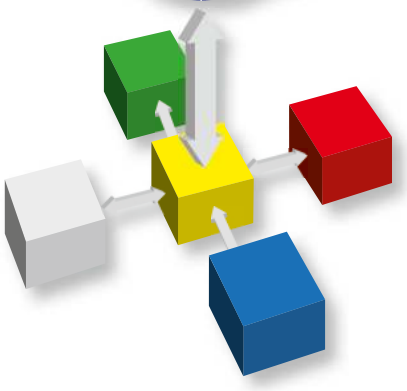
Le reti telematiche e le reti aziendali



Comunicazione: si ritrovano in questa Unità termini analoghi a quelli trattati nell'Unità "La comunicazione"; annotali man mano e ripassane il significato (sorgente/emittente, canale, ricevente/destinatario ecc).

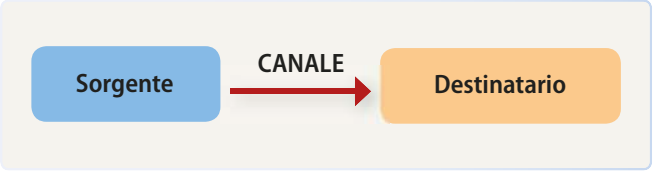
Nel Modulo 1 e 2 abbiamo illustrato la tendenza all'automatizzazione dei processi aziendali attraverso l'uso dei computer; nella prima Unità di questo nuovo Modulo ci soffermeremo sulle tecnologie e gli strumenti che oggi rendono possibile la **comunicazione** tra computer, permettendo lo scambio di dati e informazioni tra utenti anche a grande distanza. Analizzeremo quindi le principali caratteristiche delle reti telematiche e le loro applicazioni in ambito aziendale.

1.1 Le telecomunicazioni

La codifica di dati eterogenei, quali voce, immagini o testi, rende possibile il trasferimento dell'informazione in essi contenuta attraverso segnali elettrici, ottici o elettromagnetici.

La **telecomunicazione (TLC)** è la disciplina che studia la comunicazione a distanza attraverso strumenti e infrastrutture specifiche per il trasferimento di informazioni sotto forma di dati codificati, trasmessi mediante segnali elettrici, ottici o elettromagnetici.

Qualsiasi sistema di comunicazione comprende i seguenti elementi:
- una **sorgente**, che codifica e trasmette i dati;
- un **canale**, attraverso cui i dati codificati vengono trasmessi;
- un **destinatario**, che riceve i dati e li decodifica.



Il canale trasmissivo è il mezzo fisico che collega sorgente e destinatario; esso può essere:
- **elettrico**, costituito da fili di rame;
- **ottico**, costituito da cavi in fibra ottica;
- **elettromagnetico**, basato su onde radio.

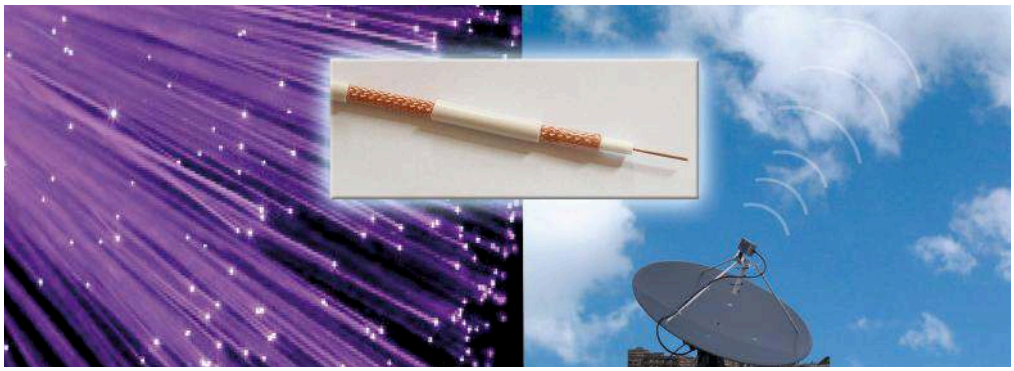
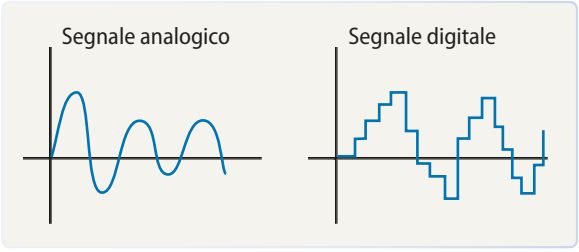


Fig. 1: Tre diversi tipi di canali (da sinistra a destra): fibre ottiche, cavo coassiale in rame, onde elettromagnetiche.



Se il canale di comunicazione (*link*) è adatto a trasmettere segnali continui si parla di **trasmissione analogica**; se trasmette segnali discreti (per esempio, sequenze di dati binari) si parla di **trasmissione digitale**. In seguito all'avvento delle nuove tecnologie digitali, che permettono migliori prestazioni a costi contenuti, la trasmissione analogica è stata via via soppiantata dalla trasmissione digitale.

ESEMPIO In Italia la televisione digitale, in cui i segnali video e audio sono trasmessi interamente su canali digitali, ha recentemente sostituito la televisione analogica.

I dati scambiati sul canale di comunicazione vengono comunemente denominati **traffico**; su un canale digitale si trasmettono sequenze di bit (zero o uno); il traffico viene quindi misurato in numero di bit scambiati.

Il **Binary Unit (Bit)** è l'unità di misura dell'informazione; può assumere due valori (0 e 1) che corrispondono a due stati differenti del segnale trasmesso (per esempio, alto o basso).

Conversioni:
1 Kbit/s = 1000 bit/s;
1Mbit/s = 10^6 bit/s.

Le **velocità di trasmissione** sono solitamente misurate in bit/s (bit trasmessi per secondo) o suoi multipli, come **Kbit/s** o **Mbit/s**.

Il **modulatore** è l'apparato che trasforma la sequenza di dati da trasmettere in un segnale elettrico; la sequenza di dati da trasmettere viene quindi detta **modulante.** Il segnale elettrico prodotto è denominato **segnale modulato** e, una volta giunto al ricevitore, subisce il processo inverso: un **demodulatore** ritrasforma il segnale elettrico in una sequenza di dati fruibile dal destinatario.

Throughput: quantità di lavoro svolta in un determinato periodo di tempo.

Signal/Noise (S/N) Ratio: Rapporto Segnale/Rumore.

I canali trasmissivi (*link*) sono caratterizzati da:

- **capacità,** velocità di trasmissione *ideale*, che indica la massima quantità di dati trasportabile;
- **throughput**, velocità di trasmissione *reale*, che indica la velocità reale misurata con cui i dati vengono trasmessi;
- **rapporto segnale/rumore (S/N)**, rapporto tra la quantità di dati utili trasmessi e la quantità totale di dati ricevuti.

Una problematica significativa nella trasmissione dati è la presenza di **interferenze sul canale** (**rumore**), dovute a fattori ambientali, climatici o umani. La presenza di interferenze nella comunicazione, i ritardi e i limiti degli apparati di trasmissione e ricezione, impediscono il raggiungimento della velocità massima di trasmissione; il rapporto segnale/rumore fornisce un'indicazione quantitativa dell'incidenza del rumore.

ESEMPIO Canali di comunicazione ottici, basati su cavi in fibra ottica, garantiscono una maggiore protezione dalle interferenze esterne, quindi un più alto rapporto segnale/rumore, rispetto ai più comuni cavi in rame. Comportano però costi di cablaggio e di manutenzione più elevati.

Le trasmissioni su un canale non sono esenti da errori: su un canale binario l'errore si traduce, per esempio, nella ricezione di 1 quando era stato trasmesso 0 o viceversa. L'**errore di trasmissione** misura il numero di bit errati rispetto al numero totale di bit ricevuti.

Overhead: indica la ridondanza.

Per prevenire e correggere gli errori di trasmissione si applicano tecniche specifiche, basate sulla **ridondanza nella trasmissione dell'informazione** (**overhead**): anziché trasmettere la sola informazione utile, per limitare l'incidenza degli errori si trasmettono più copie della stessa sullo stesso canale o su canali separati. Canali dedicati alla rilevazione degli errori rappresentano la soluzione migliore perché non sono sensibili alle medesime interferenze dei canali principali, ma risultano molti costosi da implementare. Le tecniche di rilevazione degli errori più comuni si basano su bit di **Controllo di parità** e/o di **Controllo di Ridondanza Ciclico (CRC)**.

APPROFONDIMENTI

Controllo di parità

Il **bit di parità** è un bit aggiuntivo che indica se il numero nella sequenza è pari (bit di parità impostato a 1) o dispari (bit di parità impostato a 0). Esso permette di rilevare alcuni possibili errori.
Per esempio, consideriamo la sequenza di trasmissione: 11011**1**
Il sesto numero è il bit di parità, che vale 1 perché nella sequenza gli 1 sono in numero pari (4).
Se il destinatario riceve la seguente sequenza: 11010**1** è evidente che è avvenuto un errore in quanto l'informazione portata dal bit di parità non è coerente: il numero di bit a 1 ricevuti è dispari (3), mentre il bit di parità è settato a 1. Potrà quindi essere eventualmente chiesta alla sorgente una ritrasmissione del messaggio.

La **rilevazione dell'errore** ha dunque il compito di identificare eventuali trasmissioni errate; la **correzione d'errore** consiste nel recuperare una porzione di

segnale corretta. Entrambe le tecniche richiedono l'aggiunta di ridondanza (nel canale principale o in uno secondario), che riduce la porzione di dati utili ricevuti nell'unità di tempo.

Il **goodput** è una frazione di throughput (velocità di trasmissione reale nell'unità di tempo) dedicata alla trasmissione di dati utili, esclusi quindi i dati ridondanti.

