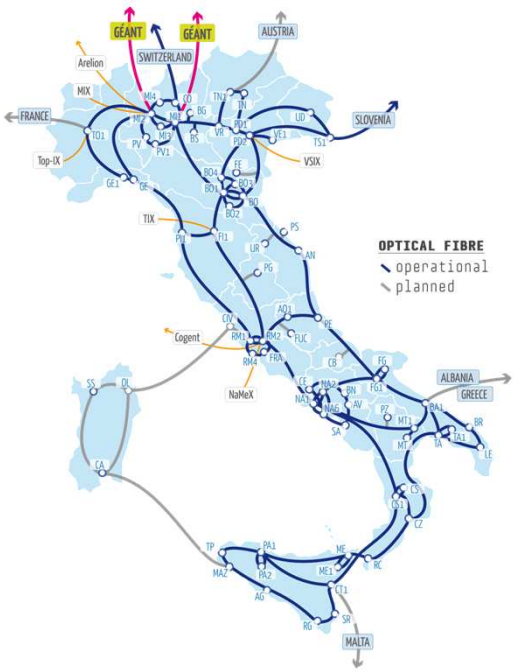

GÉANT
GÉANT
AUSTRIA
SWITZERLAND
Arelion
MIX
FRANCE
SLOVENIA
Top-IX
VSIX
TIX
Cogent
NaMeX
ALBANIA
GREECE
MALTA
OPTICAL FIBRE
operational
planned

Sistemi Interconnessi

“Fun” Internet-connected devices

Amazon Echo

Internet refrigerator

IP picture frame

Pacemaker & Monitor

Tweet-a-watt: monitor energy use

Web-enabled toaster + weather forecaster

Security Camera

Slingbox: remote control cable TV

AR devices

Fitbit

Internet phones

sensorized, bed mattress

Smart TV

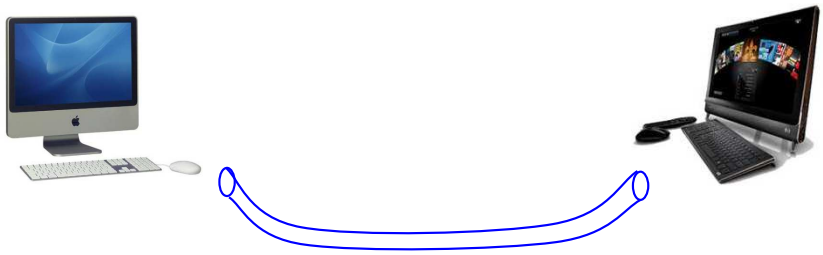
Cloud Computing

“The interesting thing about cloud computing is that we’ve redefined cloud computing to include everything that we already do…. I don’t understand what we would do differently in the light of cloud computing other than change the wording of some of our ads.” (Larry Ellison - CEO Oracle)

Organizzazione di un sistema di comunicazione

Un sistema di comunicazione è composto da due parti:

1) Un mezzo fisico
2) Una struttura logica (software)



What's a protocol?

Human protocols:

- "what's the time?"
- "I have a question"
- introductions

… specific messages sent

… specific actions taken when message received, or other events

Network protocols:

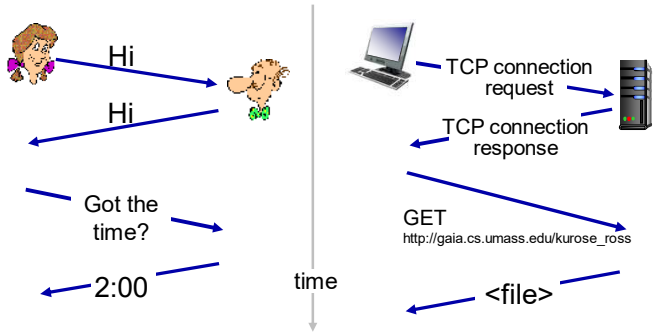
- computers (devices) rather than humans
- all communication activity in Internet governed by protocols

Protocols define the format, order of messages sent and received among network entities, and actions taken on msg transmission, receipt

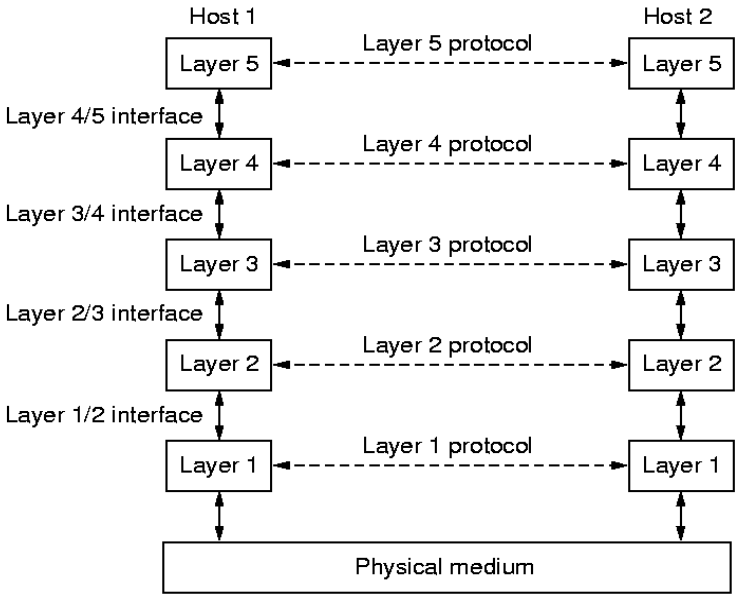
I protocolli definiscono il formato, l'ordine di messaggi inviati e ricevuti tra entità della rete, e Azioni intraprese su MSG Trasmissione, ricezione

What's a protocol?

A human protocol and a computer network protocol:

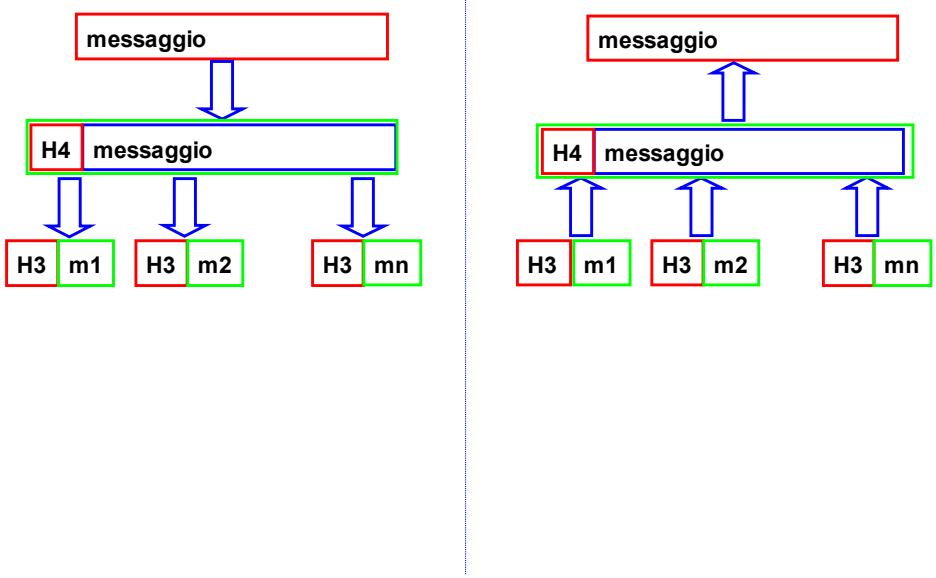


Protocolli

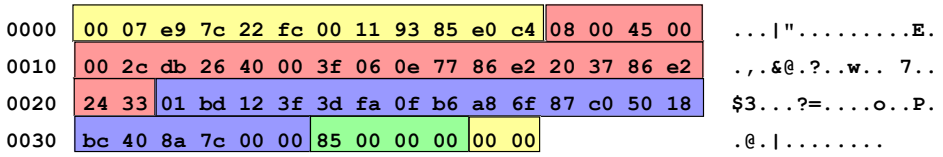

Host 1
Host 2
Layer 5
Layer 5 protocol
Layer 5
Layer 4/5 interface
Layer 4
Layer 4 protocol
Layer 4
Layer 3/4 interface
Layer 3
Layer 3 protocol
Layer 3
Layer 2/3 interface
Layer 2
Layer 2 protocol
Layer 2
Layer 1/2 interface
Layer 1
Layer 1 protocol
Layer 1
Physical medium

Schema di comunicazione

Schema di comunicazione



Protocol Headers



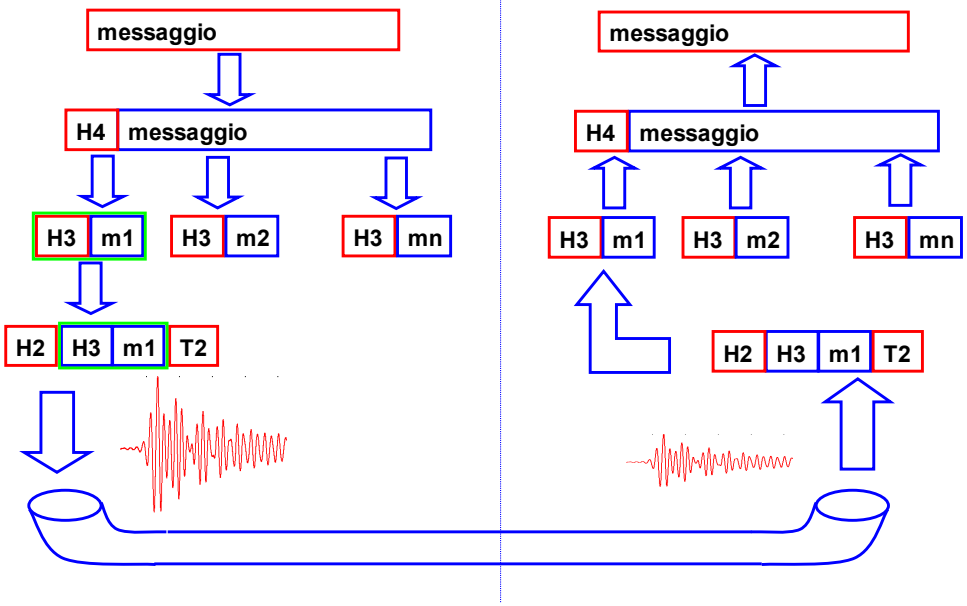

```
Ethernet Header:
src addr:  00 07 e9 7c 22 fc
dest addr: 00 11 93 85 e0 c4
IP Header:
src addr:  134.226.36.55
dest addr: 134.226.36.51
TCP Header:
src port:  445
dest port: 4671
NetBios Information
```

Header Information (56 bytes)

Communication overhead

Payload (4 bytes)

Schema di comunicazione



Problemi

Gli utenti (le applicazioni) voglio un canale di comunicazione (virtuale) affidabile e privo di errori.

Il canale virtuale è implementato utilizzando canali fisici

- il canale fisico può essere simplex, half-duplex o full-duplex
- i messaggi a basso livello non possono essere di lunghezza arbitraria
- un trasmettitore veloce non deve sommergere un ricevitore lento
- bisogna determinare il percorso (migliore ?) per arrivare a destinazione
- l'ordine d'arrivo dei messaggi deve essere uguale a quello di spedizione

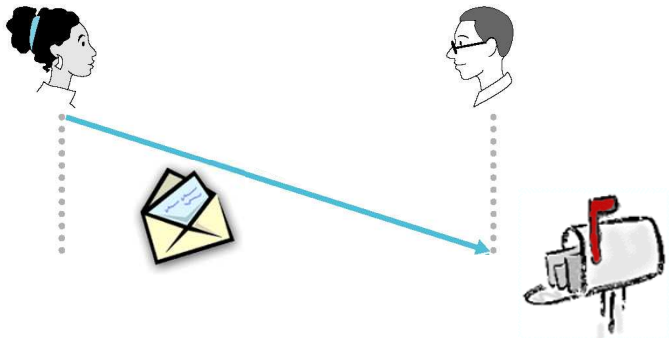
La comunicazione

Connectionless ⇔ **Connection oriented**

Affidabile ⇔ **Non affidabile**

La connessione

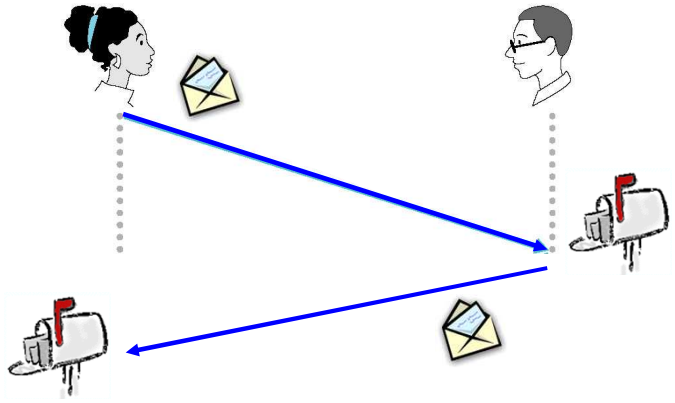
Sistema Connectionless



un protocollo di rete connection-less, ossia senza connessione, si distingue per il fatto che lo scambio di dati a pacchetto tra mittente e destinatario (o destinatari) non richiede l'operazione preliminare di creazione di un circuito, fisico o virtuale, su cui instradare l'intero flusso dati in modo predeterminato e ordinato nel tempo (sequenziale).

