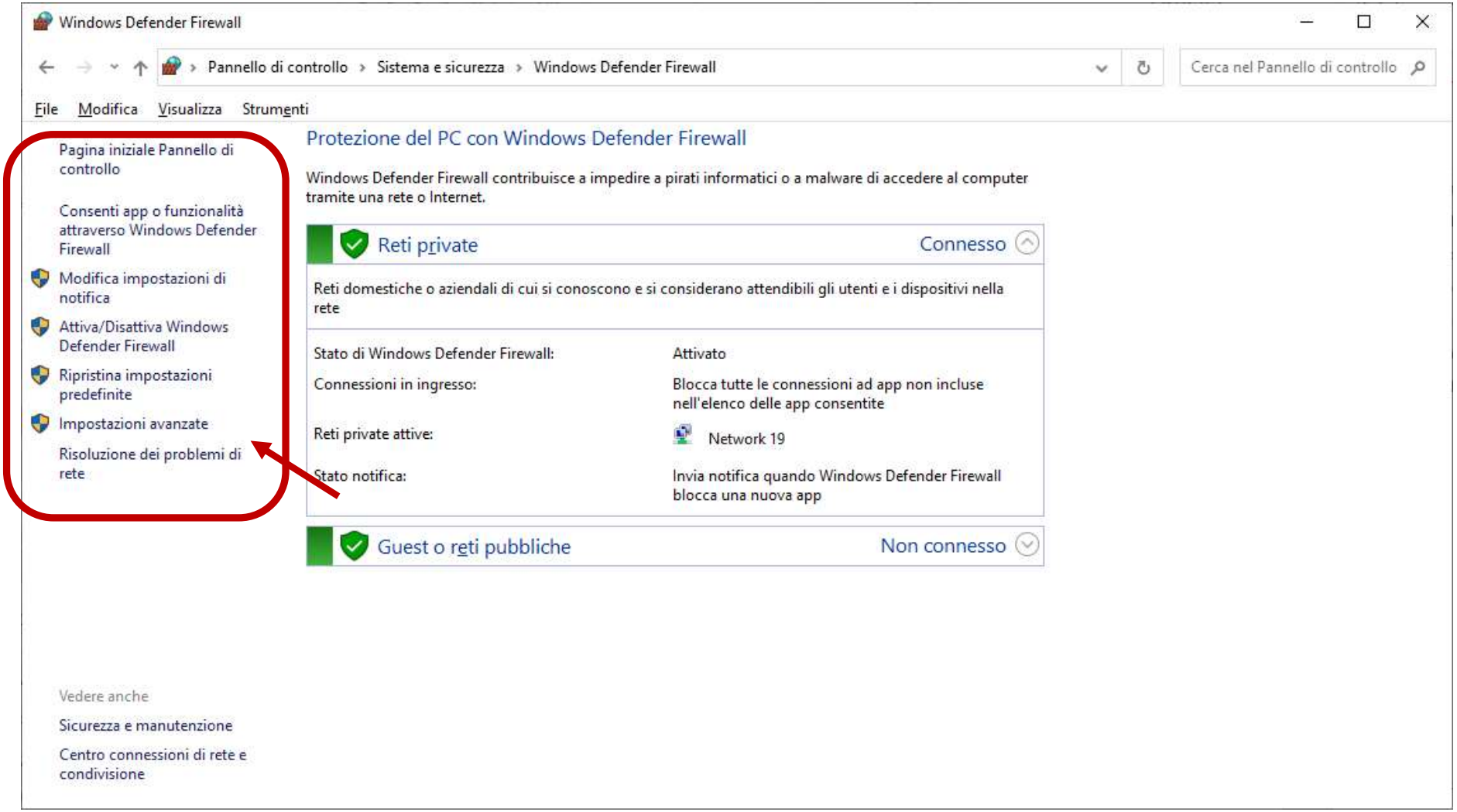
Firewall


Pannello di controllo
Pannello di cont...
Cerca nel Pannello di controllo
Modifica le impostazioni del computer
Visualizza per: Categoria
Sistema e sicurezza
Rivedi lo stato del computer
Salva copie di backup dei file con Cronologia file
Backup e ripristino (Windows 7)
Rete e Internet
Visualizza attività e stato della rete
Hardware e suoni
Visualizza dispositivi e stampanti
Aggiungi un dispositivo
Modifica impostazioni comuni dei dispositivi portatili
Programmi
Disinstalla un programma
Account utente
Cambia tipo di account
Aspetto e personalizzazione
Orologio e area geografica
Cambia data, ora o formato dei numeri
Accessibilità
Impostazioni automatiche
Ottimizza visualizzazione

Firewall


Sistema e sicurezza
Pannello di controllo › Sistema e sicurezza
File Modifica Visualizza Strumenti
Pagina iniziale Pannello di controllo
Sistema e sicurezza
Rete e Internet
Hardware e suoni
Programmi
Account utente
Aspetto e personalizzazione
Orologio e area geografica
Accessibilità
Sicurezza e manutenzione
Controlla lo stato del computer e risolvi i problemi
Modifica le impostazioni di Controllo dell'account utente
Windows Defender Firewall
Controlla stato del firewall
Consenti app attraverso Windows Firewall
Sistema
Visualizza quantità di RAM e velocità del processore
Consenti accesso remoto
Avvia Assistenza remota
Visualizza il nome del computer
Opzioni risparmio energia
Cambia comportamento dei pulsanti di alimentazione
Modifica impostazioni di sospensione del computer
Cronologia file
Salva copie di backup dei file con Cronologia file
Ripristina file con Cronologia file
Backup e ripristino (Windows 7)
Backup e ripristino (Windows 7)
Ripristinare file dal backup
Crittografia unità BitLocker
Gestione BitLocker
Spazi di archiviazione
Gestisci spazi di archiviazione
Cartelle di lavoro
Gestisci Cartelle di lavoro
Strumenti di amministrazione
Libera spazio su disco
Deframmenta e ottimizza unità