Classificazione dei sistemi di comunicazione

I canali di comunicazione possono essere classificati in base al numero di sorgenti/destinatari coinvolti.

La **comunicazione punto-punto** (*point-to-point* o *unicast*) avviene quando una sorgente comunica con un destinatario mediante un canale di collegamento diretto.

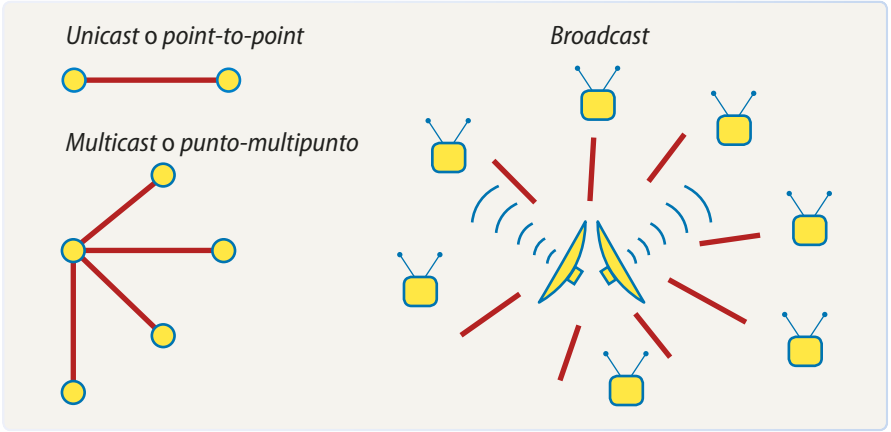
Un esempio di comunicazione point-to-point è la comunicazione tra due computer collegati direttamente via cavo mediante porta seriale.

La **comunicazione punto-multipunto** (*point-to-multipoint* o *multicast*) avviene quando una sorgente comunica con più destinatari selezionati.

Un esempio di comunicazione point-to-multipoint è la televisione *on-demand*, dove la sorgente trasmette il segnale video e audio a specifici destinatari abilitati.

La **comunicazione broadcast** avviene quando una sorgente comunica con tutte le entità, in numero non definibile a priori, in grado di ricevere il segnale.

Un esempio di comunicazione broadcast è quella legata alle trasmissioni radio ad alta potenza, in cui il segnale è ricevibile da tutti gli utenti dotati di apposita antenna.



Un'ulteriore possibile classificazione riguarda la tipologia di scambio che avviene durante la comunicazione tra sorgente e ricevitore.

La **comunicazione half-duplex** avviene quando le entità comunicanti assumono un ruolo specifico di trasmettitore o ricevitore, eventualmente intercambiabile, ma non possono comunicare e ricevere contemporaneamente.

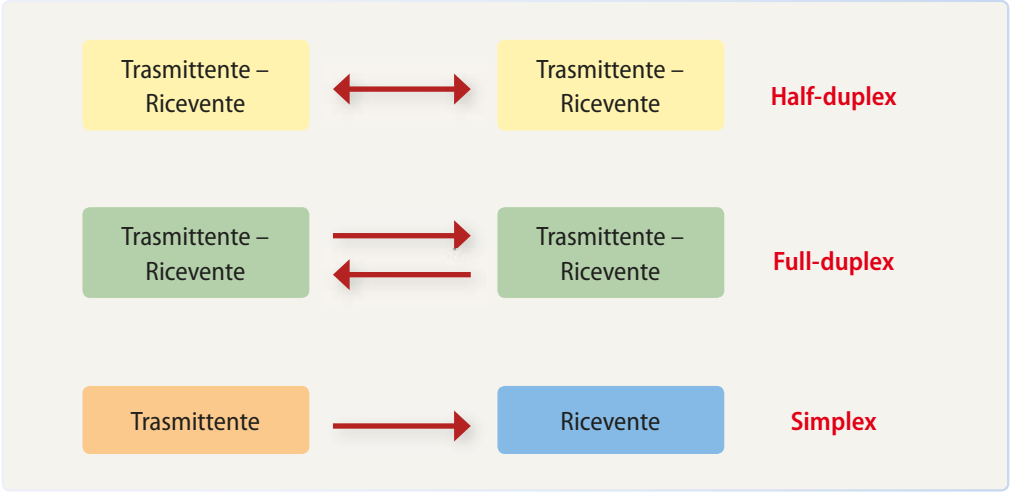
Un esempio di comunicazione half-duplex è quella che viene instaurata mediante le radio *walkie-talkie* in cui si utilizza solitamente una parola chiave (per esempio, "Passo") per indicare la fine della trasmissione e cedere quindi il ruolo di trasmettitore all'interlocutore.
Come spiegato più avanti una possibile variante alla comunicazione half-duplex è la comunicazione simplex.

La **comunicazione full-duplex** si ha quando le entità comunicanti possono trasmettere e ricevere contemporaneamente.

La comunicazione tra persone è tipicamente full-duplex; la sovrapposizione di più voci genera ovviamente problemi di interferenza tra segnali che devono essere opportunamente gestiti attraverso tecniche di sincronizzazione.

La **comunicazione simplex** avviene quando le entità comunicanti assumono il ruolo prefissato a priori e non intercambiabile di trasmettitore e di ricevitore. Rappresenta una possibile variante alla comunicazione half-duplex.

Per esempio, nel caso dei segnali televisivi tradizionali (non video on-demand), le emittenti svolgono sempre il ruolo di trasmettitori mentre gli utenti provvisti di antenne quello di ricevitori. In figura sono rappresentate le diverse tipologie di scambio.



1.2 La telematica e le reti telematiche

Il connubio tra informatica e telecomunicazioni permette lo scambio di dati e informazioni generate, collezionate o rielaborate mediante l'ausilio del computer.

La **telematica** è la disciplina che studia la combinazione efficace di tecniche proprie delle telecomunicazioni e dell'informatica per realizzare il trasferimento a distanza di dati ed informazioni.

ICT: acronimo di *Information and Communication Technology*, "Tecnologie dell'informazione e della comunicazione".

Le **tecnologie dell'informazione e della comunicazione**, abbreviate spesso con l'acronimo **ICT**, rappresentano l'insieme delle tecnologie che permettono il connubio tra informatica e telecomunicazioni.

Le tecnologie informatiche sono lo strumento per la rielaborazione automatica dei dati e dell'informazione, mentre le telecomunicazioni forniscono l'infrastruttura su cui si basa la comunicazione.

Reti telematiche

L'informatica utilizza strumenti, tecnologie e protocolli in grado di far comunicare utenti a distanza; la comunicazione lega le risorse remote attraverso canali di comunicazione.

La **rete telematica** è un sistema di comunicazione che permette l'interconnessione di strutture telefoniche e/o informatiche al servizio di utenti distribuiti su aree geografiche di qualsiasi ampiezza.

I computer collegati in rete sono denominati **host** o **terminali**.
La telefonia ha rappresentato il primo strumento per la comunicazione a distanza; la condivisione di risorse attraverso i computer rappresenta il passo successivo. La possibilità di condividere risorse in remoto ha avuto un impatto enorme dal punto di vista sociale e scientifico; a livello aziendale costituisce un decisivo apporto ad una efficace operatività. Le aziende necessitano infatti di:

- condividere risorse (dati, analisi, risultati, prospetti ecc.);
- elaborare in modo distribuito i dati a disposizione.

ESEMPIO La comunicazione intra-aziendale e inter-aziendale si pone come elemento chiave per lo sviluppo dei processi aziendali e gestionali. La raccolta e l'analisi dei dati prodotti localmente deve essere condivisa con le altre sedi aziendali e gli stakeholder esterni per poter sincronizzare ed ottimizzare i processi aziendali. È il tema trattato nelle Unità dedicate al sistema informativo e alla comunicazione aziendale.

Le risorse tecnologiche locali necessarie per l'analisi dei dati sono spesso insufficienti per il raggiungimento degli obiettivi prefissati; il **processo di elaborazione distribuito** consiste nello sfruttare risorse remote di memorizzazione, calcolo e analisi. Tale processo rappresenta una grande risorsa per ottimizzare i processi aziendali.

ESEMPIO I **database distribuiti** sono basi di dati in cui la memorizzazione e la gestione dei dati avviene in modo non centralizzato, sfruttando risorse di elaborazione remote collegate in rete. Si utilizzano, a tal fine, specifici sistemi di gestione delle basi di dati, chiamati *Distributed Data Base Management Systems* (**DDBMS**).

1.3 I protocolli di comunicazione

Quando le persone comunicano tra loro si attengono, anche inconsapevolmente, a regole per adattare lo strumento di comunicazione al contesto, sincronizzare lo scambio di informazioni e uniformarsi al linguaggio di comunicazione prescelto.

ESEMPIO Nella **comunicazione verbale** chi parla si attiene (se la conosce!) alla lingua usata dai presenti per permettere la piena comprensione da parte degli interlocutori; inoltre regola il tono di voce in base al contesto (per esempio, una stanza con molto rumore di sottofondo) e al messaggio che vuole trasmettere, usando, per esempio, un tono autoritario o rassicurante. Inoltre cerca di sincronizzarsi in modo da evitare la sovrapposizione di voci tra chi comunica.

Analogamente, la comunicazione tra computer in una rete telematica necessita di *protocolli di comunicazione* ben definiti per risultare efficace.

Il **protocollo di comunicazione** è un insieme di regole e di messaggi che governano la comunicazione tra due entità telematiche.

I protocolli descrivono:
- gli apparati hardware che intervengono nella comunicazione;
- le procedure di sincronizzazione e temporizzazione della comunicazione;
- la sintassi della comunicazione (il formato dei dati scambiati);
- la semantica della comunicazione (gli algoritmi utilizzati per instaurare, realizzare e gestire la comunicazione).

