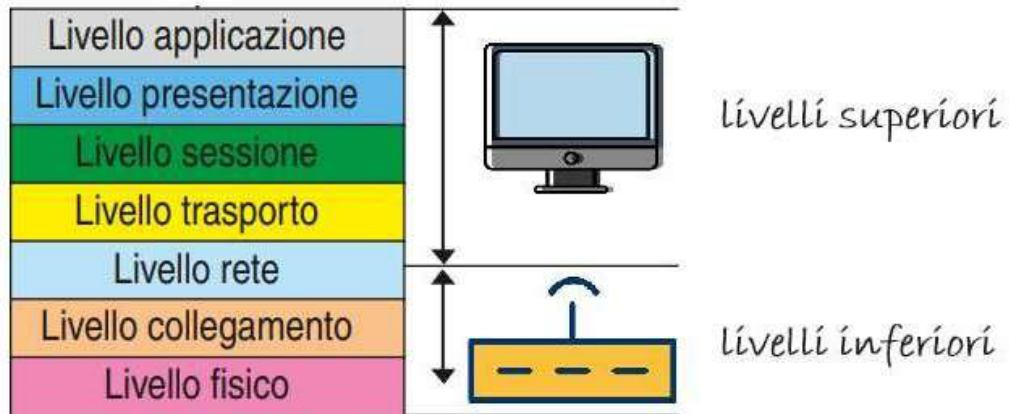


# Introduzione al Modello OSI



- Quando parliamo di comunicazione tra computer, ci riferiamo all'interazione e allo scambio di dati tra diverse macchine
- Il suo obiettivo principale è garantire che i dispositivi di diverse aziende possano comunicare tra loro in modo fluido e trasparente
- Il Modello OSI cerca di fare lo stesso per i computer: fornire un "linguaggio universale" per la comunicazione tra dispositivi

# Struttura del Modello OSI



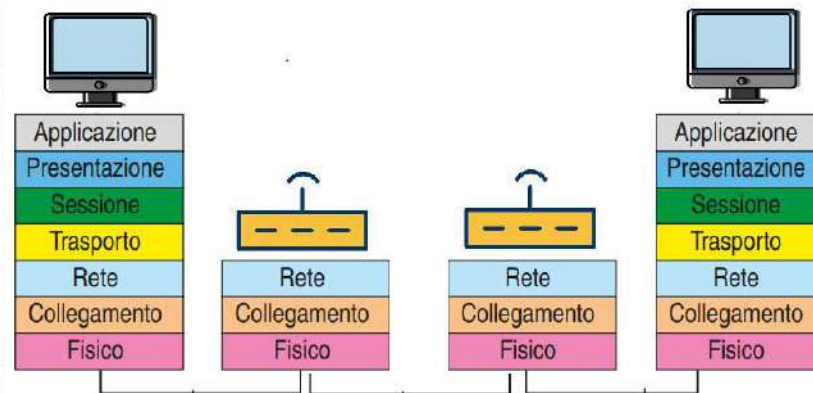
Il Modello OSI è organizzato in **sette livelli**, ognuno dei quali ha una funzione specifica. Questi livelli sono raggruppati in due categorie principali:

- **Livelli inferiori:** Questi livelli gestiscono la comunicazione e il trasporto dei dati tra sistemi
- **Livelli superiori:** Questi livelli si occupano delle applicazioni e dei servizi che gli utenti finali vedono e utilizzano



# Tipologie di Dispositivi nel Modello OSI

- **Sistema terminale:** Questi dispositivi sono l'origine o la destinazione finale dei dati
- **Sistema intermedio:** Questi dispositivi facilitano la comunicazione tra sistemi terminali

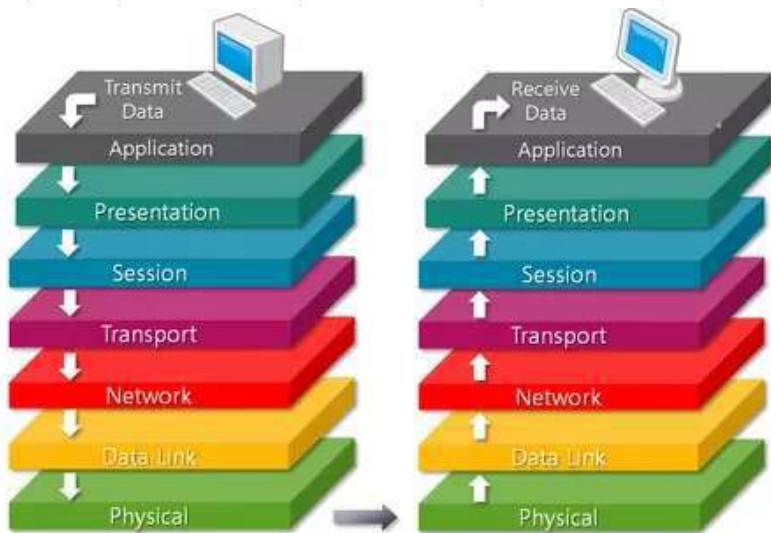




# Descrizione Funzionale dei Livelli OSI

- **Ogni livello del Modello OSI ha un compito unico nel processo di comunicazione**
- Nel corso delle prossime lezioni, approfondiremo ciascuno di questi livelli, esaminando le loro funzioni specifiche e come contribuiscono all'intero processo di comunicazione

# Livelli OSI



**Ogni strato comunica solo con gli strati adiacenti, inviando dati al livello sottostante e ricevendo dati da quello superiore**

- 1. *Strato fisico*: si occupa della trasmissione e ricezione dei bit grezzi su un canale di comunicazione.
- 2. *Strato di collegamento*: costruisce e gestisce link tra nodi adiacenti.
- 3. *Strato di rete*: inoltra i pacchetti tra i nodi sulla rete.
- 4. *Strato di trasporto*: fornisce comunicazione tra le applicazioni sui nodi finali.
- 5. *Strato di sessione*: gestisce le sessioni di comunicazione.
- 6. *Strato di presentazione*: si occupa della rappresentazione dei dati.
- 7. *Strato di applicazione*: fornisce servizi di rete agli utenti finali.



# Comprendere il Livello Fisico


- Il mondo della comunicazione tra dispositivi è vasto e complesso
- Tuttavia, prima che due dispositivi possano "parlare" tra loro, devono stabilire una **connessione fisica**
- Questa connessione è ciò che forma la base di tutte le comunicazioni digitali e viene gestita dal livello fisico

## Scopo



- Il livello fisico non si preoccupa del significato o della struttura dei dati. Si concentra solo sulla conversione dei dati in segnali e sulla loro trasmissione.



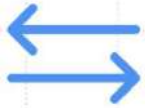


Il livello fisico si occupa della trasmissione e della ricezione di sequenze di bit non strutturate attraverso un canale di comunicazione

Questi bit rappresentano dati che i dispositivi, come i computer, desiderano condividere tra loro

Vengono convertiti in segnali, che possono essere elettrici, ottici o radio, a seconda del mezzo di comunicazione utilizzato

# Componenti chiave del Livello Fisico



## Dispositivi di Interfacciamento:

Questi sono dispositivi specializzati, come le porte seriali, che fungono da intermediari tra il dispositivo che invia i dati e il mezzo di comunicazione

## Caratteristiche Meccaniche:

Riguardano l'interfaccia fisica tra il dispositivo sorgente e il mezzo di comunicazione

