MODELLO OSI

Caratteristiche generali

Standard OSI

- Lo standard OSI definisce un **modello di riferimento** per lo scambio di informazioni tra due calcolatori.



PRINCIPALI OBIETTIVI DEL MODELLO OSI

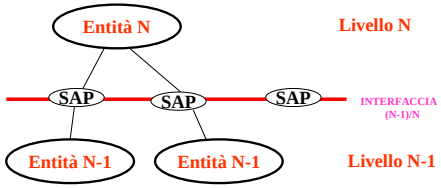
- Fornire una base comune per la realizzazione di standard nel settore dell'interconnessione di sistemi informatici e di telecomunicazione.
- Facilitare l'interconnessione tra apparati prodotti da aziende diverse.
- Costruire una struttura di riferimento per realizzare una rete aperta e trasparente per l'utente

Architettura Modello OSI

- Architettura a livelli con i seguenti componenti principali:
  - I livelli (layers)
  - Le entità (entities)
  - I punti di accesso al servizio SAP (Service Access Points)
  - Le connessioni (connections)
- I livelli adiacenti comunicano attraverso le interfacce.
- Ogni livello è composto da una o più entità.
- Entità appartenenti allo stesso livello su sistemi diversi vengono dette peer-entities
- Le entità di livello N, eccetto per il livello 1, utilizzano per comunicare i servizi del livello N-1.
- Le entità di livello 1 comunicano direttamente tramite i mezzi trasmissivi che le interconnettono.

SAP

- Le entità forniscono e utilizzano i servizi tramite i SAP
- Ogni SAP posta nell'interfaccia tra il livello N e il livello N-1 è identificata da un (N-1) indirizzo univoco per essere identificata e ritrovata

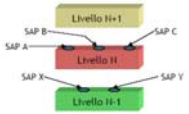


- Analogia con il telefono
  - SAP: presa telefonica
  - Indirizzi SAP: indirizzo telefonico

Servizi

- La scelta di uno o l'altro servizio viene fatta accedendo al livello attraverso un punto particolare a seconda del servizio richiesto, utilizzando i *Service Access Point* (SAP)

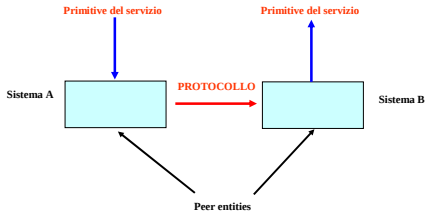
- Esempio:
- Servizio A: connection oriented affidabile
- Servizio B: connection oriented non affidabile
- Servizio C: connectionless non affidabile
- Servizio X: connection oriented affidabile
- Servizio Y: connectionless affidabile



Entità

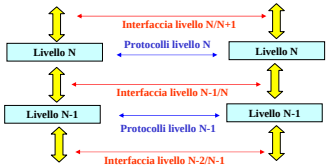
- Le entità servono per lo scambio di informazioni tra due sistemi
- Una entità di livello N (N-identità) per scambiare informazioni con una entità di pari livello (peer entity) attiva primitive di servizio fornite dal livello N-1, ma deve fornire l'indirizzo dell'entità a livello N con cui vuole aprire la connessione
- Ogni entità è definita da un titolo che la identifica in modo univoco in tutta la rete; infatti, le entità in un sistema distribuito possono spostarsi da un sistema all'altro.
- Ogni N-entità è collegata all'interfaccia del livello N-1 mediante un (N-1)SAP
- Una connessione tra due N-entità viene definita mediante gli indirizzi di livello N-1 degli (N-1)SAP ai quali esse sono collegate.

Peer entities (Entità di pari livello)



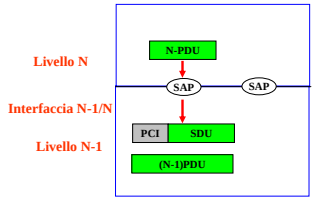
Protocolli

- Le operazioni specifiche di un livello e quindi la cooperazione tra entità appartenenti a quel livello sono realizzate mediante un insieme di protocolli
- Due entità di livello N su sistemi diversi possono scambiarsi informazioni solo se viene stabilita una connessione nel livello N-1 utilizzando un protocollo di livello N-1
- Livelli di ordine N possono comunicare solo attraverso protocolli di livello N



Passaggio di informazioni tra livelli

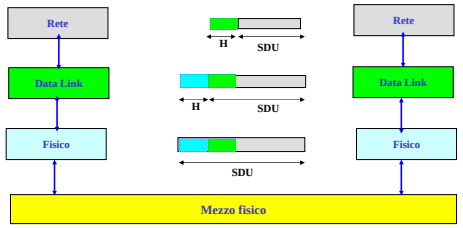
- I dati generati da un protocollo di livello N sono detti N-PDU (Protocol Data Unit)
- I dati a livello N sono contenuti in SDU (Service Data Unit)
- PCI (Protocol Control Information): contiene le informazioni di controllo del protocollo



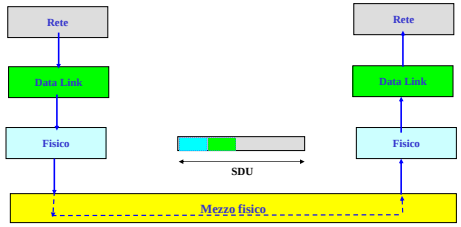
- Spesso al posto di PDU si usano i termini pacchetto o trama a seconda del livello in cui si opera
- Termini spesso usati per i PDU:
  - segmento o transport PDU per il livello di trasporto
  - Pacchetto a livello di rete
  - Trama o frame a livello di data-link

Nome per il PCI: busta

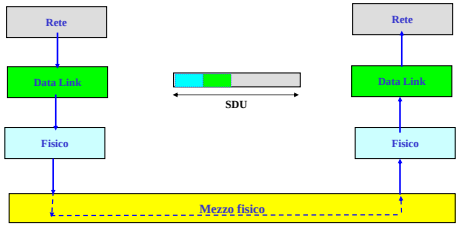
Imbustamento multiplo



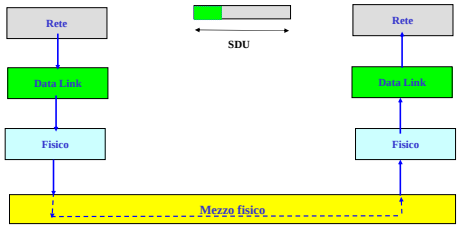
Imbustamento multiplo



Imbustamento multiplo



Imbustamento multiplo



Primitive

- Le primitive sono procedure che permettono di attivare i servizi forniti dal livello inferiore
- In ambito OSI sono previsti quattro tipi di primitive di servizio
  - Request
  - Indication
  - Response (non usata a livello 2)
  - Confirm
- Qualunque primitiva OSI rientra in una di queste categorie

Primitive di servizio

- Request — **L'entità richiede che il servizio faccia qualcosa**
- Indication
- Response
- Confirm

Primitive di servizio

- Request
- Indication
- Response
- Confirm

All'entità viene notificato un evento

Primitive di servizio

- Request
- Indication
- Response
- Confirm

L'entità vuole rispondere a un evento

Primitive di servizio

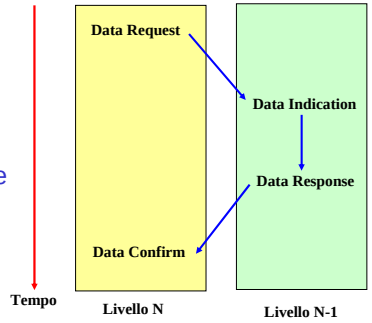
- Request
- Indication
- Response
- Confirm

E' arrivata la risposta a una richiesta precedente

Primitive di servizio

Esempio: Due livelli dello stesso sistema

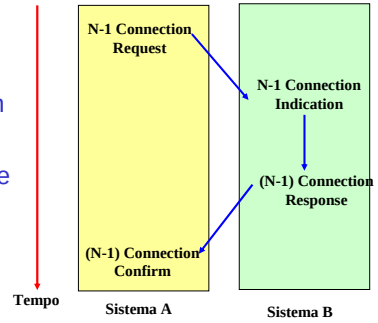
- Request
- Indication
- Response
- Confirm



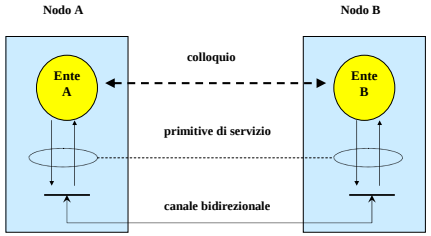
Primitive di servizio

Esempio: Connessione tra due sistemi

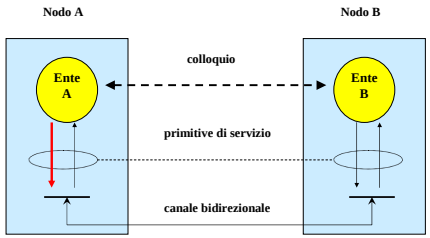
- Request
- Indication
- Response
- Confirm



Entità colloquianti tramite primitive

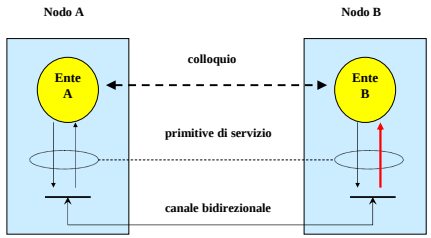


Primitive



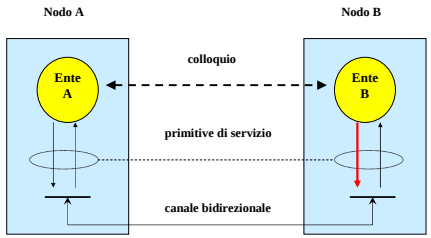
Richiesta di A

Primitive



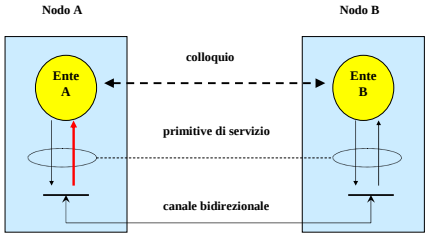
Indicazione verso B

Primitive



Risposta di B

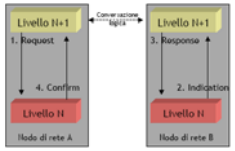
Primitive



Conferma verso A

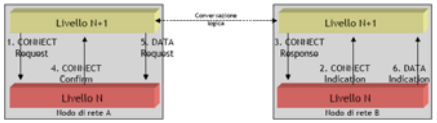
Primitive di servizio

- Un'entità si serve dei ***servizi*** offerti dal livello inferiore, tramite le ***primitive***, per comunicare (in senso *logico*) con l'entità di pari livello di un altro nodo di rete
- Da questo segue che, per ogni Request, esiste un'Indication all'entità pari
- Inoltre, se viene richiesto il riscontro, ad una coppia Request – Indication corrisponde una coppia Response – Confirm