UTILE A SAPERSI

Enti internazionali per i protocolli di comunicazione

I principali enti internazionali che raccolgono normative relative a protocolli di comunicazione sono:

ANSI (*American National Standard Institute*)
ISO (*International Standard Organization*)
ITU-T (*International Telecommunication Union – Telecommunication Standardization Sector*)
ETSI (*European Telecommunication Standard Institute*)
IEEE (*Institute of Electrical and Electronics Engineers*).

I computer, gli apparati di rete e i pacchetti software che vengono utilizzati nell'ambito delle reti telematiche devono dunque uniformarsi a regole di comunicazione condivise.

I protocolli applicati nella rete Internet sono raccolti e pubblicati sotto forma di specifici documenti tecnici denominati **Request for Comments (RFC)**.

Modello ISO/OSI

OSI: acronimo di *Open System Interconnession*.

I principali protocolli di comunicazione sono stati raccolti dall'ISO nel cosiddetto **modello OSI.**

I protocolli di comunicazione ISO/OSI sono stati standardizzati al fine di garantire la possibilità di comunicazione tra computer e apparati aventi caratteristiche software o hardware differenti. Non tutte le architetture di protocolli sono conformi al modello OSI, tuttavia i principi fondamentali definiti dal modello sono oggi universalmente accettati.

Il modello OSI definisce una struttura gerarchica di organizzazione di protocolli che viene denominata anche **modello a livelli** o **a strati**, in cui ogni livello ha i suoi specifici protocolli di comunicazione; la pila ISO/OSI è la seguente:

Livello 7	Applicazione (*application level*)
Livello 6	Presentazione (*presentation level*)
Livello 5	Sessione (*session level*)
Livello 4	Trasporto (*transport level*)
Livello 3	Rete (*network level*)
Livello 2	Collegamento (*data link level*)
Livello 1	Fisico (*physical level*)

Header: "testata"; nelle applicazioni telematiche si traduce con "intestazione".

Il modello OSI prevede un'organizzazione gerarchica: i servizi forniti da ciascun livello utilizzano sia le proprie funzioni sia i servizi forniti dagli strati inferiori. All'unità dati da trasmettere si associa un'intestazione (**header**) per fornire informazioni relative al servizio (come interpretare i dati, dove mandarli, come rilevare gli errori ecc.), che verranno utilizzate dagli apparati di rete per l'erogazione dei servizi.

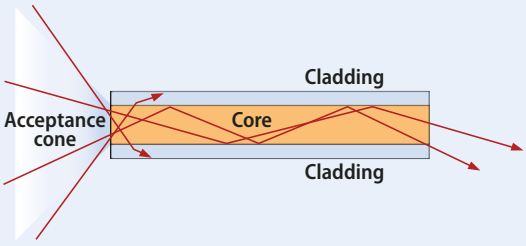
L'**incapsulamento dei dati** è il processo che permette la comunicazione tra servizi differenti di pari livello mediante l'intermediazione dei livelli inferiori. Secondo il principio dell'incapsulamento, ogni livello definisce una specifica unità dati che "incapsula" le unità dati di livello sottostante e aggiunge un'intestazione propria.

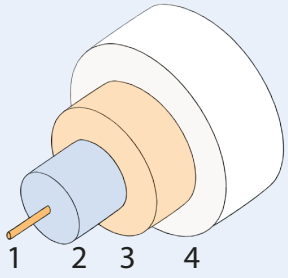
Il **livello fisico** (1) opera sui singoli bit e fornisce gli strumenti meccanici, fisici e funzionali per la connessione fisica. Per esempio, per una trasmissione su fibra ottica vanno specificati i tipi di apparati, di modulazione, di trasmissione del segnale ecc.

APPROFONDIMENTI

Nucleo e mantello

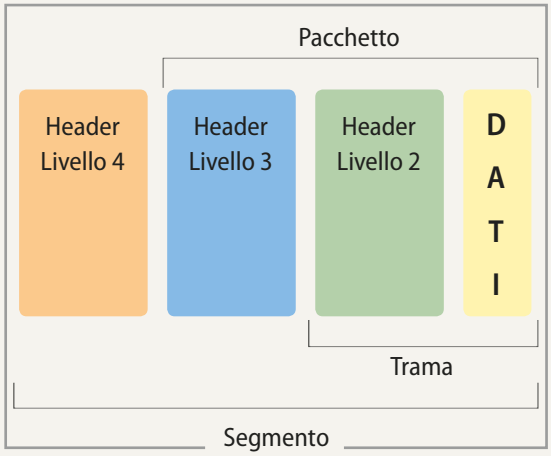
Una fibra ottica è composta da strati concentrici di materiale vetroso puro. Lo strato più interno è denominato **nucleo** (*core*) ed è spesso circa 10 µm (10 millesimi di mm); è rivestito da uno strato denominato **mantello** (*cladding*), spesso circa 125 µm. Successivi strati (*buffer* e *jacket*) possono ricoprire il mantello per proteggere il segnale da interferenze esterne. La propagazione del raggio ottico sfrutta, a livello quantistico, un fenomeno simile alla riflessione totale dell'ottica classica; il raggio rimane "intrappolato" all'interno del *core* a causa di un angolo di incisione sul *cladding* che supera una soglia massima o angolo di riflessione totale, dipendente dal materiale.





1 core, 2 cladding, 3 buffer, 4 jacket

IP: acronimo di *Internet Protocol* in quanto protocollo adottato nella rete Internet.



Al **livello collegamento** (2) le unità dati sono chiamate **trame** (*frame*). L'intestazione contiene solitamente l'informazione su come gestire problemi di sincronizzazione, la rilevazione di errore ecc.

Al **livello rete** (3) le unità dati sono i **pacchetti**. Secondo il principio dell'incapsulamento, un pacchetto contiene l'intestazione propria e i dati provenienti dai livelli sottostanti (sequenza di bit a livello fisico e intestazione a livello collegamento). I protocolli di livello 3, tra cui il più noto è **IP**, gestiscono l'indirizzamento del traffico verso le destinazione attraverso opportune tecniche di *indirizzamento*.

Al **livello trasporto** (4) l'unità dati è il **segmento**. I

protocolli di livello 4 (per esempio, TCP e UDP) gestiscono la comunicazione tra due terminali sorgente e destinazione anche non collegati direttamente, integrando funzionalità quali il recupero degli errori di trasmissione.

I **livelli sessione** (5) e **presentazione** (6) si occupano, rispettivamente, della sicurezza e della codifica e conversione dei dati.

Infine, il **livello applicazione** (7) permette ai software applicativi di accedere alla rete sfruttando servizi di trasferimento e condivisione file, gestione della posta elettronica, reperimento di pagine Web ecc. Nell'Unità seguente sono descritti alcuni esempi molto conosciuti di protocolli appartenenti a questo livello.

Per il funzionamento di un servizio applicativo, i dati incapsulati fino al livello applicazione, vengono "de-incapsulati" man mano dagli apparati di livello inferiore per accedere alle informazioni relative. Apparati e servizi di pari livello accedono all'informazione al corretto livello di incapsulamento grazie ad un procedimento di incapsulamento e de-incapsulamento dei dati che permette di usufruire dei servizi forniti dai protocolli di livello sottostante.

1.4 La classificazione delle reti

Le reti di computer possono essere caratterizzate da estensioni geografiche molto diverse; le caratteristiche della rete e i mezzi trasmissivi utilizzati devono quindi adeguarsi alle esigenze e ai vincoli geografici imposti dalla rete stessa. In base al tipo di rete analizzata si applicano quindi tecnologie e protocolli differenti.

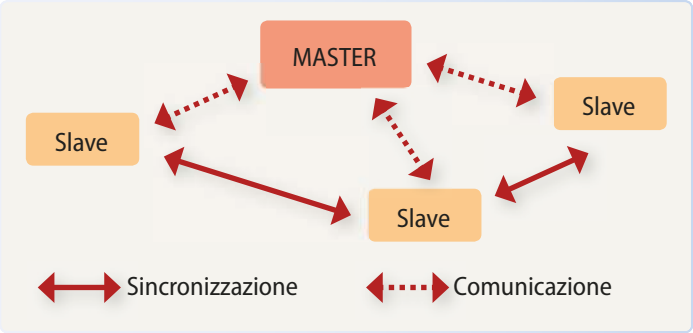
Una classificazione basata sull'estensione geografica della rete prevede le seguenti categorie:
- reti personali o *Personal Area Network* (PAN);
- reti locali cablate o *Wired Local Area Network* (LAN);
- reti locali Wireless o *Wireless Local Area Network* (WLAN);
- reti metropolitane o *Metropolitan Area Network* (MAN);
- reti geografiche o *Wide Area Network* (WAN).

Reti personali

La **rete personale** (PAN) è una rete informatica composta da:
- dispositivi, di solito portabili, aventi copertura di rete limitata dell'ordine di alcuni metri che comunicano attraverso segnali radio;
- canale basato su collegamenti USB (cablato) o senza fili (Wireless); in quest'ultimo caso si basa su segnali di tipo elettromagnetico.

Le reti personali sono utilizzate per mettere in collegamento dispositivi vicini al fine di scambiare dati o per accedere a reti geografiche, per esempio Internet; gli apparati utilizzati (console, telefonini, palmari ecc.) sono solitamente associati ad uno specifico utente utilizzatore: da questo deriva il nome di rete "personale". Il protocollo più utilizzato per realizzare reti personali nel contesto Wireless è **Bluetooth** (802.15).

