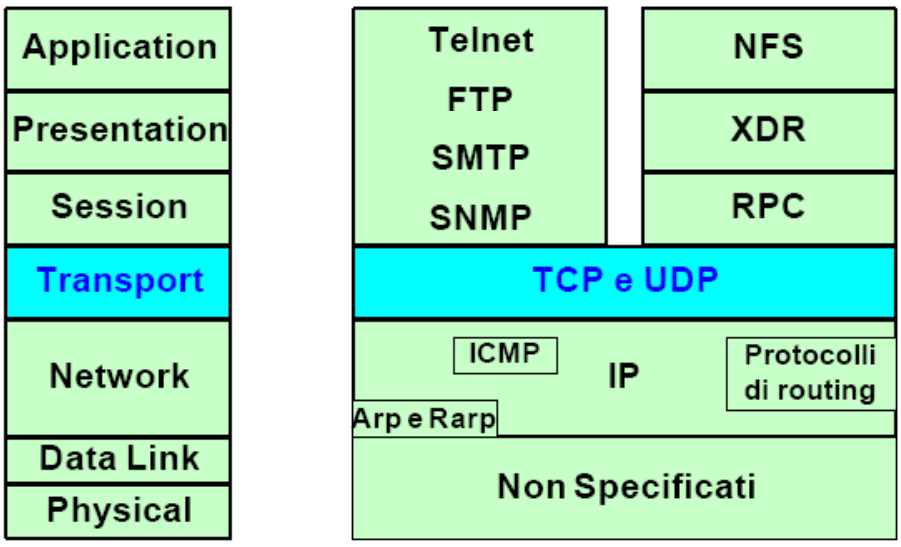
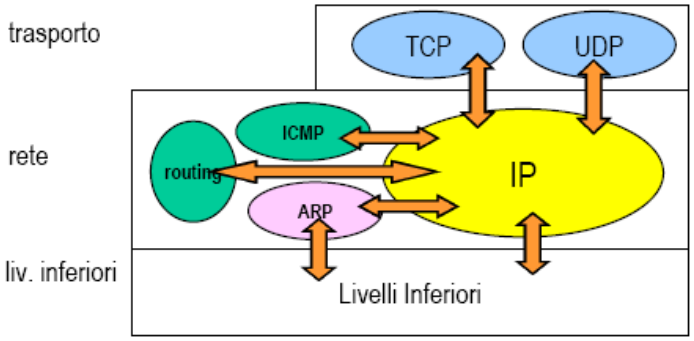
TCP/IP

Principali caratteristiche

I protocolli TCP e UDP

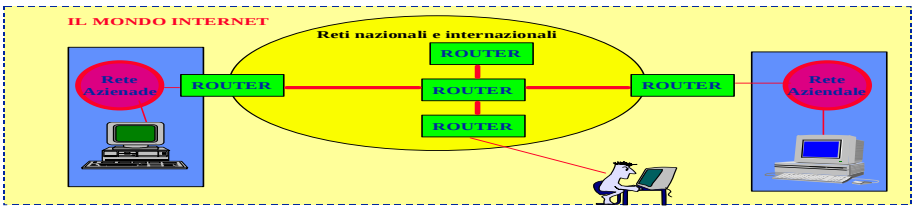


TCP/IP



Caratteristiche del modello TCP/IP

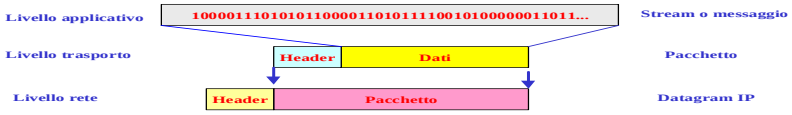
Struttura generale della rete Internet



- Le reti in Internet sono collegate tra loro mediante i router, che provvedono ad indirizzare il traffico a seconda dell'indirizzo contenuto nel messaggio. Ogni rete ha un indirizzo diverso.
- La rete Internet utilizza per il trasferimento dati un insieme di **protocolli**; i più noti sono :
  - **IP (Internet Protocol);**
  - **TCP (Transmission Control Protocol).**
- I protocolli e le regole utilizzate nella rete Internet sono specificati mediante standard noti con il nome di RFC (Request For Comments).

Struttura del modello TCP/IP

- L'insieme dei protocolli TCP/IP serve a consegnare i dati all'utente in modo affidabile..
- I dati sono divisi in:
  - **pacchetti :** il protocollo TCP numera i pacchetti e provvede ad inserire in ogni pacchetto un header, che contiene le informazioni necessarie per realizzare il servizio.
  - **datagram:**il protocollo IP trasforma il pacchetto TCP in un datagram e inserisce un header, che contiene le informazioni necessarie (quale ad esempio l'indirizzo del computer di destinazione) per trasferire l'informazione attraverso la rete.



Il modello TCP/IP può essere pensato suddiviso in tre livelli

- **servizio di consegna dei datagram:** viene svolto dal protocollo IP
- **servizio di trasporto dei pacchetti:** viene svolto dal protocollo TCP o UDP
- **servizi applicativi:** contiene i diversi programmi applicativi utili per l'utente (FTP, telnet,..)