## Caratteristiche dei Segnali:

Queste definiscono come i dati vengono convertiti in segnali

## Procedura di Connessione e Disconnessione:

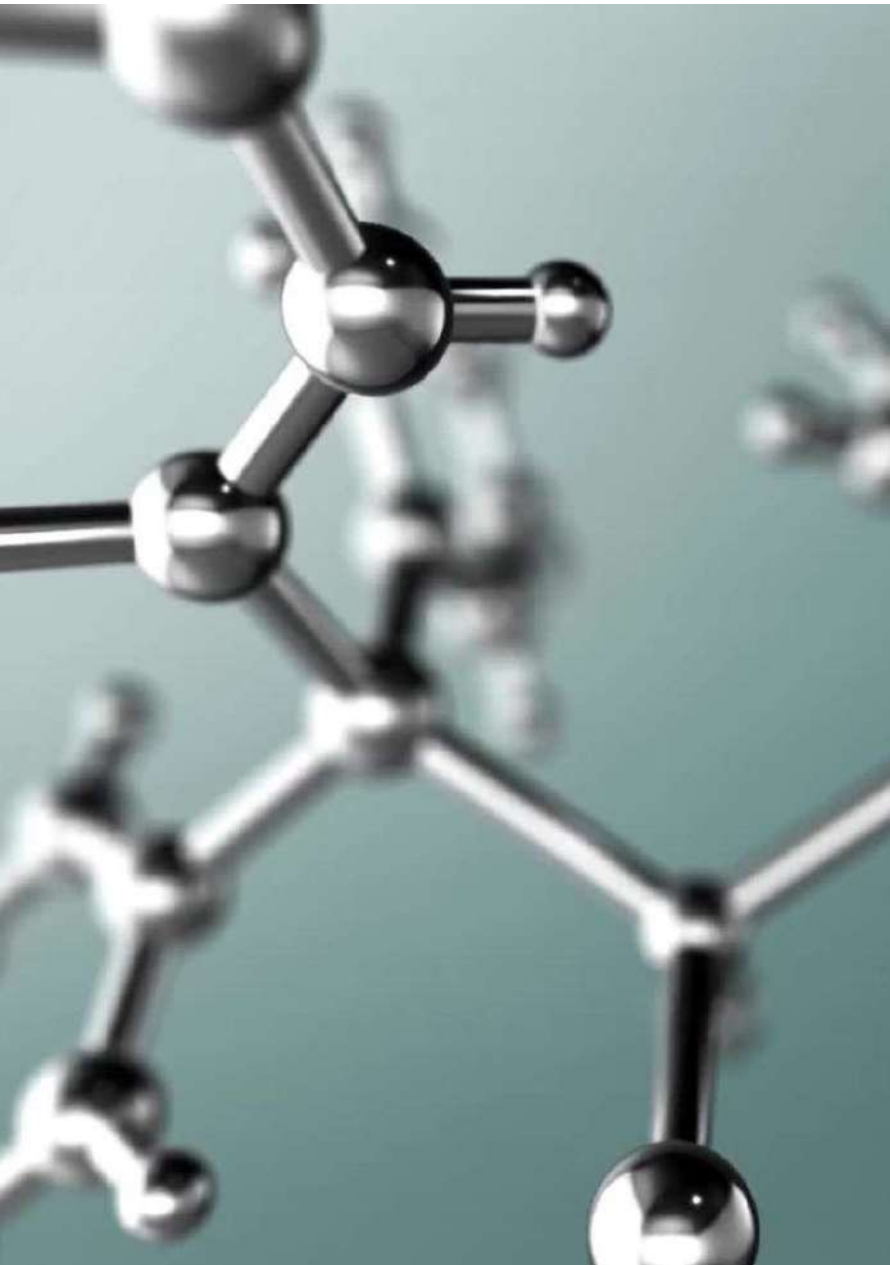
Definiscono come viene stabilita e interrotta una connessione tra due dispositivi

## Specifiche dei Cavi e Connettori:

Queste sono le specifiche fisiche del mezzo di comunicazione utilizzato

## Operazioni di Multiplexazione e Modulazione:

Queste operazioni permettono l'invio efficiente di segnali attraverso il mezzo di comunicazione



# Conclusione

- Il livello fisico è essenziale per qualsiasi forma di comunicazione digitale
- Anche se potrebbe sembrare meno "glamour" di altri livelli che gestiscono applicazioni e servizi visibili all'utente, senza un livello fisico robusto e funzionante, la comunicazione semplicemente non avverrebbe
- È la fondamentale "autostrada" su cui viaggiano tutti i nostri dati

# Esplorando il Livello di Collegamento (Data Link)




IMMAGINATEVI DI INVIARE UN MESSAGGIO  
ATTRAVERSO UNA LINEA TELEFONICA



MENTRE IL MESSAGGIO VIAGGIA,  
POTREBBERO VERIFICARSI DELLE  
DISTORSIONI, FORSE A CAUSA DI  
INTERFERENZE O ALTRI FATTORI ESTERNI



QUESTE DISTORSIONI POTREBBERO  
ALTERARE IL MESSAGGIO ORIGINALE,  
RENDENDOLO IRRICONOSCIBILE  
ALL'ARRIVO



Mentre il livello fisico si occupa semplicemente di trasmettere sequenze di bit tra dispositivi, il livello di collegamento assicura che questi bit siano organizzati e interpretati correttamente

Se le lettere sono messe insieme in modo casuale, non formano parole comprensibili

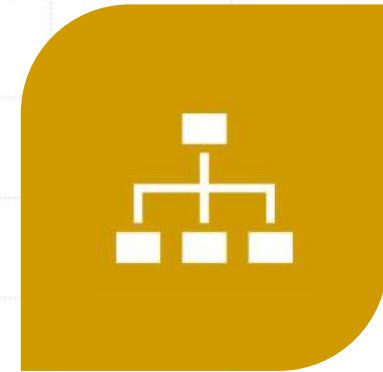
Il livello di collegamento fa qualcosa di simile con i bit, organizzandoli in "frame" o "trame" comprensibili



UNO DEI COMPITI PRINCIPALI  
DEL LIVELLO DI  
COLLEGAMENTO È DIVIDERE  
LA SEQUENZA DI BIT IN  
FRAME



QUESTI FRAME SONO POI  
SUDDIVISI IN DIVERSI CAMPI,  
CIASCUNO CON UNA  
FUNZIONE SPECIFICA



QUESTO PROCESSO DI  
DIVISIONE E ORGANIZZAZIONE  
GARANTISCE CHE I DATI SIANO  
INTERPRETATI  
CORRETTAMENTE QUANDO  
RAGGIUNGO LA LORO  
DESTINAZIONE

# Protocollo di Collegamento

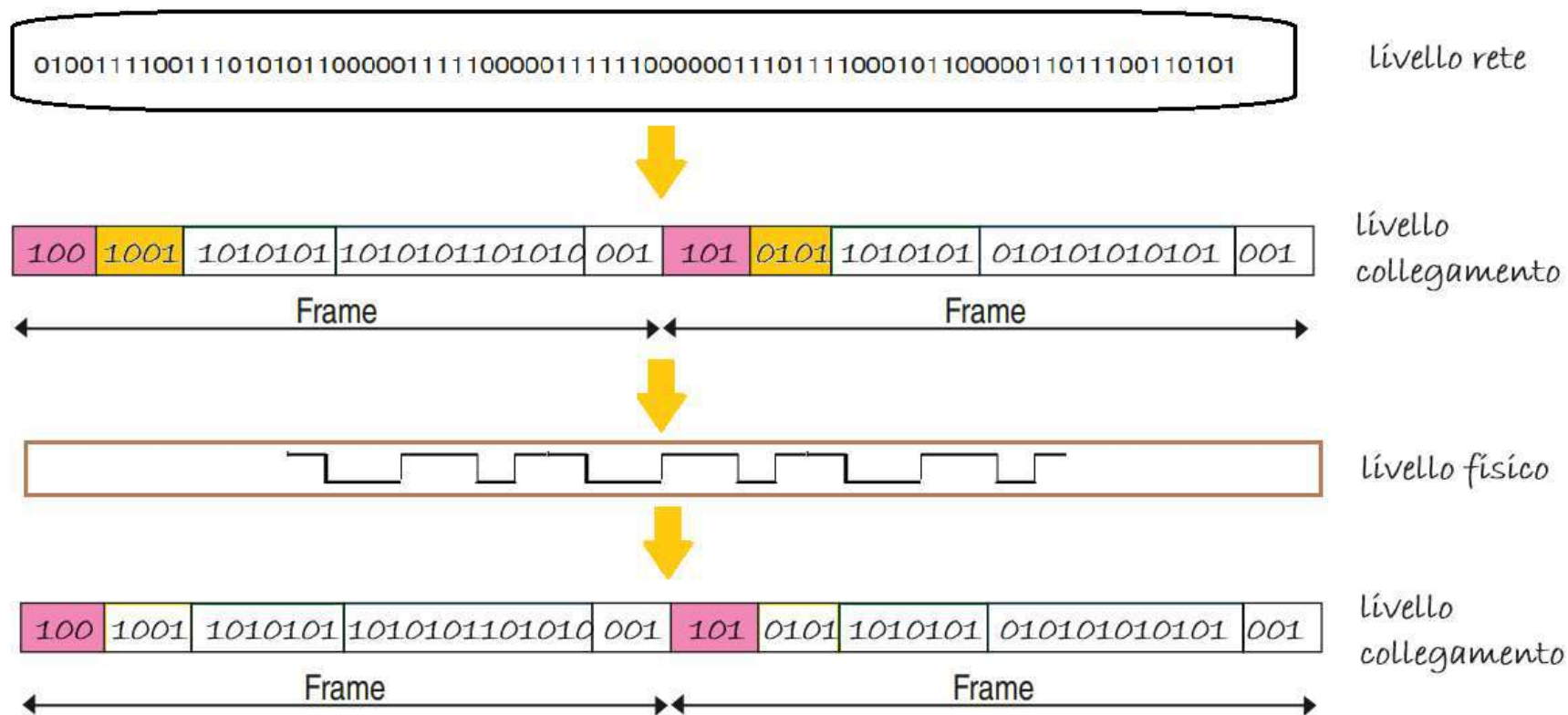
Il protocollo di collegamento è una serie di regole e procedure che determinano come i dati vengono inviati e ricevuti