ESEMPIO Un'applicazione recente è l'integrazione di dispositivi Bluetooth nelle automobili per consentire al guidatore di rispondere al cellulare senza staccare le mani dal volante. L'uso di dispositivi "vivavoce" basati su tecnologia Bluetooth permette di creare una rete personale in grado di connettere l'utente guidatore alla rete telefonica cellulare senza compromettere la sicurezza di guida.



Le reti personali sono, solitamente, di tipo **master-slave**: il dispositivo *master* si occupa di temporizzare e gestire la comunicazione; quando un dispositivo *slave* vuole comunicare deve attendere il via libera dal master, il quale distribuisce il servizio a intervalli di tempo prefissati per ciascun slave in collegamento. Le reti personali gestiscono un numero massimo di *host* e offrono meccanismi di sicurezza per garantire la privacy della comunicazione.

Master: supervisore.
Slave: schiavo.

Reti locali

Le **reti locali (LAN)** sono caratterizzate da un'estensione maggiore rispetto a quella di una rete personale, ma comunque limitata a qualche decina di km.

Una LAN è composta da terminali collegati da un canale condiviso; in base al tipo di canale utilizzato le reti locali si suddividono in:
- cablate (Wired LAN);
- wireless (Wireless LAN).

Le reti cablate sfruttano cavi elettrici coassiali in rame o canali in fibra ottica; le reti Wireless utilizzano invece segnali elettromagnetici.

ESEMPIO Una piccola azienda può utilizzare una LAN costituita da una rete di PC collegati tra loro. Viene denominata WLAN (Wireless LAN) se utilizza la tecnologia Wireless per mettere in collegamento, per esempio, i PC portatili dei dipendenti con la rete aziendale.

LAN cablate e Wireless LAN sono pienamente integrabili tra loro e interfacciabili facilmente a reti geografiche, come Internet. La connessione dei terminali alla rete Wireless e l'interconnessione tra rete cablata e rete Wireless è resa possibile da terminali o apparati dedicati chiamati **Access Point**. Qualora la rete e l'Access Point a cui i terminali accedono siano pubbliche, l'Access Point viene anche denominato **Hot Spot**.

ESEMPIO Reti locali Wireless pubbliche, gratuite o a pagamento, possono essere installate nei parchi, nei centri commerciali e negli edifici pubblici (università, biblioteche, ospedali ecc.).

I terminali che accedono alla rete locale devono essere provvisti di una **scheda rete** (Wireless, nel caso delle WLAN) compatibile con il protocollo di comunicazione utilizzato.

APPROFONDIMENTI

Protocolli ISO/OSI

I protocolli ISO/OSI definiti per le reti locali fanno riferimento ai livelli:
– fisico (1);
– collegamento (2).
Non sono presenti protocolli di livello rete (3) specifici per la gestione dell'invio dei dati da un punto all'altro della rete.
L'identificazione di mittente e destinatario avviene attraverso un indirizzo lungo 48 bit, associato a ciascuna scheda di rete, denominato **indirizzo MAC**.
Per trasmettere correttamente le trame da una sorgente a un destinatario, l'indirizzo è specificato nell'intestazione (*header*) della trama di livello 2.

Topologie di reti locali

La **topologia** è lo studio dei luoghi e delle forme; nell'ambito delle reti telematiche descrive i collegamenti tra gli host appartenenti alla rete.

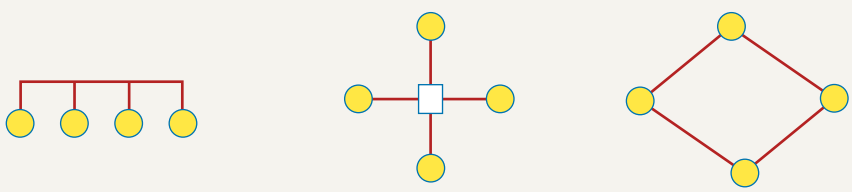
ESEMPIO In cartografia si rappresenta la dislocazione spaziale dei luoghi e i collegamenti (pedonali, stradali o ferroviari) che consentono lo spostamento da un luogo a un altro. Analogamente, la rappresentazione topologica di una rete permette di descrivere quali collegamenti fisici o logici intercorrono tra i diversi terminali o apparati collegati in una rete.

Terminale: apparato collegato ad una rete, che può essere un dispositivo mobile o, più frequentemente, un computer.

La rappresentazione topologica della rete evidenzia solitamente i collegamenti fisici esistenti (cavi di collegamento) tra i diversi terminali; in alcuni casi si rappresentano anche i collegamenti logici che determinano limitazioni di connettività (per esempio, nelle reti Wireless la copertura di ricezione e trasmissione di un **terminale**).

Le principali topologie per reti locali sono le seguenti:

- **topologia a bus**: tutti i terminali sono collegati ad un canale condiviso;
- **topologia a stella**: un nodo centrale collega tutti gli altri nodi della rete, mediante collegamenti dedicati punto-punto. Il nodo centrale può agire passivamente da ripetitore di segnale (centro stella passivo) o da terminale vero e proprio (centro stella attivo). Il centro stella ha un ruolo fondamentale perché garantisce la connettività; si rendono quindi necessari meccanismi di sicurezza per consentire soluzioni di backup in caso di guasto;
- **topologia ad anello**: i nodi sono collegati in circolo. Anche in questo caso, il malfunzionamento di un nodo compromette l'intera rete.



A bus A stella Ad anello

Protocolli per reti locali

I protocolli standard più utilizzati nell'ambito delle reti locali cablate sono **Ethernet** e 802.3; per le reti locali Wireless i protocolli di riferimento sono quelli relativi alla classe 802.11 (802.11a, 802.11b, ...).

1 Gbit/s: è pari a 10^9 bit/s (un miliardo di bit/s).

Le reti locali cablate sono in grado di garantire alte velocità di trasmissione; le reti Wireless offrono velocità di trasmissione di gran lunga inferiori che, come nel caso delle reti cablate, dipendono dal protocollo utilizzato.

ESEMPIO il protocollo **GigaBit Ethernet** è in grado di gestire fino a 100 **Gbit/s** di velocità di trasmissione, basandosi, a livello fisico, su collegamenti in fibra ottica. La velocità di trasmissione teorica con il **protocollo 802.11g** per WLAN è di 54 Mbit/s = 0,054 Gbit/s.

Nelle reti locali il canale di comunicazione è condiviso tra tutti i partecipanti; servono quindi protocolli di gestione degli accessi, di sincronizzazione in trasmissione e in ricezione e di gestione di eventuali accessi simultanei, che possono generare collisioni tra traffico generato da terminali diversi.

APPROFONDIMENTI

Collision Detection e Collision Avoidance

La differenza principale tra reti cablate e reti Wireless è la gestione delle collisioni tra traffico generato da host differenti.
Nel caso delle reti cablate è infatti possibile rilevare una collisione (**Collision Detection**) mettendosi in ascolto sul canale condiviso; si utilizzano quindi protocolli che regolano e permettono l'accesso multiplo di più host al canale condiviso e rilevano eventuali collisioni in atto.

Nel caso delle reti Wireless non è possibile, in generale, rilevare una collisione ascoltando il canale e trasmettendo al contempo. Per l'accesso multiplo al canale condiviso si utilizzano quindi tecniche più conservative di prevenzione delle collisioni (**Collision Avoidance**); prima di trasmettere si verifica per un certo tempo se il canale condiviso è libero; solo allora si trasmettono i dati.

Reti metropolitane e geografiche (MAN e WAN)

Le **reti metropolitane (MAN)** sono reti con estensione delimitata a un perimetro metropolitano; esse estendono il modello di rete locale per fornire la connettività a reti geografiche (per esempio Internet).

Le **reti di comunicazione geografiche (WAN)** coprono estensioni territoriali vaste per interconnettere reti metropolitane e locali situate anche a grande distanza. L'esempio più importante di rete geografica, di estensione planetaria, è la **rete Internet**. Sottoreti private che forniscono la connettività a Internet sono gestite da operatori telefonici o da fornitori di servizi Internet.

I protocolli di comunicazione usati in reti metropolitane si basano principalmente su collegamenti in fibra ottica (per esempio, GigaBit Ethernet, FDDI, SONET/SDH), che trovano minore applicazione nell'ambito delle reti locali a causa degli elevati costi di cablaggio e manutenzione e per le differenti esigenze di riconfigurazione e aggiornamento.

1.5 Gli apparati di rete

Gli host appartenenti a una rete sono collegati mediante apparati le cui funzionalità corrispondono a un determinato livello ISO/OSI, a seconda dello scopo per cui sono installati.

Repeater e **hub** sono apparati a livello fisico (1) che "rigenerano" il segnale permettendo così, per un numero di limitato di volte, di estendere la dimensione della rete.

I cavi coassiali di rame comportano infatti un'attenuazione del segnale, più evidente rispetto ai cavi in fibra ottica; l'effetto negativo è quello di aumentare la

probabilità di errore in ricezione; se tale probabilità supera una soglia massima la ricezione corretta diventerà impossibile.
A differenza del repeater, che possiede una sola porta d'uscita, l'hub è in grado di ritrasmettere il segnale su più porte.

Bridge e **switch** sono apparati di livello collegamento (2) capaci di interconnettere LAN diverse che utilizzano gli stessi protocolli di livello superiore.

Albero: struttura composta da nodi collegati da archi, in cui ogni nodo ha al più un arco in uscita.

Gli apparati bridge e switch immagazzinano e inoltrano le trame memorizzando gli indirizzi MAC delle destinazioni e scegliendo la porta da cui inoltrare la trama in modo "intelligente". Essi applicano un algoritmo di **spanning tree** per generare una struttura logica ad **albero** in base alla quale inoltrare le trame, evitando così cicli e sovraccarichi della rete.
Si differenziano, a seconda se operano su due porte o più porte, un bridge e uno switch.

