Protocollo IP e collegati
Introduzione

Il collante che tiene insieme la rete Internet è il protocollo di livello rete, comunemente chiamato IP (*Internet Protocol*). A differenza dei vecchi protocolli di livello rete, il protocollo IP è stato progettato tenendo in mente le problematiche di *internetworking*. Il compito del protocollo IP è quello di fornire una modalità *best-effort* per trasportare dei datagrammi (pacchetti) IP dall'origine alla destinazione senza preoccuparsi se le macchine si trovino nella stessa rete o se ci siano altre reti tra le due macchine.

La comunicazione in Internet avviene nel seguente modo: il livello di trasporto gestisce le informazioni in forma di *data stream* che vengono frammentati in datagrammi a livello di rete. Risulta quindi fondamentale comprendere la modalità con cui viene costruito un pacchetto IP.

Tale sezione presenta i seguenti argomenti all'interno del capitolo relativo al pacchetti IP:

- **formato del pacchetto IP**;
- **problemi di indirizzamento**;
- **classi di indirizzi A, B, C, D**;
- **netmask e valori possibili**;
- **indirizzi privati e indirizzi pubblici**;
- **logical IP subnet**.

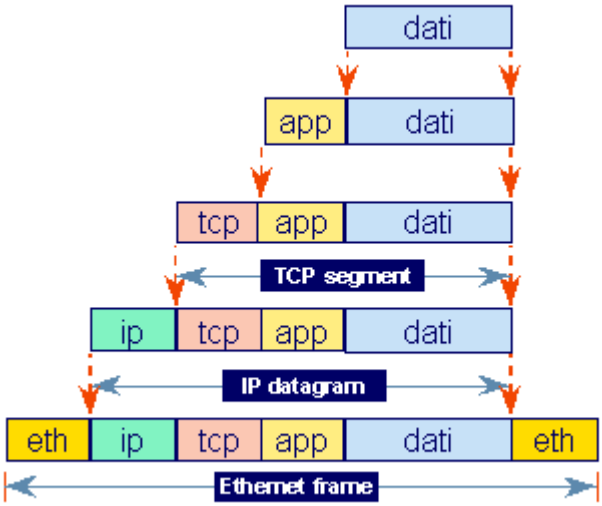
La sicurezza delle connessioni ad Internet sta divenendo sempre più importante, in questa sezione vengono illustrate le principali tecniche che consentono di avere un accesso sicuro alla rete. Come noto, la *suite* di protocolli TCP/IP è in realtà un insieme abbastanza complesso di molteplici protocolli. Nella parte finale di questa sezione vengono presentati alcuni protocolli, che insieme a più noti protocolli TCP e IP, giocano un ruolo fondamentale all'interno della rete Internet (per esempio i protocolli NAT e PAT, i quali tra l'altro consentono di risolvere il problema della carenza di indirizzi pubblici).

La sezione relativa alle soluzioni e ai protocolli correlati contiene le seguenti sezioni:

- **protocolli correlati a IP e loro impiego**;
- **ICMP**;
- **ARP/RARP**.