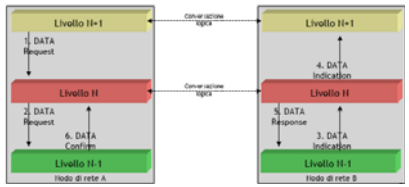
Esempio 1 : servizi e primitive

- I livelli N+1 dei nodi di rete A e B si scambiano informazioni usando un servizio connection-oriented senza riscontro, offerto dai rispettivi livelli N
- Il servizio CONNECT è *a riscontro*, il servizio DATA è in questo *senza riscontro*



Esempio 2 : servizi e primitive

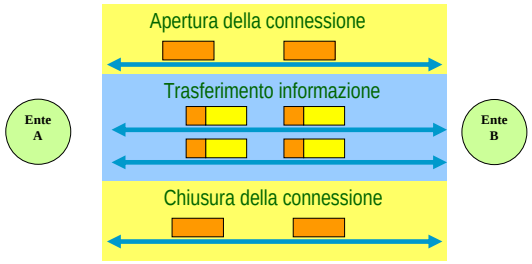
- I livelli N+1 dei nodi di rete A e B si scambiano dati usando un servizio connection-less *senza riscontro*, offerto dai rispettivi livelli N
- I rispettivi livelli N si servono poi di un servizio connection-less *a riscontro* (offerto dai livelli N-1) per dialogare



Modalità di comunicazione

- modalità a connessione
  - instaurazione della connessione
  - trasferimento dell'informazione
  - rilascio delle connessione
- modalità senza connessione
  - una sola fase

Servizio a connessione



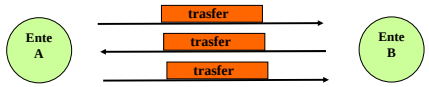
Servizio a connessione

Si distinguono 3 fasi

- **chiamata**
  - **si instaura la sessione e ci si mette d'accordo sulle modalità di svolgimento della sessione**
- **trasferimento dell'informazione**
- **abbattimento**

Servizio senza connessione

- **Il trasferimento dati avviene in modo autonomo, senza preventivo accordo**
- **non lega fra loro i diversi trasferimenti effettuati fra gli stessi utenti**
- **non consente i servizi tipici del trasferimento a connessione**



Esempi di colloquio a connessione

- **Un caso particolare è la connessione telefonica, in cui le PDU trasmesse sono i bit**
- **Protocolli di livello 2: HDLC, LAPB, LAPD**
- **Protocolli di rete: X.25, Frame Relay**
- **Protocollo di trasporto: TCP**

Esempi di colloquio senza connessione

- **Protocolli MAC di livello 2: Ethernet, token ring**
- **Protocolli di rete: IP**
- **Protocollo di trasporto: UDP**

Modalità di servizio

- Servizi con conferma: in tali servizi il livello N ricevente conferma l'avvenuta ricezione
- Servizi senza conferma: in tali servizi il livello N ricevente non conferma l'avvenuta ricezione

Servizio Confermato

- Request
- Indication
- Response
- Confirm

Servizio Non Confermato

- Request
- Indication

Servizio connected oriented

8 primitive

Connect.request ( )	
Connect.indication( )	
Connect.response ( )	
Connect.confirm( )	
Data.request ( )	**Si cerca di inviare i dati**
Data.indication ( )	**Sono arrivati dei dati**
Disconnect.request ( )	**Si vuole terminare la connessione**
Disconnect.indication ( )	**L'altra entity vuole terminare**

Protocolli con e senza connessione

- Tutti i livelli (tranne quello fisico) consentono di scegliere tra due modalità
  - Modalità connessa (Connectioned Oriented Network Service)
  - Modalità non-connessa (Connectioned Less Network Service)
- Un livello può fornire al livello superiore servizi connesso, non connesso o entrambi
- Questa scelta può variare da livello a livello e da architettura ad architettura
- Lo standard ISO originale (OSI 7498) prevedeva solo la modalità connessa, tuttavia a causa dell'importanza della modalità non connessa (soprattutto con l'avvento delle reti moderne) è stato inserita anche la modalità non-connessa mediante l'aggiunta di un emendamento allo standard stesso

Servizi orientati alla connessione

- Sono presenti tre fasi:
  - Fase 1: Creazione della connessione
  - Fase 2: Trasferimento dei dati
  - Fase 3: Chiusura della connessione

- Modello telefonico
  - si apre la connessione
  - si scambiano i messaggi
  - si chiude la telefonata

Servizi orientati alla connessione

- Nella fase 1 due peer-entities si accordano per il trasferimento di PDU e soltanto durante questa fase saranno scambiati gli indirizzi completi del mittente e del destinatario
- Nella fase due (trasferimento delle PDU) deve essere specificato soltanto l'identificativo della connessione scelta durante la fase 1.
- Un servizio orientato alla connessione fornisce una modalità di trasferimento affidabile e in modo sequenziale
- Se qualcosa non funziona correttamente la comunicazione può essere riavviata (reset) oppure terminata (released)
- Per controllare che tutte le PDU siano ricevute correttamente sono utilizzati metodi di numerazione di pacchetti e di verifica della corretta ricezione dei pacchetti (ACK)
- La correzione di errori nelle PDU può essere effettuata mediante tecniche di ritrasmissione

Servizi non orientati alla connessione o connectionless

- La comunicazione ha luogo in una sola fase:
  - il pacchetto (o PDU) viene inviato nella rete e viene affidato al sistema di instradamento.

- Modello postale
  - si affida il messaggio al sistema di inoltro

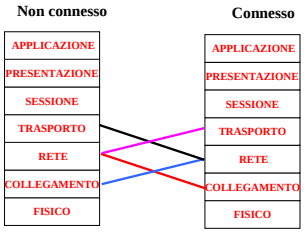
Servizi non orientati alla connessione o connectionless

- Il pacchetto deve contenere l'indirizzo completo del destinatario
- Un protocollo non connesso può solo rilevare la presenza di errori, scartando le PDU errate, ma non può correggerli attraverso meccanismi di ritrasmissione poiché in un pacchetto non è possibile fare riferimento ad altri pacchetti.
- Un protocollo non connesso è generalmente più efficiente di quello connesso per traffico di tipo bursty
- Un protocollo non connesso non garantisce l'affidabilità del trasferimento e quindi richiede almeno un protocollo di livello superiore sia di tipo connesso,

Confronto tra protocolli con o senza connessione

Caratteristica	Servizio con connessione	Servizio senza connessione
Setup iniziale	Necessario	Assente
Indirizzo di Destinazione	Durante la fase Iniziale	In ogni pacchetto
Ordine dei pacchetti	Garantito	Non garantito
Controllo degli errori	Si	No
Controllo di flusso	Si	No
Negoziazione di opzioni	Si	No
Identificazione di connessione	Si	No

Protocolli con e senza connessione



- Il livello 1 non è né con né senza connessione
- I livelli 2, 3 e 4 possono operare in entrambe le modalità e in tutte le combinazioni
- I livelli 5,6 e 7 devono comportarsi globalmente in modo connesso e non connesso

- Il livello 2 è generalmente non connesso quando si opera sulle LAN (canale affidabile) e di tipo connesso su reti WAN
- Il livello 3 è connesso per i telecomunicazionisti e non connesso per gli informatici
- Il livello 4 è in pratica sempre connesso anche quando il livello 3 è connesso perché spesso l'affidabilità di tale livello non è considerata sufficiente

Primitive

- Request
- Indication
- Response
- Confirm

Servizi affidabili

- Utilizzano le primitive response/confirm per gestire la ritrasmissione in caso di errori
- Garantiscono la ricezione completa e corretta di tutti i messaggi
- Possono introdurre ritardi inaccettabili

Servizi non affidabili

- Non garantiscono la corretta ricezione dei messaggi
- Utilizzano soltanto le primitive request/response

Esempi di servizi affidabili e non affidabili

- Reliable connection oriented: trasferimento di file
  - I file devono essere ricevuti interamente (senza pezzi mancanti e nell'ordine giusto)
- Non- reliable connection oriented: trasmissioni isocrone (quali voce e video)
  - Si deve mantenere le relazioni temporali tra i bit del flusso dati. Sono accettabili disturbi ogni tanto, piuttosto che interruzioni temporanee ma avvertibili
- Non reliable connectionless o datagram service: distribuzione di posta pubblicitaria
  - Non è importante se qualche messaggio viene perduto
- Reliable Connectionless o acknowledged datagram service: messaggio di cui si vuole essere sicuri che è arrivato

Modello OSI

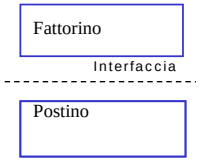
- È un modello (non un'architettura di rete)
  - Definisce i livelli e dice COSA devono fare
- Per ogni livello sono stati definiti degli standard
  - definiscono COME deve funzionare

Organizzazione del servizio postale: altra visione

ROSSI	TAKAMURA
Segretaria	Segretaria
Fattorino	Fattorino
Postino	Postino
Smistamento	Smistamento
Stazione	Stazione
Viaggio	

Strati: ogni strato implementa un servizio
- attraverso le sue azioni interne allo strato
- confida sui servizi forniti dagli strati sottostanti
- ha uno strato corrispondente e reciproco

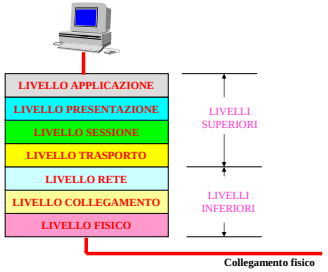
Interfacce e API



- **Interfaccia**
  Insieme di regole che permettono a due entità di scambiarsi reciproci servizi
- **Application Programming Interface**
  Regole e definizioni per scambio dati tra programmi

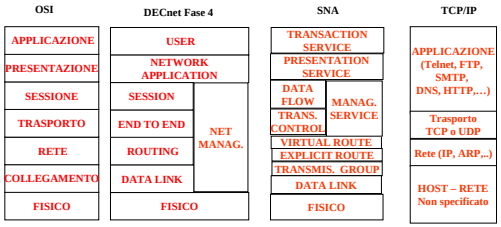
Struttura del modello OSI

- Lo standard OSI utilizza una struttura composta da **7 livelli** o strati.



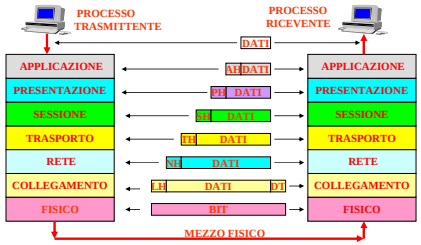
Principali architetture di rete

- SNA (System Network Architecture), architettura IBM
- DNA (Digital Network Architecture), nota come DECnet della Digital
- TCP/IP (Internet Protocol Suite)
- OSI

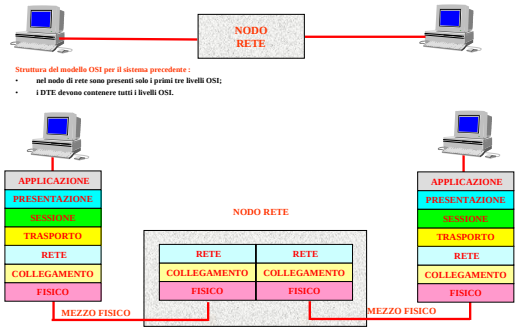


Organizzazione dei dati

- Ogni livello aggiunge un'intestazione ai dati forniti dal livello superiore. Il livello 2 introduce anche una coda (DT) alla fine dei dati. Il livello 1 non introduce nessuna intestazione, ma converte i simboli in una sequenza di bit.
- Il livello n non altera i dati forniti dal livello superiore.
- In ricezione il livello n utilizza soltanto i dati introdotti dal livello n in trasmissione. Ciascun livello opera in modo autonomo e dialoga solo con il corrispondente livello in trasmissione.