La connessione

Connectionless ⇔ Connection oriented

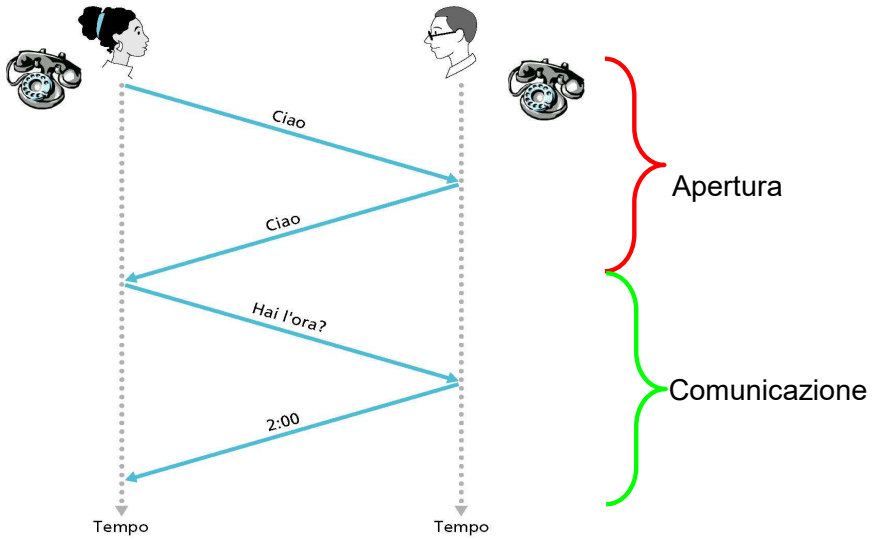


La comunicazione orientata alla connessione è una modalità di comunicazione di rete nelle telecomunicazioni e nelle reti di computer, in cui viene stabilita una sessione di comunicazione o una connessione semipermanente prima che qualsiasi dato utile possa essere trasferito