Una delle sue funzioni più importanti è rilevare eventuali errori che si possono verificare durante la trasmissione

Se, ad esempio, un frame viene danneggiato durante la trasmissione, il protocollo di collegamento può identificare l'errore e richiedere una ritrasmissione del frame danneggiato

**Un protocollo efficace è essenziale per garantire che i dati siano trasmessi in modo accurato e affidabile.**

# Funzionamento





## Funzioni Principali del Livello di Collegamento



**Organizzazione dei Bit:** Divide i bit in frame strutturati per una migliore interpretazione



**Rilevamento degli Errori:** Identifica e gestisce errori nella trasmissione dei dati



**Accesso Multiplo:** Gestisce l'accesso di più dispositivi allo stesso canale di comunicazione



**Regolazione della Velocità:** Gestisce la trasmissione tra dispositivi che operano a diverse velocità



**Fornitura di Servizi:** Offre servizi al livello superiore, il livello di rete, per facilitare la comunicazione



# Conclusione

- Il livello di collegamento è una componente essenziale nel mondo della comunicazione tra dispositivi
- Garantisce non solo che i dati vengano trasmessi, ma anche che vengano interpretati correttamente
- Senza un efficace livello di collegamento, la comunicazione tra dispositivi sarebbe soggetta a errori e interruzioni, rendendo difficile, se non impossibile, condividere informazioni in modo efficace

# Livello di rete:



QUANDO INVIAMO UN MESSAGGIO DA UN DISPOSITIVO ALL'ALTRO, NON VIENE INVIATO MAGICAMENTE AL DESTINATARIO

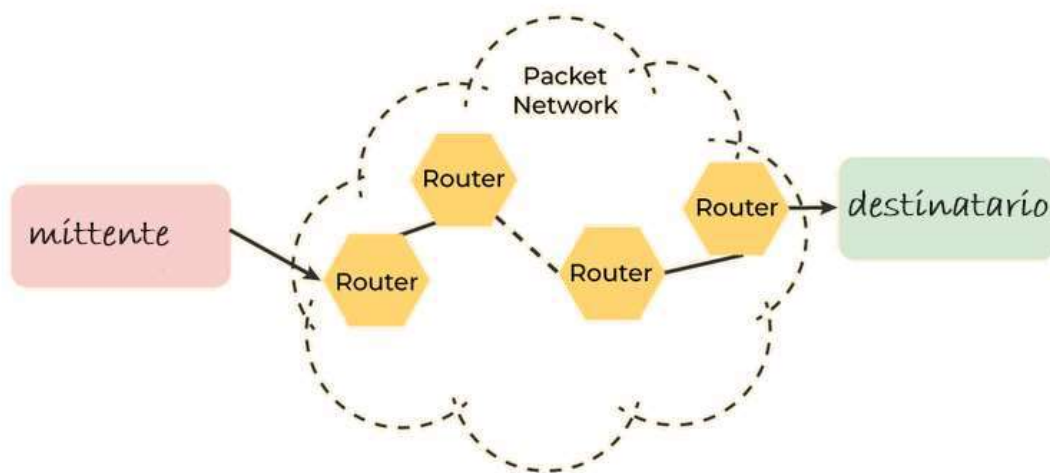


PASSA ATTRAVERSO UNA SERIE DI "PUNTI DI CONTROLLO" PER GARANTIRE CHE ARRIVI A DESTINAZIONE



QUESTO PROCESSO È SIMILE A QUANDO SPEDIAMO UN PACCO: NON VA DIRETTAMENTE AL DESTINATARIO, MA PASSA ATTRAVERSO VARI CENTRI DI SMISTAMENTO

Nel mondo delle reti, questo processo è gestito dal **livello di rete** e si chiama *instradamento*.



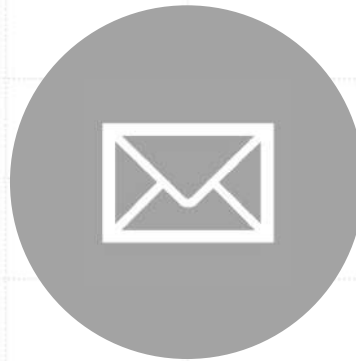
Il compito principale del livello di rete è dunque garantire che i dati inviati da un dispositivo (il mittente) raggiungano un altro dispositivo (il destinatario), anche se questi due dispositivi non fanno parte della stessa rete. Questo processo prende il nome di **routing**.

Il *routing* è il processo mediante il quale i dati vengono inviati dalla sorgente alla destinazione attraverso una serie di dispositivi intermedi, come router e switch

# Da Sorgente a Destinazione: Il Viaggio dei Dati



MENTRE IL LIVELLO FISICO SI PREOCCUPA DEI BIT E DEI SEGNALI ELETTRICI, E IL LIVELLO DI COLLEGAMENTO SI OCCUPA DEI FRAME, IL LIVELLO DI RETE SI OCCUPA DEI PACCHETTI



QUESTI PACCHETTI CONTENGONO L'INDIRIZZO DEL MITTENTE E DEL DESTINATARIO, CHE AIUTA IL LIVELLO DI RETE A DETERMINARE COME INVIARE I DATI ALLA DESTINAZIONE CORRETTA



QUANDO IL NUMERO DI RETI TRA IL MITTENTE E IL DESTINATARIO AUMENTA, AUMENTA ANCHE LA POSSIBILITÀ DI AVERE MOLTEPLICI PERCORSI

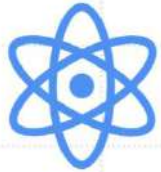
Il livello di rete decide quale di questi percorsi è il migliore per quel particolare pacchetto di dati.



# Internetworking: Collegare reti diverse

- Un altro compito cruciale del livello di rete è l'**internetworking**
- In un mondo dove esistono molte reti diverse, con diversi protocolli e tecnologie, è fondamentale avere un sistema che permetta a queste reti di comunicare tra loro
- Ma se hanno un interprete che conosce entrambe le lingue, possono comunicare attraverso l'interprete

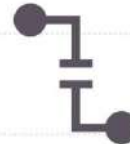
# Compiti essenziali del livello di rete



Queste includono la **multiplazione**, che permette a più flussi di dati di condividere lo stesso circuito fisico



**controllo della congestione**, che assicura che la rete non venga sovraccaricata da troppi dati



Altri compiti includono **l'interconnessione di diverse reti**



la fornitura di servizi al livello superiore, noto come livello di trasporto

Il livello di rete gioca un ruolo cruciale nella comunicazione dei dati, assicurando che i pacchetti di dati vengano inviati e ricevuti in modo efficiente e accurato.

# Gestione e Affidabilità dei Dati: Il Livello di Trasporto

Quando un dispositivo invia un messaggio attraverso una rete, quel messaggio non viaggia come un'entità unica

Questi segmenti viaggiano attraverso la rete e possono prendere percorsi diversi

A causa delle variazioni nel traffico di rete e di altri fattori, questi segmenti potrebbero non arrivare al destinatario nello stesso ordine in cui sono stati inviati



# Affidabilità nella Trasmissione

- **Una delle sfide più grandi nella comunicazione di rete è assicurarsi che i dati vengano inviati e ricevuti correttamente**
- Il livello di trasporto gioca un ruolo cruciale nel rilevare e correggere questi problemi
- Il livello di trasporto lavora in background per risolvere questi problemi e fornirti un'esperienza di visione fluida



# Affidabilità nella Trasmissione

A causa delle variazioni nel traffico di rete e di altri fattori, questi segmenti potrebbero non arrivare al destinatario nello stesso ordine in cui sono stati inviati.

Il compito di assicurare che questi segmenti vengano riassemblati correttamente, nel giusto ordine, spetta al livello di trasporto.



# Scopo

- Quando il livello di trasporto rileva che un segmento di dati è stato perso o è corrotto durante la trasmissione, può richiederne la ritrasmissione. Questo garantisce che i dati vengano ricevuti correttamente e senza errori.

# Funzioni Chiave del Livello di Trasporto

- Una delle principali funzioni del livello di trasporto è **la segmentazione dei dati**. Questo significa dividere i dati in segmenti gestibili che possono essere trasmessi attraverso la rete.
- Un altro compito importante è il **controllo end-to-end**. Questo significa monitorare l'intera trasmissione dei dati, dall'origine alla destinazione, per rilevare e correggere errori. Questo garantisce un servizio affidabile e di alta qualità.
- Il livello di trasporto si preoccupa anche della **qualità del servizio**. Questo significa assicurarsi che i dati vengano trasmessi in modo efficiente e senza interruzioni o ritardi.
- Infine, il livello di trasporto fornisce servizi al livello immediatamente superiore, noto come livello di sessione.