I **router** sono apparati di livello rete (3) essenziali per la costruzione di reti geografiche e per suddividere (in gergo tecnico, "partizionare") reti locali composte da un numero elevato di host in reti di dimensioni più limitate.

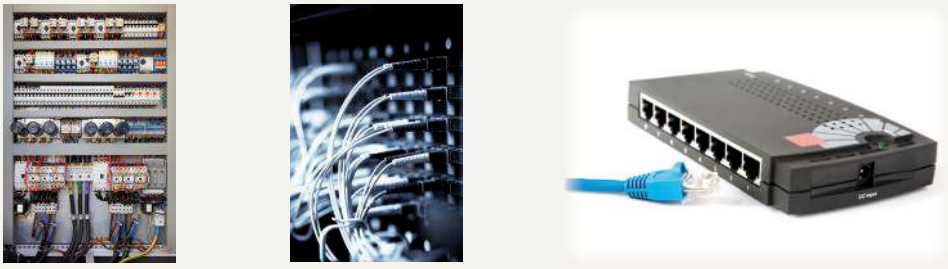


Fig. 2: Da sinistra, switch, router e hub.

I router sono in grado di interconnettersi sia a reti locali sia a reti geografiche e di scegliere il percorso da far seguire a un pacchetto che da una sorgente deve raggiungere una destinazione; per compiere questa scelta, si avvalgono di specifici protocolli, denominati **protocolli di routing**.

I **gateway** sono apparati di livello applicazione (7), si differenziano dai router in quanto sono in grado, per assumere decisioni riguardo all'instradamento di un pacchetto, di analizzare non solo l'intestazione ma anche il contenuto.

AULADIGITALE
Approfondimento
• Spam

Per esempio, i gateway di posta elettronica sono in grado di analizzare le caratteristiche di un messaggio email per scegliere come gestirlo e instradarlo verso le opportune destinazioni o filtrarlo classificandolo come "spam".

1.6 Internet

Internet: il termine vuole indicare che si tratta di una *rete di reti*.

Ideata in ambito universitario per diffondere informazioni scientifiche a una comunità ristretta, **Internet** è ora una rete geografica su scala mondiale ad accesso pubblico, ovvero un sistema di reti interconnesse accessibile a tutti gli utenti senza vincoli; negli ultimi anni è divenuta sempre più strumento di comunicazione globale, superando il miliardo di utenti connessi nel mondo.

Inoltre offre come applicazione servizi di vario genere, tra cui il popolare World

Wide Web e la posta elettronica; tali servizi sono di tipo **client-server**: un terminale, denominato **server**, fornisce i servizi a utenti/clienti previa richiesta esplicita da parte di terminali **client**.

Internet Service Provider: fornitori di servizi Internet.

Gli **Internet Service Provider** sono gestori privati che forniscono il servizio di connettività a Internet alle utenze private; la rete degli Internet Service Provider è organizzata con criterio gerarchico e sfrutta collegamenti veloci in fibra ottica per garantire la connettività a livello fisico.

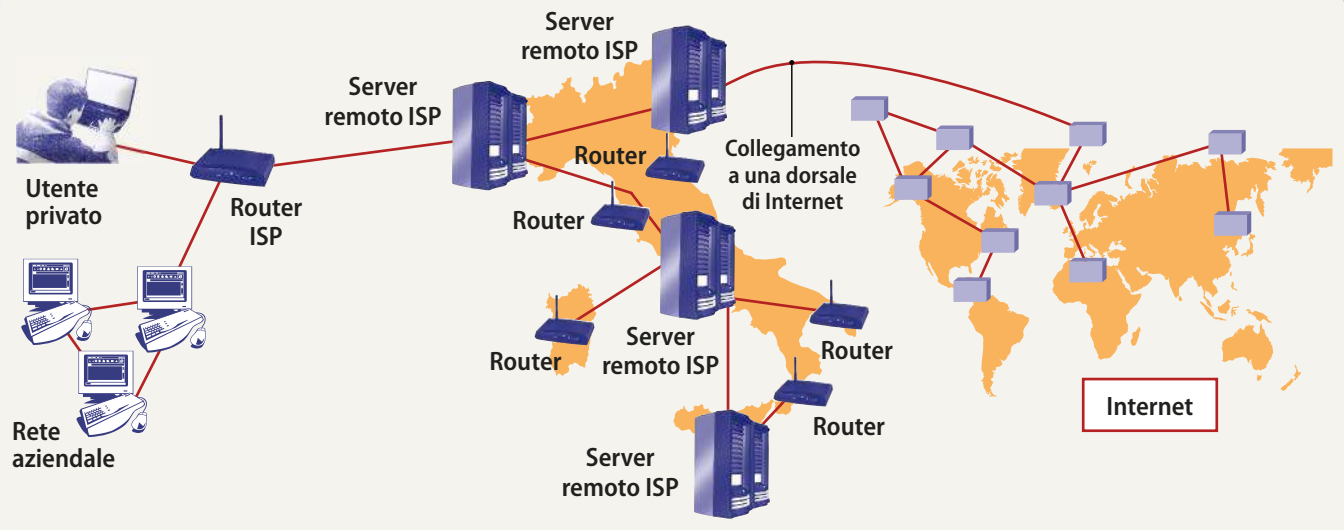


Fig. 3: Rete di ISP.

Internet si basa su una collezione di protocolli, che la rendono versatile e funzionale; al tradizionale modello a strati ISO/OSI si sostituisce un modello semplificato composto di tre strati, denominato **Internet Protocol Suite** (tab. 1), che ingloba tutte le funzionalità principali, lasciando a protocolli e algoritmi il compito di definire i servizi offerti ai singoli livelli.
L'Internet Protocol Suite non specifica il livello fisico e il collegamento; prevede invece l'uso di IP e TCP come protocolli principali di livello rete (3) e livello trasporto (4). L'infrastruttura di Internet è quindi uno standard indipendente dai singoli apparati o software proprietari ed è in grado di connettere reti nazionali e sovranazionali.

Tab. 1

ISO/OSI		Internet Protocol
Livello 7: Applicazione		Applicazione (Protocolli per Web, posta elettronica, …)
Livello 6: Presentazione		
Livello 5: Sessione		
Livello 4: Trasporto		TCP/UDP
Livello 3: Rete		IP + altri
Livello 2: Collegamento		Non specificati
Livello 1: Fisico		

A livello rete, i pacchetti viaggiano su Internet tra sorgente e destinazione passando per un certo numero di nodi intermedi (denominati anche **hop**); il protocollo IP applica una **commutazione di pacchetto** grazie alla quale singoli pacchetti possono condividere un cammino con altri pacchetti, eventualmente abbinati a sorgenti e destinatari diversi.

La **commutazione di pacchetto** è un metodo di commutazione con il quale per ogni pacchetto e per ogni hop compiuto nella rete si sceglie l'hop successivo verso la destinazione in base alle condizioni della rete.

La commutazione di pacchetto evita di riservare risorse dedicate a una specifica comunicazione e di prevedere un percorso dedicato tra sorgente e destinatario, come accadeva, per esempio, nella rete telefonica tradizionale.
Il percorso del singolo pacchetto è adattato al reale stato della rete, associando eventualmente percorsi differenti a pacchetti per la medesima destinazione.

Indirizzamento IP

Il protocollo IP è il protocollo per eccellenza di livello rete ISO/OSI (livello 3); la sua applicazione in Internet ha reso IP uno standard di riferimento per tutte le reti, pubbliche o private, che si interfacciano con la rete Internet.

IP permette di gestire l'indirizzamento degli host appartenenti a reti telematiche; a ciascun host o apparato viene assegnato un **indirizzo binario univoco** su 32 bit. Se un apparato di rete (per esempio, un bridge o uno switch) possiede più porte, ad esso viene assegnato un indirizzo differente per ciascuna porta; se un host è interconnesso a reti IP di differenti tecnologie, ad esso viene associato un indirizzo IP per ciascuna rete.

Per comodità di lettura, gli indirizzi IP, nella più comune versione del protocollo (IPv4), sono rappresentati in ottetti (8 bit = 1 byte), che vengono rappresentati in base 10 e separati da un punto.

ESEMPIO L'indirizzo IP, rappresentato nel formato standard 128.4.5.3, equivale in formato binario a:

10000000 00000100 **00000101** 00000011

Leggendo da sinistra a destra, i primi 8 bit convertiti in decimale corrispondono a 128 in base 10, i successivi 8 bit a 4 e gli ultimi due ottetti, rispettivamente, a 5 e a 3.

L'assegnazione degli indirizzi IP può essere:
- *statica*, ovvero attribuita manualmente dall'esperto;
- *dinamica*, assegnata da una procedura automatica o semi-automatica di configurazione di rete.

UTILE A SAPERSI

IP e MAC

L'indirizzo IP è differente dall'indirizzo MAC assegnato a livello collegamento (2), in quanto l'indirizzo MAC è associato a ciascuna scheda di rete ed è immutabile mentre l'indirizzo IP è un indirizzo che può variare nel tempo.

Gli indirizzi vengono scelti oculatamente in modo da semplificare la ricerca di una destinazione. Ogni indirizzo IP è suddiviso in due parti: l'identificatore della rete (**net ID**) e l'identificatore dell'host (**host ID**). La presenza dell'identificatore di rete consente di raggruppare gli indirizzi degli host appartenenti ad una **sottorete logica**; la sottorete che accorpa host e apparati aventi proprietà (logistiche o spaziali) comuni. Normalmente si associano le sottoreti logiche alle **reti locali**.

La **rete locale** è una porzione di rete che racchiude solo host o apparati di livello 2 tra loro interconnessi.
La **sottorete logica IP** è l'insieme di host e apparati di una rete con tecnologia IP aventi il medesimo identificatore di rete (net ID).