La connessione

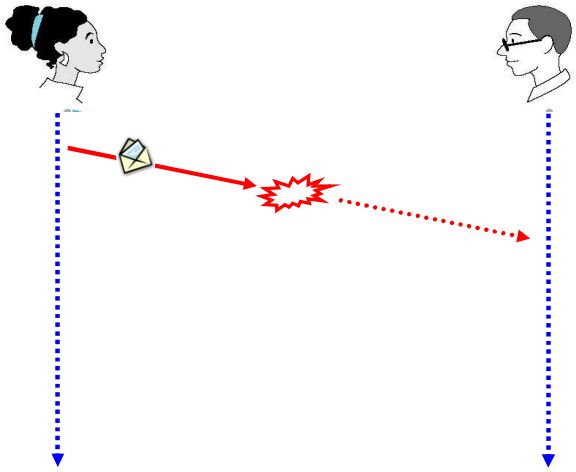
La connessione

Sistema Connection oriented

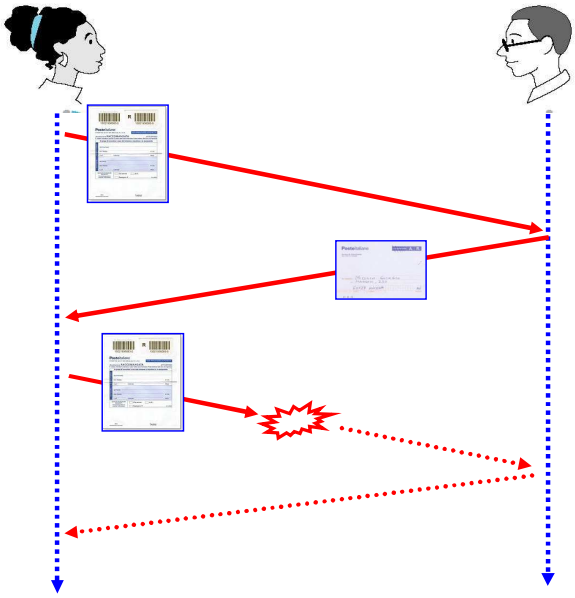


Affidabilità

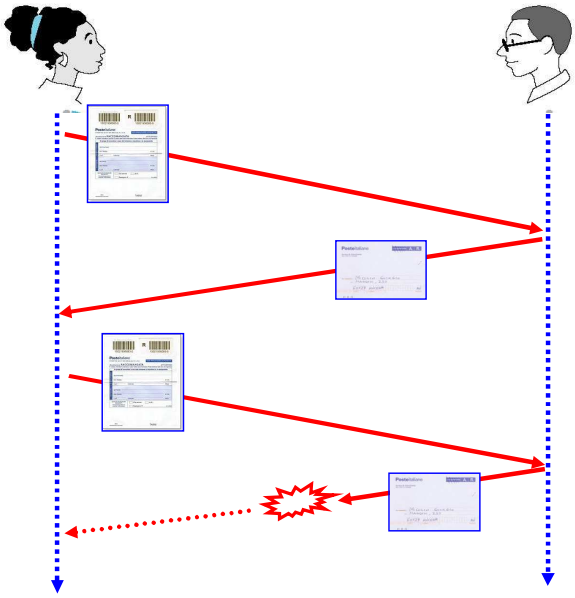
Affidabile ⇔ Non Affidabile



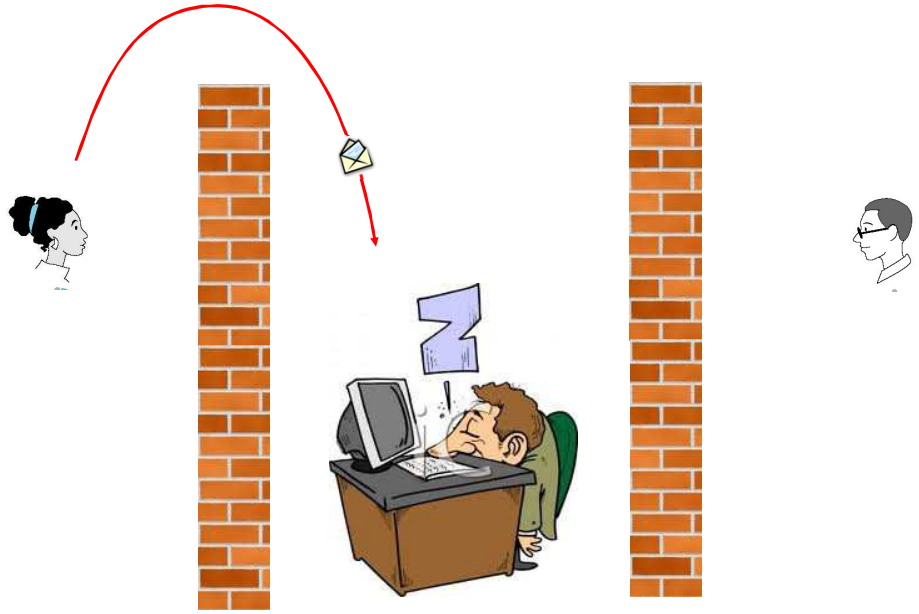
Affidabilità



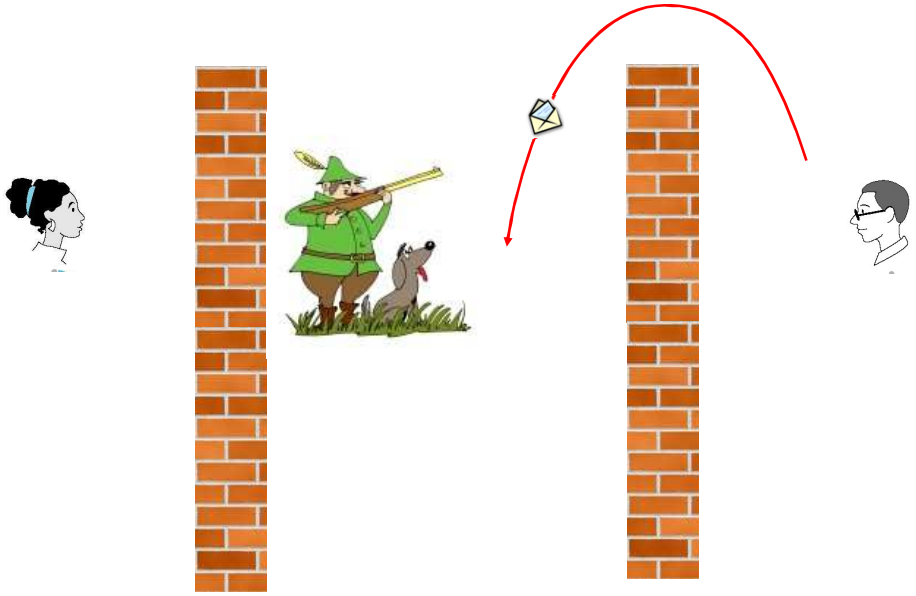
Affidabilità



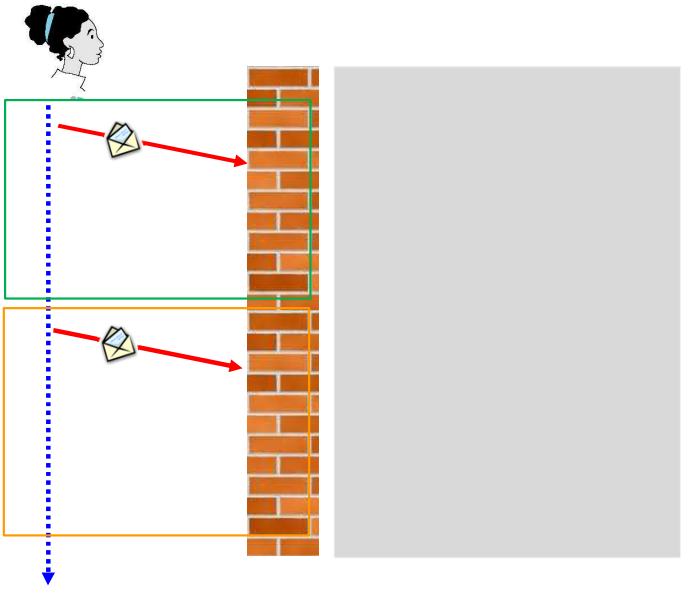
Affidabilità



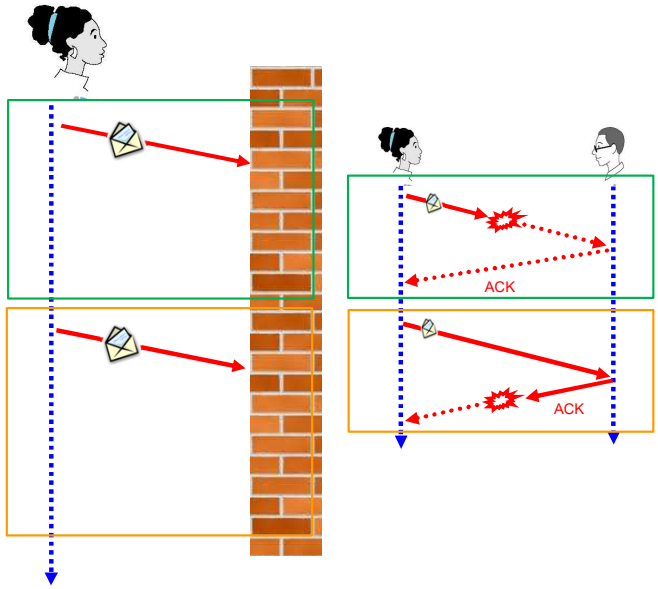
Affidabilità



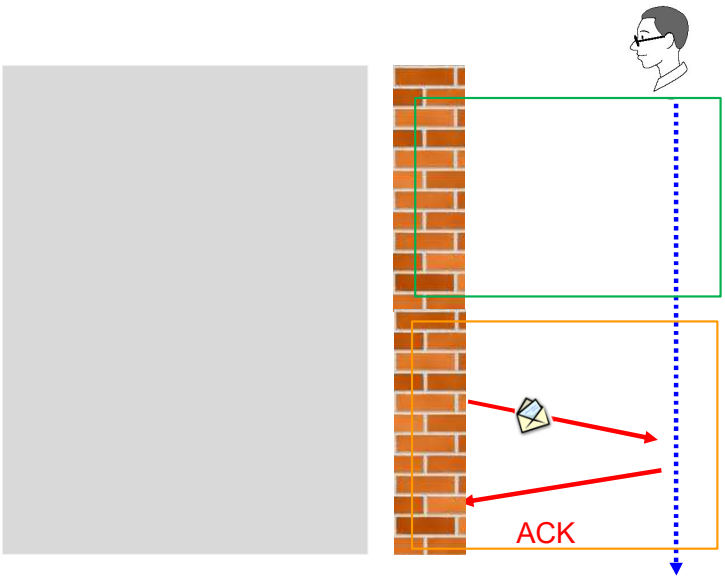
Affidabilità



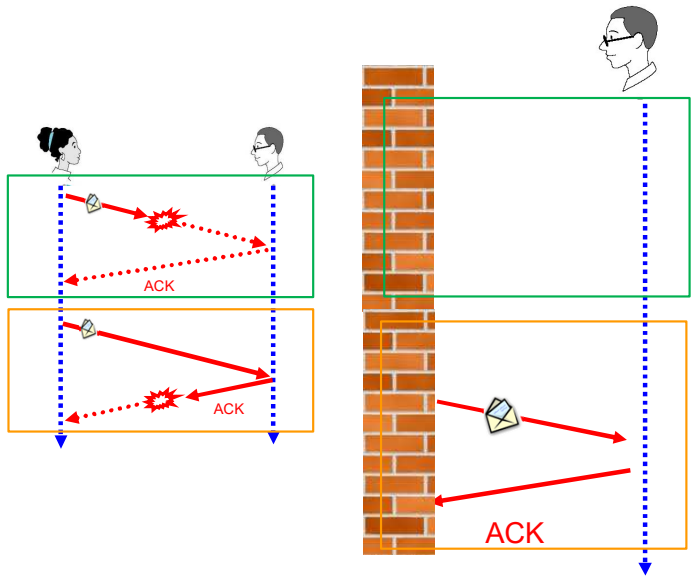
Affidabilità



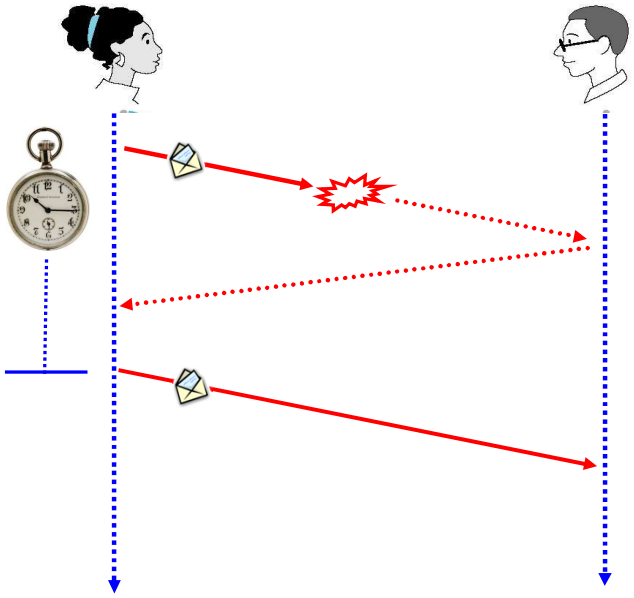
Affidabilità



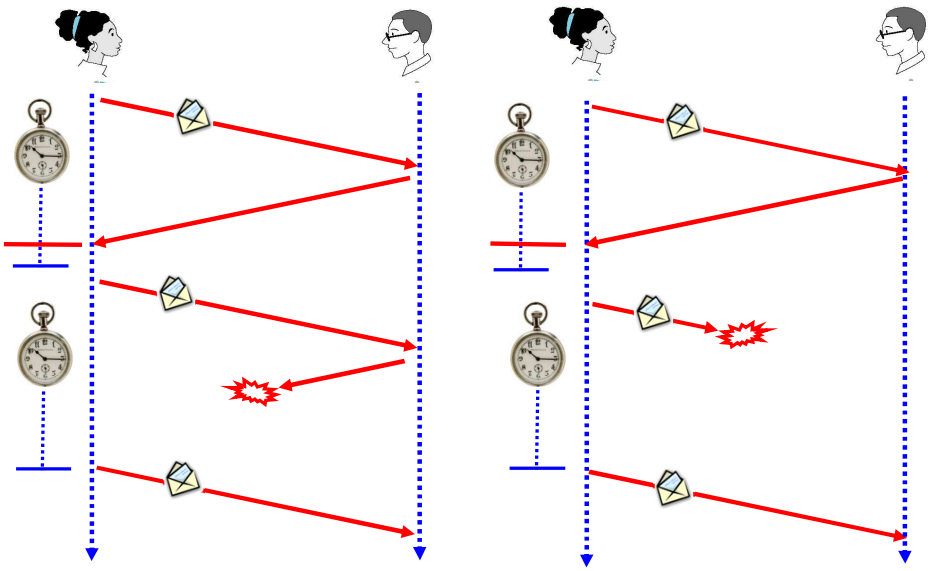
Affidabilità



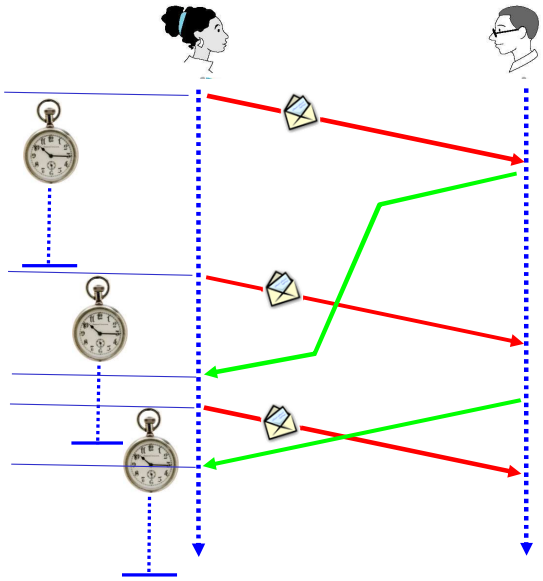
Affidabilità



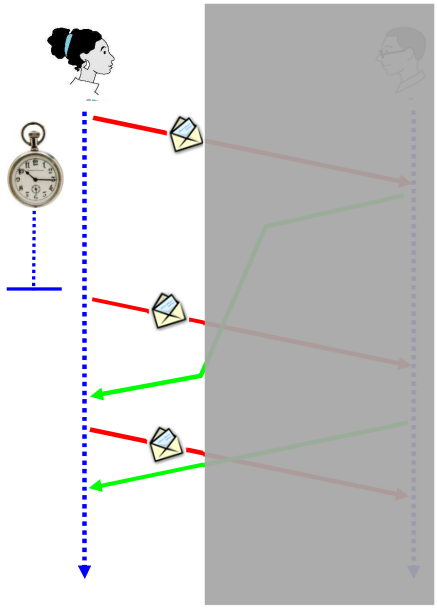
Affidabilità



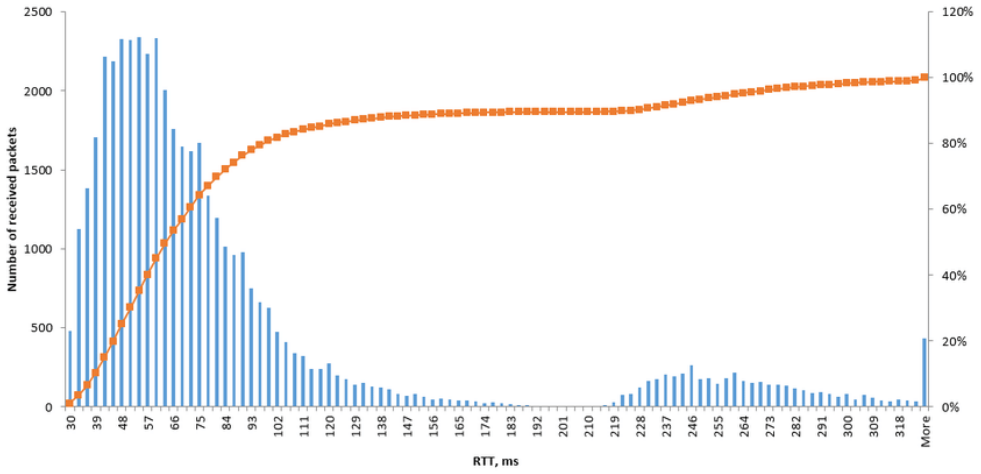
Affidabilità



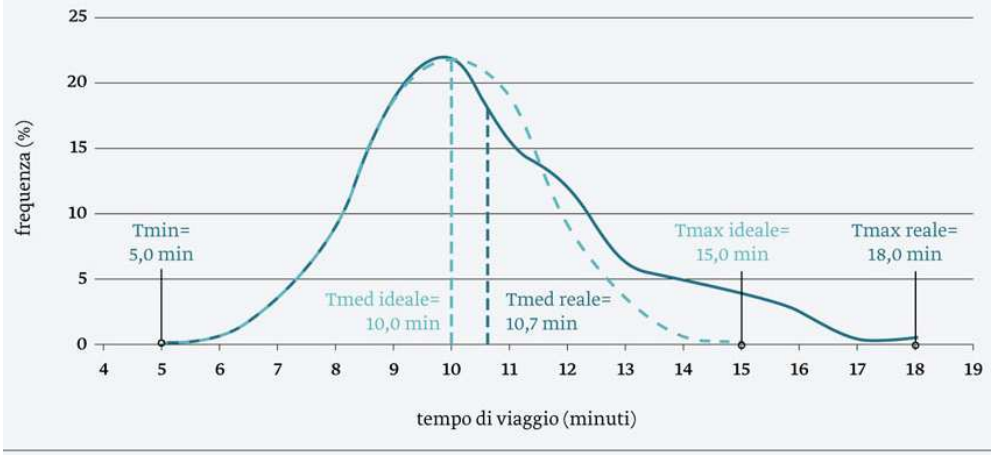
Affidabilità



Distribuzione tempi



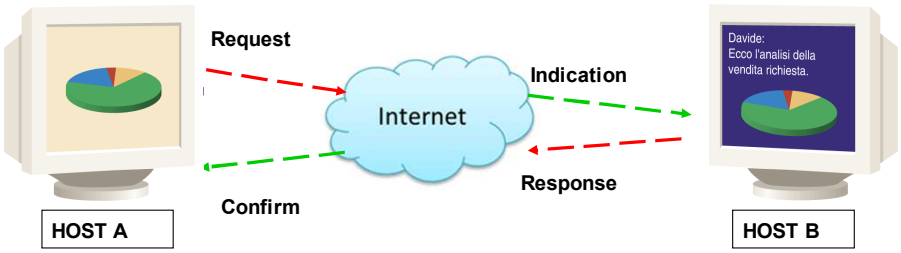
Distribuzione tempi



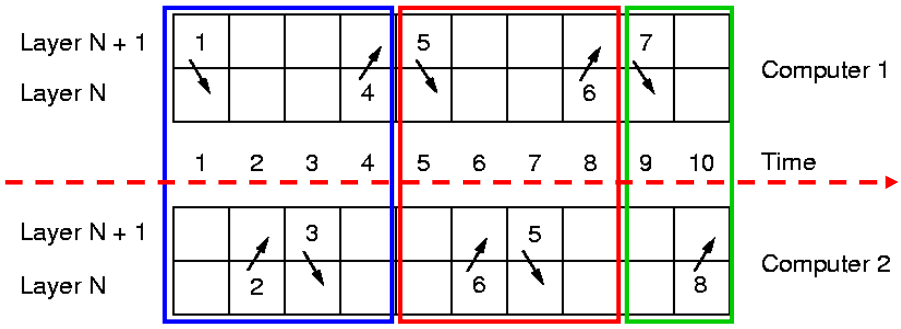
Tipi di Servizi

	Service	Example
Connection-oriented	Reliable message stream	Sequence of pages
	Reliable byte stream	Remote login
	Unreliable connection	Digitized voice
Connection-less	Unreliable datagram	Electronic junk mail
	Acknowledged datagram	Registered mail
	Request-reply	Database query