## Livello di Sessione

- Nel panorama della comunicazione digitale, il semplice trasferimento di messaggi tra dispositivi non è l'unico obiettivo
- Queste sessioni non sono solo scambi di dati tra due macchine, ma possono coinvolgere anche molteplici dispositivi
- Le sessioni garantiscono che ci sia un flusso strutturato e ordinato di dati tra le parti coinvolte



Esempi?

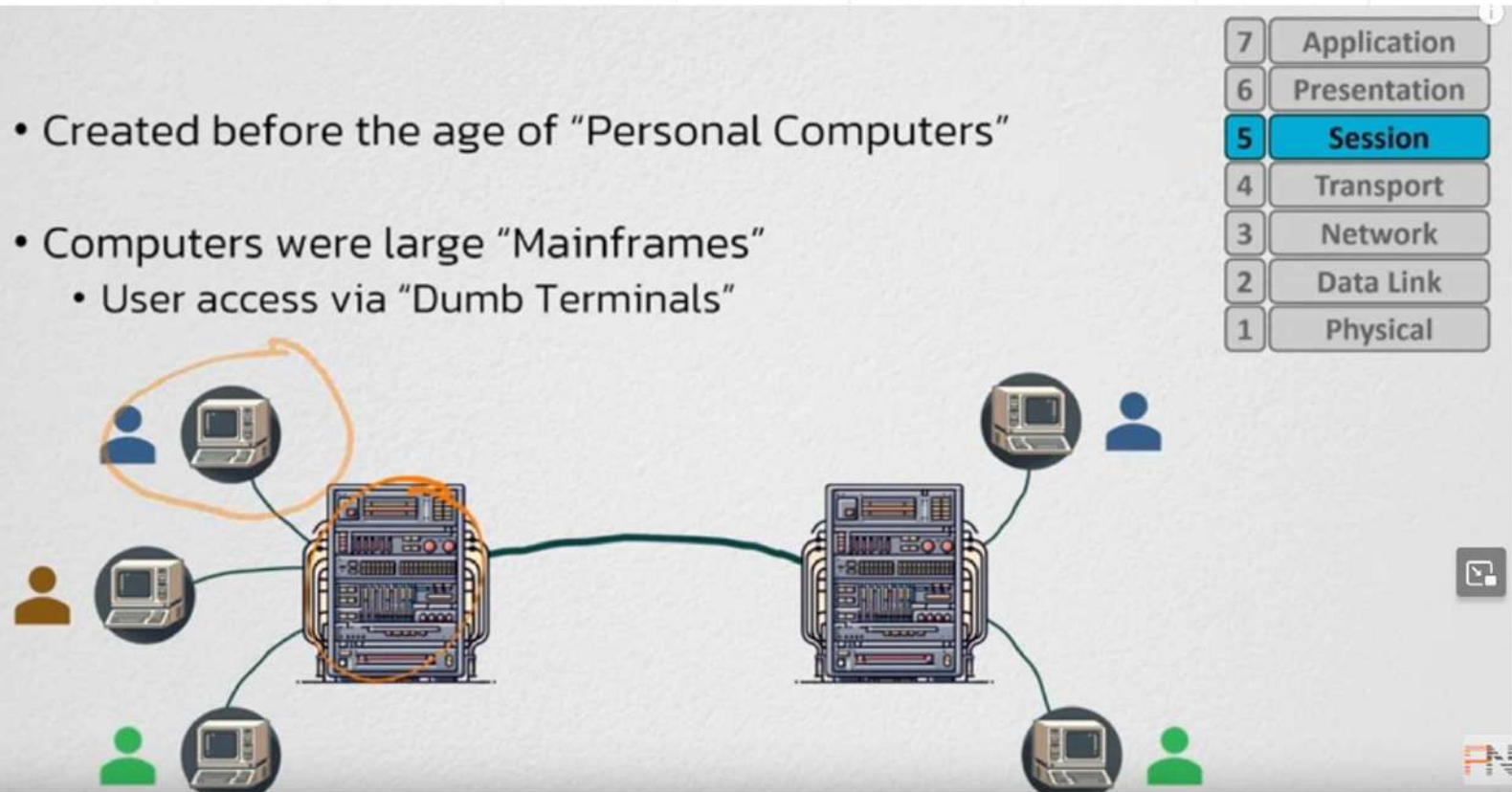
- 
- USER ----> mail
    - ----> torrent
    - -----> web ----> youtube
      - > mail (web)
      - > ...

Server < ---- > Pippo  
< ---- > Pluto  
< ---- > ...

Utente > molteplici servizi

# Storia

- Created before the age of "Personal Computers"
- Computers were large "Mainframes"
  - User access via "Dumb Terminals"



The diagram illustrates a mainframe network architecture. Two large mainframe computers are connected by a central green line. Each mainframe is connected to several dumb terminals (represented by computer icons) and users (represented by person icons). An orange circle highlights the terminals and users connected to the left mainframe, and another orange circle highlights the left mainframe itself. A vertical list of protocol layers is shown on the right, with the 'Session' layer (level 5) highlighted in blue.

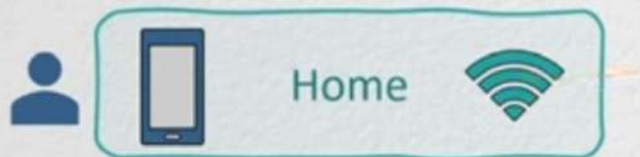
7	Application
6	Presentation
5	Session
4	Transport
3	Network
2	Data Link
1	Physical

Utente blu parla con utente blu, Verde parla con verde  
4 livelli sono uguali → Come faccio a distinguere?

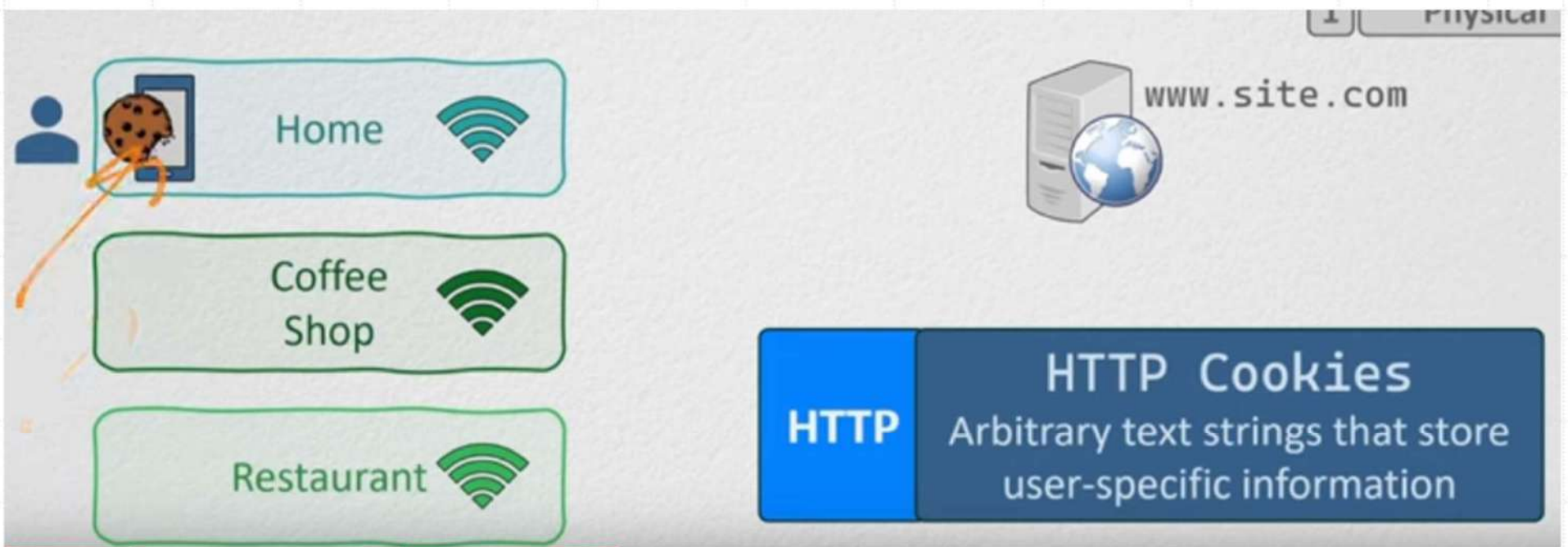


Non solo mainframe ...