Nella notazione standard a fianco dell'indirizzo è indicato il numero di bit che, leggendo da sinistra a destra, fanno parte del net ID; la restante parte (a destra del net ID) andrà a comporre l'host ID.

ESEMPIO Nell'indirizzo IP 128.4.5.3/ 24 il numero 24 a fianco dell'indirizzo IP vero e proprio indica che i primi 24 bit da sinistra dell'indirizzo IP, in rosso nella rappresentazione binaria, compongono l'identificatore di rete, mentre i restanti 8, in blu compongono l'identificatore dell'host:

10000000 00000100 00000101 00000011
net ID host ID

Nella rappresentazione decimale 128.4.5.3 i primi tre numeri decimali corrispondono all'identificatore di rete, mentre l'ultimo numero rappresenta l'identificatore di host.
Per convenzione, gli indirizzi con host ID impostato a zero (nell'esempio, gli ultimi 8 bit uguali a zero) non identificano un singolo host, ma sono utilizzati per identificare l'intera sottorete.
Per esempio, 128.4.5.0/24 identifica la sottorete che comprende gli indirizzi da 128.4.5.1 a 128.4.5.255.

Subnet mask: "maschera della sottorete" viene spesso abbreviato con il termine **netmask**.

Un'altra possibile notazione per distinguere tra net ID e host ID in un indirizzo IP è l'uso della **subnet mask**.

La subnet mask è il numero binario di 32 bit in cui i primi *n* bit (da sinistra) sono impostati a 1 e identificano la porzione dell'indirizzo IP associata all'identificatore di rete, mentre i restanti assumono valore 0 e identificano l'host ID. Per ottenere la porzione di rete di un indirizzo IP data la sua subnet mask, è sufficiente confrontare bit a bit, leggendo da sinistra a destra, e selezionare quei bit dell'indirizzo IP che sono associati ad un 1 nella subnet mask.

Il confronto corrisponde a un'operazione binaria di AND tra l'indirizzo IP e la subnet mask.

ESEMPIO Riprendendo l'esempio precedente, la subnet mask è:

11111111 11111111 11111111 00000000

Per ricavare il net ID è sufficiente fare la selezione dei bit aventi il corrispondente nella subnet mask settato a 1:

10000000 00000100 00000101 00000011
AND
11111111 11111111 11111111 00000000
=
10000000 00000100 00000101 00000000

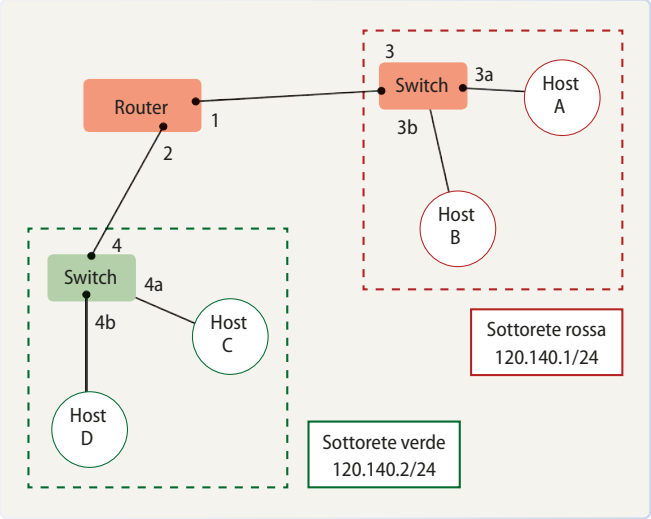
La porzione in rosso del risultato è il net ID relativo all'indirizzo IP considerato (128.4.5.3/24).

Apparati di rete e sottoreti

Un apparato di livello 2 (per esempio, uno switch) ha un indirizzo IP per ciascuna porta di connessione con altri apparati o host. Siccome tutte le porte appartengono alla medesima rete locale, gli indirizzi assegnati a ciascuna porta dello switch e agli host rispettivamente collegati saranno logicamente abbinati

alla stessa sottorete, quindi avranno il medesimo identificatore di rete ma un differente identificatore di host.
I router sono apparati di livello rete (3) che servono a interconnettere reti locali differenti; quindi gli indirizzi IP associati a porte diverse del router hanno identificatori di rete differenti.

Fig. 4: Reti e sottoreti.



Porta	Indirizzo IP	Porta	Indirizzo IP
1	120.140.1.1/24	2	120.140.2.1/24
3	120.140.1.2/24	4	120.140.2.2/24
3a	120.140.1.3/24	4a	120.140.2.3/24
3b	120.140.1.4/24	4b	120.140.2.4/24
host A	120.140.1.5/24	host C	120.140.2.5/24
host B	120.140.1.6/24	host D	120.140.2.6/24

ESEMPIO In figura è rappresentato un primo esempio di rete basata su tecnologia IP. La presenza di un router partiziona la rete in due sottoreti distinte, identificate rispettivamente dai colori rosso e verde. Entrambe le sottoreti hanno netmask 255.255.255.0, ovvero i primi 24 bit caratterizzano l'identificatore di rete, mentre i restanti 8 identificano gli host presenti.
La sottorete rossa è associata all'identificatore di rete 120.140.1 (che identifica la sottorete 120.140.1.0/24) mentre quella verde è associata a 120.140.2 (sottorete 120.140.2.0/24).

Una porzione di rete come quella rappresentata in rosso in figura, composta da host collegati da uno switch (apparato di livello 2), è un esempio di rete locale i cui indirizzi IP sono stati assegnati in modo da abbinare la sottorete logica associata 120.140.1/24 ai rispettivi host e apparati di rete.

Sicurezza informatica

Router: apparati di livello rete (3) dediti all'instradamento del traffico verso le rispettive destinazioni.

I **router** che connettono una sottorete o una rete alla rete geografica esterna devono essere provvisti di meccanismi di filtraggio del traffico in ingresso e in uscita, per garantire la riservatezza dei dati scambiati e la sicurezza della rete nei confronti di attacchi informatici.

Firewall: "muro antifuoco".

Appositi apparati o strumenti software e/o hardware installati sui router, denominati **firewall**, permettono il controllo degli accessi da/verso l'esterno e il monitoraggio e filtraggio del traffico in ingresso e in uscita.

Firewall è un apparato di rete, hardware o software, in grado di monitorare il traffico e gli accessi a un rete.

Sono comunemente denominate **Intranet** le reti private, costruite con tecnologia Internet, in cui l'accesso è interdetto o limitato mediante firewall.
La sicurezza informatica deve proteggere le informazioni contenute nelle basi di dati aziendali. Per esempio, le macchine di monitoraggio della produzione e di

DBMS: sistemi per la gestione delle basi di dati, collezioni organizzate di dati.

controllo di qualità forniscono flussi di dati continui o intermittenti che devono essere processati; essi vengono memorizzati in opportuni server dislocati all'interno della rete Intranet aziendale. La gestione, la memorizzazione e l'aggiornamento dei dati sono realizzati mediante opportuni **DBMS.**

L'accesso alle basi di dati aziendali va gestito da esperti informatici mediante strumenti di configurazione forniti dal DBMS. Il diritto di accesso (in lettura e scrittura) ai dati immagazzinati nella base di dati aziendale può essere gestito in modo gerarchico in funzione del reparto di appartenenza o del ruolo assunto da ciascun dipendente aziendale o stakeholder.

La Intranet aziendale deve essere opportunamente configurata mediante meccanismi di controllo per limitare l'accesso degli utenti ai singoli host e ai dati immagazzinati nel server. Il controllo di accesso può essere effettuato mediante l'assegnazione di nomi utente e password al personale.

I livelli di sicurezza della Intranet devono prevedere controlli specifici sui servizi Internet principali, come la posta elettronica o il Web.

Assegnazione degli indirizzi IP e instradamento del traffico a livello rete

Un problema fondamentale è l'assegnazione degli indirizzi IP.
Per le reti private è possibile utilizzare gruppi limitati di indirizzi noti di cui, per convenzione, non si fa uso nelle reti pubbliche. Esempi di indirizzi IP utili per indirizzamenti privati sono:

- 10.0.0.0/16, ovvero gli indirizzi compresi tra 10.0.0.1 e 10.0.255.255;
- 192.168.0.0/16, ovvero gli indirizzi compresi tra 192.168.0.1 e 192.168.255.255;
- 172.16.0.0/11, ovvero gli indirizzi compresi tra 172.16.0.1 e 172.31.255.255.

Per le reti pubbliche la problematica di assegnare correttamente gli indirizzi IP pubblici risulta più complessa, in quanto reti geografiche come Internet possono includere miliardi di host e il numero di indirizzi IP disponibili è limitato.
Si è stabilito quindi un criterio di classificazione che permette di assegnare gli indirizzi IP e le relative sottoreti in base alla classe d'importanza della destinazione; le 5 classi scelte (A, B, C, D, E) identificavano classi di indirizzi di tipologia e importanza differenti. Le sottoreti più autorevoli (per esempio, quelle relative alla classe A) possiedono un identificatore di rete (net ID) più basso al fine di raggruppare un maggior numero di host all'interno della medesima sottorete. Per esempio, gli indirizzi di classe A compresi tra 50.0.0.0 e 107.255.255 con subnet mask 255.0.0.0 devono indirizzare i grandi snodi di traffico Internet su scala mondiale. Questo procedimento porta però a uno spreco di indirizzi perché gran parte degli host sono di categoria inferiore e la presenza eventuale di un numero limitato di host in una sottorete pubblica autorevole (per esempio, 100 host nella sottorete 50.0.0.0/8) rende la restante parte di indirizzi inutilizzabile (gli indirizzi da 50.0.0.101 a 50.255.255.254).