Esempio di un sistema per la trasmissione dati : si considera due DTE e un nodo di commutazione



APPLICAZIONE
PRESENTAZIONE
SESSIONE
TRASPORTO
RETE
COLLEGAMENTO
FISICO

Livello fisico

- Il livello fisico definisce le caratteristiche dei segnali e dei dispositivi necessari per connettere due o più DTE mediante un canale fisico
  Il livello fisico fornisce indicazioni sulle interfacce meccaniche, elettriche e procedurali.
- I principali aspetti definiti dal livello fisico sono:
  - le forme d'onda utilizzate per trasmettere i simboli;
  - durata temporale di ciascun simbolo;
  - regole per l'attivazione e la disattivazione del collegamento fisico tra due punti;
  - caratteristiche dei cavi e dei connettori;
  - interfaccia tra il DTE e il DCE;
  - operazione di multiplazione dei segnali;
  - operazioni di modulazione.

Mezzi trasmissivi

Elettrici

Doppino non schermato, Cavo coassiale

- **Ottici**

  Fibra ottica, Raggi Laser

- **Radio**

  Ponti radio, Satelliti, Reti Cellulari

Doppino

Detto anche coppia (pair), è il mezzo trasmissivo classico della telefonia

Due fili di rame ritorti (binati, twisted) per ridurre le interferenze elettromagnetiche

Costi ridotti e installazione semplice



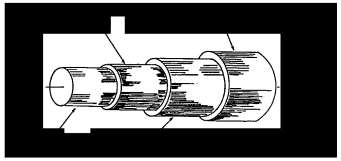
Cavo coassiale

- **Un connettore centrale e una o più calze di schermo.**
- **Maggiore schermatura dai disturbi esterni, minori interferenze**
- **Costi leggermente più elevati, maggiore difficoltà di installazione**



Fibre ottiche

Minuscolo e flessibile filo di vetro costituito da due parti con indici di rifrazione diversi.



Interfacce tra DTE e DCE

L'interfaccia meccanica, elettrica e procedurale tra DTE e DCE è definita dai seguenti standard:

- **EIA RS 232-C** - standard definito per **velocità inferiori a 20 kbit/s e per lunghezze del cavo di collegamento tra DTE e DCE inferiori a 15 m.** Utilizza una trasmissione sbilanciata dei segnali.
- **CCITT V.24** - analogo al precedente
- **EIA RS-449** - Lo standard è diviso in :
  - **RS-422** - specifica l'uso di doppini telefonici per velocità tra 100 kbit/s e 10 Mbit/s;
  - **RS-422-A** - specifica l'interfaccia elettrica nel caso di *trasmissione bilanciata*, in cui ciascuno dei circuiti principali di collegamento tra DTE e DCE utilizza due fili senza una massa comune. In questo modo è possibile ottenere velocità fino a 10 Mbit/sec con un cavo di lunghezza massima uguale a 60 m.
  - **RS-423-A**- specifica l'interfaccia elettrica. Questo standard utilizza una *trasmissione sbilanciata*, come nel RS-232-C, in cui tutti i circuiti condividono una massa elettrica comune.

Standard di interfaccia

Specificano le interconnessioni tra DTE e DCE

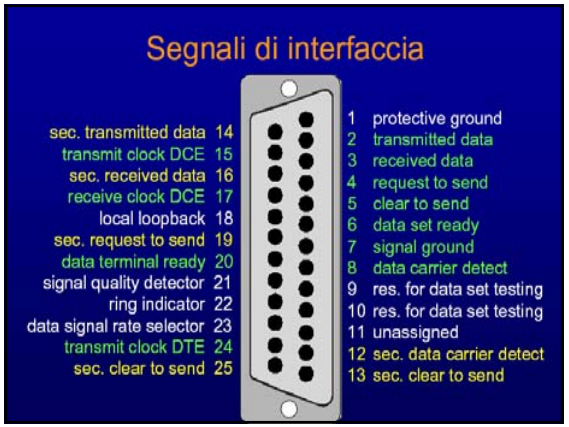
I principali sono:

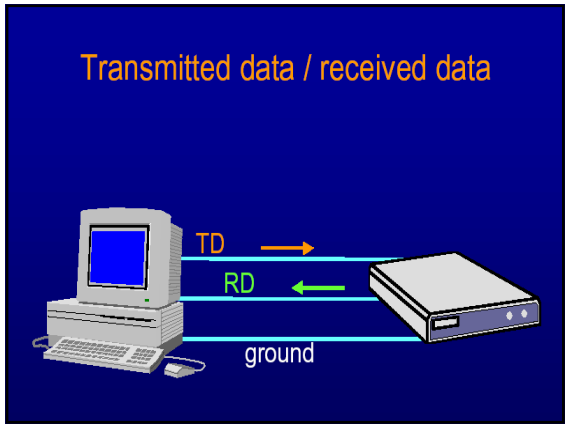
1. **RS-232 (o equivalenti CCITT V.24 e V.28)**
2. **V.35**
3. **G.703 e G.704**

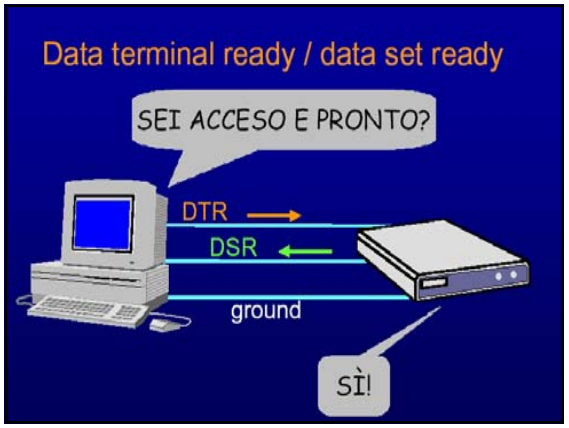
RS 232

Standard per la trasmissione seriale a bassa velocità (sino a 19200 b/s)

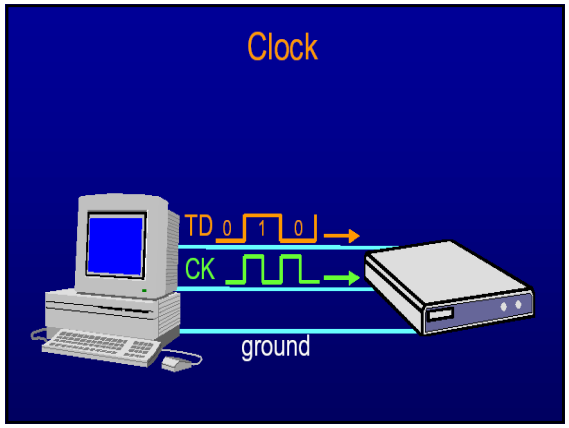
- **Utilizza un connettore a 9 o 25 pin (vaschetta)**
- **Prevede 8 segnali + 1 schermatura**

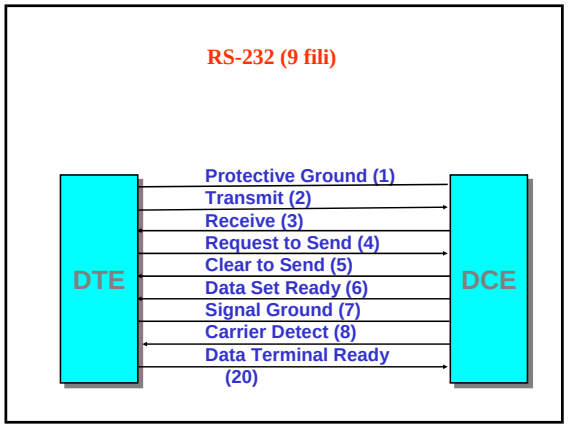


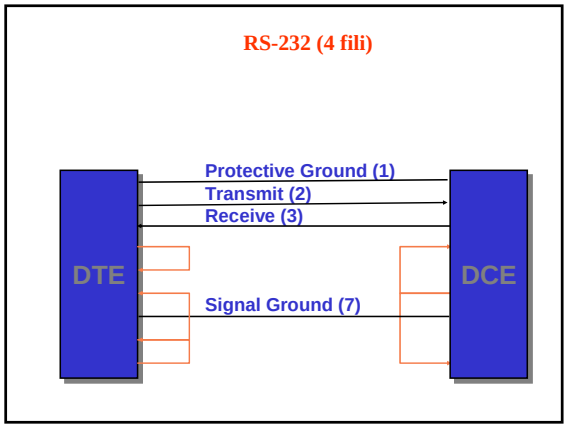

Transmitted data / received data
TD
RD
ground


Data terminal ready / data set ready
SEI ACCESO E PRONTO?
DTR
DSR
ground
SÌ!


Controllo di flusso (handshake)
SEI PRONTO A RICEVERE
I DATI DA INVIARE?
RTS
CTS
ground
SÌ!

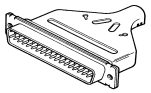

Clock
TD 0 1 0
CK
ground


RS-232 (9 fili)
DTE
DCE
Protective Ground (1)
Transmit (2)
Receive (3)
Request to Send (4)
Clear to Send (5)
Data Set Ready (6)
Signal Ground (7)
Carrier Detect (8)
Data Terminal Ready
(20)


RS-232 (4 fili)
DTE
DCE
Protective Ground (1)
Transmit (2)
Receive (3)
Signal Ground (7)

Standard seriali

RS-232



Connettore 25 pin (vaschetta)

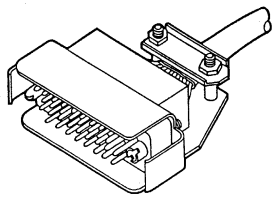


Connettore 9 pin

- è lo standard più diffuso per il collegamento DTE-DCE
- prima versione pubblicata nel 1969, l'ultima revisione risale a 1987 (RS232-D USA e V.28/V.24 EUROPA)
- connettore standard a 25 pin ma più comune quello a 9 pin (es.dietro ai PC)

V.35

Standard simile a RS-232, ma per velocità superiori a 19200 b/s



Standard seriali

RS-422, RS-423, RS-449, RS-530 e V.35

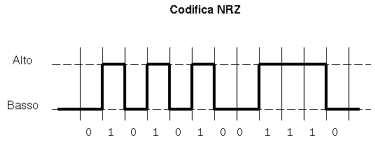
- raggiungono velocità fino a 10 Mb/s impiegando la modalità di
- trasmissione bilanciata: vengono trasmessi contemporaneamente 2 segnali opposti su due fili

Tipi di codifica del segnale digitale

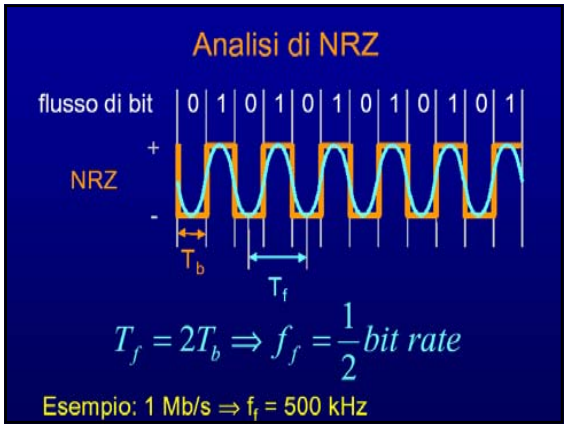
- NRZ (Non Return to Zero)
- Manchester
- NRZI (Non Return to Zero Inverted)
- MLT-3

- In ogni codifica si definisce un intervallo di switch o di campionamento, corrispondente all'intervallo temporale in cui e' definito un bit. L'inverso di questo intervallo e' la frequenza di bit.
- Si definisce frequenza fondamentale, che e' la massima frequenza di switch necessaria al tipo di codifica.
- A seconda del tipo la frequenza fondamentale puo' essere la frequenza di bit o un sottomultiplo di essa, ed influenza la larghezza della banda necessaria alla trasmissione di un segnale con una certa bit rate.