- Layer 5 distinguishes between **user sessions**
  - Identifies a user independent from L2, L3, or L4 addresses



7	Application
6	Presentation
5	Session
4	Transport
3	Network
2	Data Link
1	Physical



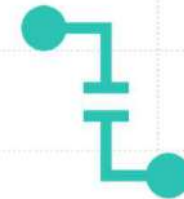
## Funzioni Chiave del Livello di Sessione



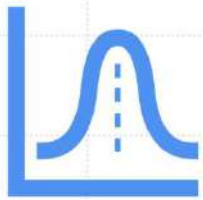
Scomporre la comunicazione in **sessioni logiche**, garantendo che il dialogo tra le applicazioni sia strutturato e ordinato



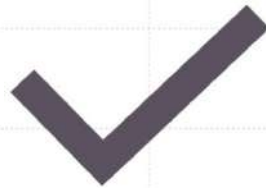
Gestire la **terminazione ordinata delle sessioni**, assicurando che non ci siano interruzioni improvvise o perdite di dati



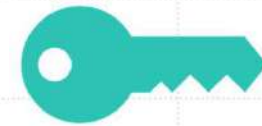
Introdurre punti di sincronizzazione per garantire che le operazioni avvengano in un ordine specifico



Un aspetto cruciale della gestione delle sessioni è la sincronizzazione



Assicurarsi che le operazioni avvengano in un ordine specifico e che certe attività siano completate prima che altre inizino, è fondamentale per la coerenza e l'integrità dei dati



Un esempio di questo sono i meccanismi a token utilizzati per garantire un accesso sequenziale alle risorse



I dispositivi non sono uguali



Il livello di sessione gioca un ruolo cruciale nel negoziare tra dispositivi con caratteristiche diverse



Decide i parametri di comunicazione, come la velocità, il tipo di controllo degli errori e il modo di trasferimento dei dati, come simplex, half-duplex o full-duplex



# Attacchi (1)

1. **Session Hijacking:** Questo attacco avviene quando un malintenzionato prende il controllo di una sessione tra due sistemi. L'hacker può intercettare e rubare un token di sessione valido per impersonare una delle parti legittime.
2. **Man-in-the-Middle (MitM) Attacks:** In questo scenario, l'attaccante si inserisce tra due parti che comunicano e può intercettare o modificare i dati scambiati. Questo può accadere durante la negoziazione della sessione o durante lo scambio di dati.
3. **Session Fixation:** L'attaccante forza un ID di sessione noto su un utente e poi utilizza quell'ID di sessione per accedere alla sessione legittima dell'utente dopo che si è autenticato.
4. **Session Replay:** L'attaccante intercetta dati validi di una sessione, come un token di autenticazione, e li riutilizza per ottenere un accesso non autorizzato.



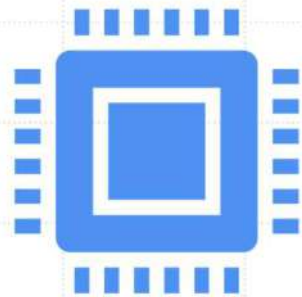
## Attacchi (2)

1. **Session Timeout Attacks:** In questo caso, l'attaccante sfrutta la cattiva gestione dei timeout di sessione per mantenere una sessione aperta e utilizzarla per scopi malevoli.
2. **Cross-site Scripting (XSS):** Anche se generalmente associato al livello applicativo, XSS può essere utilizzato per rubare i cookie di sessione e quindi prendere il controllo della sessione di un utente.
3. **Cross-site Request Forgery (CSRF):** Questo attacco costringe un browser utente a eseguire azioni indesiderate su un sito web al quale è attualmente autenticato, sfruttando la fiducia che il sito ha nella sessione dell'utente.

# Livello di Presentazione

- Immagina di avere due dispositivi che "parlano" linguaggi diversi. Se inviassimo un messaggio da uno all'altro senza alcuna traduzione, potrebbe esserci una grave incomprensione.
- Il livello di presentazione si assicura che ciò non accada, gestendo la **sintassi** e la **semantica** delle informazioni.





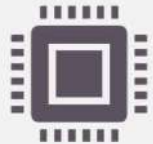
Quando parliamo di comunicazione tra dispositivi o sistemi, un aspetto cruciale è come **i dati vengono rappresentati e interpretati**



Qui entra in gioco il livello di presentazione, **che agisce come un traduttore tra le applicazioni e i livelli sottostanti** del modello di comunicazione



Nelle fasi iniziali dello sviluppo delle reti, esistevano diversi formati di dati



Alcuni dispositivi lavoravano con sequenze di 8 bit, mentre altri utilizzavano formati di 16 bit o addirittura 36 bit



Per garantire una comunicazione fluida, fu introdotta l'Abstract Syntax Notation, un linguaggio comune per la rappresentazione dei dati

- Layer 6 determines how to interpret the 1s and 0s

ASCII  
8 bits



E

T

(space)



/



s

i

www.site.

01000111 01000101 01010100 00100000 00101111 01110011 01101001

**HTTP** ASCII encoding

- 7
- 6**
- 5
- 4
- 3
- 2
- 1

# Standardizzazione e Formati dei Dati

- Un dato standardizzato può essere interpretato correttamente da qualsiasi dispositivo nella rete, indipendentemente dalle sue caratteristiche native.



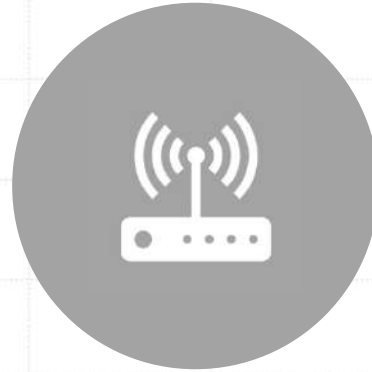
# Complessità dei Dati e Sicurezza

- Con l'avvento di contenuti multimediali, la presentazione dei dati è diventata più complessa
- Il livello di presentazione si assicura che questi dati siano correttamente strutturati e interpretati dai dispositivi di destinazione
- Inoltre, in un'era in cui la sicurezza dei dati è di fondamentale importanza, il livello di presentazione **gioca un ruolo cruciale nella cifratura dei dati**, garantendo che le informazioni sensibili siano protette durante la trasmissione

## Funzioni Principali del Livello di Presentazione



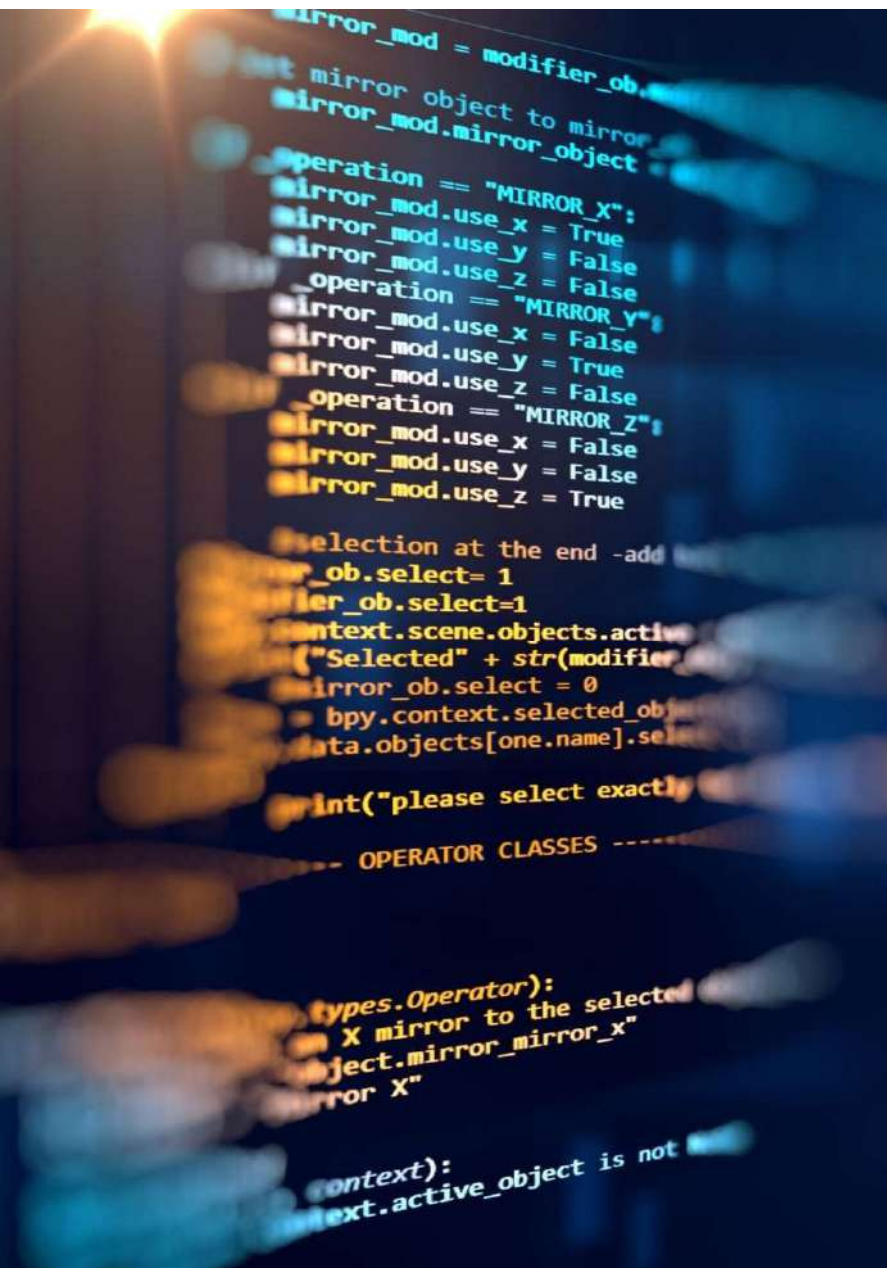
RAPPRESENTAZIONE DEI DATI: TRADURRE I DATI IN UN FORMATO CHE PUÒ ESSERE COMPRESO SIA DALLA SORGENTE CHE DALLA DESTINAZIONE