Le problematiche di instradamento del traffico da sorgente a destinazione sono strettamente legate alla tipologia di indirizzamento IP scelto. Assegnare indirizzi IP distinti a ciascun host sarebbe impraticabile; inoltre, host vicini sono di solito

interessati a traffico comune. Aggregare le destinazioni secondo criteri gerarchici permette di memorizzare in modo compatto nei router l'informazione su come instradare i pacchetti che arrivano verso le opportune destinazioni.

UTILE A SAPERSI

IP versione 6

Una parziale soluzione al problema della carenza di indirizzi IP è stato il passaggio da IP versione 4 (IPv4) a IP versione 6 (IPv6). La nuova versione del protocollo permette, tra l'altro, una maggiore capacità di indirizzamento, in quanto adotta indirizzi estesi su 128 bit. Le problematiche principali legate a IPv6 sono dovute alla complessa compatibilità con la versione precedente e alla necessità di aggiornamento di apparati e software che adottano la precedente versione.

La procedura di commutazione di pacchetto applicata in Internet prevede che il percorso di un pacchetto verso una destinazione venga scelto passo passo e adattato alle condizioni della rete. Questo implica che, in linea teorica, ciascun router intermedio dovrebbe aver memorizzato al suo interno gli indirizzi IP relativi a miliardi di destinazioni. In realtà, la conoscenza di un router è *miope*, ovvero conosce bene il suo vicinato, ma meno dettagliatamente il resto del mondo.

Approfondimento
• L'instradamento del traffico

La facoltà di aggregare le destinazioni possibili in sottoreti permette di memorizzare in ciascun router in modo compatto l'informazione su come raggiungere destinazioni affini, eventualmente mediante il passaggio attraverso nodi intermedi. Tale informazione viene raccolta in opportune **tabelle d'instradamento** memorizzate all'interno di ciascun router; un pacchetto verrà quindi indirizzato ("instradato") nella giusta direzione in base alle informazioni in esse contenute.

I protocolli che creano, aggiornano e gestiscono le tabelle d'instradamento sono protocolli di livello rete (3), denominati **protocolli di routing**.

Il **protocollo di routing** è un protocollo di livello rete che armonizza e ottimizza la procedura di creazione e uso delle tabelle di instradamento nei vari router della rete, prevedendo sincronizzazioni, aggiornamenti, armonizzazioni e scelte vincolate dalle politiche dei gestori di rete (ISP).

Le scelte politiche di gestione della rete, automatizzate e configurabili in modo limitato dall'esperto nel caso dei protocolli di routing più semplici, divengono strettamente dipendenti dalle politiche di amministrazione e gestione dei Service Provider nel caso delle reti geografiche o metropolitane.

L'aggiornamento periodico delle tabelle di instradamento è fondamentale in quanto un eventuale guasto o temporaneo malfunzionamento potrebbe compromettere la ricezione di traffico da/verso un host o un insieme di host. Sono dunque previste tecniche di reazione ai guasti e uso della ridondanza per limitare al minimo il disservizio causato da eventuali guasti.

Rete locale: termine che indica il raggruppamento degli host e degli apparati aventi il medesimo identificatore di rete (net ID).

Protocollo ARP e consegna diretta

La consegna di pacchetti destinati a host situati nella medesima **rete locale** avviene mediante **consegna diretta**. Un router che deve gestire un pacchetto in entrata verifica l'associazione tra l'identificatore di rete del pacchetto e quelli

delle sottoreti logiche abbinate alle sue porte; qualora riscontri una corrispondenza, instrada il pacchetto a destinazione mediante *consegna diretta*.

Analogamente al caso delle reti geografiche, l'informazione su come raggiungere una destinazione mediante consegna diretta viene scambiata tra gli apparati interni alla **rete locale** e memorizzata in apposite tabelle, denominate **tabelle di ARP**. Le destinazioni sono identificate da uno specifico indirizzo, denominato **indirizzo MAC**, che permette di distinguere i dispositivi differenti collegati alla medesima rete locale e quindi aventi il medesimo indirizzo IP.
Un protocollo analogo, denominato **Reverse Address Resolution Protocol (RARP)** permette di gestire la problematica inversa ovvero associare un indirizzo IP al rispettivo MAC locale per poter, per esempio, inoltrare il traffico locale sulla rete Internet.

Approfondimento
- Il protocollo Address Resolution Protocol (ARP)
- Il Network Address Traslator (NAT)

ARP request - ARP reply: rispettivamente "Richiesta ARP" e "Risposta ARP".

1.7 Caso di studio: una rete aziendale

L'avvento delle reti telematiche e delle telecomunicazioni ha permesso di compiere in ambito aziendale un passo importante verso l'internazionalizzazione dei mercati e la globalizzazione. Molte aziende affidano oggi gran parte delle loro attività commerciali e gestionali a servizi telematici che permettono l'interazione con clienti e fornitori remoti.

Come introduzione alle principali problematiche relative alla progettazione di una rete aziendale, sulla base dei concetti presentati nel corso di questa Unità, viene di seguito analizzato un caso di studio riferito alla rete aziendale di un'azienda dolciaria multinazionale.

Situazione operativa

La SweetCookies spa, azienda dolciaria multinazionale, possiede più stabilimenti dislocati in diversi continenti. Ciascun stabilimento è organizzato in reparti; oltre a quelli produttivi sono presenti i reparti dedicati ai rapporti con i fornitori, al controllo qualità, ai rapporti con la clientela.
La sede centrale dell'azienda comprende i reparti relativi a marketing, amministrazione e finanza.

Caratteristiche della rete

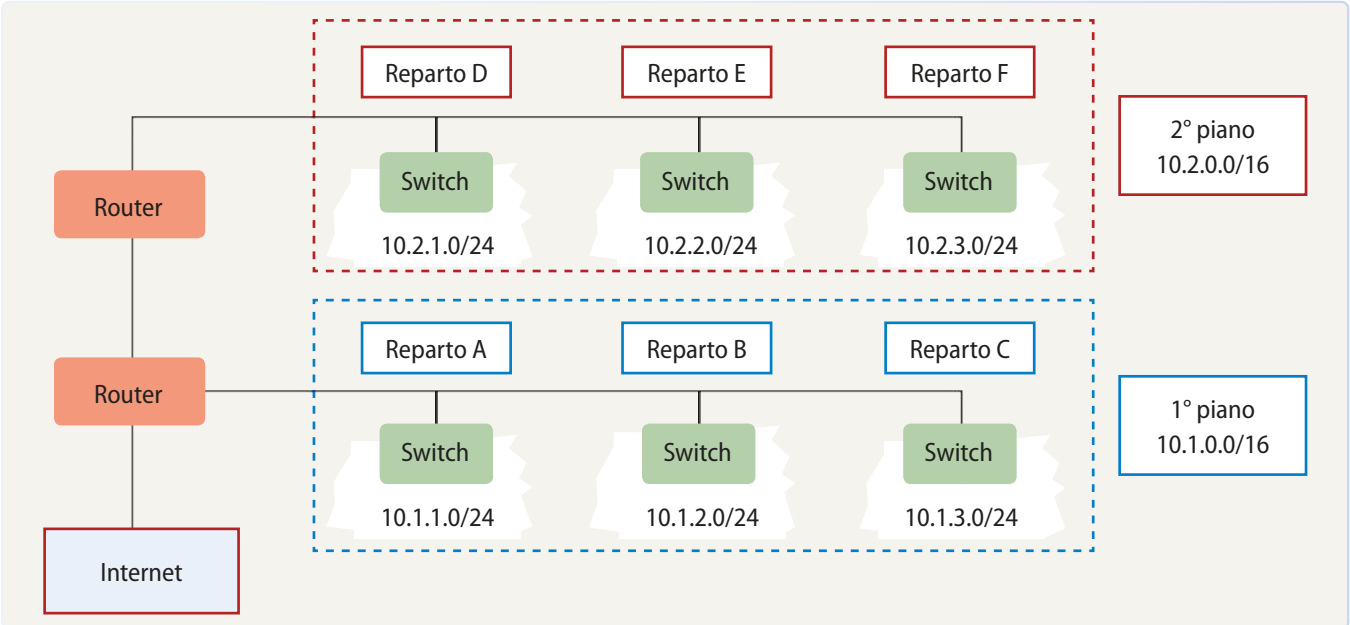
I diversi stabilimenti sono collegati alla rete Internet tramite appositi router che instradano il traffico da/verso le opportune destinazioni.
Il collegamento tra la rete centrale e i vari stabilimenti su rete geografica è concordata dall'azienda con specifici Internet Service Provider (ISP), che forniscono la connettività e soddisfano eventuali richieste di qualità del servizio e affidabilità del collegamento, compatibilmente con la tecnologia impiegata e gli accordi stipulati.
Ogni stabilimento racchiude potenzialmente centinaia di host:
- PC fissi e portatili dei dipendenti;
- stampanti e apparati di rete;
- apparati che forniscono dati per il controllo di qualità e il monitoraggio della produzione;
- server Web che gestiscono la posta elettronica, il sito Web dell'azienda, le vendite online attraverso strumenti di **e-commerce**.

E-commerce: termine che identifica le transazioni commerciali realizzate per via telematica.