Primitive di servizio

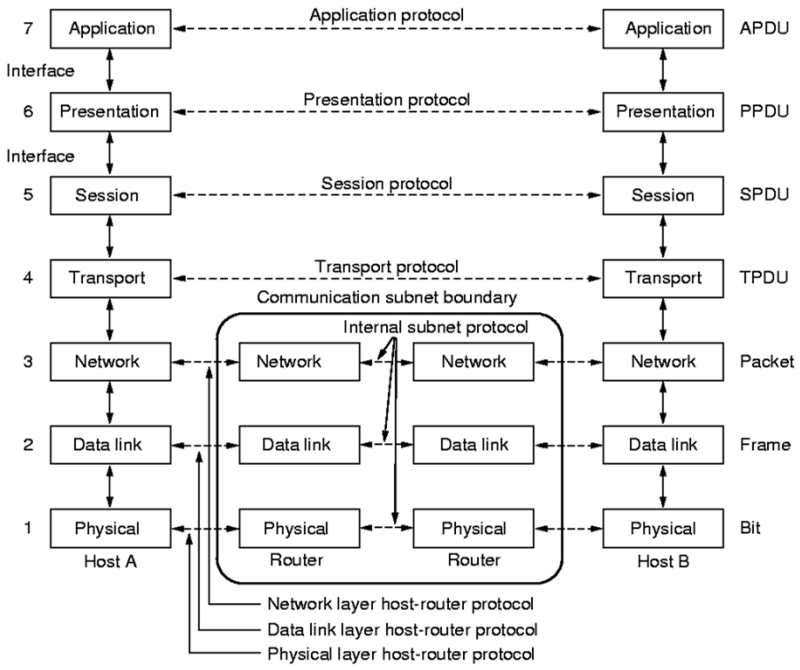


Primitive di servizio



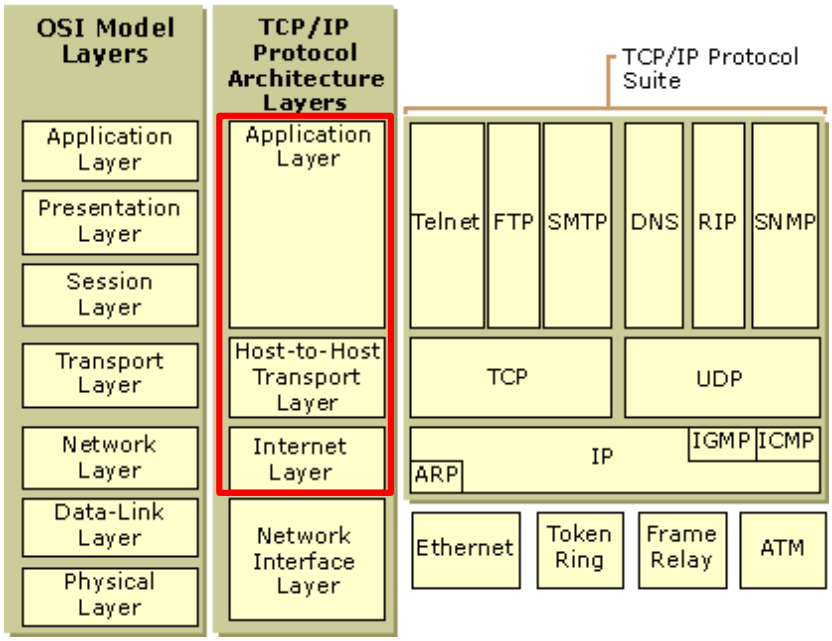
1) CONNECT.request
2) CONNECT.indication
3) CONNECT.respose
4) CONNECT.confirm
5) DATA.request
6) DATA.indication
7) DISCONNECT.request
8) DISCONNECT.indication

Il modello OSI



I sette livelli del modello di riferimento OSI, illustrati nella Figura 1.23 (b), sono: applicazione, presentazione, sessione, trasporto, rete, collegamento e fisico. Le funzionalità di cinque di questi livelli sono più o meno le stesse degli omonimi della controparte Internet, quindi consideriamo i due livelli aggiuntivi presenti nel modello di
riferimento OSI: il livello di presentazione e quello di sessione. Il ruolo del livello di presentazione è fornire servizi che consentono ad applicazioni che vogliono comu nicare di interpretare il significato dei dati scambiati. Questi servizi comprendono la
compressione e la cifratura dei dati (che sono auto esplicative) come pure la descrizione dei dati che libera le applicazioni dalle preoccupazioni riguardo al formato interno nel quale sono rappresentati/memorizzati, che potrebbe essere diverso da un
computer a un altro. Il livello di sessione fornisce la delimitazione e la sincronizza zione dello scambio di dati, compresi i mezzi per costruire uno schema di controllo
e di recupero degli stessi.

OSI e TCP/IP

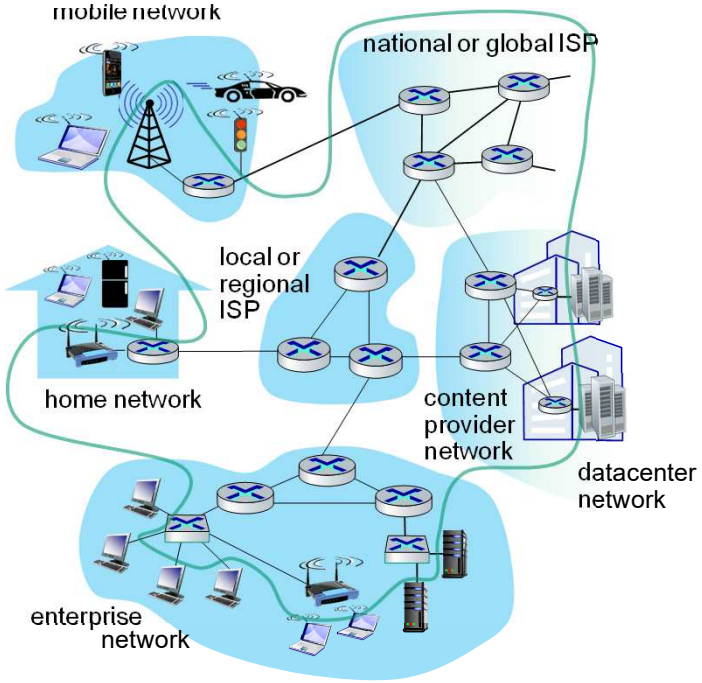


25 Reti di Calcolatori 38

TCP (Transmission Control Protocol) è uno dei protocolli principali della suite di protocolli Internet. Si trova tra i livelli di applicazione e di rete che vengono utilizzati per fornire servizi di consegna affidabili. È un protocollo orientato alla connessione per le comunicazioni che aiuta nello scambio di messaggi tra i diversi dispositivi su una rete.

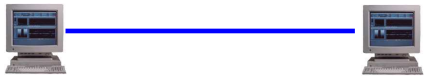
L'Internet Protocol Address, in breve "indirizzo IP" o semplicemente "IP", si basa sul protocollo Internet, su cui poggia anche Internet stesso. Esso rappresenta l'indirizzo chiaramente identificabile di un dispositivo (ad esempio computer, server web, stampanti) in una rete interna o esterna.