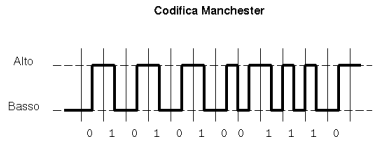
Codifica NRZ



- La codifica Non Return to Zero prevede due livelli di voltaggio (o altro fenomeno fisico), basso ed alto, corrispondenti ai bit 0 ed 1. Ogni bit occupa un intervallo di switch. Le transizioni avvengono ai confini tra intervalli di switch.
- Per NRZ esiste il problema della sincronizzazione, che viene risolto allungando le sequenze di bit da trasmettere ed inserendo bit aggiuntivi che garantiscano un numero minimo di transizioni regolarmente, p.es. 4B5B o 5B6B.
- La codifica NRZ con 5B6B e' prevista dallo standard IEEE 802.12 e raggiunge velocita' di 100 Mb/s su doppini di rame e fibre ottiche.

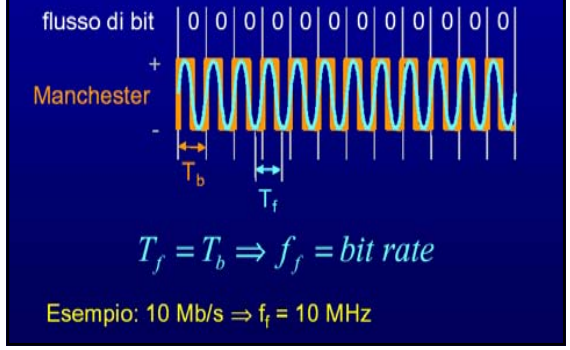


Codifica di Manchester

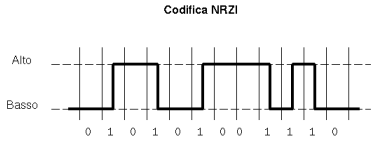


- In ogni intervallo di switch avviene almeno una transizione, a meta' dell'intervallo stesso. La transizione e' da livello basso ad alto per uno 0 e da alto a basso per un 1. In caso di due bit consecutivi differenti vi e' una sola transizione per intervallo, se i bit consecutivi sono uguali avviene una ulteriore transizione di ritorno all'inizio dell'intervallo.
- La codifica di Manchester si chiama anche codifica differenziale.
- E' garantita la sincronizzazione e nel caso peggiore richeide il doppio di banda rispetto alla codifica NRZ.
- La codifica di Manchester e' usata nelle reti Ethernet a 10 Mb/s e Token Ring.

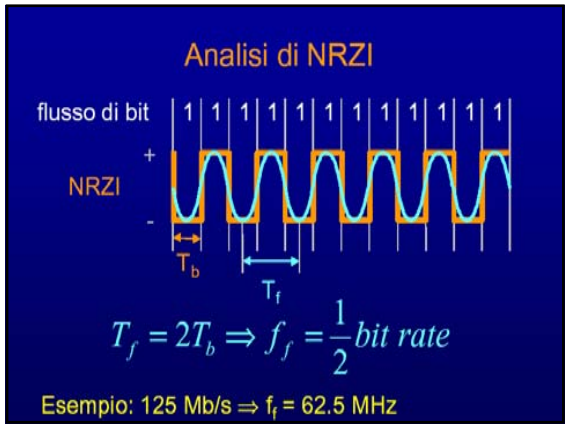
Analisi della codifica Manchester



Codifica NRZI

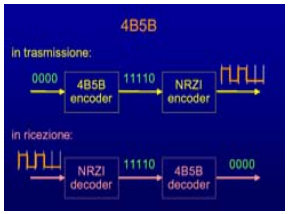


- Il *Non Return to Zero Inverted on one* prevede una transizione per i bit a 1, a meta' dell'intervallo di switch, e nessuna transizione per i bit a 0.
- In caso di una lunga sequenza di zeri consecutivi si potrebbe avere la perdita di sincronizzazione.
- La massima frequenza è determinata dalla sequenza di tutti 1 e risulta uguale a quella di NRZ
- La codifica NRZI e' usata per FDDI su fibra ottica.



Codifica 4B-5B

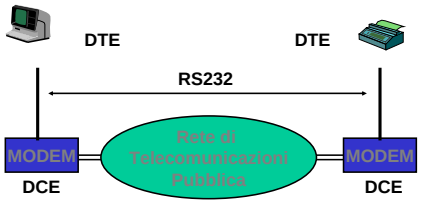
- Per garantire il sincronismo si utilizza una codifica dei dati da trasmettere: 4B5B
- Si codifica gruppi di 4 bit in gruppi di 5 bit in modo che la sequenza contenga un numero prestabilito di 1 per avere un certo numero di transizioni



MODEM: MOdulatore e DEModulatore

Si utilizzano per effettuare trasmissioni seriali su rete pubblica
Trasformano il segnale da digitale ad analogico e viceversa
Rendono il segnale idoneo alla trasmissione su rete pubblica

Esempio di utilizzo di MODEM



Standard per Modem

V.21	**300 b/s**
V.22	**1200 b/s (Bell 212A)**
V.22 bis	**2400, 1200 b/s**
V.23	**75/1200 b/s usato per Videotel**
V.32	**9600, 4800 b/s**
V.32 bis	**14400, 12000, 9600, 7200, 4800 b/s**
V.34	**33600, 31200, 28800, 26400, 24000, 21600, 19200, 16800, 14400, …. b/s**

Livello di collegamento o data-link

- Il livello di collegamento garantisce una comunicazione sufficientemente affidabile ed efficiente tra nodi adiacenti
- Permette la condivisione del mezzo trasmissivo tra diversi utenti (Reti locali)
- Servizi offerti al livello di rete:
  - Senza connessione e senza riscontro
  - Senza connessione e con riscontro
  - Con connessione e con riscontro

Livello di collegamento
Tipi di servizi

- Servizi senza connessione e senza riscontro
  - Adatti al caso in cui il mezzo trasmissivo è affidabile
  - Tipicamente usato nelle LAN
  - Introduce ritardi minimi
  - adatto a servizi real-time (es.audio/video)

- Servizi senza connessione ma con riscontro
  - Utilizzati quando il mezzo trasmissivo è poco affidabile
  - Richiede la trasmissione di messaggi di riscontro
  - Un messaggio di riscontro che viene perso può provocare la ricezione multipla di un pacchetto

Livello di collegamento
Tipi di servizi

- Servizi con connessione e con riscontro
  - Prevede la numerazione e il controllo del corretto ricevimento di tutti i pacchetti
  - Garantisce che ogni pacchetto venga ricevuto una ed una sola volta
  - Garantisce che tutti i pacchetti vengano ricevuti nello stesso ordine con cui sono stati trasmessi

Funzioni del livello data-link

- Costruzione dei frame o impacchettamento dei dati
  - permette di dividere i dati trasportati dal livello fisico in frame
- Controllo degli errori
- Controllo di flusso

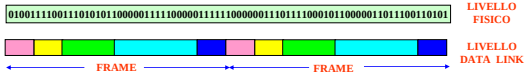
Protocolli del livello data-link

- Definiscono il formato della trama
- Definiscono i messaggi di feedback per il controllo di flusso
- Definiscono gli algoritmi per la gestione trasmissione e per l'accesso al mezzo

APPLICAZIONE
PRESENTAZIONE
SESSIONE
TRASPORTO
RETE
COLLEGAMENTO
FISICO

Livello di collegamento o data link

- Il livello di data link organizza una struttura nei dati trasmessi dividendoli in frame o trame e provvede alla trasmissione in modo corretto di tali frame.



- **A livello fisico i dati sono una sequenza senza nessuna struttura**
- **A livello di collegamento ogni gruppo di dati (rappresentati nel disegno con colre diverso) hanno un significato e svolgono operazioni diverse**

PRINCIPALI FUNZIONI SVOLTE DAL LIVELLO DI COLLEGAMENTO

- **suddivide in frame i bit forniti dal livello fisico;**
- **controlla la presenza di errori e può gestire meccanismi di correzione di tali errori;**
- **regola il flusso in trasmissione in modo che un ricevitore lento non risulti sommerso dai dati da parte di un trasmettitore veloce.**
- **fornisce servizi al livello di rete**
- **definisce l'accesso multiplo da parte di diversi utenti allo stesso canale di comunicazione**

Introduzione dei caratteri di inizio e fine

- In questo sistema sono introdotti dei caratteri ASCII all'inizio ed alla fine del frame;
- Il frame ha inizio con i due caratteri DLE STX, mentre termina con i caratteri DLE ETX.

Dati da trasmettere

A	B	C	D	E

Dati trasmessi

DLE	SLX	A	B	C	D	E	DLE	ETX

- Può accadere che i caratteri DLE STX o DLE ETX si presentino casualmente tra i dati e quindi si verifichino incertezze sull'inizio o la fine di un frame. Per ovviare a questo problema, il livello di collegamento inserisce un carattere DLE prima di un carattere DLE presente nei dati.

Dati da trasmettere

A	B	DLE	C	D	E

Dati trasmessi

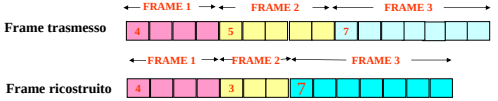
DLE	SLX	A	B	DLE	DLE	C	D	E	DLE	ETX

Conteggio dei caratteri

- Nell'intestazione del frame viene inserito un campo che specifica il numero di caratteri che costituiscono il frame . Attraverso tale informazione il livello di data link al ricevitore può determinare la lunghezza del frame ricevuto.