Protocollo IP

Funzioni svolte dal protocollo IP

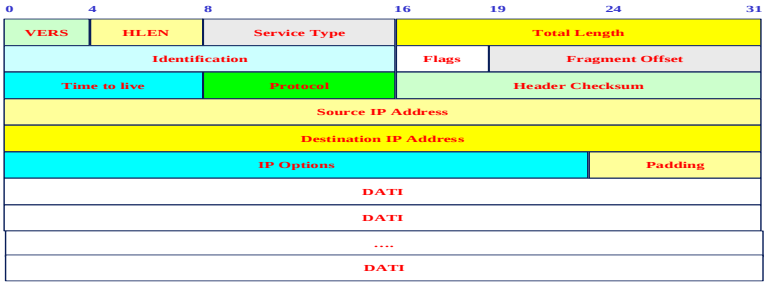
- definisce il **formato** dei dati che vengono trasmessi all'interno della rete.
- realizza la funzione di **routing**, ovvero il meccanismo con cui si sceglie il percorso per la trasmissione dei dati.
- prevede una serie di regole che determinano come devono essere processati i pacchetti, come e quando devono essere generati i messaggi di errore e le condizioni per le quali un pacchetto deve essere scartato.

Versioni del protocollo IP

- Le diverse versioni del protocollo IP sono indicate con la sigla IPvN, dove N indica il numero della versione.
  - **La versione IPv4 è quella attualmente utilizzata;**
  - **La versione IPv6 sarà introdotta nei prossimi anni.**

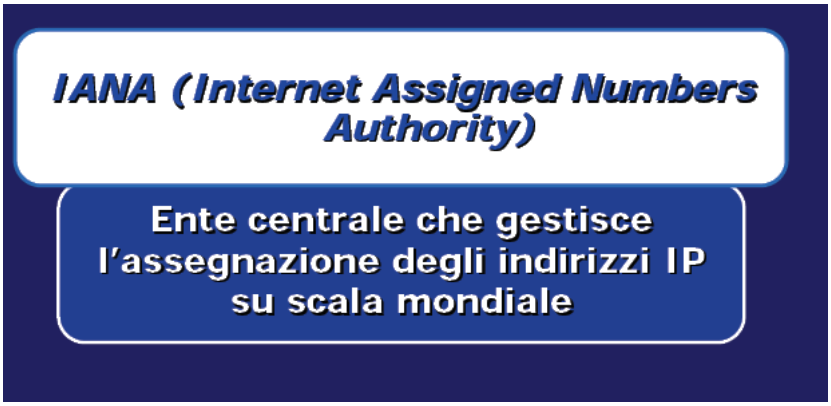
Formato datagram IP

- **Formato del datagram IP (versione 4)**



- **La massima lunghezza del datagram è 65.535 byte.**
- **Gli indirizzi IP della sorgente e del destinatario hanno una lunghezza di 32 bit.**

Indirizzi IP



Indirizzi IP

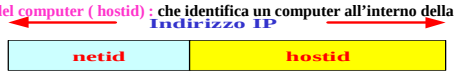
- Ogni computer connesso a Internet ha un **indirizzo IP**

Rappresentazione degli indirizzi IP

- Gli indirizzi IP possono essere espressi in diversi modi:
  - **in forma binaria: formato da 32 bit .**
    - **Esempio :** 10000010000011100000001000011110
  - **in forma decimale: formato da 4 numeri decimali .**
    - **Esempio :** l'indirizzo corrispondente al precedente indirizzo binario è 130.14.2.30
  - **in forma simbolica: formato da alcuni caratteri simbolici separati da punti.**
    - **Esempio :** ltt.ing.unisi.it

Formato Indirizzo IP

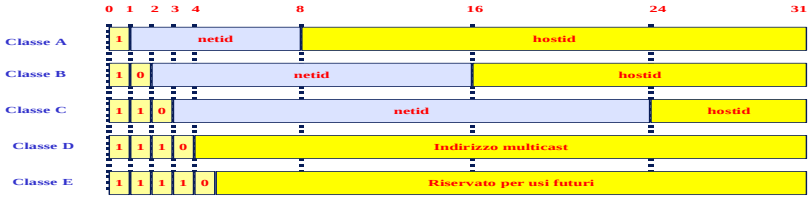
- L'indirizzo IP può essere suddiviso in due campi :
  - **indirizzo della rete (netid): che identifica l'indirizzo su cui si trova l'utente;**
  - **indirizzo del computer (hostid) : che identifica un computer all'interno della rete.**



Classi indirizzi IP

Gli indirizzi IP possono essere divisi in 5 classi:

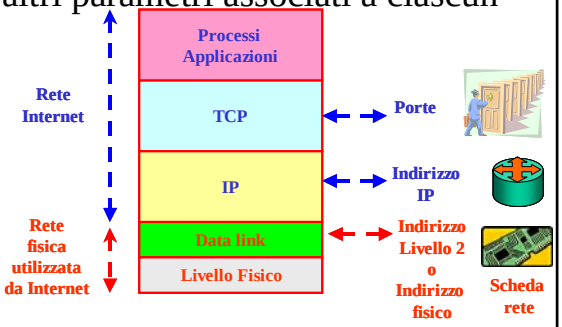
- **Classe A**: utilizza 7 bit per netid e 24 per hostid. Possono perciò esistere un numero massimo di 128 reti di classe A, ciascuna delle quali può contenere al massimo 2^{24}= 15.777.216 computer.
- **Classe B**: utilizza 14 per bit per netid e 16 per hostid. La classe B è adatta a reti che hanno un numero di computer compreso tra 256 e 2^{16} = 65536.
- **Classe C**: utilizza 21 bit per netid e 8 bit per hostid. La classe C viene utilizzata per reti che hanno un numero di computer inferiore a 256.
- **Classe D**: è riservata ad applicazioni di multicast.
- **Classe E**: definita per usi futuri. Sono facilmente riconoscibili in quanto il primo campo dell'indirizzo è compreso tra 240 e 255.



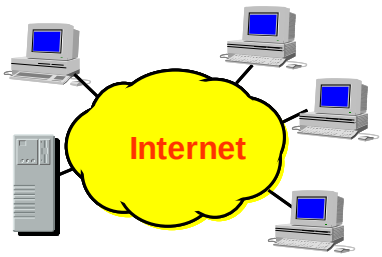
Per convenzione, l'indirizzo di una rete è quello con hostid uguale a 0.

Gli Indirizzi e le porte in Internet

- Le reti di telecomunicazione e i protocollo TCP/IP utilizzano indirizzi o altri parametri associati a ciascun pacchetti.



- In Internet si ha:
  - Indirizzi di livello 2 o indirizzi fisici: ogni scheda di rete ha un suo indirizzo fisico; oggi si utilizzano indirizzi a 48 bit e ogni scheda di erte ha un suo indirizzo unico valido a livello internazionale.
  - Indirizzi di livello 3: in Internet sono gli indirizzi IP, che consentono l'instradamento dei pacchetti
  - Porte: ogni applicazione attiva su un PC è associata a una porta.

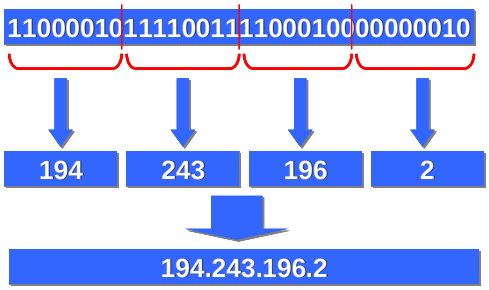


Indirizzi IP

- Ogni macchina visibile su Internet deve avere un indirizzo IP (analogo al numero di un telefono) diverso
- Un indirizzo IP è formato da 32 bit
- Esempio di indirizzo: 11000010111100111100010000000010

Notazione Decimale di un indirizzo IP

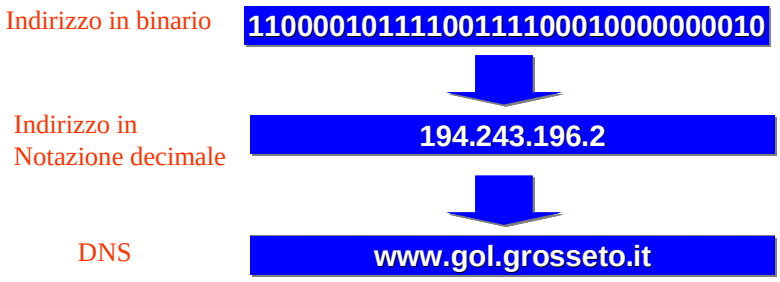
- La notazione decimale consente di avere una rappresentazione più semplice da ricordare



Indirizzi IP

DNS(Domain Name System)

- Esempio:
  - Indirizzi simbolici: sono semplici da ricordare (o scrivere) e possono avere dei significati facilitando la ricerca.



Indirizzi IP

Classi di indirizzi IP

- Un indirizzo IP è diviso in due parti:
  - Netid : identifica la rete a cui un computer è collegato
  - Hostid: identifica la macchina nell'interno della rete

- *La lunghezza dei campi netid e hostid è variabile*
- Si possono avere 5 classi di indirizzi IP a seconda della lunghezza di netid e hostid:
  - *Classe A*
  - *Classe B*
  - *Classe C*

  } Classi utilizzate per le applicazioni tradizionali

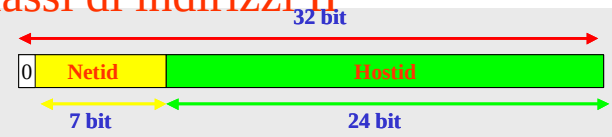
  - *Classe D (Indirizzi di multicast)*
  - *Classe E (non utilizzata)*