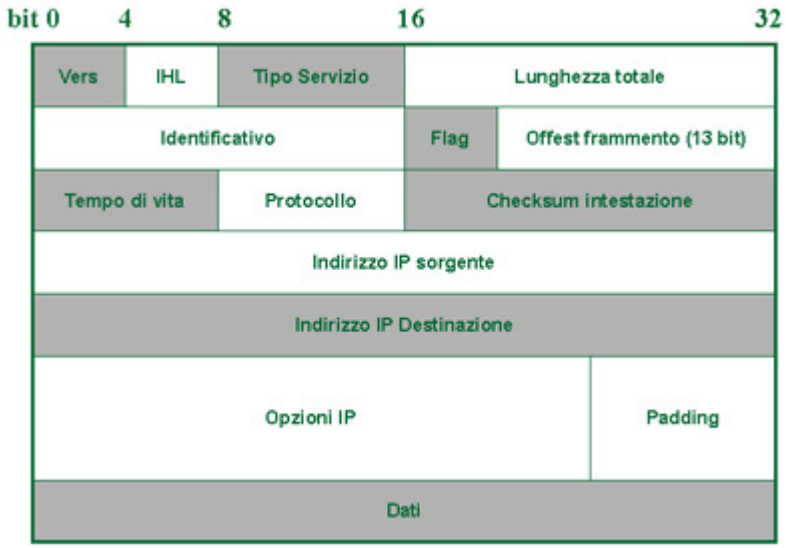
Formato del pacchetto IP

Il protocollo IP



Quando un'applicazione invia dei dati, utilizzando l'architettura **TCP/IP**, i dati vengono mandati verso il basso attraverso tutti i livelli della pila protocollare fino ad essere trasmessi dal livello fisico. Ogni livello aggiunge delle informazioni di controllo, preponendo degli **header** (ed a volte aggiungendo anche dei *trailer*) ai dati che riceve. I dati d'utente, ai quali viene preposta un'intestazione (*header*) dallo strato di applicazione, vengono passati al protocollo dello strato di trasporto (in questo caso si tratta del protocollo TCP, sebbene il funzionamento sia del tutto analogo nel caso si utilizzi **UDP**): quest'ultimo esegue varie operazioni e aggiunge un'intestazione alla **PDU** che gli è stata inviata. L'unità di dati prende ora il nome di segmento. Lo strato di trasporto fornisce quindi il segmento allo strato di rete, che presta anch'esso servizi specifici e aggiunge un'intestazione. Questa unità (che la terminologia di Internet definisce ora **datagramma**) viene passata ai livelli inferiori, dove lo strato di collegamento dati aggiunge la propria intestazione e una coda (*trailer*); l'unità di dati (che ora prende il nome di trama) viene poi trasmessa in rete dallo strato fisico. In figura è mostrato un esempio di imbustamento dei dati, nell'ipotesi che la sottorete sia una LAN di tipo *Ethernet*.

Il pacchetto IP



Il protocollo IP fornisce i seguenti servizi:

- trasmissione di un **datagram** *host-to-host* (indirizzamento);

- funzioni di **routing**;
- frammentazione e riassemblaggio dei *datagram*.

Il protocollo non fornisce:

- **controllo di flusso**;
- **controllo d'errore**;
- **controllo di sequenza**.

I *router* in rete elaborano il pacchetto fino a livello IP, per vedere quale sia l'indirizzo di destinazione; attraverso la tabella di instradamento viene deciso su quale interfaccia inviare il pacchetto. IP supporta le operazioni di frammentazione: il termine di frammentazione indica un'operazione in cui una PDU viene suddivisa o segmentata in unità più piccole. Questa funzione è necessaria perché non tutte le reti adottano la stessa dimensione per le PDU. Senza l'impiego della frammentazione, un *router* sarebbe incaricato di gestire le incompatibilità tra le dimensioni delle PDU delle diverse reti. IP risolve il problema fissando regole di frammentazione per i *router* e regole di riassemblaggio nell'*host* ricevente.

I campi del pacchetto IP

Il campo versione identifica la versione del protocollo IP del pacchetto; quella oggi in uso prevalente è IPv4, sebbene ci si stia indirizzando verso l'uso della versione IPv6 (denominata anche IPng, IP *next generation*).

Il campo lunghezza dell'intestazione (IHL) contiene 4 bit impostati a un valore che indica la lunghezza dell'intestazione dei datagrammi. La lunghezza è misurata in parole di 32 bit; solitamente, un'intestazione senza opzioni di qualità del servizio (QoS) è costituita da 20 *byte* (quindi 20 * 8 = 160 bit, ovvero 5 raggruppamenti da 32); di conseguenza il valore del campo della lunghezza è di norma 5.

Il campo tipo di servizio (TOS) può essere utilizzato per classificare i pacchetti e offrire un servizio differenziato (QoS).

Il campo lunghezza totale specifica la lunghezza totale del datagramma IP. Si misura in *byte* e comprende la lunghezza dell'intestazione e dei dati. IP sottrae il campo lunghezza dell'intestazione dal campo lunghezza totale, per calcolare le dimensioni del campo dati. La lunghezza massima possibile per un datagramma è di 65.535 *byte*.

Il protocollo IP utilizza tre campi nell'intestazione per controllare la frammentazione e il riassemblaggio dei datagrammi. Questi sono il campo identificatore, *flag* e scostamento del frammento.

Il campo identificatore serve all'*host* ricevente per designare in modo univoco ciascun frammento di un datagramma proveniente dall'indirizzo di origine.

Il campo *flag* contiene i bit che determinano se il datagramma può essere frammentato: in caso affermativo, uno dei bit può essere impostato in modo tale da determinare se il frammento è l'ultimo del datagramma.

Il campo scostamento del frammento contiene un valore che specifica la posizione relativa del frammento nel datagramma originale; il valore si misura in unità di otto *byte*.