- Il sistema è molto sensibile agli errori
- Esempio



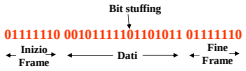
Tecnica di bit stuffing

- Le trame iniziano e finiscono con la sequenza
  01111110
- Per evitare che queste sequenze siano confuse con dati informativi, il livello di collegamento analizza i bit informativi e se incontra cinque bit uguali ad 1 inserisce uno 0

- Esempio

Dati da trasmettere **0010111111101011**

Dati trasmessi



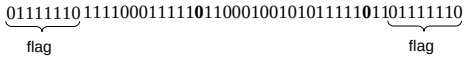
Protocolli orientati al bit

informazione
da trasmettere 1111000111111100010010101111111

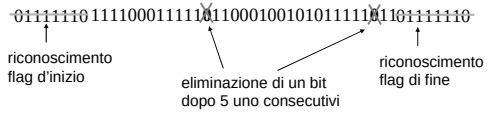
inserimento bit di stuffing

1111000111110**0**1100010010101111110**0**11

trama



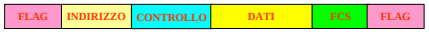
ricezione



Struttura del Frame HDLC

Il protocollo utilizzato a livello di collegamento è HDLC (High Level Data Link Control) o sue versioni semplificate.

FORMATO DEL FRAME HDLC



FLAG	Sequenza 01111110 che individua inizio e fine di un frame
INDIRIZZO	Indirizzo della stazione ricevente
CONTROLLO	Campi per il controllo del collegamento
DATI	Dati informativi - campo di lunghezza variabile
FCS	Simboli di ridondanza per la rivelazione degli errori

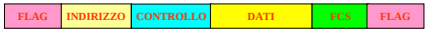
Protocollo HDLC

- Derivano dal protocollo SDLC (Syncronous Data Link Control) utilizzato nell'architettura IBM SNA
- L'ANSI ha standardizzato SDLC come ADCCP (Advanced Data Communication Control Procedure) e l'ISO come HDLC (High-level Data Link Control)
- Il CCITT (poi ITU) ha derivato da HDLC LAP (Link Access Procedure) prima, LAPB (Link Access Procedure Balanced) poi
- Nelle reti locali esiste inoltre sottostrato (MAC) per risolvere problema di accesso multiplo

HDLC (High Level Data Link Control)

- Standard ISO derivato dal protocollo IBM/SNA SDLC (Synchronous Data Link Control)
- Altri protocolli della stessa famiglia:
  - LAPB (Link Access Procedure Balanced)
  - LAPD (Link Access Procedure D-channel)
  - LAPF (Link Access Procedure to Frame mode Bearer Services)
  - LLC (Logical Link Control) - 802.2

Struttura del Frame HDLC

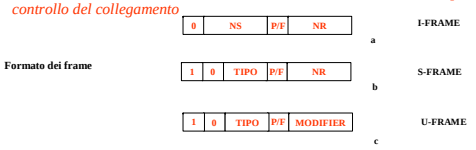


- **Campo indirizzo**
  - Lungo 1 byte, contiene l'indirizzo della stazione ricevente;
  - nel caso di un frame di risposta contiene l'indirizzo della stazione che sta rispondendo.

Struttura del Frame HDLC



- Campo di controllo: lungo 1 o 2 byte, viene utilizzato per diversi scopi
- Esistono tre usi del campo di controllo:
  - *Frame Informativo o I-Frame* : serve a trasmettere le informazioni dell'utente
  - *Frame di Supervisione o S-Frame* : serve a trasmettere informazioni per la gestione del collegamento
  - *Frame non numerato o U-Frame: serve a trasmettere indormazioni per il controllo del collegamento*



HDLC e CDN

- HDLC è idoneo a collegare tramite un CDN:
  - due bridge remoti
  - due router monoprotocollo
- HDLC non fornisce un supporto multiprotocollo nativo e non è quindi adatto a collegare:
  - router multiprotocollo di costruttori diversi
  - brouter

Protocollo SLIP

- E' nato nel 1984 ed è il più vecchio protocollo di livello data link dell'Internet Protocol Suite.
- Molto semplice, nacque per collegare via modem macchine Sun ad Internet. Spedisce sulla linea pacchetti IP
- Ha diverse limitazioni:
  - non c'è controllo degli errori;
  - supporta solo IP, e per di più solo indirizzi statici;
  - non è uno standard ufficiale di Internet.

Protocollo PPP

- Per migliorare le cose, IETF ha prodotto uno standard ufficiale, il ***Point to Point Protocol*** (RFC 1661, 1662 e 1663). Esso è adatto sia a connessioni telefoniche che a linee router-router.
- Il protocollo PPP fornisce le seguenti funzionalità:
  - framing;
  - rilevamento degli errori;
  - un protocollo di controllo per attivare, testare e diasattivare la linea (***LCP, Link Control Protocol***, RFC 1570);
  - supporto di molteplici protocolli di livello network;
  - una famiglia di protocolli per negoziare opzioni di livello network (***NCP, Network Control Protocol***):
  - per ogni livello network supportato c'è un differente NCP;
  - ad esempio, nel caso di IP, NCP viene usato per negoziare un indirizzo IP dinamico;

Protocollo PPP

- Il protocollo è modellato su HDLC, ma presenta alcune differenze:
  - è orientato al carattere e non al bit e utilizza il character stuffing;
  - un campo apposito fornisce il supporto multiprotocollo al livello network.

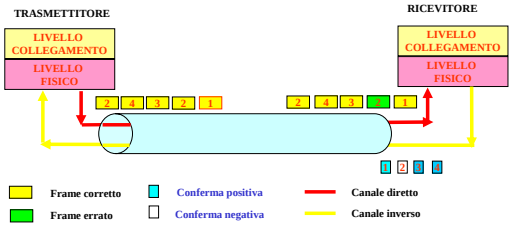
Formato del frame

FLAG	INDIRIZZO	CONTROLLO	PROTOCOL	DATI	FCS	FLAG

FLAG	01111110 come in HDLC
INDIRIZZO	11111111 non ci sono indirizzi in quanto non si gestisce linee multipunto
CONTROLLO	00000011 Rappresenta il valore di default
PROTOCOL	Indica il protocollo di livello 3 e c he si trova nel campo dati (IP, IPX, Novel,..)
DATI	Campo di lunghezza variabile
FCS	Codifica 2 o 4 byte

Tecniche di controllo degli errori

- Le tecniche di controllo di errore consentono di correggere gli errori introdotti dal sistema di comunicazione.
- Il modello OSI utilizza le tecniche ARQ (Automatic Repeat reQuest), in cui sono ritrasmessi i frame che contengono errori.



Protocolli ARQ

- I protocolli ARQ (Automatic Repeat reQuest) sono molto utilizzati per il controllo degli errori
- Il nodo A trasmette un pacchetto e aspetta un riscontro da B. Dopo un prefissato tempo, se non viene ricevuto il riscontro il pacchetto deve essere ritrasmesso
- Se il traffico è bidirezionale, il riscontro può viaggiare nell'intestazione di uno dei pacchetti in arrivo da B ad A (piggybacking)

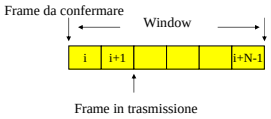
- Possibili problemi:
  - Duplicazioni dei pacchetti : un pacchetto viene ricevuto ma il riscontro viene perduto nella rete oppure il riscontro viene cambiato dal canale.

Protocolli sliding window

- Ogni frame spedito è numerato, da 0 a $N=2^n-1$ (numero progressivo su n bit)

- Trasmettitore
- Il trasmettitore mantiene una finestra di trasmissione che contiene i numeri d'ordine dei pacchetti che può spedire
- permette di spedire frame prima di aver ricevuto i riscontri dei frame precedenti
- i frame appartenenti alla finestra vengono memorizzati per eventuali ritrasmissioni

- Il limite superiore aumenta di 1 quando si trasmette un frame, mentre diminuisce di 1 quando si riceve un riscontro



Protocolli sliding window

- Ricevitore
- Il ricevitore opera nel seguente modo:
  - mantiene una finestra di ricezione attraverso i numeri d'ordine dei pacchetti che può ricevere
  - consente di riconoscere e scartare frame duplicati a causa di riscontri andati perduti
  - permette di accettare frame non ordinati (a causa di frame persi o di ritrasmissioni)

Codici utilizzati

- Sono stati standardizzati i seguenti codici ciclici:
  - ***CRC-12***: $x^{12} + x^{11} + x^3 + x^2 + x^1 + 1$;
  - ***CRC-16***: $x^{16} + x^{15} + x^2 + 1$;
  - ***CRC-CCITT***: $x^{16} + x^{12} + x^5 + 1$;

Codice con 16 bit di ridondanza

- errori singoli e doppi;
- errori di numero dispari di bit;
- errori burst di lunghezza <= 16;
- 99.997% di burst lunghi 17;
- 99.998% di burst lunghi 18.

Controllo d'errore

- In ricezione è possibile che venga riconosciuta una sequenza di bit diversa da quella trasmessa (bit errati)

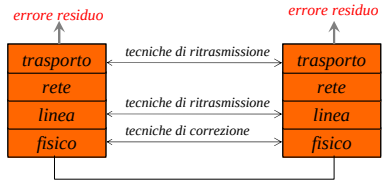
10011010100100100101000101000

10001010100110100101000011000

- cause:
  - rumore termico (mezzi trasmissivi, apparati di ricezione e trasmissione)
  - interferenza da altre trasmissioni sullo stesso mezzo
  - disturbi elettromagnetici
  - perdite di sincronismo
  - ecc.

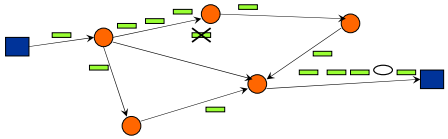
Controllo d'errore

- I livelli della pila possono introdurre dei rimedi agli errori collaborando ad offrire un servizio con basso errore residuo



Perdita di pacchetti

- In una rete è possibile che una unità informativa vada persa
- la tecniche di controllo d'errore vengono usate anche per il recupero dei pacchetti persi



Tecniche di controllo

- Correzione (FEC - forward error correction)
  - codifica di canale
  - aggiunta di ridondanza in trasmissione
  - uso della ridondanza in ricezione per rimediare ai bit errati (se in numero contenuto)
  - teoria dei codici
  - esempio: codice a ripetizione (N volte lo stesso bit); correzione di N/2 -1 errori

Tecniche di controllo

- Ritrasmissione (ARQ - Automatic Repeat reQuest)
  - aggiunta di ridondanza in trasmissione per ogni unità informatica (FCS - Frame Check Sequence)
  - uso della ridondanza in ricezione per rivelare la presenza di errori
  - uso di messaggi di servizio per la richiesta di ritrasmissioni o la conferma di corretta ricezione
  - esempio di FCS: bit di parità

*00110011001110011010010011*1*0*

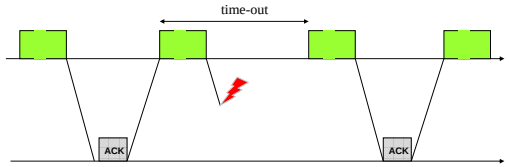
*00110101100011110010100011*0*1*

Protocolli di ritrasmissione

- regole applicate da trasmettitore e ricevitore per rivelare e correggere errori mediante ritrasmissione: protocollo
- messaggi:
  - ACK (acknowledgement): riscontro positivo
  - NACK: riscontro negativo
  - ENQ: richiesta di ripetizione ultimo comando
- anche i messaggi di servizio possono essere corrotti da errori!
- è necessario un canale di ritorno da ricevitore a trasmettitore (no canali monodirezionali)