Crea e formatta le partizioni del disco rigido
Visualizza i registri eventi
Pianifica attività

Firewall


Windows Defender Firewall
Pannello di controllo › Sistema e sicurezza › Windows Defender Firewall
Cerca nel Pannello di controllo
File Modifica Visualizza Strumenti
Pagina iniziale Pannello di controllo
Consenti app o funzionalità attraverso Windows Defender Firewall
Modifica impostazioni di notifica
Attiva/Disattiva Windows Defender Firewall
Ripristina impostazioni predefinite
Impostazioni avanzate
Risoluzione dei problemi di rete
Protezione del PC con Windows Defender Firewall
Windows Defender Firewall contribuisce a impedire a pirati informatici o a malware di accedere al computer tramite una rete o Internet.
Reti private
Connesso
Reti domestiche o aziendali di cui si conoscono e si considerano attendibili gli utenti e i dispositivi nella rete
Stato di Windows Defender Firewall:
Attivato
Connessioni in ingresso:
Blocca tutte le connessioni ad app non incluse nell'elenco delle app consentite
Reti private attive:
Network 19
Stato notifica:
Invia notifica quando Windows Defender Firewall blocca una nuova app
Guest o reti pubbliche
Non connesso
Vedere anche
Sicurezza e manutenzione
Centro connessioni di rete e condivisione

Tipi di firewall

Un **firewall** personale protegge un singolo **client** o un singolo **server.**

Un **firewall** perimetrale protegge un'intera **rete** o sottorete, filtrando il traffico tra interna ed esterno.

I **firewall** di nuova generazione includono ispezione a livello applicativo, rilevamento di intrusioni, **VPN** integrate, filtraggio **URL** e controllo delle applicazioni.

La corretta configurazione dei **firewall** è essenziale per la sicurezza dei dati sanitari, spesso considerati tra i più sensibili in assoluto.

Protocolli di rete

Un **protocollo** di **rete** è un insieme di regole che definisce come i dispositivi comunicano, come formattano i dati e come gestiscono errori e ritrasmissioni.