Tipologie di rete



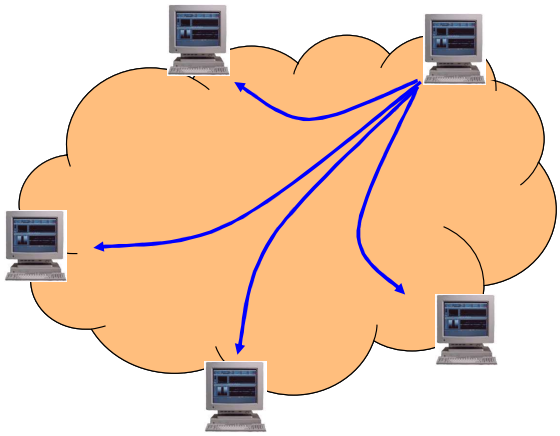
Tipologie di Rete

Punto – Punto

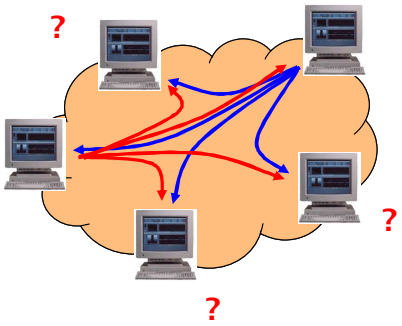


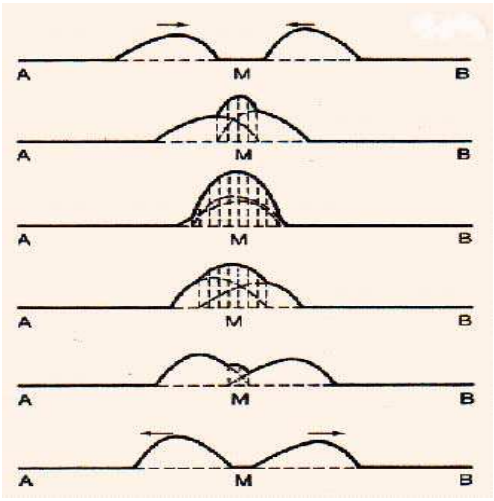
Broadcast

Tipologie di Rete



Tipologie di Rete

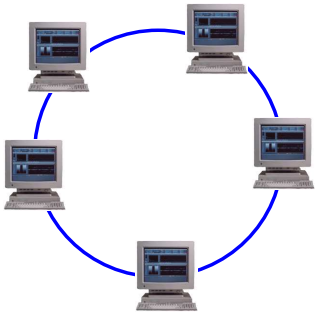




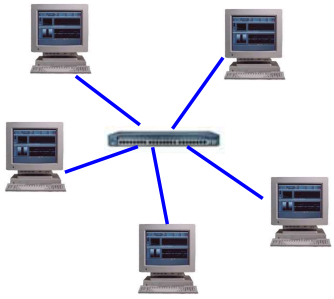
Broadcast

A Bus condiviso

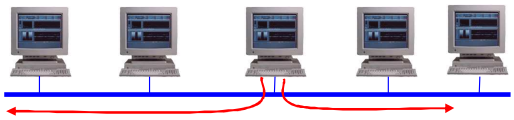
Ad Anello

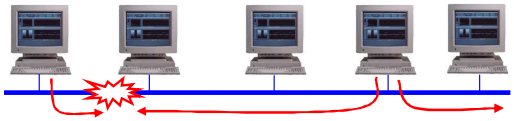


A Stella

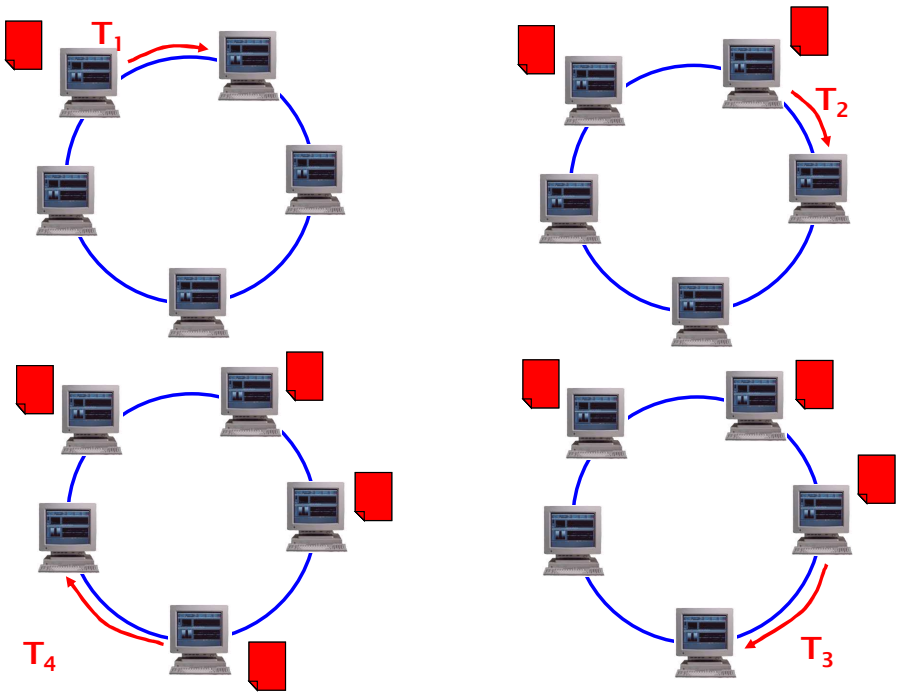


Broadcast

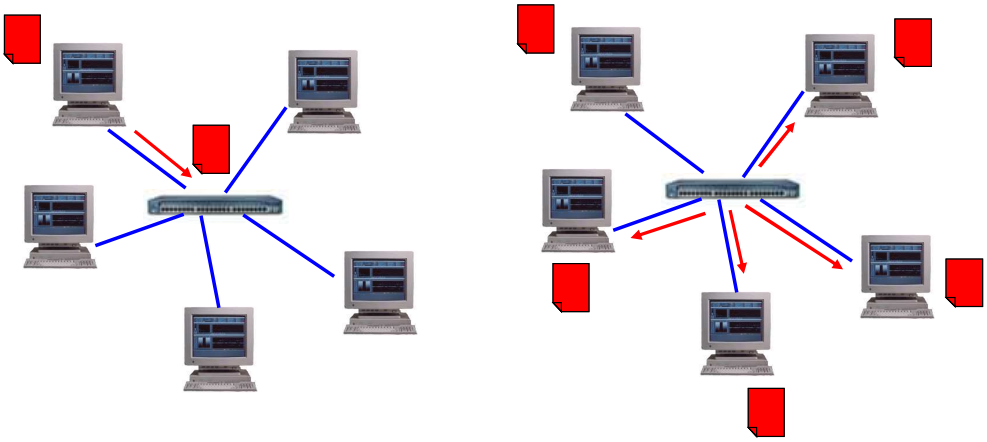




Broadcast

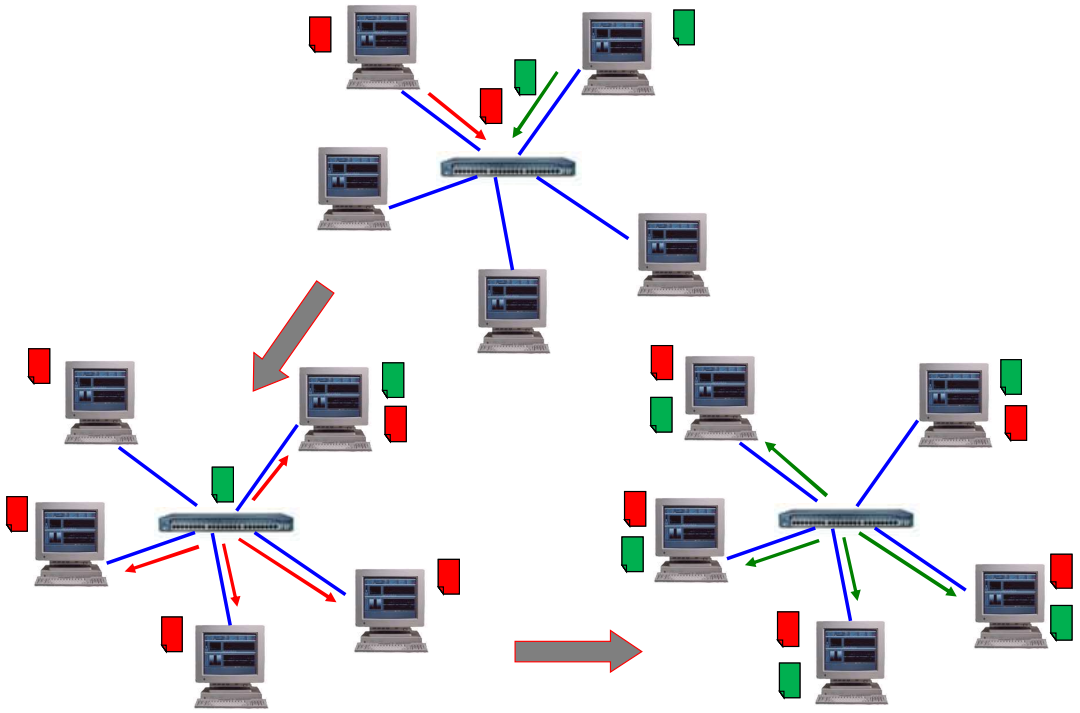


Broadcast



Università di Catania

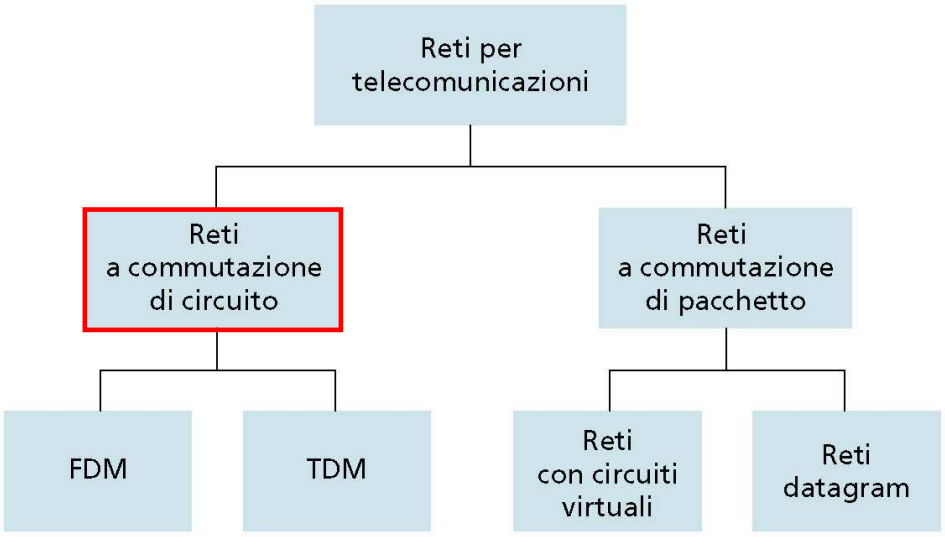
Broadcast



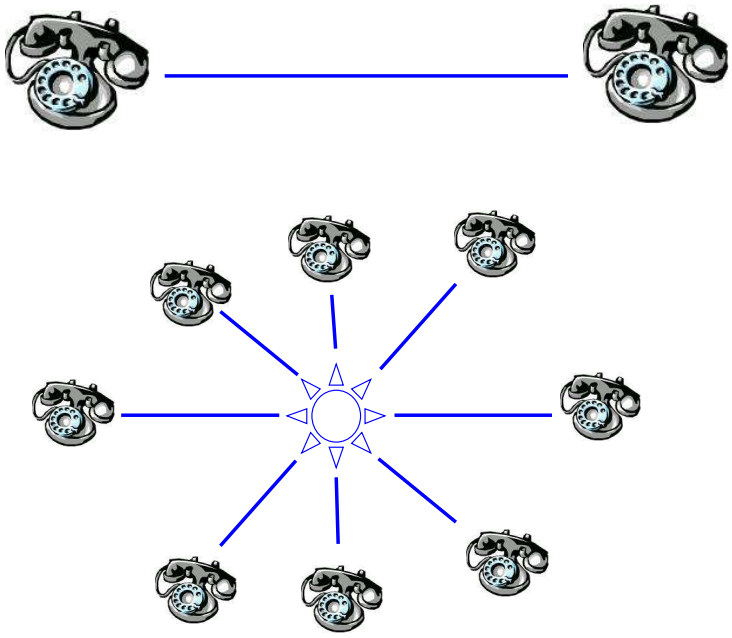
Tassonomia

Interprocessor distance	Processors located in same	Example
1 m	Square meter	Personal area network
10 m	Room	Local area network
100 m	Building	
1 km	Campus	
10 km	City	Metropolitan area network
100 km	Country	Wide area network
1000 km	Continent	
10,000 km	Planet	The Internet

Tassonomia


Reti per telecomunicazioni
Reti a commutazione di circuito
Reti a commutazione di pacchetto
FDM
TDM
Reti con circuiti virtuali
Reti datagram

Sistema Telefonico

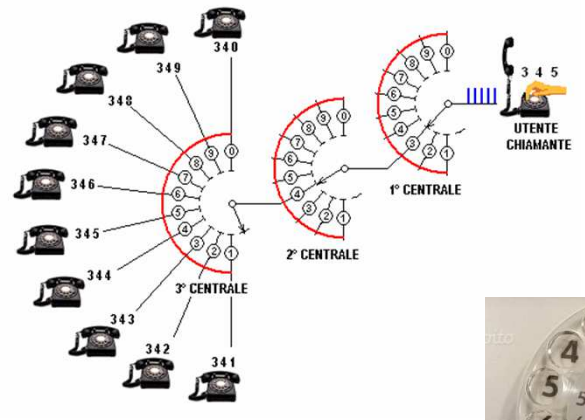


Sistema Telefonico

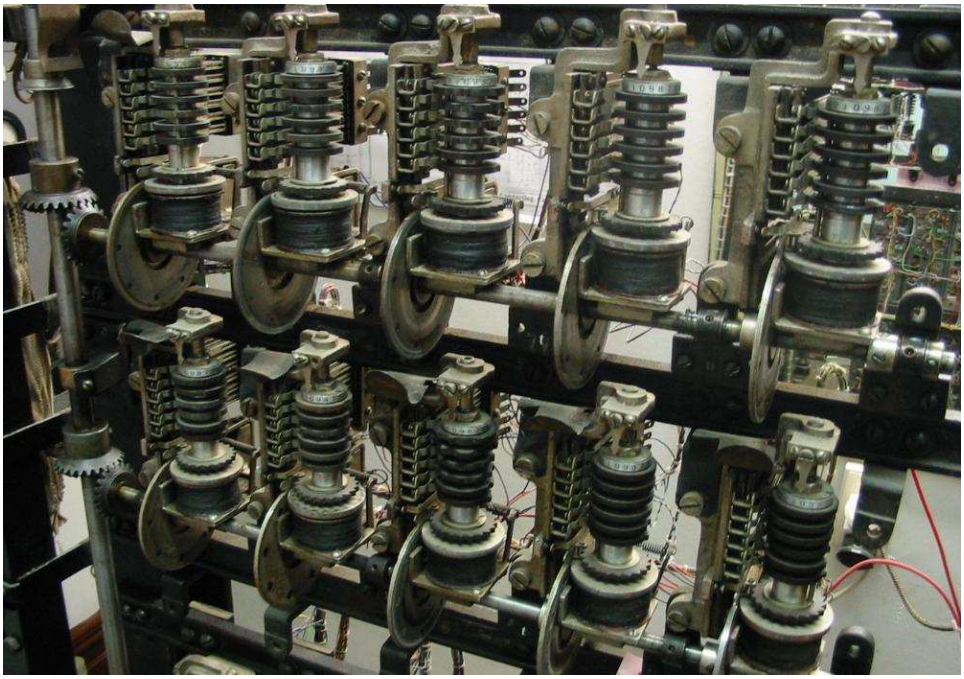
Cosa manca?