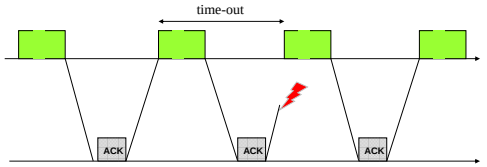
Protocollo *Stop and Wait*

- trasmettere un pacchetto e aspettare il riscontro positivo prima di trasmettere il successivo
- ritrasmissione dopo time-out o NAK



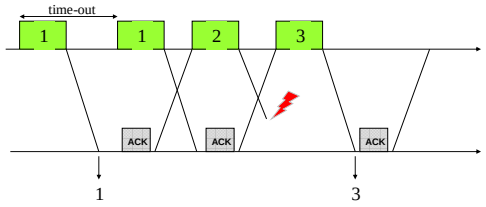
Protocollo *Stop and Wait*

- problema: se si perde l'ACK la trama viene ritrasmessa di nuovo (duplicazione di pacchetti ai livelli superiori)
- rimedio: numerazione delle trame (SN)



Protocollo *Stop and Wait*

- problema: errata interpretazione di un ACK
- rimedio: numerazione anche degli ACK (RN)

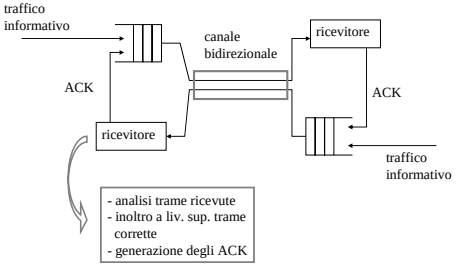


Protocollo *Go-back-n*

- Il trasmettitore può trasmettere fino a *n* pacchetti senza aver avuto il riscontro
- se il riscontro non arriva si ricomincia a trasmettere dalla prima trama non riscontrata ("torna indietro di *n* trame")
- possibile funzionamento full-duplex perché i ritardo negli ACK non sono molto critici

Protocollo *Go-back-n*

- Funzionamento full-duplex



Protocollo *Go-back-n*

- Piggy-backing: gli ACK possono anche essere inseriti negli header dei pacchetti che viaggiano in direzione opposta



- SN: numero di sequenza della trama
- RN: trama attesa in direzione opposta, ovvero riscontro cumulativo delle trame fino a RN-1

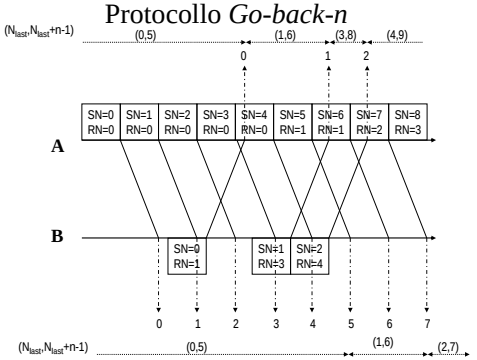
Protocollo *Go-back-n*

- Trasmettitore:
  - N_{last}: ultimo riscontro ricevuto
  - Nc: numero corrente disponibile per prossima trama
  - regole:
    - ogni nuova trama viene accettata per la trasmissione solo se $Nc < N_{last} + N$, altrimenti viene messa in attesa; se $Nc < N_{last} + N$ la trama viene trasmessa con SN pari a Nc e il valore di Nc viene incrementato di uno (Nc := Nc+1);
    - ad ogni riscontro RN ricevuto, si pone Nlast = RN;
    - i pacchetti nella finestra vengono trasmessi senza vincoli di temporizzazione; alla fine la ritrasmissione deve ripartire dalla trama N_{last}.

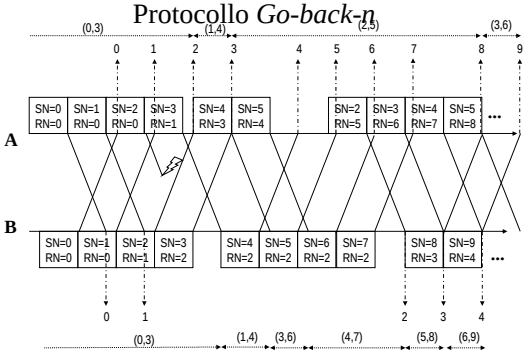
Protocollo *Go-back-n*

- Ricevitore:
  - regole
    - se viene ricevuta correttamente una trama con SN=rn, questa viene inoltrata ai livelli superiori e si pone rn:=rn+1;
    - ad istanti arbitrari ma con ritardo finito, RN viene trasmesso al mittente utilizzando le trame in direzione opposta.
  - intervallo N_{last} e (N_{last}+nN1): finestra di trasmissione

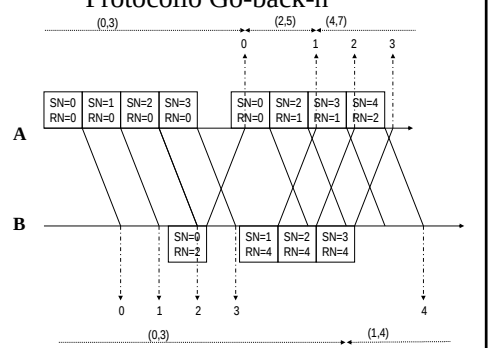
Protocollo *Go-back-n*



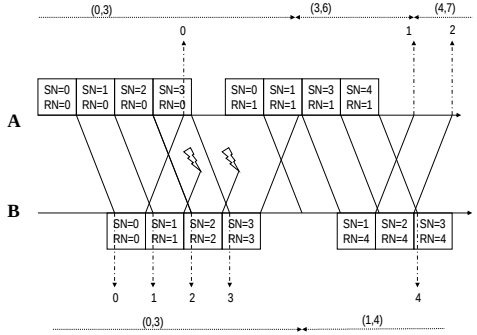
Protocollo *Go-back-n*



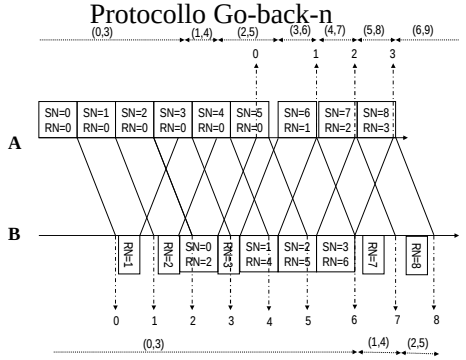
Protocollo Go-back-n



Protocollo Go-back-n



Protocollo Go-back-n



Selective Reject

- Il go back n impone la ristrasmissione anche di pacchetti in realtà ricevuti correttamente
- come alternativa e' possibile pensare di ritrasmettere i soli pacchetti errati: e' questo il funzionamento *selective reject*
- Per consentire un funzionamento di tipo SR sono necessarie funzionalità aggiuntive:
  - riordino dei pacchetti fuori sequenza
  - informazione di ACK per ogni pacchetto

Selective Reject

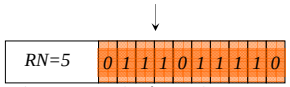
- Riordino pacchetti
  - occorre mantenere un buffer e inoltrare ai livelli superiori solo le sequenze corrette



  - associato a finestra di trasmissione come go-back-n

Selective Reject

- Trasmissione degli ACK
  - ACK singoli per ogni pacchetto
    - ritrasmissione per i pacchetti senza ACK dopo un time-out
  - ACK cumulati piu' bitmap



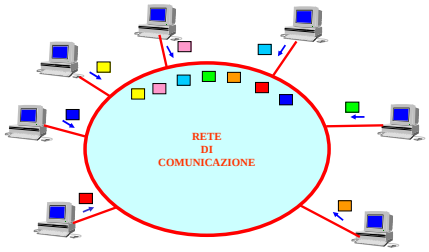
  - l'informazione necessaria e' maggiore

Osservazioni sul controllo d'errore

- Uso del NACK
  - come inviare un NACK dopo la ricezione di una trama errata
  - occorre sapere il SN della trama errata, ma se e' errata …
  - se arriva la trama dopo posso ipotizzare che sia andata persa la trama precedente, ma nei meccanismi in cui non e' garantita la consegna in ordine non e' possibile

Accesso multiplo

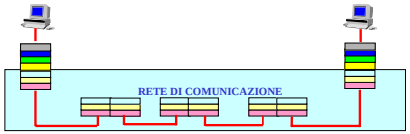
- Le tecniche di accesso multiplo consentono di suddividere il canale di comunicazione tra gli utenti in modo da evitare interferenze.



Livello di rete



Il livello di rete rappresenta spesso il confine tra la rete di comunicazione e i computer.

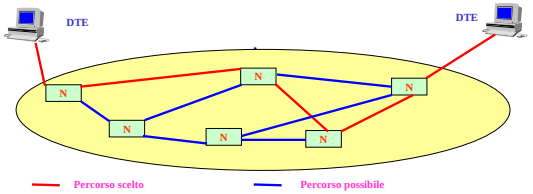


Principali funzioni svolte dal livello di rete :

- servizi offerti al livello di trasporto;
- multiplazione di due o più flussi di dati sullo stesso circuito fisico;
- instradamento o (routing) dei dati dalla stazione di partenza a quella di arrivo. L'instradamento può avvenire mediante due tecniche diverse:
  - circuiti virtuali, in cui tutti i pacchetti utilizzano lo stesso percorso;
  - datagram, in cui i pacchetti possono utilizzare percorsi diversi.
- controllo della congestione della rete;
- interconnessione di reti;
- controllo di errori.

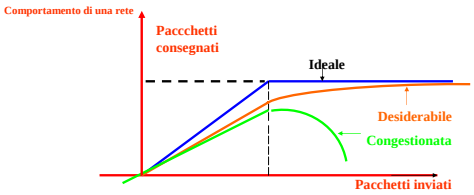
Instradamento dei dati

- Il livello di rete definisce il percorso che deve seguire i dati nella rete di comunicazione per andare dal DTE di trasmissione al DTE in ricezione.



Controllo della Congestione della rete

- Quando in una rete sono presenti troppi pacchetti, le prestazioni della rete degradano rapidamente. Questo fenomeno prende il nome di congestione della rete.
- Le cause che possono provocare la congestione di una rete sono varie; le principali sono:
  - **un traffico troppo pesante nella rete, per cui la rete entra in crisi e non è in grado di smaltire correttamente i pacchetti;**
  - **i nodi del sistema di comunicazione sono troppo lenti rispetto al traffico e non sono in grado di gestire i messaggi in ingresso;**
  - **le linee di uscita dai nodi di commutazione sono troppo lente per gestire il traffico.**



Controllo della Congestione della rete

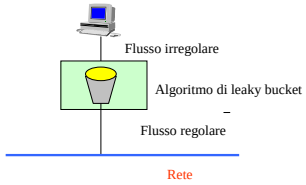
- Il ***controllo della congestione*** è un problema globale di tutta la rete, ed è ben diverso dal problema del controllo di flusso nei livelli data link, network (nel caso dei servizi connection oriented) e trasporto, che invece riguarda una singola connessione sorgente-destinazione.
- Ci sono due approcci al problema della congestione:
  - ***open loop*** (senza controreazione);
  - ***closed loop*** (con controreazione).
- Il primo cerca di impostare le cose in modo che la congestione non si verifichi, ma poi non effettua azioni correttive.
- Il secondo tiene sott'occhio la situazione della rete, intraprendendo le azioni opportune quando necessario.