La suite **TCP/IP** fornisce i **protocolli** fondamentali per la comunicazione in **Internet** e nelle **LAN.**

Sopra questi si appoggiano **protocolli** applicativi specifici: **HTTP** per il web, **FTP** per il trasferimento di file, SMTP e IMAP per la posta elettronica, **DNS** per la risoluzione dei nomi.

In sanità, questi **protocolli** sono usati per accedere ai portali clinici, inviare referti, consultare basi dati e integrare sistemi diversi.

Protocollo HTTP

HTTP (HyperText Transfer Protocol) è il **protocollo** usato per trasferire pagine web, immagini e contenuti ipertestuali.

Segue un modello richiesta/risposta: un **client** invia una richiesta **HTTP** a un **server,** che risponde con uno status e un contenuto.

Nella sua forma originaria **HTTP** non cifrava i dati, rendendoli leggibili da chiunque intercettasse il traffico.

Per questo oggi è quasi sempre sostituito da **HTTPS,** che aggiunge cifratura e autenticazione.

Protocollo HTTPS

HTTPS combina **HTTP** con un livello di cifratura basato su TLS.

La comunicazione tra **client** e **server** viene cifrata, rendendo molto difficile l'intercettazione o la modifica dei contenuti.

I certificati digitali permettono di verificare l'identità del **server** e prevenire attacchi di tipo man-in-the-middle.

Per i dati sanitari, l'uso di **HTTPS** è imprescindibile: referti, dati clinici e informazioni sensibili non devono mai transitare in chiaro su **Internet.**

FTP, FTPS e SFTP

FTP (File Transfer Protocol) è uno dei **protocolli** storici per il trasferimento di file tra **client** e **server.**

Nella forma base non offre cifratura, risultando inadeguato per dati sensibili.

FTPS aggiunge un layer di cifratura TLS a **FTP,** mentre **SFTP** è un **protocollo** distinto che utilizza il canale cifrato di SSH.

In ambito sanitario, **SFTP** è spesso utilizzato per lo scambio sicuro di immagini diagnostiche, dataset di ricerca e documentazione amministrativa tra strutture diverse.

Posta elettronica: SMTP e IMAP

SMTP (Simple Mail Transfer Protocol) è il **protocollo** utilizzato per inviare email dai **client** ai **server** e tra **server** di posta.

IMAP e POP3 sono **protocolli** per l'accesso alle caselle di posta; IMAP consente di mantenere la posta sul **server,** facilitando l'accesso da più dispositivi.

Per la tutela dei dati è fondamentale utilizzare versioni cifrate (ad esempio SMTPS, IMAPS) che proteggano le credenziali e i contenuti.

Nelle aziende sanitarie, la posta elettronica deve rispettare requisiti normativi e può essere integrata con sistemi di PEC per comunicazioni ufficiali.

DNS – Domain Name System

Il **DNS** traduce nomi simbolici (come www.example.org) in indirizzi **IP** numerici.

Senza **DNS,** gli utenti dovrebbero ricordare indirizzi **IP** per ogni servizio, cosa impraticabile in **Internet.**

Il sistema **DNS** è gerarchico e distribuito: i **server DNS** si scambiano informazioni per risolvere richieste da ogni parte del mondo.

Negli ospedali si utilizzano **server DNS** interni per risolvere i nomi dei **server** clinici (ad esempio i sistemi **PACS, RIS,** directory aziendali e applicativi gestionali).

Virtualizzazione

La **virtualizzazione** consente di eseguire più macchine virtuali su un singolo **server** fisico, condividendo risorse come CPU, RAM e storage.

Ogni macchina virtuale ha il proprio sistema operativo e le proprie applicazioni, isolati logicamente dagli altri.

La **virtualizzazione** facilita alta disponibilità, riduzione dei costi hardware, snapshot, migrazioni a caldo e ambienti di test.