Il parametro tempo di durata (TTL, *Time To Live*) serve per misurare il tempo di presenza di un datagramma in rete. Ogni *router* quando riceve un pacchetto controlla questo campo, e lo scarta se il

valore TTL è uguale a zero; prima di inoltrare nuovamente il pacchetto, il campo TTL viene diminuito di una unità. Il campo TTL indica quindi il numero di tratti che il pacchetto può attraversare, e può essere usato dai *router* per evitare che i pacchetti entrino in cicli infiniti, ma anche da un *host* per limitare la durata della presenza di segmenti in rete.

Il campo protocollo serve per identificare il protocollo dello strato immediatamente superiore a IP che deve ricevere il datagramma. È simile al campo tipo, presente nella trama **Ethernet**.

Il campo *checksum* dell'intestazione viene utilizzato per rilevare eventuali errori che possono essersi verificati nella sola intestazione. I controlli non vengono eseguiti sul flusso dei dati dell'utente. Se da un lato ciò consente di usare un algoritmo di *checksum* piuttosto semplice, in quanto non deve operare su molti *byte*, dall'altro richiede che un protocollo di livello superiore esegua un controllo degli errori sui dati dell'utente.

IP trasporta due indirizzi nel datagramma: l'indirizzo di origine e l'indirizzo di destinazione, che conservano lo stesso valore per tutto il trasferimento.

Il campo opzioni serve per identificare vari servizi supplementari.

Il campo riempimento può essere utilizzato per far sì che l'intestazione del datagramma sia allineata ad una delimitazione precisa di 32 bit.

Infine il campo dati contiene i dati dell'utente. La combinazione dei dati e dell'intestazione non può superare 65.535 *byte*.

Problemi di indirizzamento

Formato dell'indirizzo IP

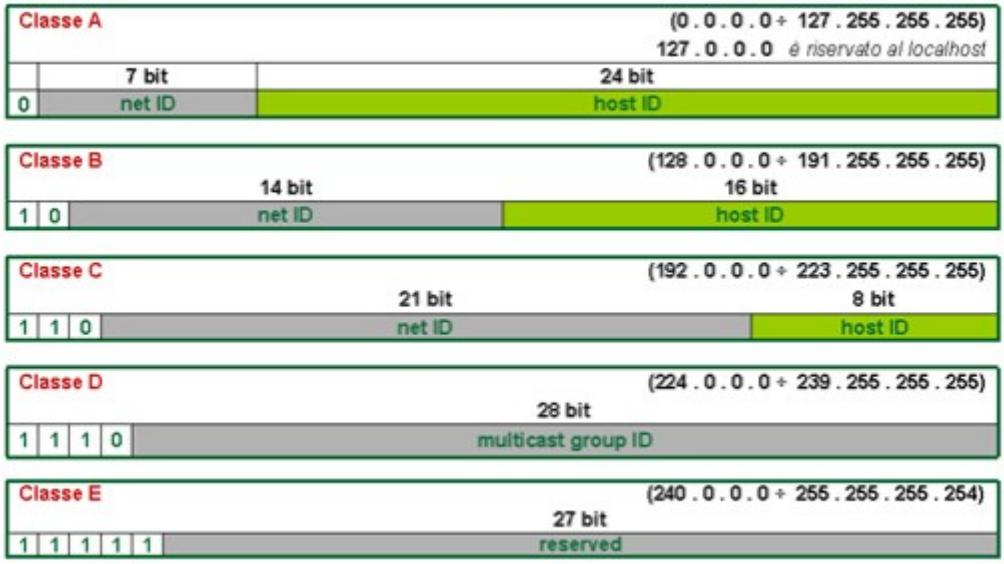
Le reti TCP/IP si avvalgono di un **indirizzo** di 32 bit (quattro *byte*); esso è espresso scrivendo i valori decimali di ciascun *byte*, separati dal carattere punto. Il suo formato è

Indirizzo IP = Indirizzo di rete (Net-Id)-Indirizzo di host (Host-Id)

L'indirizzo, con i bit relativi alla parte di **host** posti a zero, risulta essere l'indirizzo della rete in cui si trova l'*host*.