COMPRESSIONE DEI DATI: RIDURRE LE DIMENSIONI DEI DATI PER UNA TRASMISSIONE PIÙ EFFICIENTE



CIFRATURA DEI DATI: PROTEGGERE I DATI DA ACCESSI NON AUTORIZZATI O DA MALINTENZIONATI



# Comunicazione tra Applicazioni

- Il software che eseguiamo spesso necessita di comunicare con altri software in remoto
- Questo processo di comunicazione distribuita è fondamentale per molte delle nostre applicazioni quotidiane
- Che si tratti di scaricare un file, accedere a un database o inviare un messaggio, queste operazioni richiedono protocolli specifici per garantire una comunicazione fluida e sicura



# Livello Applicativo

- Il livello applicativo rappresenta la cima della gerarchia nel modello di comunicazione di rete
- Questo strato è la prima linea di interazione con gli utenti, permettendo loro di avviare e utilizzare le applicazioni che necessitano di comunicazione di rete
- Questo livello serve come ponte tra le reti informatiche e gli utenti



- Layer 7 determines what the interpreted characters do
  - i.e., application commands

7	Application
6	Presentation
5	Session
4	Transport
3	Network
2	Data Link
1	Physical



G E T (space) / s i m

01000111 01000101 01010100 00100000 00101111 01110011 01101001 01101101

HTTP

GET  
Request a Webpage

```
GET /simple.html HTTP/1.1
Host: pracnet.net
```

# Comunicazione tra Applicazioni

- Anche se ci sono molte applicazioni personalizzate, esistono protocolli standardizzati che devono essere seguiti per assicurare la compatibilità e la comunicazione tra diverse reti e piattaforme.

## Funzioni Chiave del Livello Applicativo



TRASFERIMENTO, ACCESSO E GESTIONE DEI FILE: QUESTO INCLUDE OPERAZIONI COME IL CARICAMENTO, IL DOWNLOAD E LA MODIFICA DEI FILE SU SERVER REMOTI



POSTA ELETTRONICA: PERMETTE AGLI UTENTI DI INVIARE E RICEVERE MESSAGGI E-MAIL



TERMINALE VIRTUALE: FORNISCE UN'INTERFACCIA PER GLI UTENTI PER INTERAGIRE CON SISTEMI REMOTI COME SE FOSSERO DIRETTAMENTE COLLEGATI A LORO

## Funzioni Chiave del Livello Applicativo

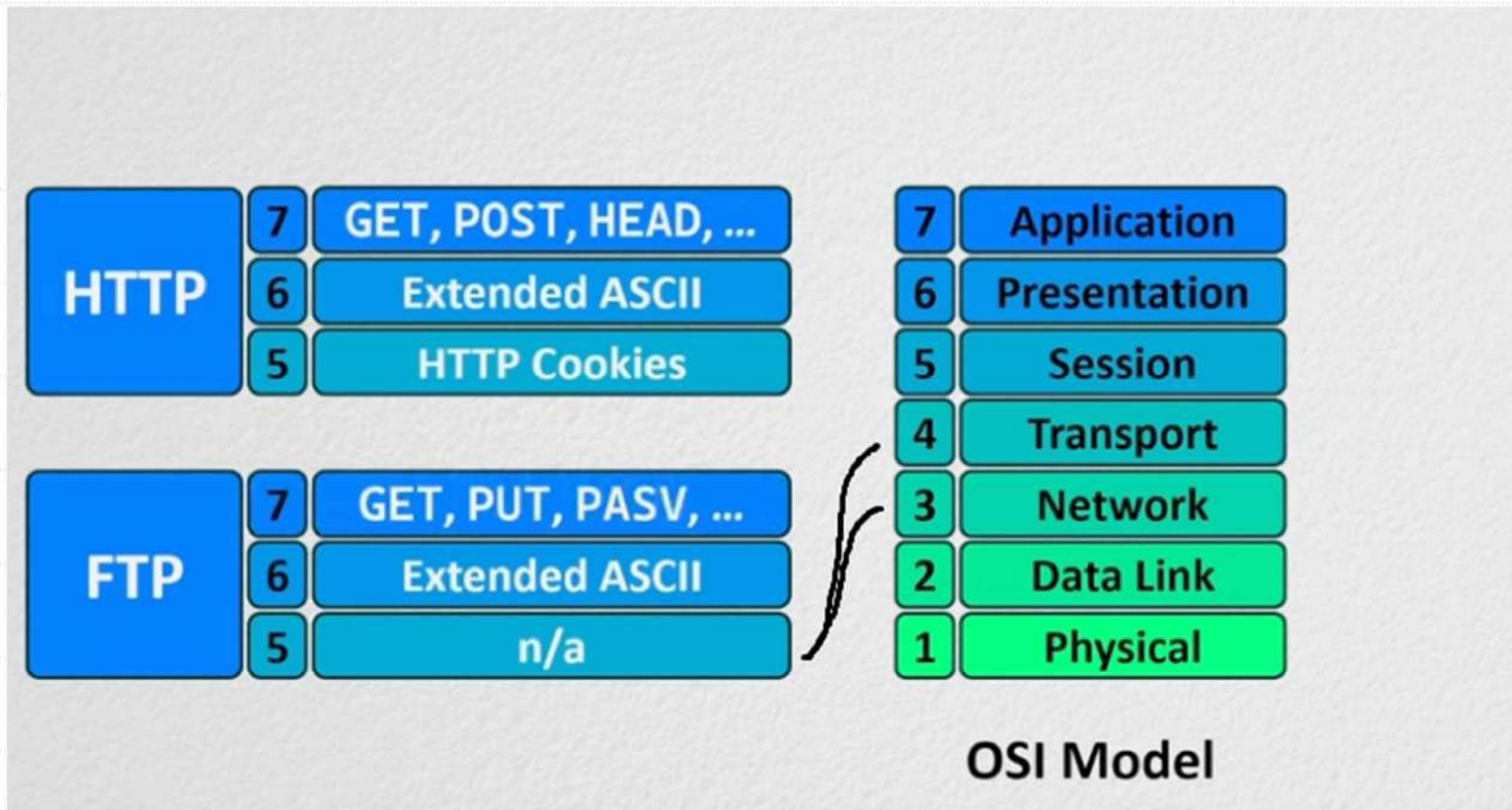


GESTIONE DEI MESSAGGI: OLTRE ALLA POSTA ELETTRONICA, QUESTO INCLUDE ALTRE FORME DI MESSAGGISTICA, COME LA MESSAGGISTICA ISTANTANEA



INTERAZIONE TRA APPLICAZIONI CLIENT-SERVER: QUESTE SONO ARCHITETTURE IN CUI UN PROGRAMMA RICHIEDE UN SERVIZIO O UNA RISORSA A UN ALTRO PROGRAMMA

Ogni protocollo implementa i livelli 5,6,7 come meglio crede ...



# Application Layer

	OSI	TCP/IP	Data Type	Protocols and Services
7	Application	Application Layer	User Data	HTTP, FTP, DNS, Telnet, SSH, NFS, NTP, SMTP, DHCP, NETCONF, RDP, SMB
6	Presentation		Encoded User Data	MIME, ASCII, PGP, TLS/SSL, XML, JSON, Data <b>Serialization</b> , gzip, deflate
5	Session		Sessions	RPC, Named Pipe, NetBIOS, RTP, SOCKS



# ESEMPIO SCAMBIO PACCHETTI

[https://en.wikipedia.org/wiki/Packet\\_analyzer](https://en.wikipedia.org/wiki/Packet_analyzer)

Wireshark interface showing a packet capture of an FTP session. The main pane displays a list of packets with columns for No., Time, Source, Destination, Protocol, Length, and Info. Packet 70 is highlighted, showing a 'Request: USER anonymous' message. The packet details pane below shows the structure of the packet, including Ethernet II, Internet Protocol Version 4, Transmission Control Protocol, and File Transfer Protocol (FTP) fields.