Traffic shaping

- In questo approccio l'idea è di forzare la trasmissione dei pacchetti a un ritmo piuttosto regolare, onde limitare la possibilità di congestioni.
- Le tecniche per il traffic shaping più importanti sono:
  - ***leaky bucket***;
  - ***token bucket***;
  - ***flow specification***.

Leaky bucket
(secchio che perde)

- L'idea è semplice, e trova un analogia reale in un secchio che viene riempito da un rubinetto (che può essere continuamente manovrato in modo da risultare più o meno aperto) e riversa l'acqua che contiene attraverso un forellino sul fondo, a ritmo costante. Se viene immessa troppa acqua, essa fuoriesce dal bordo superiore del secchio e si perde.
- Sull'host si realizza (nell'interfaccia di rete o in software) un leaky bucket, che è autorizzato a riversare sulla rete pacchetti con un fissato data rate e che mantiene, nei suoi buffer, quelli accodati per la trasmissione.
- Se l'host genera più pacchetti di quelli che possono essere contenuti nei buffer, essi si perdono.



Algoritmo token bucket
(secchio di gettoni)

- Questa tecnica consente di avere un flusso irregolare che esce sulla rete.
- Un utente che non trasmette o trasmette pochi dati acquista un credito trasmissivo
- Quando un utente ha dati da trasmettere , utilizza il suo credito disponibile e inizia a trasmettere fino all'esaurimento dei dati o del credito
- Il secchio contiene dei ***token***, che si creano con una cadenza prefissata (ad esempio uno ogni millisecondo) fino a che il loro numero raggiunge un valore M prefissato, che corrisponde all'aver riempito il secchio di token.
- Per poter trasmettere un pacchetto (o una certa quantità di byte), deve essere disponibile un token.
- Se ci sono k token nel secchiello e h > k pacchetti da trasmettere, i primi k sono trasmessi subito (al data rate consentito dalla linea) e gli altri devono aspettare dei nuovi token.
- Una differenza importante rispetto al leaky bucket è che i pacchetti non vengono mai scartati (il secchio contiene token, non pacchetti). Se necessario, si avverte il livello superiore, produttore dei dati, di fermarsi per un pò.

Flow specification

- Il traffic shaping è molto efficace se tutti (sorgente, subnet e destinazione) si accordano in merito.
- Un modo di ottenere tale accordo consiste nello specificare:
  - le caratteristiche del traffico che si vuole inviare (data rate, grado di burstiness, ecc.);
  - la qualità del servizio (ritardo massimo, frazione di pacchetti che si può perdere, ecc.).
- Tale accordo si chiama ***flow specification*** e consiste in una struttura dati che descrive le grandezze in questione.

- Sorgente, subnet e destinatario si accordano di conseguenza per la trasmissione.
- Questo accordo viene preso prima di trasmettere, e può essere fatto sia in subnet connesse (e allora si riferisce al circuito virtuale) che in subnet non connesse (e allora si riferisce alla sequenza di pacchetti che sarà trasmessa).

Interconnessione di reti eterogenee

- Esistono architetture di rete con caratteristiche e protocolli diversi, e che differiscono notevolmente tra loro per:
  - i servizi offerti dai vari livelli (connection oriented o no, reliable o no, ecc.);
  - le modalità di indirizzamento;
  - la dimensione massima dei pacchetti.
- Per connettere fra loro reti eterogenee si devono superare problemi non banali, tra i quali:
  - difformità nei servizi offerti (ad esempio, un servizio connected viene offerto solo su una delle reti);
  - difformità nei formati dei pacchetti e degli indirizzi;
  - difformità, nelle subnet, dei meccanismi di controllo dell'errore e della congestione;
  - difformità nella dimensione massima dei pacchetti.

APPLICAZIONE
PRESENTAZIONE
SESSIONE
TRASPORTO
RETE
COLLEGAMENTO
FISICO

Livello di trasporto

- Il livello di trasporto separa i livelli di comunicazione da quelli informatici (più vicini all'applicazione)

Le principali funzioni svolte dal livello di trasporto sono:

- **servizi offerti al livello di sessione;**
  - **Canale punto-punto affidabile , che consegna i dati in ordine e senza errori (con connessione)**
  - **Invio di messaggi isolati con o senza garanzia di consegna (senza connessione)**
  - **Broadcasting di messaggi amolti destinatari (senza connessione)**
- **definizione della qualità del servizio;**
- **controllo del flusso dei dati;**
- **segmentazione e assemblaggio dei dati;**
- **scelta della rete di trasporto;**
- **controllo end-to-end dei dati per prevenire errori e malfunzionamenti e fornire perciò un servizio affidabile al livello di sessione.**

- Il livello di trasporto opera su base end-to-end

Livello di trasporto

- I servizi del livello di trasporto possono essere:
  - servizi affidabili orientati alla connessione (tipici di questo livello);
  - servizi datagram (poco usati in questo livello).
- Essi sono molto simili, come caratteristiche, a quelli corrispondenti del livello di rete, ed hanno gli analoghi vantaggi e svantaggi.
- La scelta effettuata a livello di trasporto può essere effettuata in modo indipendente dal sottosistema di comunicazione (primi tre livelli)

Qualità di servizio

Il livello di trasporto può migliorare la qualità di servizio (QoS) rivelando errori, pacchetti perduti o altri inconvenienti non rivelati alla rete sottostante.

Principali parametri della qualità di servizio nel livello di trasporto

- Ritardo incontrato nell'attraversare la rete;
- Throughput o efficienza, definito come il numero di bit informativi inviati all'utente in 1 sec e il numero di bit informativi che potrebbero essere trasmessi in tale intervallo di tempo.
- Tasso errore residuo: Il tasso di errore residuo presente nei dati dopo il livello di trasporto in ricezione.
- Priorità : Indica la priorità da dare ad alcuni tipi di dati.
- Probabilità di fallimento del trasferimento o reseilence

- L'utente può specificare sia i valori desiderati, sia i valori minimi accettabili.
- Nella fase di instaurazione della connessione tra i due livelli di trasporto viene effettuata la negoziazione della QoS
  - Se non è possibile fornire la qualità di servizio richiesta :
    - O si adegua la QoS richiesta
    - O non si effettua la connessione

APPLICAZIONE
PRESENTAZIONE
SESSIONE
TRASPORTO
RETE
COLLEGAMENTO
FISICO

Livello di sessione

- Il livello di sessione ha la funzione di permettere il dialogo tra programmi applicativi che girano su elaboratori diversi. Il dialogo richiede che venga creata una connessione logica o sessione tra i due programmi.
- Le attività presenti nel livello di sessione sono state standardizzate sia da ISO e da CCITT
- CCITT ha emanato uno standard X.215, che definisce le modalità con cui due programmi sincronizzano lo scambio di dati e stabiliscono dei punti intermedi che permettono di recuperare eventuali malfunzionamenti o di sospendere temporaneamente una sessione per riprenderla in un momento successivo.

- Principali funzioni svolte dal livello di sessione
  - servizi offerti al livello di presentazione
  - formazione della connessione con un altro utente, che viene generalmente indicata con il nome di sessione.
  - sincronismo

Sincronismo

- Il sincronismo viene organizzato inserendo alcuni punti facilmente riconoscibili detti **punti di sincronismo** nell'interno di un messaggio. Se durante una sessione si verificano dei problemi all'istante t, la sessione è in grado di essere ristabilita correttamente ripartendo dal punto di sincronismo precedente.



APPLICAZIONE
PRESENTAZIONE
SESSIONE
TRASPORTO
RETE
COLLEGAMENTO
FISICO

Livello di presentazione

- Il livello di presentazione è costituito da un insieme di funzioni che permettono di definire un formato di riferimento comune in modo da permettere lo scambio di dati tra programmi applicativi in modo intellegibile.
- Si possono definire il tipo di caratteri utilizzati (alfabeto), il tipo dei campi e dei sottocampi, cioè tutto quanto è necessario per consentire che un messaggio generato con un certo programma applicativo venga interpretato correttamente dal livello di presentazione del destinatario
- Il livello di presentazione potrebbe anche non esistere nei casi di macchine omogenee
- Principali funzioni svolte dal livello di presentazione
  - rappresentazione dei dati;
  - compressione dei dati;
  - cifratura dei dati.

Livello di presentazione

- Anche questo livello come quello di sessione, ha visto le sue funzionalita' venirsi a definire con il passare del tempo. Forse occorrerebbe chiamarlo in modo piu' appropriato il Livello di rappresentazione. Il livello di Presentazione ha il compito di preservare il *significato* del messaggio trasportato.
- Le sue funzioni principali sono:
  - fornire un passaggio dal livello Applicazione al livello Sessione
  - fornire un metodo di specifica di strutture dati complesse
  - gestire l'insieme di strutture dati richieste dagli applicativi
  - convertire i dati fra rappresentazioni interne ed esterne

Rappresentazione dati

- Architetture di calcolatore diverse hanno metodi diversi di rappresentare i dati in memoria, in registri della CPU, su linee di comunicazione, ecc. Particolari aspetti sono:
- dimensione in byte di un numero intero, intero corto, lungo, in doppia o quadrupla precisione
- se l'intero venga rappresentato col byte piu' o meno significativo per primo
- se un byte venga rappresentato col bit piu' o meno significativo per primo
- quale codice numerico venga usato per rappresentare i caratteri:
  - ASCII
  - EBCDIC
  - UNICODE
  - codici ISO Latin-1, Latin-2, ecc.
  - codici JIS giapponesi, ecc
- metodo di rappresentazione dei numeri in virgola mobile, numero di byte usati, doppia e quadrupla precisione, ecc.
- Il problema delle diverse rappresentazioni viene solitamente risolto, come in TCP/IP con la definizione di una rappresentazione standard di rete, esterna, un *Network Order*.
- In questo caso e' compito del livello di Presentazione fornire le routines di conversione da rappresentazione interna ad esterna e viceversa.
- ISO ha sviluppato una metodologia di scopo molto ampio, tesa a descrivere le strutture dati usate nel problema di rappresentare, codificare, trasmettere e decodificare le informazioni. Questa metodologia si chiama **Abstract Syntax Notation** ed e' nota con l'acronimo **ASN.1**.