Non sono i nodi ad avere un indirizzo IP, bensì le interfacce. Quindi se un nodo ha tre interfacce (ad esempio un *router*), esso ha tre indirizzi IP. Gli indirizzi IP sono univoci a livello mondiale e sono assegnati da un'unica autorità (in realtà l'autorità assegna al gestore di una rete un indirizzo di rete; sarà poi il gestore a decidere quali indirizzi dare alle proprie macchine). Inoltre, l'indirizzo IP non identifica l'*host* in quanto tale, ma la connessione di un *host* alla relativa rete. Di conseguenza, se una macchina *host* viene spostata in un'altra rete, il suo indirizzo deve essere cambiato. Per indicare non una macchina nella sottorete, ma la sottorete, si mettono a zero i bit della parte di indirizzo di *host*; per indicare tutte le macchine attestate sulla sottorete, cioè l'indirizzo di **broadcast** sulla sottorete, si mettono a uno i bit della parte di indirizzo di *host*. Quindi il numero di *host* possibili in una certa sottorete è pari alla dimensione dello spazio di indirizzamento della parte di *host-id* diminuita di 2.

Classi di indirizzi IP



Gli indirizzi IP sono suddivisi in cinque classi:

Classe A. Provvedono alle reti che hanno un numero cospicuo di *host*. Il campo dell'ID dell'*host* è di 24 bit, pertanto possono essere identificati circa 16 milioni di *host* per ogni rete di questo tipo. Sette bit sono dedicati all'ID di rete, per un massimo di 128 reti di classe A.
Classe B. Sono utilizzati per reti di dimensioni intermedie. Si possono avere al massimo circa 16000 reti di classe B, ciascuna con una dimensione massima di circa 64000 indirizzi.
Classe C. Sono utilizzati per numerose reti con pochi *host*. Le reti di classe C contengono meno di 256 *host* e sono individuate da 21 bit nell'ID di rete.
Classe D. Sono riservati al **multicasting** (RFC 1112).
Classe E. Sono riservati per usi futuri.

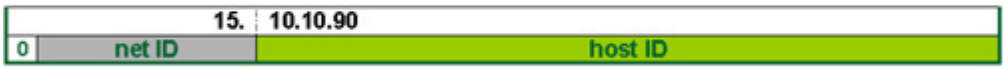
Lo spazio di indirizzamento va partizionato tra le varie classi di indirizzi, in modo che non vi siano sovrapposizioni tra classi diverse. Questo si ottiene fissando, per ogni classe, particolari configurazioni nel primo *byte*.

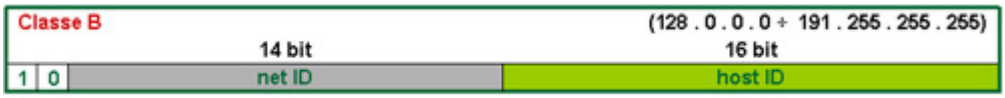
Classi di indirizzi A, B, C, D

classi A e B

Una rete di classe A è rappresentata dal primo bit (bit più significativo) a zero. I primi otto bit (0-7) identificano il numero della rete, e i rimanenti bit (8-31) identificano il numero dell'*host* all'interno della rete. Con questa rappresentazione si possono ottenere 128 (27) reti di classe A, ciascuna con un numero massimo di 16777216 (224) - 2 *host*. Gli indirizzi di classe A sono riconoscibili dal primo numero dell'indirizzo compreso tra 0 e 127.

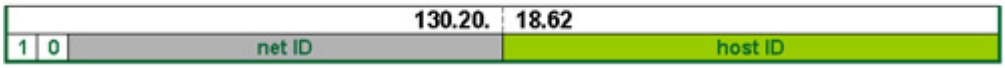
esempio





Una rete di classe B è rappresentata da un 1 ed uno 0 come primi due bit. I primi 16 bit (0-15) identificano il numero della rete, e gli ultimi 16 bit (16-31) identificano il numero dell'*host* all'interno della rete. Con questa rappresentazione si possono ottenere 16384 (214) reti di classe B, ciascuna con un numero massimo di 65536 (216) - 2 *host*. Gli indirizzi di classe B sono riconoscibili dal primo numero dell'indirizzo compreso tra 128 e 191.