Negli ospedali, molti servizi (tra cui **PACS, RIS,** database e applicativi clinici) vengono eseguiti su infrastrutture virtualizzate per migliorare flessibilità e resilienza.

Che cos’è il Cloud Computing

Il *cloud computing* è un modello che permette di **utilizzare risorse informatiche tramite Internet senza possederle fisicamente**. Significa che server, spazio di archiviazione, software, database o intere piattaforme possono essere erogati da un fornitore esterno e raggiunti semplicemente attraverso un browser o un’applicazione.

Per l’utente non cambia la funzionalità: cambia *dove* avviene l’elaborazione.
Il cloud permette scalabilità immediata, aggiornamenti automatici, elevata disponibilità e un **modello di costo basato sull’uso effettivo** invece che su investimenti iniziali elevati.

I tre modelli di servizio del cloud

Il cloud non è tutto uguale. Esistono tre grandi modelli, ciascuno con un diverso grado di controllo da parte dell'utente:

- **IaaS – Infrastructure as a Service:** il livello più vicino all'hardware.
- **PaaS – Platform as a Service:** il livello dedicato agli sviluppatori.
- **SaaS – Software as a Service:** il livello orientato all'utente finale.

Si differenziano per *quanto* del sistema gestisce il provider e quanto resta a carico dell'utente.

IaaS: Infrastructure as a Service

L'IaaS fornisce componenti infrastrutturali virtualizzati: server, rete, sistemi operativi, capacità di calcolo, firewall, storage. È come avere un "data center virtuale" dove è possibile costruire i propri sistemi come si preferisce.

In questo modello l'utente mantiene il controllo di molte parti: può installare software, configurare il sistema operativo e decidere l'architettura delle applicazioni. Il provider si occupa dell'hardware, della disponibilità della rete, della scalabilità e della sicurezza fisica.

A cosa serve davvero?
È ideale quando si vuole creare ambienti personalizzati senza comprare server fisici.

***Esempio sanitario*:** un ospedale può ospitare il proprio sistema RIS/PACS o basi dati ad alto volume direttamente nel cloud, mantenendo il pieno controllo sulle configurazioni e sulla sicurezza logica.

PaaS: Platform as a Service

Il PaaS offre un ambiente di sviluppo completo: sistemi operativi, librerie, database, strumenti di testing, servizi di deployment. Gli sviluppatori non devono più preoccuparsi dell'infrastruttura: server, aggiornamenti, patch, load balancing, scalabilità e sicurezza sono gestiti automaticamente dal provider.

È un modello che accelera la creazione delle applicazioni. Il team si concentra sul codice, non sui problemi di configurazione o sulle manutenzioni dei server.

Perché è utile?
Per creare applicativi rapidamente, ridurre i costi di sviluppo e evitare complessità inutili.

***Esempio sanitario*:** un piccolo team IT può sviluppare un'app per consultare referti o un sistema di telemonitoraggio usando servizi cloud già pronti (ad esempio Google App Engine o Azure App Services), senza costruire l'infrastruttura da zero.