Indirizzi IP

Classi di indirizzi IP

Indirizzi classe **A**

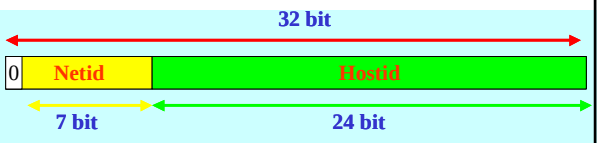
- **Netid:** 7 bit
- **Hostid**: 24 bit



- **N. classi A:** 2^7=128
- **N. indirizzi per ogni classe :** 2^{24} = 16.777.216
- Riservati a grandi organizzazioni
- ***Indirizzi di classe A con rappresentazione decimale :*** ***sono quelli che hanno il primo numero compreso tra 0 e 127***

Indirizzi classe B

- **Netid:** 14 bit
- **Hostid**: 16 bit



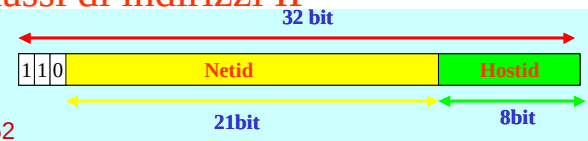
- **N. classi A:** 2^{14} = 16.384
- **N. indirizzi per ogni classe :** 2^{16}= 65.536
- Riservati a medio-grandi organizzazioni
- ***Indirizzi di classe B con rappresentazione decimale:*** ***sono quello che hanno il primo numero compreso tra 128 e 181***

Indirizzi IP

Classi di indirizzi IP

Indirizzi classe C

- **Netid:** 21 bit
- **Hostid**: 8 bit



- **N. classi A:** 2^{21} = 2.097.152
- **N. indirizzi per ogni classe :** 2^8= 256
- Riservati a piccole organizzazioni
- ***Indirizzi di classe C con rappresentazione decimale:*** ***sono quello che hanno il primo numero compreso tra 182 e 231***

Indirizzi classe D

Indirizzi classe E

Indirizzi IP

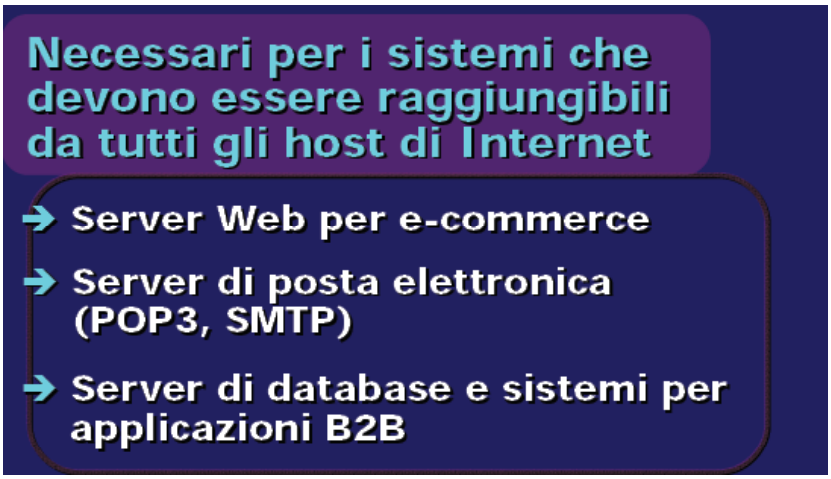
Indirizzi Pubblici e privati

- Gli indirizzi IP si dividono in:
  - Indirizzi IP pubblici: sono indirizzi validi su Internet
  - Indirizzi IP privati: sono indirizzi validi nella rete interna, ma non visibili sulla rete esterna

• Indirizzi Privati

- Gli indirizzi IP privati devono essere scelti in modo da non creare confusione con gli indirizzi IP pubblici, per questo essi sono stati standardizzati (RFC 1597 e RFC 1918).
- Si possono utilizzare le seguenti classi di indirizzi privati:
  - Classe A (una sola rete) : rete 10.x.x.x
  - Classe B (16 reti adiacenti): reti 172.16.x.x ... 172.31.x.x
  - Classe C (256 reti adiacenti) : reti 192.168.0.x ... 192.168.255.x

Indirizzi pubblici



Indirizzi IP
Indirizzi statici e dinamici

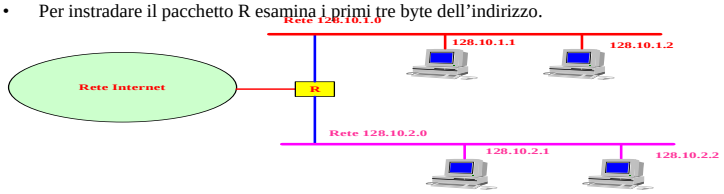
- La traduzione di indirizzi IP da parte del NAT può avvenire in diversi modi:
  - Univoco, ossia ad un indirizzo privato viene fatto corrispondere un indirizzo fisico IP. La corrispondenza può essere:
    - ✓ Statica (usato oggi per i server)
    - ✓ Dinamica
  - Non univoco, realizzato basandosi coppia Indirizzo-Porta; in questo caso si ha un NAPT (Network Address Port Traslation) o un IP Masquerading o un NAT-PAT.