Sistema Telefonico

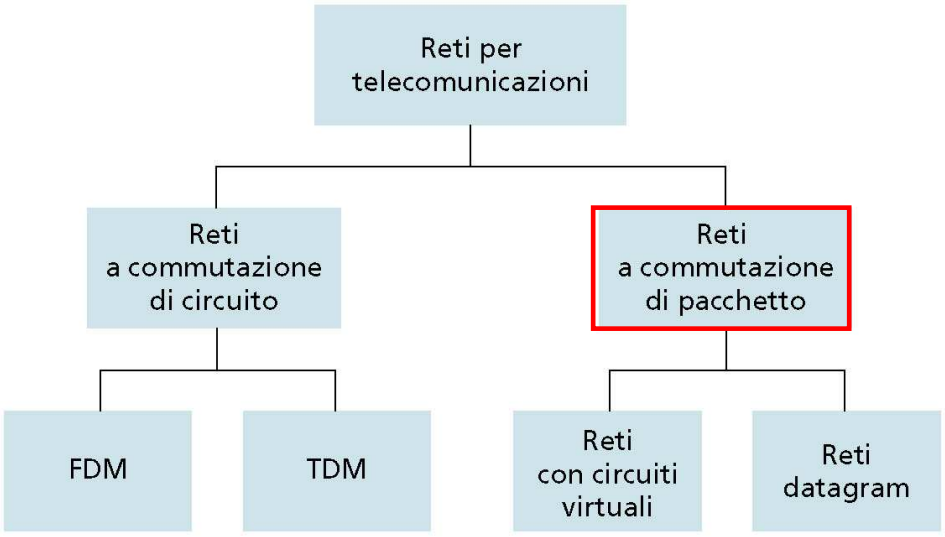
Commutazione di circuito



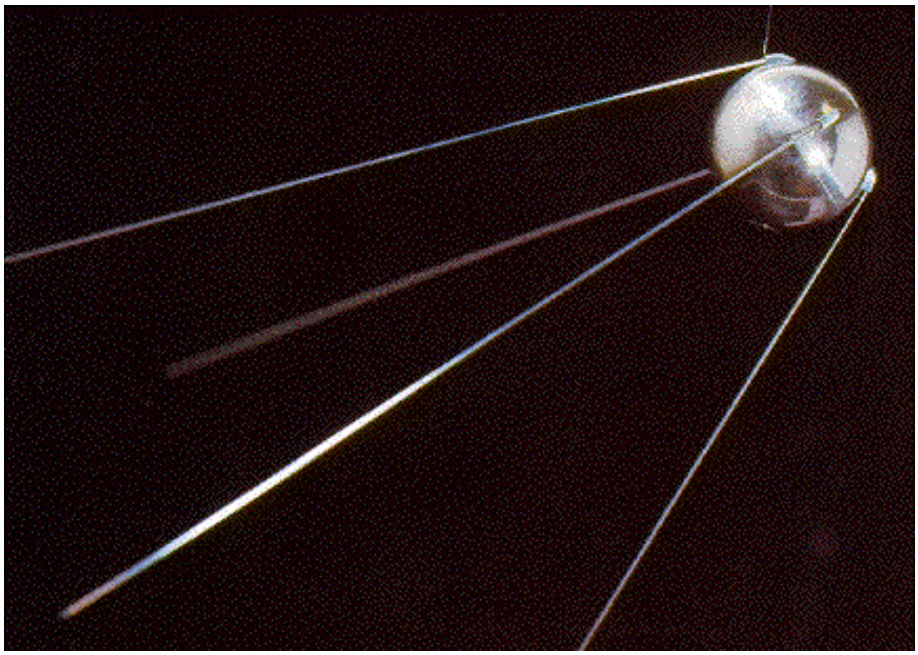
Commutazione di circuito



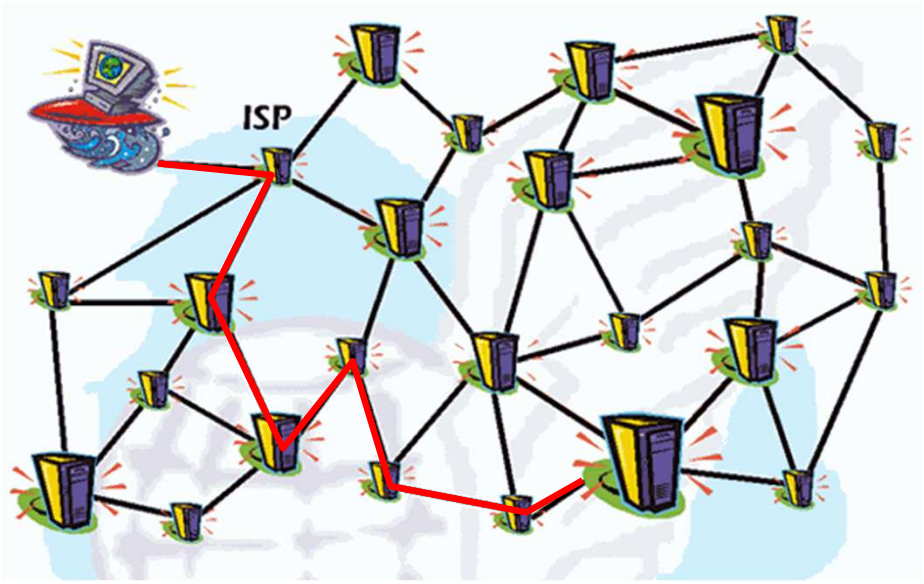
Tassonomia


Reti per telecomunicazioni
Reti a commutazione di circuito
Reti a commutazione di pacchetto
FDM
TDM
Reti con circuiti virtuali
Reti datagram

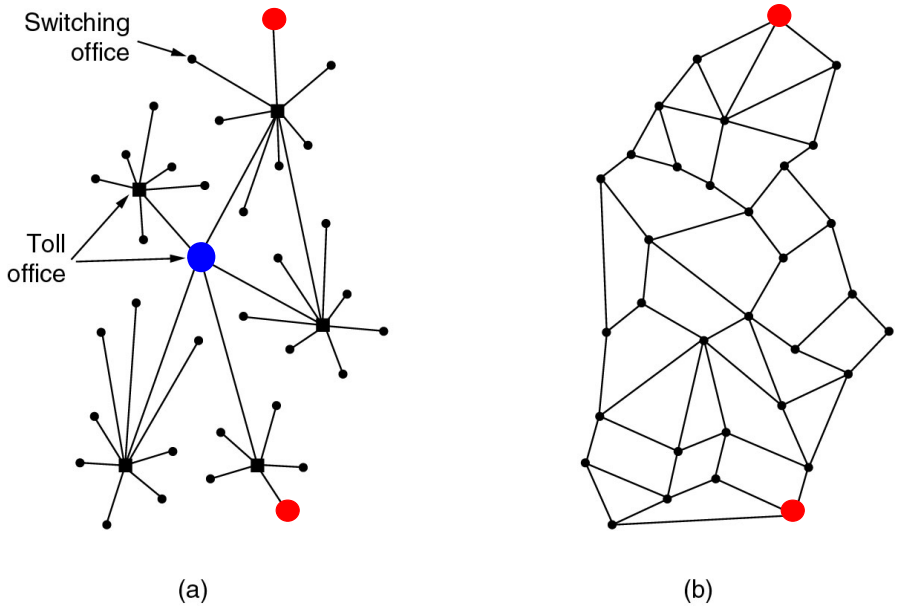
What is this?



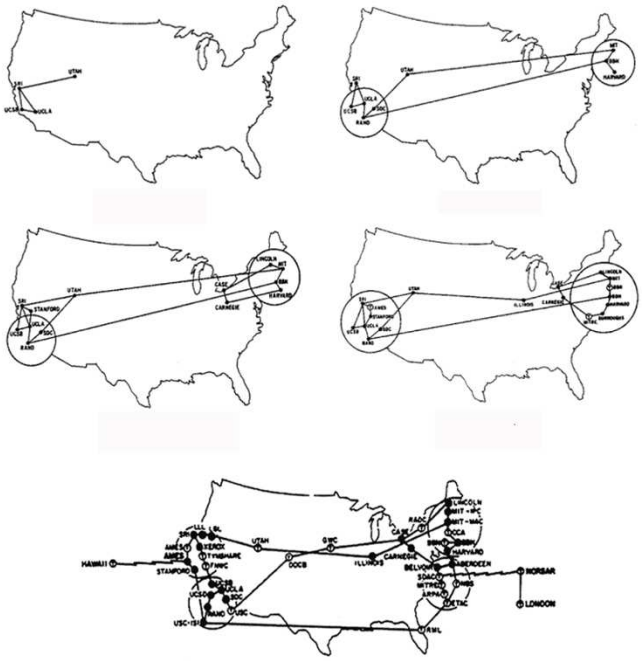
Commutazione di pacchetto



Commutazione di circuito vs di pacchetto



Arpanet



Arpanet

Leonard Kleinrock di
e il primo IMP

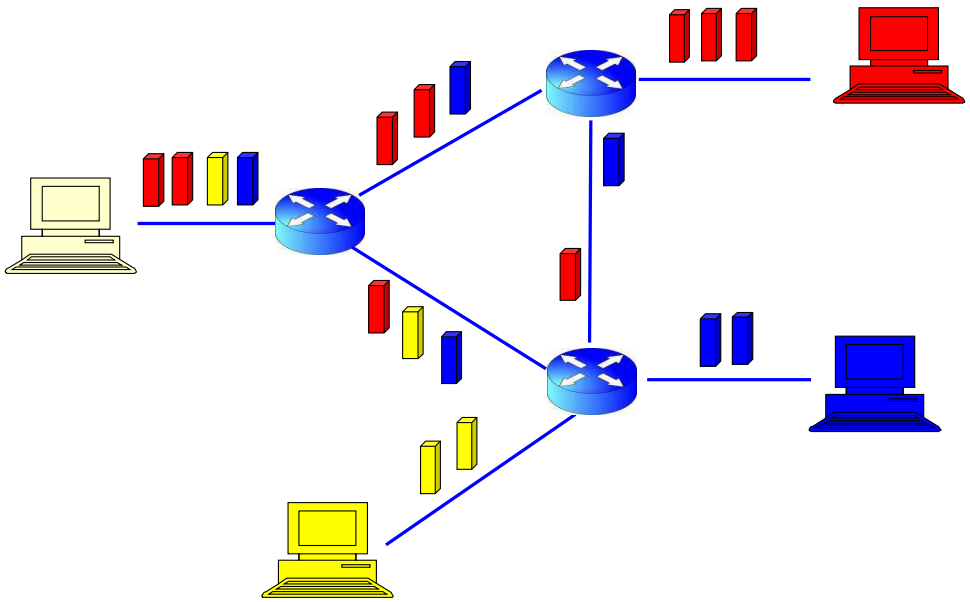
DATE	METER	PROBLEM & REMEDY	OPERATOR	DOWNTIME
29Oct69	1750	IMPTST RUNNING - TESTING LINE TO UCSB - LINE IS OPEN SO 'B' REG IS COUNTING ERRORS BUT SHOULD CEASE COUNTING IF TEL.Co. GETS LINE FIXED.	T. THACH	
		CHARLEY PLEASE CALL BEN AT SRI !		
29Oct69	2100	LOADED OP. PROGRAM FOR BEN BARKER BBN	CSK	
	22:30	Talked to SRI Host to Host	CSC	
		Left op. imp. program running after sending a host dead message to imp.	CSC	
30Oct69	1030	Stopped op. prog Started IMPTST to trace line trouble on TGW1 (UCSB)	T. THACH	