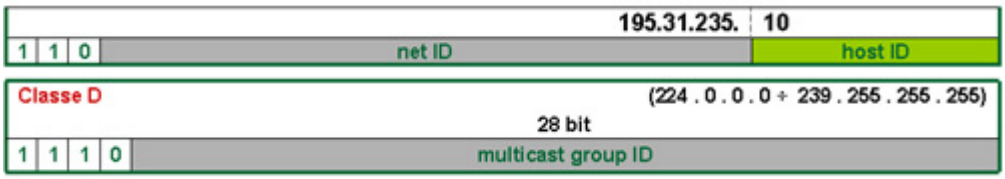
esempio



classi C e D

Una rete di classe C è rappresentata dai primi tre bit aventi valore rispettivamente 1,1, e 0. I primi 24 bit (0-23) identificano il numero della rete, e gli ultimi 8 bit (24-31) identificano il numero dell'*host* all'interno della rete. Con questa rappresentazione si possono ottenere 2097152 (221) reti di classe C, ciascuna con un numero massimo di 256 (28) - 2 *host*. Gli indirizzi di classe C sono riconoscibili dal primo numero dell'indirizzo, compreso tra 192 e 223.

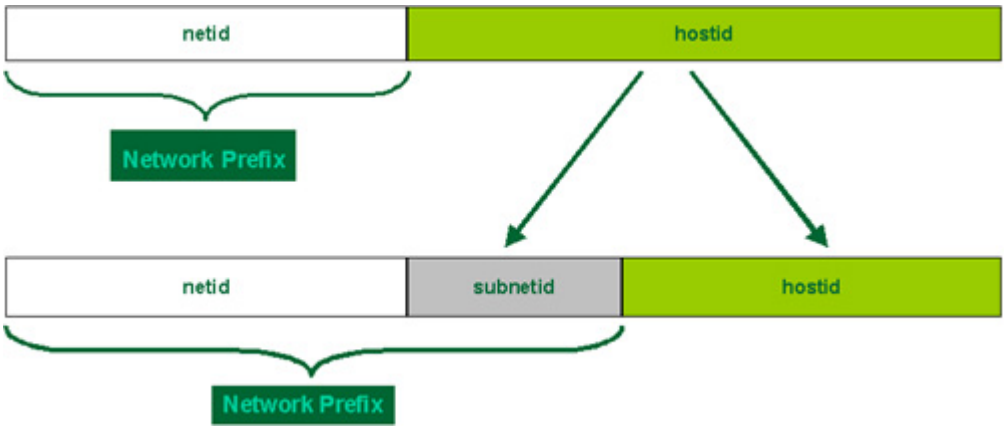
esempio



La classe D prevede che il primo *byte* contenga un valore compreso tra 224 e 239. Tale classe è riservata alla trasmissione di datagrammi IP in modalità ***multicasting***.