Sottoreti IP

- Per ridurre il numero degli indirizzi di rete necessari per il funzionamento di Internet, si può utilizzare la tecnica di subnet addressing o subnetting, che consente di condividere lo stesso indirizzo di rete IP a più reti fisiche.

Esempio:

- Il router R utilizza la stessa rete in classe B 128.10.0.0 per le due reti fisiche.
- Tutti i router vedono un'unica rete 128.10.0.0
- Il terzo byte dell'indirizzo (generalmente riservato a hostid) viene utilizzato da R per distinguere le due reti.
- Per instradare il pacchetto R esamina i primi tre byte dell'indirizzo.



Subnettizazzione di un indirizzo IP

- L'indirizzo IP viene diviso in:
  - Indirizzo rete Internet (IP);
  - Indirizzo rete fisica;
  - Indirizzo host.

- L'ampiezza dei campi di netid e hostid può essere divisa in modo dinamico mediante la procedura di netmask.
- La netmask è composta :
  - **bit uguale a 1 :** in corrispondenza dei campi di netid e subnet;
  - **bit uguale a 0 :** in corrispondenza dei campi di hostid.
- La netmask è rappresentata in binario o in decimale.
  - **Esempio :** la netmask 11111111 11111111 11111111 00000000 corrisponde all'indirizzo 255.255.255.0 ed indica che il campo dell'host coincide con l'ultimo byte.
- Dato un un indirizzo IP , per estrarre l'indirizzo della rete e del subnet si effettua un'operazione AND bit a bit tra l'indirizzo IP e la netmask.
- **Operazione AND - definita dalle seguenti relazioni:**
  - 0+0=0+1=1+0=0 ; 1+1=1
- Esempio: Consideriamo l'indirizzo IP 128.10.2.2 (in binario 100000000 00001010 00000010 00000010); utilizzando la netmask 255.255.250.0 (in binario 11111111 11111111 1111101000000000) ed effettuando l'operazione AND tra le due sequenze si ottiene la sequenza bianria 10000000 00001010 00000010 00000000e quindi l'indirizzo 128.10.200. Per cui l'indirizzo IP 128.10.2.2 appartiene alla rete 128.10.2.0. La rete 128.10.2.0 è una sottorete della rete in classe B 128.10.0.0. Utilizzando la netmask con l'indirizzo IP 128.10.3.4 si ottiene ancora 128.10.2.0 e quindi anche questo indirizzo IP appartiene alla stessa rete di 128.10.2.2

Esempio

indirizzo AND *netmask* = prefisso di rete

10000010.00000100.01100111.11111100 (=130.4.103.252)

AND logico con la *netmask*

11111111.11111111.11111100.00000000 (=255.255.252.0)

=

10000010.00000100.01100100.00000000 (=130.4.100.0)

130.4.100.0/22

(/22 indica la dimensione della maschera)

Routing

- Ogni volta che un messaggio giunge in un router viene analizzato l'indirizzo di destinazione.
- Se vi è una corrispondenza con l'indirizzo di una interfaccia il router provvede al mappaggio dell'indirizzo IP nell'indirizzo fisico e alla consegna del pacchetto alla destinazione.
- Se invece non vi è corrispondenza, si provvede a consultare le tabelle routing
- Le tabelle di routing contengono un elenco di indirizzi di sotto-reti (parte host posta a 0) e in corrispondenza l'indirizzo di un router indicato come *first-hop* .
- A ciascun indirizzo di rete è associata anche una netmask. I router first-hop contenuti nella tabella di routing sono router immediantemente vicini, ovvero raggiungibili attraverso una delle sottoreti cui sono collegate le interfacacce del router considerato.

Esempio

network	netmask	first hop
131.175.21.0	255.255.255.0	131.17.123.254
131.175.16.0	255.255.255.0	131.17.78.254
131.56.0.0	255.255.0.0	131.17.15.254
131.155.0.0	255.255.0.0	131.17.15.254
0.0.0.0	0.0.0.0	131.17.123.254

interface eth0

IP address	131.17.123.1
netmask	255.255.255.0

interface eth1

IP address	131.17.78.1
netmask	255.255.255.0

interface eth2

IP address	131.17.15.12
netmask	255.255.255.0

- Per scoprire a quale router first-hop deve essere inoltrato il messaggio viene confrontato l'indirizzo di destinazione con gli indirizzi di rete contenuti nella tabella di routing.
- In particolare viene fatto un AND bit a bit tra indirizzo di destinazione e netmask associata alla riga della tabella e viene confrontato il risultato con l'indirizzo di rete associato.
- Se il confronto dà esito positivo per più righe della tabella viene selezionata la tabella con la netmask che ha il maggior numero di 1 (si dice comunemente che vale il principio del prefisso più lungo).