Cifratura dei dati

- **Le attivita' di supporto alla sicurezza possono essere distribuite a vari livelli di qualsiasi modello di comunicazione.**
- **Per il modello OSI i punti piu' adatti sono i livelli Fisico, di Trasporto e di Presentazione.**
- **Quanto piu' in alto si va' nel modello, tanto piu' aumenta la possibilita' di avere software complesso e di maggiore efficacia (e piu' lento).**
- **E' da notare che mentre l'operazione di cifratura avviene a livello Presentazione, l'uso dei dati generati come certificati e segnature elettroniche avviene tipicamente a livello Sessione, come parte dell'attivita' di Identificazione e Autorizzazione.**
- **Gli algoritmi di cifratura sono moltissimi e le implementazioni numerose. Alcune si vanno imponendo di fatto:**
  - **DES (*Data Encryption Standard*) in varie forme: e' a chiave singola e riservato ai cittadini Americani**
  - **Kerberos - a chiave singola, promosso tra gli altri dalla Sun**
  - **vari schemi basati su RSA - a chiave doppia (privata e pubblica), con limitazioni di copyright e di uso da parte dei governi**
  - ***Pretty Good Privacy* (PGP) - a chiave doppia, in varie versioni, alcune delle quali soggette a pesanti restrizioni**

APPLICAZIONE
PRESENTAZIONE
SESSIONE
TRASPORTO
RETE
COLLEGAMENTO
FISICO

Livello applicativo

- Questo e' lo strato software che interagisce con l'utente e che compie il vero lavoro finale per cui il calcolatore e' stato acquistato.
- Esempi di applicativi:
  - file transfer
  - accesso remoto ai file
  - esecuzione di comandi remoti
  - scambio di messaggistica e posta elettronica
  - sessioni di terminale virtuale
  - servizi di directory
  - gestione di basi di dati
  - grafica in rete
  - sistemi di transazioni in rete
  - sistemi informativi
  - interazioni in tempo reale
  - servizi cooperativi

Standard sull'architettura di un sistema sicuro (standard ISO 7498-2)

- Lo standard ISO 7498-2 descrive le caratteristiche e le funzionalità necessarie per garantire la sicurezza in reti aperte quali quelle definite dal modello OSI.
- Le norme ISO 7498-2 definiscono due tipi di attacchi:
  - attacchi passivi
  - attacchi attivi
  - identificano i servizi di sicurezza adatti ad impedire tali attacchi.

Attacchi passivi

- Un attacco passivo ha il fine di acquisire informazioni sul contenuto dei dati, sulle attività di una organizzazione, sulla ubicazione degli interlocutori e sulla struttura del sistema telematico.
- Il sistema di sicurezza pertanto deve fornire i seguenti servizi:
  - *riservatezza dei dati*: garantisce la riservatezza di ogni singola unità di informazione in una comunicazione proteggendo tutti i dati trasmessi, ricevuti e memorizzati.
  - *riservatezza della connessione*: garantisce la riservatezza di tutti i dati trasmessi sulla singola connessione. Protegge solo i dati di una particolare connessione selezionandoli in funzione degli indirizzi di rete dell'applicazione od altro.
  - *riservatezza di campi selezionati*: garantisce la riservatezza di particolari informazioni raggruppate all'interno dei dati utente.
  - *riservatezza del flusso di traffico*: il servizio impedisce l'acquisizione di informazione dalla osservazione delle caratteristiche del traffico dati (ad esempio, dall'osservazione della quantità o della direzione del traffico su di un canale di comunicazione).

Attacchi attivi (1/2)

- Gli attacchi attivi rappresentano i casi in cui un utente non autorizzato non si limita soltanto a leggere i dati o altre informazioni, ma interviene direttamente nel sistema o nel processo di comunicazione.
- Per creare di evitare attacchi attivi, lo standard ISO 7498-2 elenca numerosi servizi di sicurezza che possono essere utilizzati, che sono elencati nel seguito.

- Autenticazione
- Questo servizio fornisce all'entità ricevente la garanzia dell'autenticità dell'entità trasmittente e dei dati ricevuti e può essere erogato in due modalità differenti
- *autenticazione per entità di pari livello*: fornisce all'entità richiedente la garanzia che l'entità dello stesso livello con la quale avviene la comunicazione sia quella dichiarata. Il servizio è fornito al momento dell'instaurazione o, talvolta, durante la fase di trasferimento dati su una connessione per confermare l'identità di una o più entità che stanno dialogando.
- *autenticazione della sorgente dati*: fornisce all'entità ricevente la garanzia che i dati provengono dall'entità di pari livello dichiarata. Il servizio si oppone ad attacchi attivi richiedendo agli interlocutori l'identificazione su ogni pacchetto dati inviato sulla connessione.

Attacchi attivi (2/4)

- Controllo degli accessi
- Il servizio impedisce agli utenti non autorizzati l'uso delle risorse disponibili, accessibili attraverso interconnessioni di sistemi OSI. Può essere applicato per proteggere globalmente una risorsa o per precludere l'uso di alcune sue funzionalità (ad esempio, nel caso di un database le funzioni di lettura, scrittura, cancellazione possono essere protette separatamente).

Attacchi attivi (3/4)

- Integrità dei dati
- Il servizio fornisce la garanzia che l'unità dati ricevuta sia integra, opponendosi così agli attacchi attivi che hanno lo scopo di modificare informazioni scambiate fra due o più utente. Il servizio rileva in ricezione se sono state apportate delle modifiche alla singola unità dati o alla sequenza delle unità dati.
- *integrità della connessione con recupero*: garantisce l'integrità di tutti i dati utente, individuando qualsiasi modifica, inserzione, cancellazione o replica di dati all'interno di una intera sequenza di pacchetti dati. Nel caso di utilizzo del servizio su protocolli muniti di meccanismi di ritrasmissione consente anche il recupero di alterazioni o modifiche. In questo caso la comunicazione non si interrompe ma il servizio segnala comunque la rilevazione dell'attacco. Se il servizio è utilizzato su protocolli non muniti di meccanismi di ritrasmissione il recupero delle informazioni non potrà essere effettuato.
- *integrità della connessione senza recupero*: come nel caso precedente il sistema si accorge di qualunque modifica dei dati, ma non può garantire il recupero dei dati originali indipendentemente da come i protocolli che supportino meccanismi di ritrasmissione dei dati.
- *integrità della connessione per campi selezionati*: garantisce l'integrità di campi selezionati all'interno dei dati utente.

Attacchi attivi (4/4)

- Antiripudio
- Il servizio fornisce la prova di una comunicazione di dati effettuata anche se il mittente o il destinatario tentano di negare tale trasmissione
- si può avere:

- *Anti ripudio con prova alla sorgente*: fornisce la prova della sorgente dei dati. Il servizio protegge il destinatario contro ogni successivo tentativo da parte del mittente di negare l'invio dei dati e il loro contenuto (come la ricezione di una lettera firmata garantisce il destinatario contro ogni tentativo di ripudio del mittente).
- *Anti ripudio con prova della consegna*: fornisce la prova della ricezione dei dati. Il servizio protegge il mittente contro ogni successivo tentativo da parte del destinatario di negare l'avvenuta ricezione dei dati (come la ricevuta di ritorno per una raccomandata).

I servizi di sicurezza nel modello OSI

- Lo standard ISO 7498-2 prevede la possibilità di inserire i servizi di sicurezza in uno o più livelli del modello OSI.
- *La loro introduzione non deve alterare in nessun modo l'indipendenza tra i vari livelli dell'architettura OSI.*
- Nel caso di servizi orientati alla connessione le entità in fase di instaurazione della connessione possono negoziare i tipi di meccanismi ed i parametri da utilizzare per tutta la durata della sessione.
- Nel caso di comunicazione non orientata alla connessione tale richiesta va ripetuta per ogni singola unità dati.
- Nel caso una entità di un certo livello abbia necessità di protezione può invocare sia un meccanismo all'interno del suo livello, sia richiedere servizi di sicurezza al livello sottostante.

Meccanismi di sicurezza nel modello OSI

- Lo standard ISO 7498-2 prevede anche l'uso di vari meccanismi per garantire la sicurezza in un sistema di comunicazione aperto, elencati brevemente nel seguito.
  - *Cifratura:* garantisce la protezione e la riservatezza dei dati.
  - *Firma digitale:* consente di verificare l'identità del mittente
  - *Controllo accessi*: impedisce l'uno di una non autorizzato e improprio di una risorsa. Il controllo degli accessi può avvenire con diversi meccanismi.
  - *Rivelazione delle modifiche:* consente di rivelare alterazioni del messaggio o del flusso dei messaggi in una sessione di una comunicazione. Esso consiste nell'aggiunta al messaggio di un'impronta cifrata, che il destinatario può ricontrollare.
  - *Mutua autenticazione:* consente ad una entità di dimostrare la propria identità oppure di verificare quella dell'interlocutore – si posso utilizzare vari meccanismi quali password o tecniche di cifratura.
  - *Controllo dell'instradamento:* Il sistema sceglie i percorsi nel sistema di comunicazione a seconda dei requisiti sulla sicurezza.

Meccanismi di sicurezza nel modello OSI

Livello fisico

- A questo livello l 'unico meccanismo di sicurezza che può essere utilizzato è la cifratura dei dati.

Livello di collegamento

- In questo livello la cifratura dei dati è utilizzata solo in quei casi in cui è necessario.
- Ad esempio nel caso di protocollo asincrono non è possibile cifrare tutti i dati poiché i bit di start e stop devono essere trasmessi in chiaro poiché servono per identificare l'inizio e la fine del frame.

Livello di rete

- Il livello di rete ha spesso un ruolo importante nella sicurezza di una comunicazione. Ad esempio, poiché ogni pacchetto di dati contiene un indirizzo di rete si possono introdurre i servizi di:
  - Autenticazione
  - controllo dell'instradamento
  - controllo accessi
- La cifratura garantisce la riservatezza della connessione nella modalità end-to-end; infatti cifrando solo la parte dati dei pacchetti in transito la rete ha tutte le informazioni necessarie per l'instradamento.

Meccanismi di sicurezza nel modello OSI

Livello di trasporto

- Utilizzando le tecniche di recupero dei pacchetti dati errati, propri di questo livello, è possibile garantire anche l'integrità dei dati con recupero.

Livello di sessione

- Non sono previsti servizi di sicurezza.

Livello di presentazione

- Il livello di presentazione consente la realizzazione di operazioni di cifratura.

Livello di applicazione

- ***Il modello OSI prevede l'uso di ogni servizio di sicurezza a questo livello. In soluzioni dove è richiesta la diversificazione del grado di protezione sulle diverse applicazioni (realizzabile, ad esempio, con una password diversa per ogni applicazione) questo livello è il più adeguato per ospitare i servizi di sicurezza. L'unico svantaggio è dovuto alla dipendenza che si crea tra la sicurezza e l'applicazione e/o il sistema operativo della macchina.***

Meccanismi di sicurezza nel modello OSI

		Livelli						
		Fisico	Data Link	Rete	Trasporto	Sessione	Presentazione	Applicazione
Servizi	Autenticazione per entità di pari livello			•	•			•
	Autenticazione dell'origine dei dati			•	•			•
	Controllo accessi			•	•			•
	Riservatezza dei dati	•	•	•	•		•	•
	Riservatezza die campi selezionati						•	•
	Riservatezza del flusso del traffico	•		•				•
	Integrità dei dati con recupero				•			•
	Integrità dei dati senza recupero			•	•			•
	Integrità dei dati per campi selezionati							•
	Anti ripudio con prova della sorgente							•
	Anti ripudio con prova della consegna							•