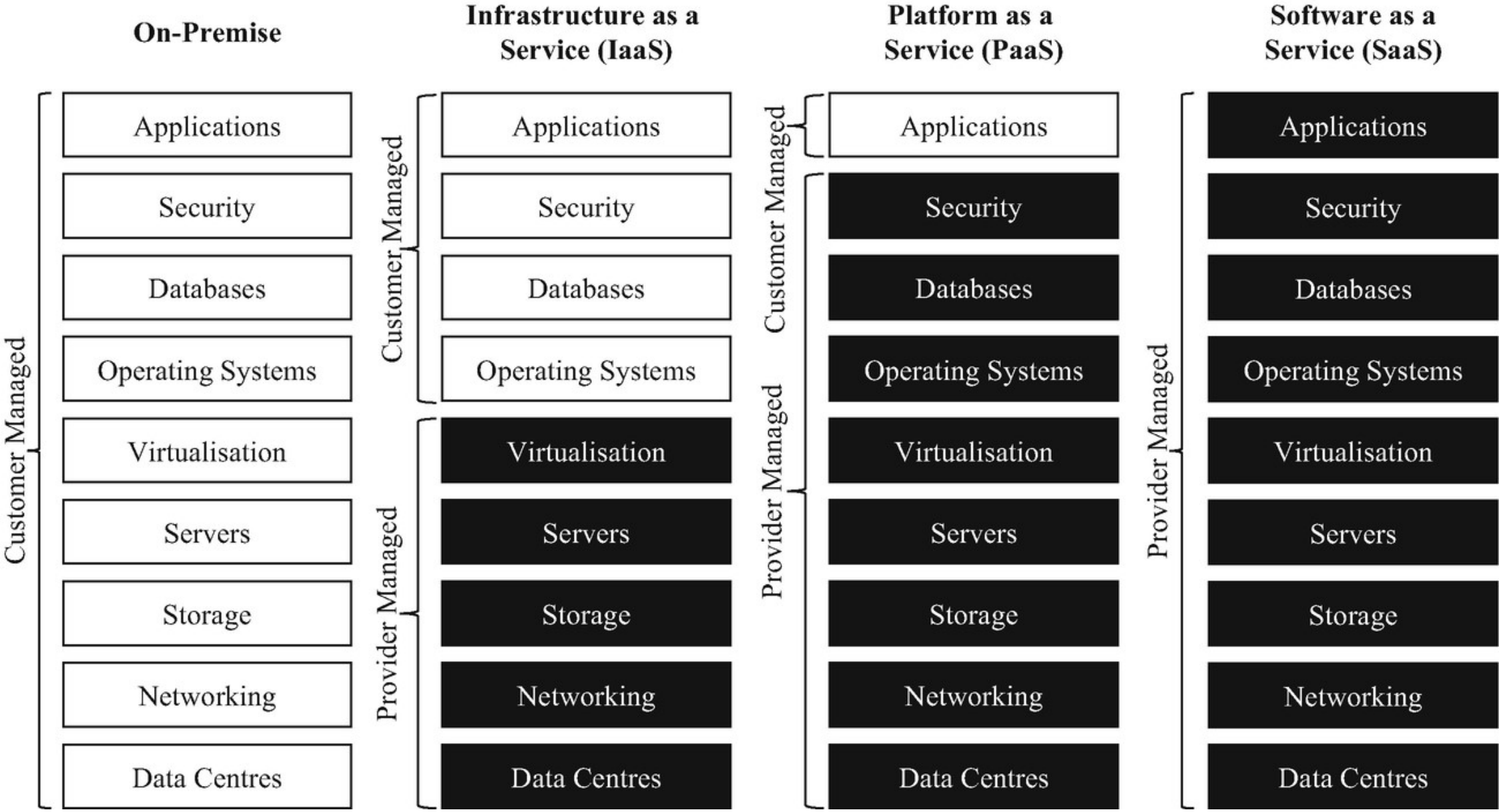
SaaS: Software as a Service

Il modello SaaS è il più semplice per l'utente. Il software non viene installato sul computer locale: si utilizza direttamente online. Tutti gli aggiornamenti, la manutenzione, la sicurezza e la disponibilità sono responsabilità del provider.

L'utente deve solo accedere al servizio, come farebbe con un sito web. Questo modello è perfetto per applicazioni standardizzate che non richiedono personalizzazioni profonde.

Perché è vantaggioso?
Elimina installazioni, problemi di compatibilità, aggiornamenti manuali e manutenzione.

***Esempio sanitario*:** piattaforme di telemedicina, posta elettronica aziendale, sistemi di prenotazione online, moduli web per la gestione dei pazienti, applicazioni condivise per referti e documenti clinici.


On-Premise
Infrastructure as a Service (IaaS)
Platform as a Service (PaaS)
Software as a Service (SaaS)
Customer Managed
Provider Managed
Applications
Security
Databases
Operating Systems
Virtualisation
Servers
Storage
Networking
Data Centres

Come cambiano responsabilità e controllo

Passando da IaaS a PaaS a SaaS, **l'utente gestisce sempre meno** e il provider gestisce sempre di più.