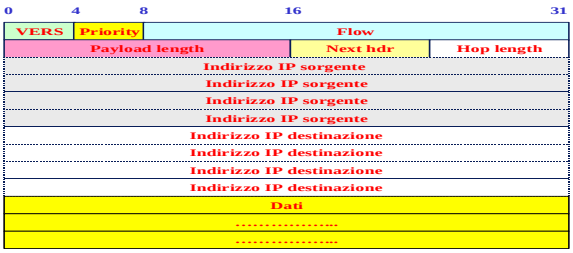
Protocollo IPv6

- Il protocollo IPV6 è stato sviluppato per sostituire IPv4, che, a causa della crescente diffusione di Internet, esaurirà lo spazio di indirizzamente nei prossimi dieci anni.
- **IPV6 introduce indirizzi IP lunghi 128 bit.**

Vantaggi offerti da IPV6 rispetto a IPV4

- semplifica le procedure di instradamento
- aumenta l'efficienza delle tabelle di instradamento
- permette la configurazione automatica di un indirizzo IP
- consente di avere un numero di indirizzi IP estremamente elevato
- Fornisce una maggiore sicurezza per l'informazione trasmessa

Formato del datagram IPv6



TCP e UDP

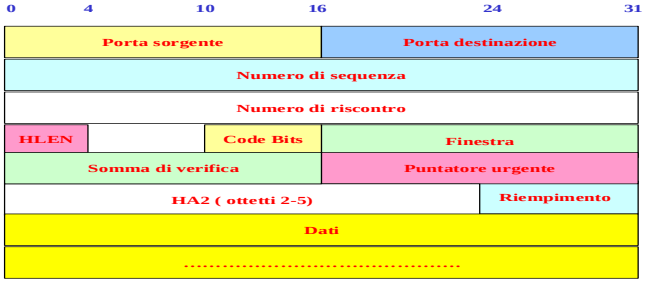
- Due protocolli di trasporto alternativi
- Realizzano funzionalità comuni a tutti gli applicativi
- Possono operare simultaneamente con molti applicativi diversi, tramite il concetto di porta

Protocollo TCP

Principali caratteristiche del protocollo TCP

- TCP (Transmission Control Protocol) è un protocollo del livello di trasporto che garantisce un trasferimento affidabile dell'informazione mediante il recupero dei datagram IP ricevuti in errore, persi nella rete oppure ricevuti più di una volta.
- È un protocollo orientato alla connessione.
- L'unità informativa del TCP si chiama segmento.

Formato del segmento TCP

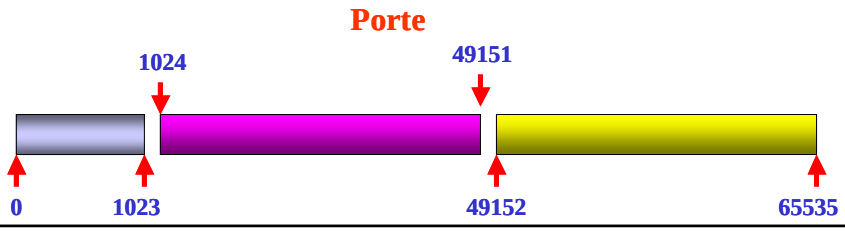


Porte TCP e UDP

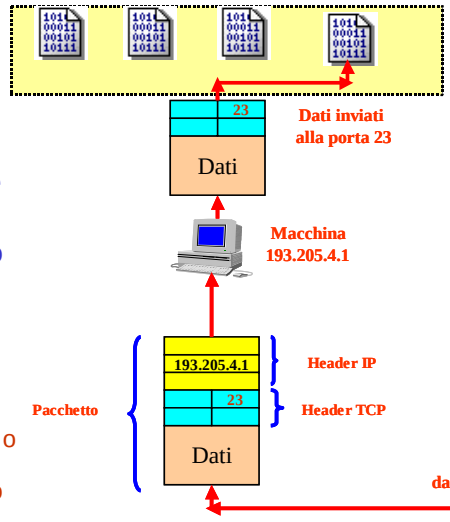
- Sono il mezzo con cui un programma client indirizza un programma server
  - un ftp client per connettersi ad un ftp server indica:
    - l'indirizzo IP dell'elaboratore remoto
    - il numero della porta associata allo ftp server
- Caratteristiche
  - indentificate da un numero naturale su 16 bit
  - 0 ... 1023 = porte privilegiate
  - 1024 ... 65535 = porte utente
  - porte statiche
    - quelle dove un server è in ascolto
  - porte dinamiche
    - quelle usate per completare una richiesta di connessione e svolgere un lavoro

Porte

- Una porta è specificata usando16 bits
- Le porte sono classificate in
  - **Well-known** (porte da 0 a 1023)
  - **Registered** (porte da 1024 a 49151)
  - **Dynamic** o **private** (porte da 49152 a 65535)



Il meccanismo delle porte



- Ogni PC può elaborare contemporaneamente varie applicazioni. E' necessario perciò inviare un pacchetto ricevuto all'applicazione corretta.
- Le porte sono utilizzate dal TCP o UDP per identificare a quale applicazione deve essere inviato un certo pacchetto una volta ricevuto dal PC a cui era destinato.