CUSTOMER SERVICE

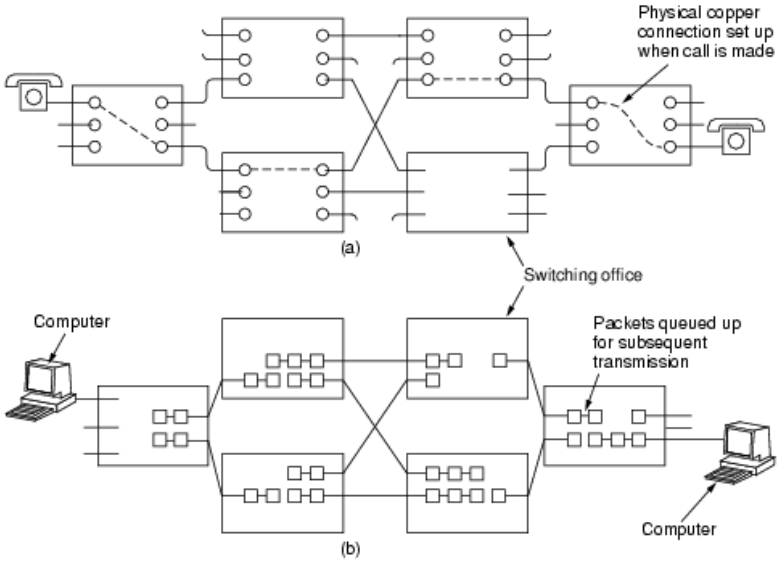
SDS-S-324

Interconnessione

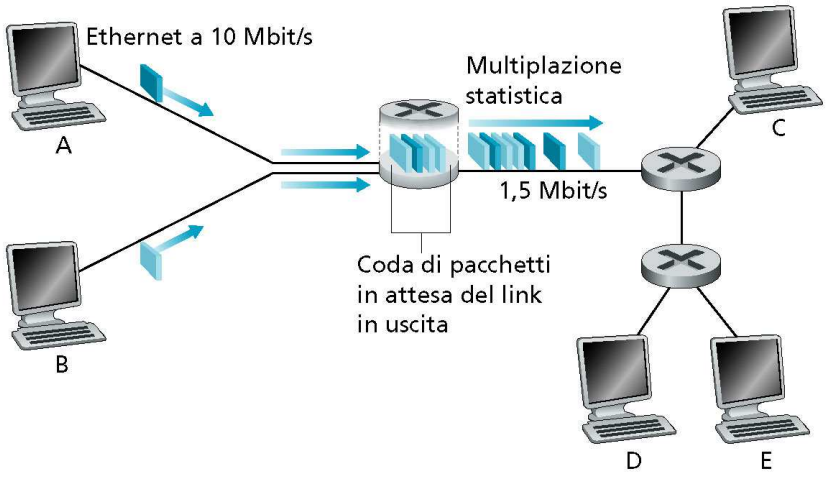
Interconnessione



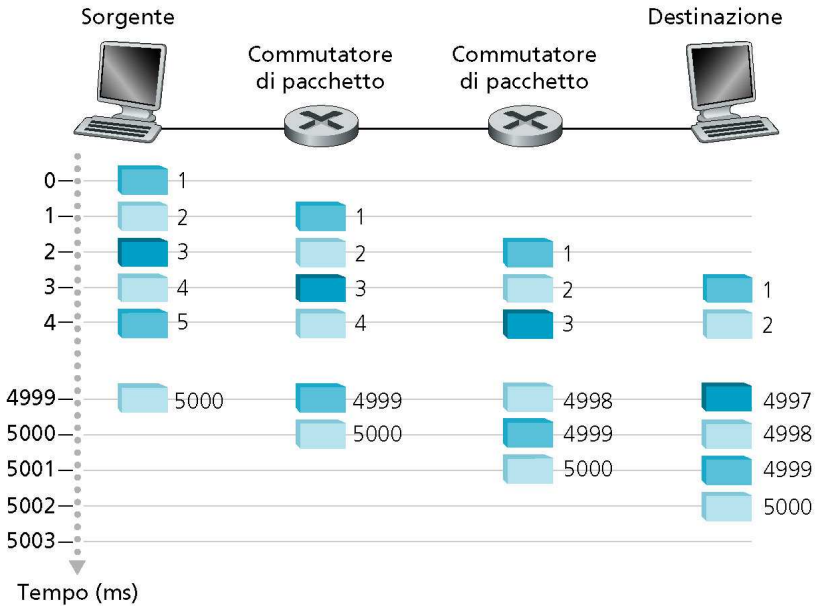
Commutazione di Pacchetto



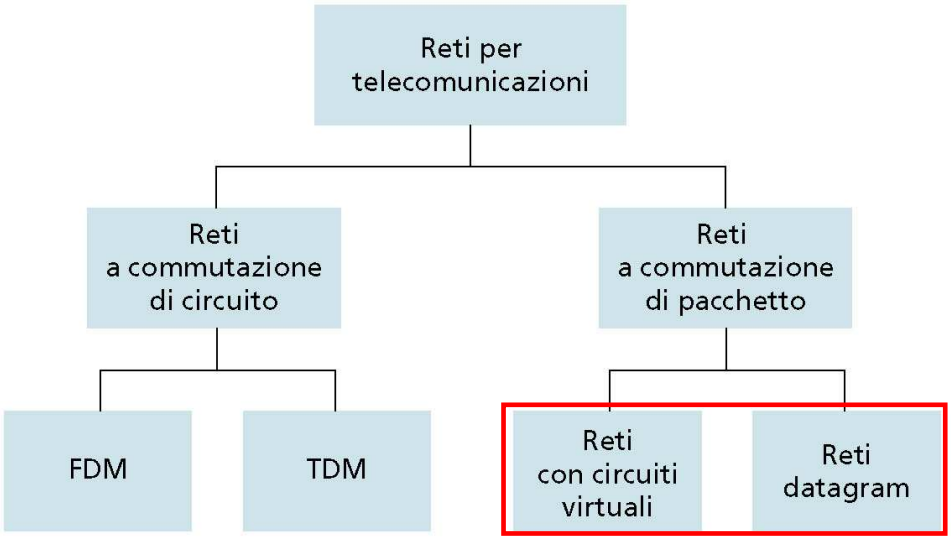
Commutazione di Pacchetto



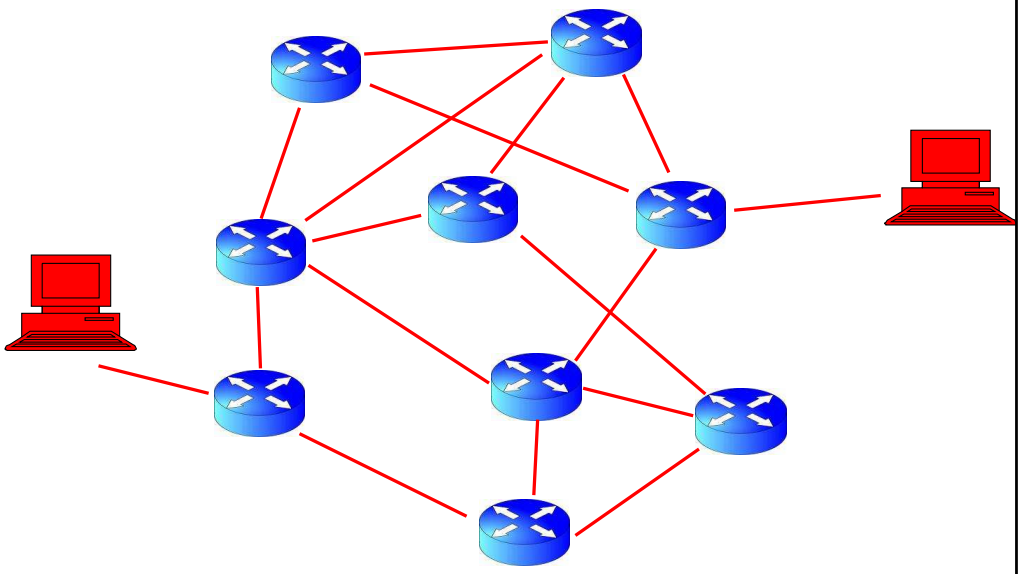
Commutazione di Pacchetto



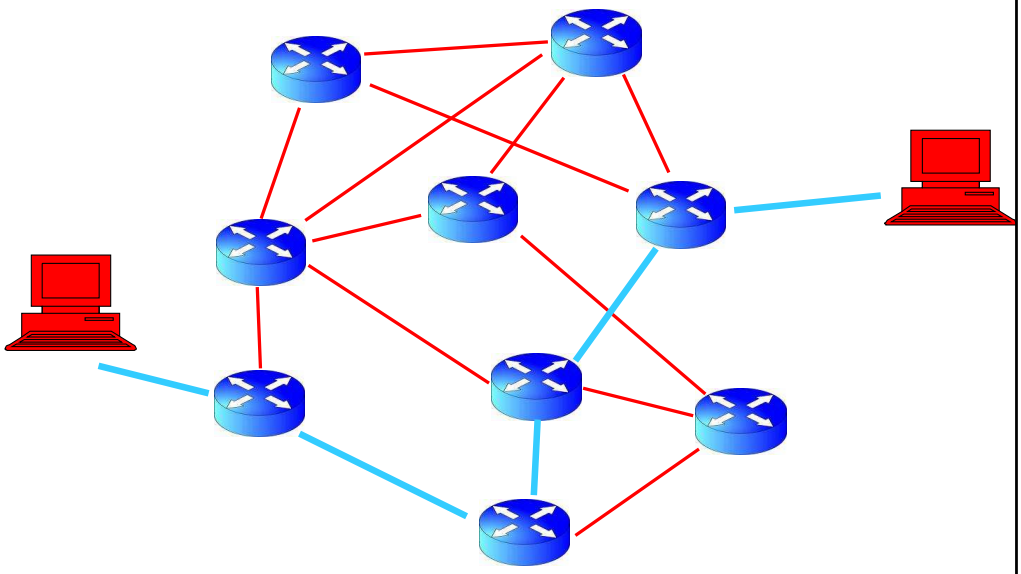
Tassonomia


Reti per telecomunicazioni
Reti a commutazione di circuito
Reti a commutazione di pacchetto
FDM
TDM
Reti con circuiti virtuali
Reti datagram

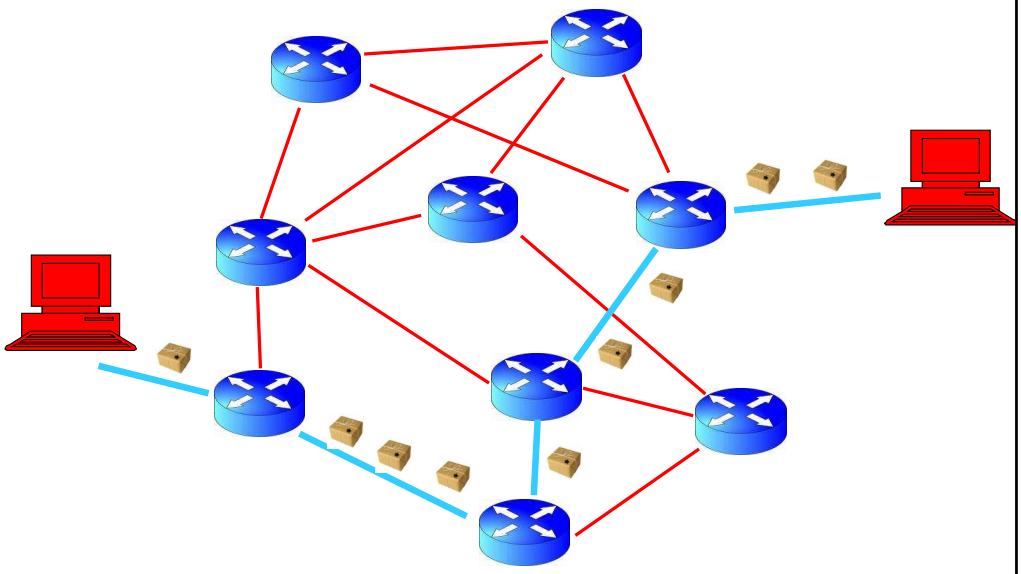
Circuiti virtuali



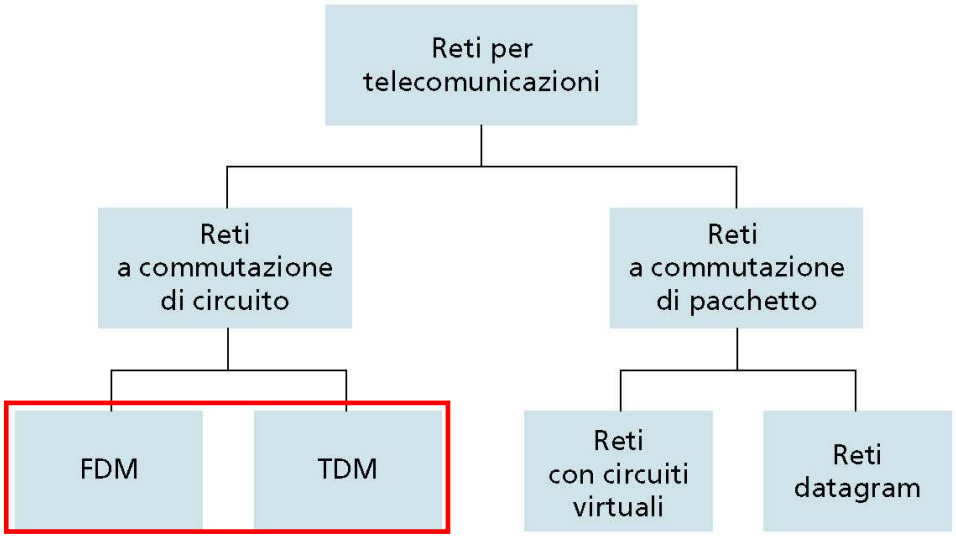
Circuiti virtuali



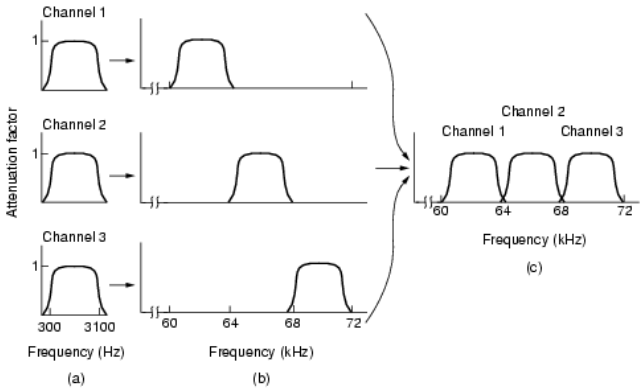
Circuiti virtuali



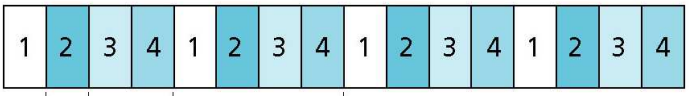
Tassonomia


Reti per telecomunicazioni
Reti a commutazione di circuito
Reti a commutazione di pacchetto
FDM
TDM
Reti con circuiti virtuali
Reti datagram