No.	Time	Source	Destination	Protocol	Length	Info
1113	2021-01-26 09:22:00.145219	ftp.cdc.gov	192.168.8.8	FTP	81	Response: 220 Microsoft FTP Service
1114	2021-01-26 09:22:00.145812	192.168.8.8	ftp.cdc.gov	FTP	70	Request: USER anonymous
1116	2021-01-26 09:22:00.219569	ftp.cdc.gov	192.168.8.8	FTP	126	Response: 331 Anonymous access allowed, send identity (e-m
1117	2021-01-26 09:22:00.220054	192.168.8.8	ftp.cdc.gov	FTP	88	Request: PASS mozilla@example.com
1119	2021-01-26 09:22:00.295638	ftp.cdc.gov	192.168.8.8	FTP	75	Response: 230 User logged in.
1120	2021-01-26 09:22:00.296807	192.168.8.8	ftp.cdc.gov	FTP	68	Request: SYST
1121	2021-01-26 09:22:00.375651	ftp.cdc.gov	192.168.8.8	FTP	70	Response: 215 Windows_NT
1122	2021-01-26 09:22:00.377128	192.168.8.8	ftp.cdc.gov	FTP	60	Request: FEAT
1123	2021-01-26 09:22:00.450040	ftp.cdc.gov	192.168.8.8	FTP	88	Response: 211-Extended features supported:
1124	2021-01-26 09:22:00.450040	ftp.cdc.gov	192.168.8.8	FTP	72	Response: LANG EN*
1126	2021-01-26 09:22:00.451225	ftp.cdc.gov	192.168.8.8	FTP	107	Response: AUTH TLS;TLS-C;SSL;TLS-P;
1127	2021-01-26 09:22:00.451225	ftp.cdc.gov	192.168.8.8	FTP	61	Request: HOST
1128	2021-01-26 09:22:00.451225	ftp.cdc.gov	192.168.8.8	FTP	91	Request: SIZE
1130	2021-01-26 09:22:00.452309	192.168.8.8	ftp.cdc.gov	FTP	68	Request: OPTS UTF8 ON
1131	2021-01-26 09:22:00.537019	ftp.cdc.gov	192.168.8.8	FTP	112	Response: 200 OPTS UTF8 command successful - UTF8 encoding
1132	2021-01-26 09:22:00.538160	192.168.8.8	ftp.cdc.gov	FTP	59	Request: PWD
1135	2021-01-26 09:22:00.612036	ftp.cdc.gov	192.168.8.8	FTP	85	Response: 257 "/" is current directory.
1136	2021-01-26 09:22:00.612426	192.168.8.8	ftp.cdc.gov	FTP	62	Request: TYPE I

> Frame 1114: 70 bytes on wire (560 bits), 70 bytes captured (560 bits) on interface \Device\NPF\_{02E41701-151E-4355-9B24-591F6D842DE9}, id 0  
> Ethernet II, Src: IntelCor\_42:70:89 (48:f1:7f:42:70:89), Dst: CiscoMer\_cc:ea:9c (2c:3f:0b:cc:ea:9c)  
> Internet Protocol Version 4, Src: 192.168.8.8 (192.168.8.8), Dst: ftp.cdc.gov (198.246.117.106)  
> Transmission Control Protocol, Src Port: 26694, Dst Port: 21, Seq: 1, Ack: 28, Len: 16  
▼ File Transfer Protocol (FTP)  
 > USER anonymous\r\n  
 [Current working directory: ]

# Inizio sessione FTP - Request

The screenshot shows a Wireshark capture of an FTP session. The main pane displays a list of packets, with packet 1114 selected. The packet details pane shows the FTP request: USER anonymous. The packet bytes pane shows the raw data of the request.

No.	Time	Source	Destination	Protocol	Length	Info
1113	2021-01-26 09:22:00.145219	ftp.cdc.gov	192.168.8.8	FTP	81	Response: 220 Microsoft FTP Service
1114	2021-01-26 09:22:00.145812	192.168.8.8	ftp.cdc.gov	FTP	70	Request: USER anonymous
1116	2021-01-26 09:22:00.219569	ftp.cdc.gov	192.168.8.8	FTP	126	Response: 331 Anonymous access allowed, send identity (e-mail address)
1117	2021-01-26 09:22:00.220054	192.168.8.8	ftp.cdc.gov	FTP	80	Request: PASS mozilla@example.com
1119	2021-01-26 09:22:00.295638	ftp.cdc.gov	192.168.8.8	FTP	75	Response: 230 User logged in.
1120	2021-01-26 09:22:00.296807	192.168.8.8	ftp.cdc.gov	FTP	60	Request: SYST
1121	2021-01-26 09:22:00.375651	ftp.cdc.gov	192.168.8.8	FTP	70	Response: 215 Windows_NT
1122	2021-01-26 09:22:00.377128	192.168.8.8	ftp.cdc.gov	FTP	60	Request: FEAT
1123	2021-01-26 09:22:00.450040	ftp.cdc.gov	192.168.8.8	FTP	88	Response: 211-Extended features supported:
1124	2021-01-26 09:22:00.450040	ftp.cdc.gov	192.168.8.8	FTP	72	Response: LANG EN*
1126	2021-01-26 09:22:00.451225	ftp.cdc.gov	192.168.8.8	FTP	107	Response: AUTH TLS;TLS-C;SSL;TLS-P;
1127	2021-01-26 09:22:00.451225	ftp.cdc.gov	192.168.8.8	FTP	61	Response: HOST
1128	2021-01-26 09:22:00.451225	ftp.cdc.gov	192.168.8.8	FTP	91	Response: SIZE
1130	2021-01-26 09:22:00.452309	192.168.8.8	ftp.cdc.gov	FTP	68	Request: OPTS UTF8 ON
1131	2021-01-26 09:22:00.537019	ftp.cdc.gov	192.168.8.8	FTP	112	Response: 200 OPTS UTF8 command successful - UTF8 encoding is on
1132	2021-01-26 09:22:00.538160	192.168.8.8	ftp.cdc.gov	FTP	59	Request: PWD
1135	2021-01-26 09:22:00.612036	ftp.cdc.gov	192.168.8.8	FTP	85	Response: 257 "/" is current directory.
1136	2021-01-26 09:22:00.612426	192.168.8.8	ftp.cdc.gov	FTP	62	Request: TYPE I

> Frame 1114: 70 bytes on wire (560 bits), 70 bytes captured (560 bits) on interface \Device\NPF\_{02E41701-151E-4355-9B24-591F6D842DE9}, id 0

> Ethernet II, Src: IntelCor\_42:70:89 (48:f1:7f:42:70:89), Dst: CiscoMer\_cc:ea:9c (2c:3f:0b:cc:ea:9c)

> Internet Protocol Version 4, Src: 192.168.8.8 (192.168.8.8), Dst: ftp.cdc.gov (198.246.117.106)

> Transmission Control Protocol, Src Port: 26694, Dst Port: 21, Seq: 1, Ack: 28, Len: 16

▼ File Transfer Protocol (FTP)

> USER anonymous\r\n

[Current working directory: ]



# Risposta (allow anonymous)

No.	Time	Source	Destination	Protocol	Length	Info
1113	2021-01-26 09:22:00.145219	ftp.cdc.gov	192.168.8.8	FTP	81	Response: 220 Microsoft FTP Service
1114	2021-01-26 09:22:00.145812	192.168.8.8	ftp.cdc.gov	FTP	70	Request: USER anonymous
1116	2021-01-26 09:22:00.219569	ftp.cdc.gov	192.168.8.8	FTP	126	Response: 331 Anonymous access allowed, send identity
1117	2021-01-26 09:22:00.220054	192.168.8.8	ftp.cdc.gov	FTP	80	Request: PASS mozilla@sample.com
1119	2021-01-26 09:22:00.295638	ftp.cdc.gov	192.168.8.8	FTP	75	Response: 230 User logged in.
1120	2021-01-26 09:22:00.296807	192.168.8.8	ftp.cdc.gov	FTP	60	Request: SYST
1121	2021-01-26 09:22:00.375651	ftp.cdc.gov	192.168.8.8	FTP	70	Response: 215 Windows_NT
1122	2021-01-26 09:22:00.377128	192.168.8.8	ftp.cdc.gov	FTP	60	Request: FEAT
1123	2021-01-26 09:22:00.450040	ftp.cdc.gov	192.168.8.8	FTP	88	Response: 211-Extended features supported:
1124	2021-01-26 09:22:00.450040	ftp.cdc.gov	192.168.8.8	FTP	72	Response: LANG EN*
1126	2021-01-26 09:22:00.451225	ftp.cdc.gov	192.168.8.8	FTP	107	Response: AUTH TLS;TLS-C;SSL;TLS-P;
1127	2021-01-26 09:22:00.451225	ftp.cdc.gov	192.168.8.8	FTP	61	Response: HOST
1128	2021-01-26 09:22:00.451225	ftp.cdc.gov	192.168.8.8	FTP	91	Response: SIZE
1130	2021-01-26 09:22:00.452309	192.168.8.8	ftp.cdc.gov	FTP	68	Request: OPTS UTF8 ON
1131	2021-01-26 09:22:00.537019	ftp.cdc.gov	192.168.8.8	FTP	112	Response: 200 OPTS UTF8 command successful - UTF8 en
1132	2021-01-26 09:22:00.538160	192.168.8.8	ftp.cdc.gov	FTP	59	Request: PWD
1135	2021-01-26 09:22:00.612036	ftp.cdc.gov	192.168.8.8	FTP	85	Response: 257 "/" is current directory.
1136	2021-01-26 09:22:00.612426	192.168.8.8	ftp.cdc.gov	FTP	62	Request: TYPE I