Alcune porte utilizzati da servizi Internet

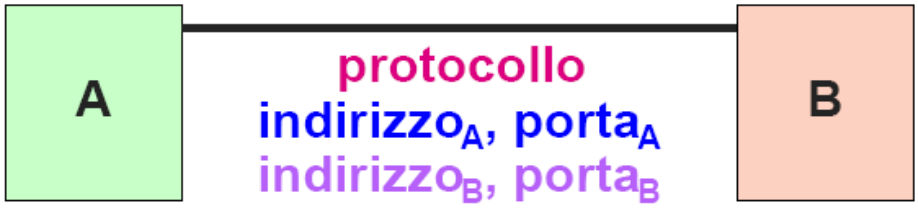
• Porta 7	ECHO	Echo
• Porta 13	DAYTIME	Daytime
• Porta 17	QUOTE	Quote of the Day
• Porta 21	FTP	File Transfer Protocol
• Porta 23	TELNET	Terminal Connection
• Porta 25	SMTP	Simple Mail Transport Protocol
• Porta 42	NAMESERVER	Host Name Server
• Porta 53	DOMAIN	Domain Name Server
• Porta 79	FINGER	Finger

TCP: Transmission Control Protocol

- Un protocollo di trasporto:
  - byte-oriented
  - connesso
- Utilizzato da applicativi che richiedono la trasmissione affidabile dell'informazione:
  - telnet
  - ftp (file transfer protocol)
  - smtp (simple mail transfer protocol)
  - rcp (remote copy)

Connessione TCP/IP

- una connessione è una quintupla:
  - protocollo = TCP o UDP
  - indirizzo = indirizzo IP (32 bit)
  - porta = punto di accesso (16 bit)



TCP: funzionalità

- Funzionalità TCP:
  - Supporto della connessione tramite circuiti virtuali
  - Error Checking
  - Controllo di flusso
  - Multiplazione e demultiplazione
  - Controllo di stato e di sincronizzazione
- TCP garantisce la consegna del pacchetto, UDP no!

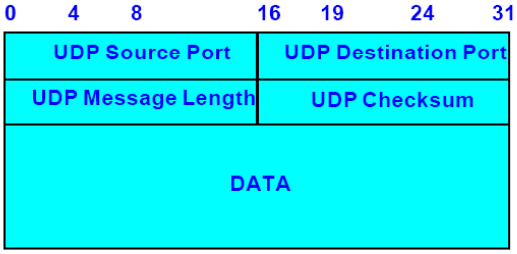
TCP: caratteristiche

- Come UDP ha il concetto di porta
- Il TCP di un nodo, quando deve comunicare con il TCP di un altro nodo, crea un circuito virtuale
- Al circuito virtuale è associato un protocollo di trasporto
  - full-duplex
  - acknowledge
  - controllo di flusso
- TCP richiede più banda e più CPU di UDP

UDP: User Datagram Protocol

- Protocollo di trasporto di tipo non connesso
- Aggiunge due funzionalità a quelle di IP:
  - multiplexing delle informazioni tra le varie applicazioni tramite il concetto di porta
  - checksum (opzionale) per verificare l'integrità dei dati

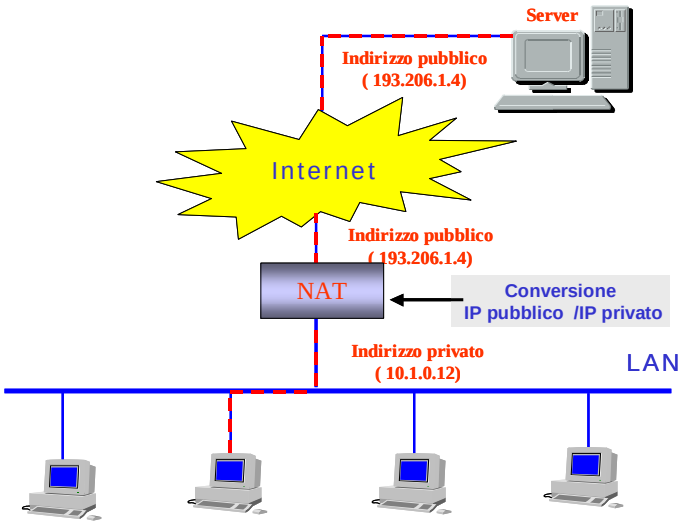
UDP: PDU



NAT (Network Address Translator)

Network Address Translator (NAT)

- Converte indirizzi pubblici su Internet in indirizzi privati utilizzati nell'interno della rete locale



NAT (Network Address Translator)

- Il NAT non è un meccanismo di sicurezza, ma può facilitare la realizzazione di politiche di sicurezza nell'interno di un'organizzazione.
- Si possosno avere:
  - NAT statico:
    - ✓ ad ogni indirizzo IP interno corrisponde un indirizzo IP esterno
  - NAT dinamico:
    - ✓ Esiste un insieme di indirizzi IP pubblici su Internet e un insieme di indirizzi IP privati.
    - ✓ Gli indirizzi privati sono adattati in modo dinamico sugli indirizzi pubblici esterni; in questo modo non vi è una corrispondenza univoca tra macchina sulla rete locale e l'indirizzo IP.
    - ✓ Sono permesse tante connessioni contemporanee quanti sono gli indirizzi IP pubblici.
  - ✓ NAT dinamici su IP e porta:
    - ✓ associa un host interno ad un IP ed una porta ogni volta che inizia una nuova connessione.
- Masquerade:
  - Si ha un solo indirizzo IP pubblico per la rete