È una scala discendente di responsabilità tecnica:

- Con l'**IaaS** controlli quasi tutto, tranne l'hardware.
- Con il **PaaS** controlli solo l'applicazione.
- Con il **SaaS** non controlli nulla della tecnica: ti limiti a usare l'APP.

Per contro, **aumenta la semplicità d'uso**: il SaaS è immediato, il PaaS è comodo, l'IaaS è potente ma richiede competenze.

Sintesi finale

Il cloud è un modo moderno e flessibile di utilizzare risorse informatiche.

- L'**IaaS** offre infrastruttura e massimo controllo: ideale per sistemi complessi o personalizzati.
- Il **PaaS** offre una piattaforma già pronta per sviluppare e distribuire applicazioni.
- Il **SaaS** offre software già funzionante, accessibile via web e subito pronto.

In ambito sanitario, i tre modelli permettono di digitalizzare più agevolemente i processi, ridurre costi e semplificare la gestione dei servizi informatici.

Cloud computing

Il **cloud** computing estende il concetto di **virtualizzazione** fornendo risorse informatiche via **Internet.**

Invece di acquistare e gestire direttamente i **server,** l'organizzazione noleggia capacità di calcolo, storage e servizi applicativi da un provider **cloud.**

I principali modelli di servizio **cloud** sono **IaaS, PaaS** e **SaaS,** che differiscono per il livello di controllo e responsabilità dell'utente.

Nel settore sanitario, il **cloud** viene utilizzato per archiviare dati, eseguire analisi su larga scala e ospitare applicazioni accessibili da più strutture.

IaaS – Infrastructure as a Service

Con **IaaS,** il provider offre infrastruttura virtuale: macchine virtuali, **rete,** storage, bilanciatori, **firewall** virtuali.

L'utente gestisce sistemi operativi, middleware, applicazioni e dati.

Questo modello garantisce grande flessibilità: si possono creare ambienti complessi senza investire in hardware fisico.

In sanità, **IaaS** può essere usato per ospitare ambienti di test, sistemi **PACS** su larga scala, data warehouse per analisi cliniche e gestionali.

PaaS – Platform as a Service

Con **PaaS,** il provider offre una piattaforma completa per sviluppare, eseguire e scalare applicazioni: sistemi operativi, database, servizi di integrazione e ambienti di esecuzione.

Gli sviluppatori si concentrano sul codice e sulla logica applicativa, senza doversi occupare di patch di sistema, installazione di middleware o configurazione complessa di **rete.**

Questo accelera i tempi di sviluppo e riduce il rischio operativo.

In ambito sanitario, **PaaS** può supportare la creazione di applicazioni custom per refertazione, portali paziente, telemonitoraggio e integrazione tra sistemi diversi.

SaaS – Software as a Service

Con **SaaS,** l'utente utilizza applicazioni complete erogate via web o tramite **client** dedicati.

Tutta l'infrastruttura sottostante (sistemi operativi, **rete, server,** database) è gestita dal provider.

L'utente si occupa soltanto della configurazione funzionale e dei dati applicativi.

Esempi in sanità includono piattaforme di **telemedicina,** sistemi di prenotazione online, suite di produttività, gestione documentale e servizi specialistici erogati da **cloud** regionali o nazionali.

Responsabilità nei modelli cloud

Nel modello **IaaS** la responsabilità tecnica dell'utente è maggiore: deve gestire in sicurezza sistemi operativi e applicazioni.

Nel modello **PaaS,** l'utente è responsabile principalmente della sicurezza e qualità del proprio codice e dei dati.

Nel modello **SaaS,** l'utente delega quasi tutto al provider e si concentra su configurazione, gestione degli accessi e corretta utilizzazione del servizio.

In ogni caso, la responsabilità finale rispetto alla protezione dei dati sanitari rimane in capo all'organizzazione sanitaria.

GRAZIE PER L'ATTENZIONE