<

- > Frame 1116: 126 bytes on wire (1008 bits), 126 bytes captured (1008 bits) on interface \Device\NPF\_{02E41701-151E-4355-9B24-591F6D842DE9}, id 0
- > Ethernet II, Src: CiscoMer\_cc:ea:9c (2c:3f:0b:cc:ea:9c), Dst: IntelCor\_42:70:89 (48:f1:7f:42:70:89)
- > Internet Protocol Version 4, Src: ftp.cdc.gov (198.246.117.106), Dst: 192.168.8.8 (192.168.8.8)
- > Transmission Control Protocol, Src Port: 21, Dst Port: 26694, Seq: 28, Ack: 17, Len: 72
- ▼ File Transfer Protocol (FTP)
  - > 331 Anonymous access allowed, send identity (e-mail name) as password.\r\n
  - [Current working directory: ]

# Invio password

SESSIONE


No.	TIME	SOURCE	DESTINATION	PROTOCOL	LENGTH	INFO
1113	2021-01-26 09:22:00.145219	ftp.cdc.gov	192.168.8.8	FTP	81	Response: 220 Microsoft FTP Service
1114	2021-01-26 09:22:00.145812	192.168.8.8	ftp.cdc.gov	FTP	70	Request: USER anonymous
1116	2021-01-26 09:22:00.219569	ftp.cdc.gov	192.168.8.8	FTP	126	Response: 331 Anonymous access allowed
1117	2021-01-26 09:22:00.220054	192.168.8.8	ftp.cdc.gov	FTP	80	Request: PASS mozilla@example.com
1119	2021-01-26 09:22:00.295638	ftp.cdc.gov	192.168.8.8	FTP	75	Response: 230 User logged in.
1120	2021-01-26 09:22:00.296807	192.168.8.8	ftp.cdc.gov	FTP	60	Request: SYST
1121	2021-01-26 09:22:00.375651	ftp.cdc.gov	192.168.8.8	FTP	70	Response: 215 Windows_NT
1122	2021-01-26 09:22:00.377128	192.168.8.8	ftp.cdc.gov	FTP	60	Request: FEAT
1123	2021-01-26 09:22:00.450040	ftp.cdc.gov	192.168.8.8	FTP	88	Response: 211-Extended features supported
1124	2021-01-26 09:22:00.450040	192.168.8.8	ftp.cdc.gov	FTP	72	Response: LANG EN*
1126	2021-01-26 09:22:00.451225	ftp.cdc.gov	192.168.8.8	FTP	107	Response: AUTH TLS;TLS-C;SSL;TLS-P;
1127	2021-01-26 09:22:00.451225	192.168.8.8	ftp.cdc.gov	FTP	61	Response: HOST
1128	2021-01-26 09:22:00.451225	192.168.8.8	ftp.cdc.gov	FTP	91	Response: SIZE
1130	2021-01-26 09:22:00.452309	192.168.8.8	ftp.cdc.gov	FTP	68	Request: OPTS UTF8 ON
1131	2021-01-26 09:22:00.537019	ftp.cdc.gov	192.168.8.8	FTP	112	Response: 200 OPTS UTF8 command successful
1132	2021-01-26 09:22:00.538160	192.168.8.8	ftp.cdc.gov	FTP	59	Request: PWD
1135	2021-01-26 09:22:00.612036	ftp.cdc.gov	192.168.8.8	FTP	85	Response: 257 "/" is current directory
1136	2021-01-26 09:22:00.612426	192.168.8.8	ftp.cdc.gov	FTP	62	Request: TYPE I

- > Frame 1117: 80 bytes on wire (640 bits), 80 bytes captured (640 bits) on interface \Device\NPF\_{02E41701-151E-4355-9B24-591F6D842DE9}, id 0
- > Ethernet II, Src: IntelCor\_42:70:89 (48:f1:7f:42:70:89), Dst: CiscoMer\_cc:ea:9c (2c:3f:0b:cc:ea:9c)
- > Internet Protocol Version 4, Src: 192.168.8.8 (192.168.8.8), Dst: ftp.cdc.gov (198.246.117.106)
- > Transmission Control Protocol, Src Port: 26694, Dst Port: 21, Seq: 17, Ack: 100, Len: 26
- ✓ File Transfer Protocol (FTP)
  - > PASS mozilla@example.com\r\n
  - [Current working directory: ]

## SESSIONE

No.	Time	Source	Destination	Protocol	Length	Info
1113	2021-01-26 09:22:00.145219	ftp.cdc.gov	192.168.8.8	FTP	81	Response: 220 Microsoft FTP Ser
1114	2021-01-26 09:22:00.145812	192.168.8.8	ftp.cdc.gov	FTP	70	Request: USER anonymous
1116	2021-01-26 09:22:00.219569	ftp.cdc.gov	192.168.8.8	FTP	126	Response: 331 Anonymous access
1117	2021-01-26 09:22:00.220054	192.168.8.8	ftp.cdc.gov	FTP	80	Request: PASS mozilla@example.c
1119	2021-01-26 09:22:00.295638	ftp.cdc.gov	192.168.8.8	FTP	75	Response: 230 User logged in.
1120	2021-01-26 09:22:00.296807	192.168.8.8	ftp.cdc.gov	FTP	60	Request: SYST
1121	2021-01-26 09:22:00.375651	ftp.cdc.gov	192.168.8.8	FTP	70	Response: 215 Windows_NT
1122	2021-01-26 09:22:00.377128	192.168.8.8	ftp.cdc.gov	FTP	60	Request: FEAT
1123	2021-01-26 09:22:00.450040	ftp.cdc.gov	192.168.8.8	FTP	88	Response: 211-Extended features
1124	2021-01-26 09:22:00.450040	ftp.cdc.gov	192.168.8.8	FTP	72	Response: LANG EN*
1126	2021-01-26 09:22:00.451225	ftp.cdc.gov	192.168.8.8	FTP	107	Response: AUTH TLS;TLS-C;SSL;T
1127	2021-01-26 09:22:00.451225	ftp.cdc.gov	192.168.8.8	FTP	61	Response: HOST
1128	2021-01-26 09:22:00.451225	ftp.cdc.gov	192.168.8.8	FTP	91	Response: SIZE
1130	2021-01-26 09:22:00.452309	192.168.8.8	ftp.cdc.gov	FTP	68	Request: OPTS UTF8 ON
1131	2021-01-26 09:22:00.537019	ftp.cdc.gov	192.168.8.8	FTP	112	Response: 200 OPTS UTF8 command
1132	2021-01-26 09:22:00.538160	192.168.8.8	ftp.cdc.gov	FTP	59	Request: PWD
1135	2021-01-26 09:22:00.612036	ftp.cdc.gov	192.168.8.8	FTP	85	Response: 257 "/" is current di
1136	2021-01-26 09:22:00.612426	192.168.8.8	ftp.cdc.gov	FTP	62	Request: TYPE I

- > Frame 1119: 75 bytes on wire (600 bits), 75 bytes captured (600 bits) on interface \Device\NPF\_{02E41701-151E-4355-9B24-591F6D842DE9}, id 0
- > Ethernet II, Src: CiscoMer\_cc:ea:9c (2c:3f:0b:cc:ea:9c), Dst: IntelCor\_42:70:89 (48:f1:7f:42:70:89)
- > Internet Protocol Version 4, Src: ftp.cdc.gov (198.246.117.106), Dst: 192.168.8.8 (192.168.8.8)
- > Transmission Control Protocol, Src Port: 21, Dst Port: 26694, Seq: 100, Ack: 43, Len: 21
- ▼ File Transfer Protocol (FTP)
  - > 230 User logged in.\r\n
  - [Current working directory: ]



<https://www.youtube.com/watch?v=1369-0r-pX0&t=75s>