Masquerade

- Il NAT possiede un unico indirizzo pubblico IP per le connessioni esterne;
- **Vantaggi**
  - Tutto il traffico verso o da Internet passa attraverso un unico punto essendo disponibile un unico indirizzo pubblico
  - Richiede la rimappatura delle porte;
  - Nasconde all'esterno la struttura del sito Web;
  - Molto difficile da attaccare
- **Svantaggi**
  - aumenta carico del router o di chi effettua la traduzione;
  - difficile allocazione dinamica indirizzi con protocolli UDP;
  - NAT interferisce con metodi di controllo dell'integrita' dei pacchetti poiche' interviene sui pacchetti modificandone l'indirizzo.

ARP e RARP

- ARP: Address Resolution Protocol
- RARP: Reverse ARP
- Protocolli in broadcast di tipo sollicitation
- ARP
  - » la stazione che vuole scoprire l'indirizzo MAC di un'altra stazione, di cui conosce l'indirizzo di livello 3, invia la richiesta in broadcast di tipo sollicitation
  - » la stazione sollecitata risponde

ARP

- Viene costruito dall'host che vuole risolvere l'indirizzo un pacchetto broadcast (request) che contiene
  - indirizzo IP del destinatario,
  - indirizzo IP ed Ehternet di chi origina la richiesta
- L'host che riconosce nel campo richiesta il proprio indirizzo IP invia un pacchetto di risposta (reply) direttamente al sender
- Sia chi origina il pacchetto sia chi lo riceve (e risponde) aggiungono una informazione nella propria tabella ARP
- Le successive comunicazioni tra i due elaboratori possono avvenire senza ulteriori richieste di ARP

Pacchetto ARP

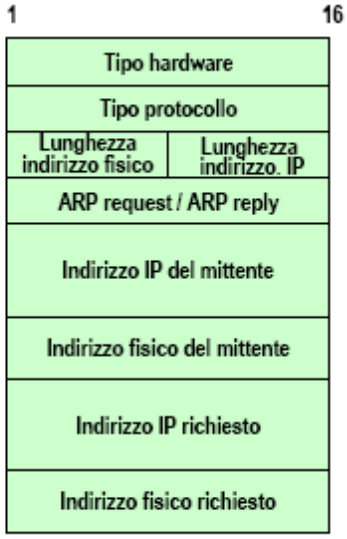


Tabelle ARP

- Corrispondenza tra indirizzi IP e Indirizzi LAN

IP addr	LAN addr	age
130.192.2.58	08-00-2b-15-47-2e	10
130.192.2.64	08-00-2b-21-56-64	12
. . . .	. . . .	. .

ICMP

- Internet Control Message Protocol
- Verificare lo stato della rete
  - » Echo request ed Echo reply
- Riportare anomalie
  - » Destination Unreachable
  - » Time Exceeded for a Datagram
  - » Parameter Problem on a Datagram
- Scoprire la netmask
  - » Introdotto nelle ultime versioni
  - » Mask Request
  - » Address Mask Reply
- Migliorare il routing
  - » Redirect

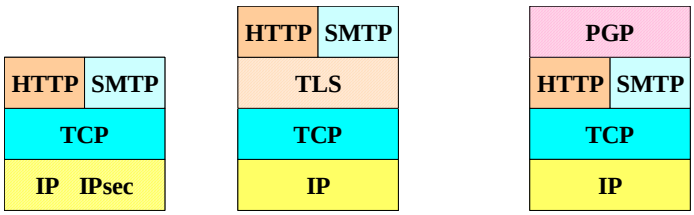
Internet e la sicurezza

- Internet è soggetta a numerosi tipi di attacchi.
- Esempi di attacchi:
  - ➢ falsificazione dell'indirizzo IP (detto anche IP spoofing) che provoca la generazione di pacchetti con indirizzi IP "falsi" (cioè di un altro utente);
  - ➢ intercettazione di pacchetti trasmessi da un utente per conoscere le informazioni trasmesse.
- Per questo motivo è importante introdurre meccanismi di sicurezza che garantiscano sia la sicurezza delle informazioni, sia la disponibilità dei servizi.

Per questo motivo è importante introdurre meccanismi che garantiscano sia la sicurezza delle informazioni, sia la disponibilità dei servizi.

Internet e la sicurezza

- Nella struttura TCP/IP la sicurezza della trasmissione dei dati può essere inserita a diversi livelli a seconda del tipo di applicazione, servizio e al livello di sicurezza desiderato. In particolare possono essere considerate tre diverse soluzioni:
  a. **sicurezza livello di rete (IPSec)**
  b. **sicurezza a livello di sessione (SSL, TLS,…)**
  c. **sicurezza a livello di applicazione (PGP , S/MIME, SET,…)**



a b c