Multiplexaggio

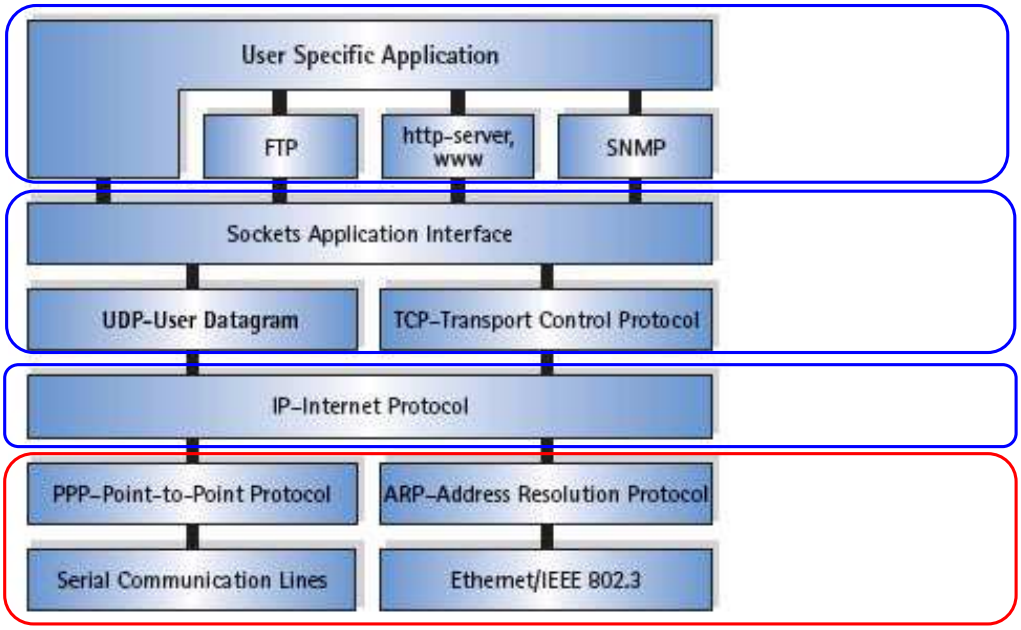


TDM

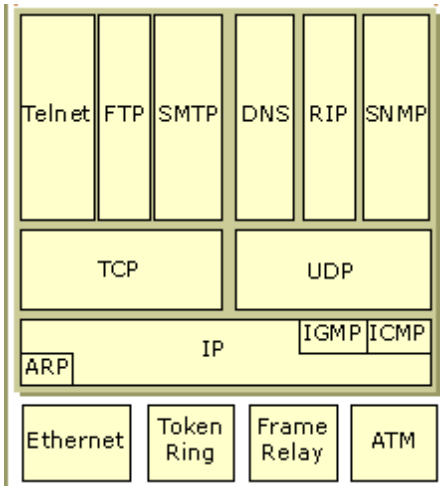


Università di Catania

TCP/IP



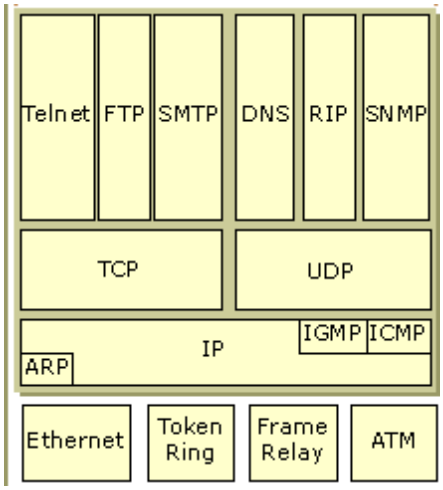
Internet Layer



Fornisce un servizio Datagram per raggiungere un host collegato ad Internet.

Richiede al livello sottostante un servizio in grado di trasportare Datagram da un host ad un altro direttamente connessi

Transport Layer



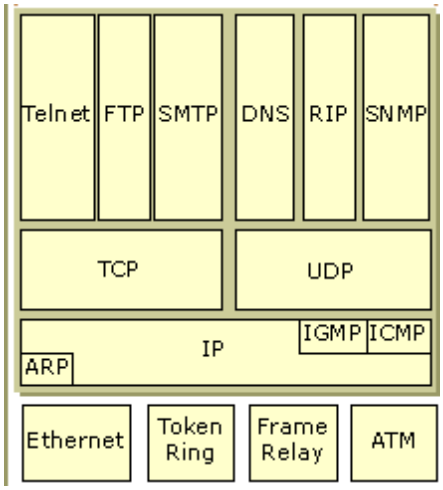
Fornisce:

- un servizio Datagram non affidabile e senza connessione (UDP)
- un servizio affidabile orientato alla connessione (TCP)

Introduce un identificatore per ogni connessione (port)

Richiede al livello sottostante un servizio in grado di trasportare Datagram da un host ad un altro non direttamente connessi.

Application Layer

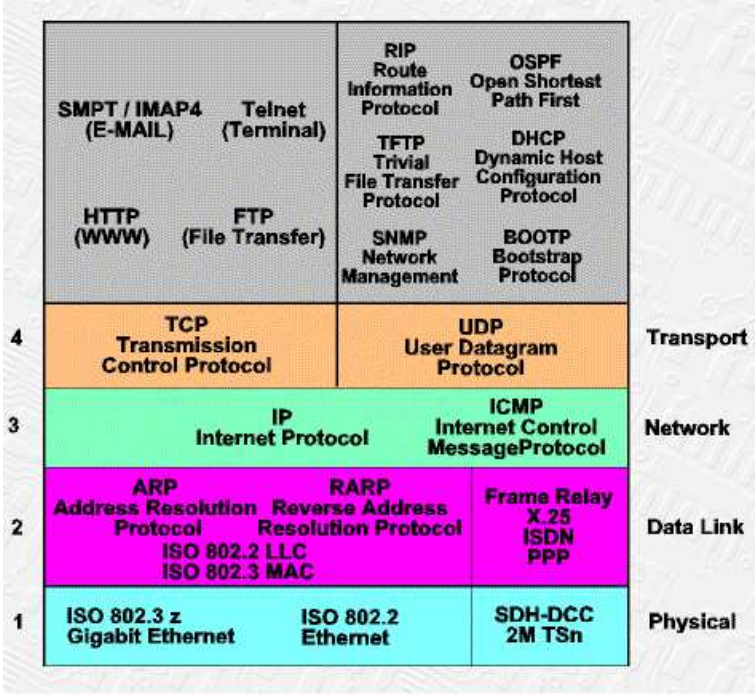


Si interfaccia direttamente con l'utente.

Richiede al livello sottostante un servizio di connessione.

L'affidabilità può essere richiesta ai livelli sottostanti o implementata localmente.

TCP/IP


SMPT / IMAP4 (E-MAIL)
Telnet (Terminal)
HTTP (WWW)
FTP (File Transfer)
RIP Route Information Protocol
OSPF Open Shortest Path First
TFTP Trivial File Transfer Protocol
DHCP Dynamic Host Configuration Protocol
SNMP Network Management
BOOTP Bootstrap Protocol
4
TCP Transmission Control Protocol
UDP User Datagram Protocol
Transport
3
IP Internet Protocol
ICMP Internet Control MessageProtocol
Network
2
ARP Address Resolution Protocol
RARP Reverse Address Resolution Protocol
ISO 802.2 LLC
ISO 802.3 MAC
Frame Relay
X.25
ISDN
PPP
Data Link
1
ISO 802.3 z Gigabit Ethernet
ISO 802.2 Ethernet
SDH-DCC
2M TSn
Physical

Network security

- field of network security:
  - how bad guys can attack computer networks
  - how we can defend networks against attacks
  - how to design architectures that are immune to attacks
- Internet not originally designed with (much) security in mind
  - *original vision:* “a group of mutually trusting users attached to a transparent network”
  - Internet protocol designers playing “catch-up”
  - security considerations in all layers!

campo della sicurezza della rete:
• come i malintenzionati possono attaccare le reti di computer
• come possiamo difendere le reti dagli attacchi
• come progettare architetture immuni agli attacchi
Internet non originariamente progettato pensando a (molta) sicurezza
• visione originale: “un gruppo di utenti che si fidano reciprocamente collegati a a reti trasparenti”
• I progettisti di protocolli Internet giocano al "recupero"
• considerazioni sulla sicurezza a tutti i livelli!

Bad guys: malware

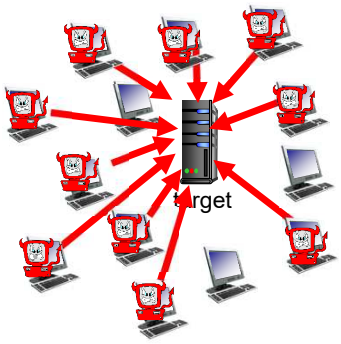
- malware can get in host from:
  - *virus:* self-replicating infection by receiving/executing object (e.g., e-mail attachment)
  - *worm:* self-replicating infection by passively receiving object that gets itself executed
- spyware malware can record keystrokes, web sites visited, upload info to collection site
- infected host can be enrolled in botnet, used for spam or distributed denial of service (DDoS) attacks

il malware può entrare nell'host da:
• virus: infezione autoreplicante ricevendo/eseguendo oggetto
(ad es. allegato di posta elettronica)
• worm: infezione autoreplicante ricevendo passivamente l'oggetto
che viene eseguito da solo
il malware spyware può registrare sequenze di tasti, siti Web visitati,
caricare le informazioni nel sito di raccolta
l'host infetto può essere registrato in botnet, utilizzato per lo spam o
Attacchi DDoS (Distributed Denial of Service).

Bad guys: denial of service

Denial of Service (DoS): attackers make resources (server, bandwidth) unavailable to legitimate traffic by overwhelming resource with bogus traffic

1. select target
2. break into hosts around the network
3. send packets to target from compromised hosts

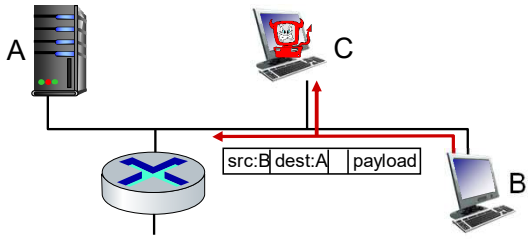


Denial of Service (DoS): gli aggressori creano risorse (server, larghezza di banda) non disponibile per il traffico legittimo tramite schiacciamento risorsa con traffico fasullo
1. selezionare l'obiettivo
2. irrompere negli host intorno alla rete
3. inviare pacchetti al target da compromesso host

Bad guys: packet interception

packet "sniffing":

- broadcast media (shared Ethernet, wireless)
- promiscuous network interface reads/records all packets (e.g., including passwords!) passing by

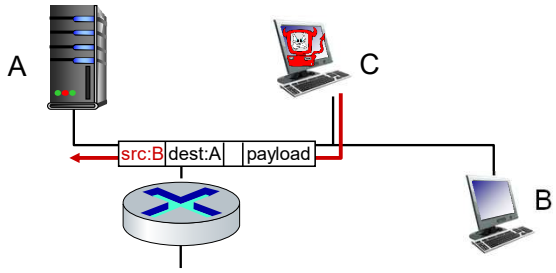


Wireshark software used for our end-of-chapter labs is a (free) packet-sniffer

pacchetto "sniffing":
mezzi di trasmissione (Ethernet condivisa, wireless)
l'interfaccia di rete promiscua legge/registra tutti i pacchetti
(ad esempio, comprese le password!) di passaggio

Bad guys: fake identity

IP spoofing: send packet with false source address



Spoofing IP: invia un pacchetto con un indirizzo di origine falso