Piano di indirizzamento e routing

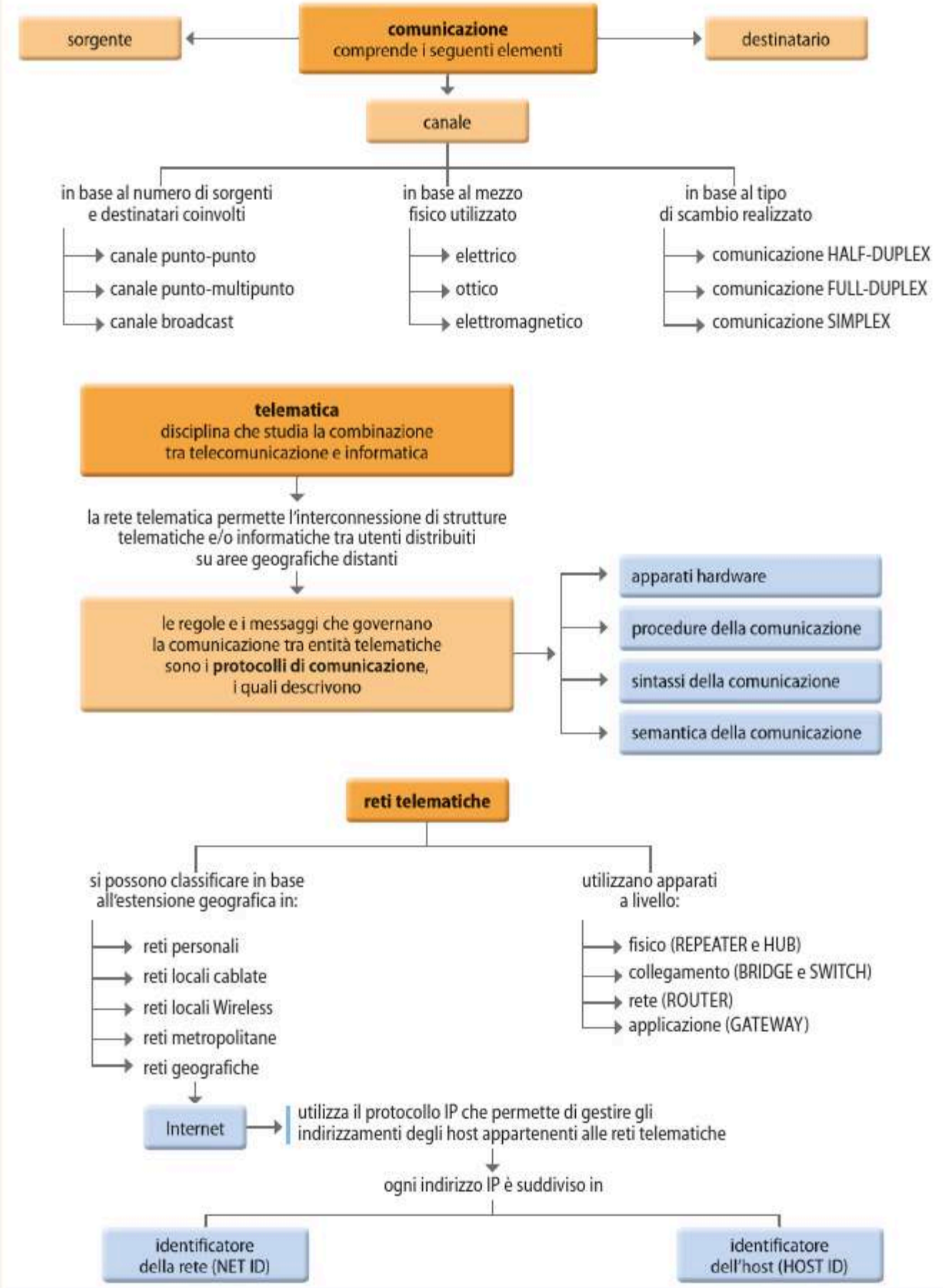
Le postazioni fisse dei dipendenti di uno stabilimento sono organizzate in reparti. I reparti interni comunicano mediante una rete locale cablata basata sulle tecnologie Ethernet e IP; a ciascun reparto viene associata una sottorete logica univoca su 24 bit.
Per esempio, il reparto A racchiuderà gli indirizzi 10.0.1.0/24, il reparto B racchiuderà gli indirizzi 10.0.2.0/24 ecc.
In questo modo è possibile indirizzare, per ciascun reparto fino a un massimo di 253 host differenti (escludendo i due host ID con tutti i bit a 0 e a 1 che, per convenzione, non vengono assegnati). Se lo stabilimento racchiude un numero considerevole di reparti, per esempio organizzati su più piani, è possibile organizzare il piano di indirizzamento su due livelli:

- un primo livello aggrega tutti gli indirizzi IP relativi a host e apparati appartenenti al medesimo piano. Per esempio, è possibile associare la sottorete logica 10.1.0.0/16 agli host del primo piano, 10.2.0.0/16 a quelli del secondo piano ecc.;
- un secondo livello permette di aggregare gli host di ciascun piano in base al reparto. Per esempio, la sottorete logica 10.1.1.0/24 aggregherà tutti gli host dislocati fisicamente al primo piano nel primo reparto (per esempio, controllo di qualità).



Gli host relativi a ciascun reparto sono collegati fisicamente ad uno switch, che permette di gestire e inoltrare il traffico nella rete locale. Gli switch sono collegati a un router che regola l'interconnessione alla rete pubblica.
Qualora la limitata ampiezza dello stabilimento permetta la presenza di un router centralizzato di interconnessione con la rete pubblica, è opportuno prevedere meccanismi di backup e la presenza di un secondo router di backup, che consente il funzionamento della rete in caso di guasti o attacchi informatici.
Qualora lo stabilimento comprenda più piani è consigliabile utilizzare un router per piano e configurare i router mediante appositi protocolli di routing che instradino il traffico da/verso la rete aziendale. In questo modo, è possibile bilanciare il traffico scambiato tra i vari reparti e quello proveniente dall'esterno, ottimizzando quindi l'uso della rete.

MAPPA CONCETTUALE



VERIFICA DELLE CONOSCENZE

1. Vero o Falso

Indica se le seguenti affermazioni sono vere o false; in quest'ultimo caso spiega sul quaderno il perché.

		V	F
1.	Il canale trasmissivo è un mezzo utilizzato nella trasmissione delle informazioni		
2.	La trasmissione analogica trasmette segnali discreti		
3.	Il Binary Unit può assumere esclusivamente due valori		
4.	Il demodulatore trasforma il segnale elettronico in una sequenza di dati che il destinatario è in grado di utilizzare		
5.	Nella comunicazione punto-multipunto una sorgente comunica con più destinatari		
6.	Nella comunicazione broadcast più sorgenti comunicano con più destinatari		
7.	Nella comunicazione simplex il trasmettitore non può diventare ricevente		
8.	I terminali sono computer collegati in rete		
9.	Le reti personali possono utilizzare canali basati su collegamenti USB		
10.	Il canale di comunicazione non è condiviso tra i partecipanti nelle reti locali		
11.	La rete Internet è un esempio di rete metropolitana		
12.	Gli switch rientrano tra gli apparati di livello collegamento (2)		
13.	Con il termine host si indica un terminale collegato alla rete Internet		
14.	I router consentono la interconnessione di reti locali differenti		
15.	Uno switch ha un indirizzo IP per ogni porta		
16.	I firewall sono formati da hardware o software che permettono di monitorare il traffico e gli accessi ad una rete		
17.	La rete Intranet è una rete pubblica con accesso limitato mediante firewall		
18.	La consegna diretta è realizzata quando il destinatario appartiene ad una rete locale a cui è collegato il router		

2. Correlazione

Stabilisci le corrispondenze logiche tra circolazione stradale e canali di comunicazione.

1.	Senso unico	**A.**	Full-duplex
2.	Senso unico alternato	**B.**	Half-duplex
3.	Doppio senso	**C.**	Simplex

1	2	3
___	___	___

3. Test a scelta multipla

Indica la risposta esatta (alcuni quesiti possono avere più risposte esatte).

a. Gli elementi della comunicazione sono:

1 canale, elettromagnetico e destinatario
2 canale, ottico e destinatario
3 sorgente, canale e destinatario
4 sorgente, ottico e destinatario

b. La trasmissione digitale trasmette:

1 segnali continui
2 segnali saltuari
3 segnali intensi
4 segnali discreti

c. Il modulatore:
1. trasforma i dati in un codice binario
2. trasforma i dati in segnali elettrici
3. consente l'interpretazione dei dati
4. corregge la sequenza di dati errati

d. Tra le principali caratteristiche dei canali trasmissivi si enumerano:
1. velocità di trasmissione ideale
2. velocità di trasmissione reale
3. dimensione della memoria centrale
4. rapporto tra la quantità di dati trasmessi e la quantità di dati ricevuti

e. Nella comunicazione half-duplex le entità comunicanti:
1. assumono il ruolo non modificabile di trasmettitore o di ricevitore
2. assumono il ruolo modificabile di trasmettitore o di ricevitore
3. possono trasmettere e ricevere contemporaneamente
4. possono trasmettere più segnali

f. I protocolli di comunicazione descrivono:
1. le norme su cui si basa la comunicazione
2. il formato dei dati
3. le procedure della comunicazione
4. la semantica della comunicazione

g. Le reti cablate:
1. sfruttano canali elettrici o in fibra ottica
2. utilizzano segnali elettromagnetici
3. non consentono l'integrabilità con le reti wireless
4. non consentono l'interfacciabilità con le reti geografiche

h. I router sono apparati:
1. a livello fisico
2. a livello di collegamento
3. a livello rete
4. a livello applicazione

i. Il protocollo IP:
1. è applicato in Internet
2. gestisce l'indirizzamento degli host appartenenti a reti telematiche
3. è un riferimento esclusivo per le reti pubbliche
4. è un riferimento esclusivo per le reti private

l. L'indirizzo IP:
1. include anche l'identificatore della rete
2. è formato solo dall'identificatore dell'host
3. è statico o dinamico
4. è sempre dinamico

m. La tabella d'instradamento indica:
1. una descrizione del traffico da inviare
2. gli indirizzi MAC del traffico da inviare
3. la porta da cui arriva il traffico
4. dove inoltrare il traffico