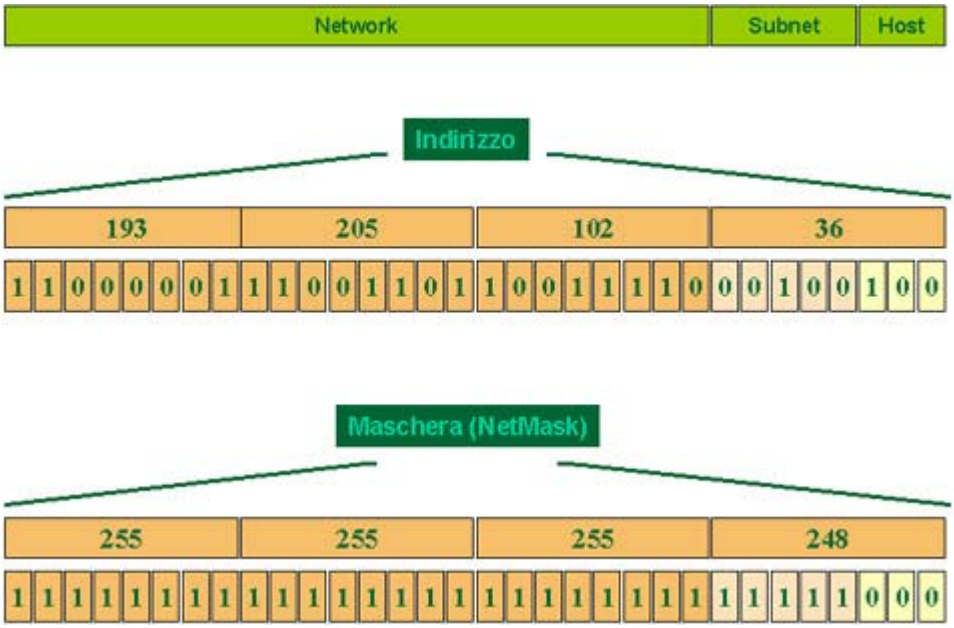
Netmask e valori possibili

***Subnet* ID**



Nel 1985, l'RFC 950 ha definito una procedura standard per supportare il *subnetting*, ovvero la divisione di una singola rete, di classe A, B o C, in sottoreti di dimensioni minori. Il *subnetting* è stato introdotto per superare alcuni dei problemi che Internet cominciava ad avere con la gerarchia di indirizzamento a due livelli (*netid* + *hostid*): la continua crescita delle tabelle di *routing*. Le organizzazioni dovevano richiedere un indirizzo di rete prima di poter installare una nuova LAN nella propria rete privata. Entrambi questi problemi sono stati affrontati aggiungendo un terzo livello gerarchico (*netid* + *subnetid* + *hostid*) allo schema di indirizzamento iniziale. Il *subnetting* ha risolto il problema della crescita delle tabelle di *routing* facendo in modo che le sottoreti di una rete non siano visibili all'esterno della rete stessa. Il percorso da Internet a qualsiasi sottorete di una certa rete IP è lo stesso, in quanto tutte le sottoreti condividono lo stesso indirizzo di rete (pur avendo differenti *subnetid*). Quindi, mentre i *router* all'interno della rete devono distinguere le singole sottoreti, i *router* di Internet hanno un'unica *entry* nella tabella di *routing* che individua tutte le sottoreti. Ciò consente all'amministratore di rete di introdurre una complessità arbitraria alla rete senza accrescere le dimensioni delle tabelle di *routing* di Internet. Il *subnetting* ha risolto il problema della continua richiesta di indirizzi IP, assegnando ad ogni organizzazione uno (o al più alcuni) indirizzi di rete. L'organizzazione è poi libera di assegnare un differente numero di sottorete per ognuna delle sue reti interne. Ciò consente ad un'organizzazione di usufruire di sottoreti addizionali, senza la necessità di richiedere ed ottenere un nuovo indirizzo di rete.

***Netmask* (esempio)**



L'ampiezza dei campi *subnet* e *host* viene definita tramite un parametro detto *netmask*. La *netmask* contiene bit a uno in corrispondenza dei campi *network* e *subnet*, e a zero in corrispondenza del

campo *host*. Per determinare la *subnet* di appartenenza di un *host* a partire dal suo indirizzo IP, basta mettere in *AND* bit a bit la *netmask* con l'indirizzo IP. L'importanza di comprendere se due indirizzi appartengono o no alla stessa *subnet* è fondamentale, in quanto nel primo caso l'*host* mittente del pacchetto lo invierà direttamente verso il destinatario (*routing* diretto), nel secondo caso lo invierà ad un *router* a valle verso la destinazione (*routing* indiretto). Questo comportamento deriva dall'assunzione implicita che *ad ogni rete logica (subnet IP) corrisponda una stessa rete fisica*. Nella figura viene mostrato ad esempio un indirizzo IP 193.205.102.36 con maschera 255.255.255.248, relativo ad una *subnet* con al massimo 6 macchine. Bisogna considerare infatti che l'indirizzo con tutti zero nella parte di *host* indica la *subnet* e l'indirizzo con tutti uno indica l'indirizzo di *broadcast* sulla sottorete.

Nella tabella seguente vengono riportati i valori che potranno assumere gli ultimi 3 bit.

bit	***host***	**quarto numero IP**
000	*subnet*	32
001	disponibile	33
010	disponibile	34
011	disponibile	35
100	disponibile	36
101	disponibile	37
110	disponibile	38
111	*broadcast* (tutti)	39

Tutti i *router* di Internet instradano in base all'indirizzo di *Network* (193.205.102) di classe C. Il *router* responsabile di questa rete procede con l'ulteriore instradamento verso le *Subnet* in base all'esame degli ulteriori 5 bit (informazione ricavata dalla maschera).

Indirizzi privati ed indirizzi pubblici

Indirizzi privati

IANA
Allocated, Non-Internet Routable IP Address Schemes

Classe	***Network Address Range***
A	da 10.0.0.0 a 10.255.255.255 (10.0.0.0/8)
B	da 172.16.0.0 a 172.31.255.255 (172.16.0.0/12)
C	da 192.168.0.0 a 192.168.255.255 (192.168.0.0/16)

La IANA (*Internet Assigned Numbers Authority*) ha riservato i tre blocchi di indirizzi indicati in figura per le reti IP private, ovvero reti IP che non sono interconnesse ad Internet. Il primo blocco (10.0.0.0/8) rappresenta un'intera classe A. Il secondo blocco (172.16.0.0/12) è costituito dall'insieme di 16 reti di classe B contigue. Il terzo blocco (192.168.0.0/16) rappresenta 255 reti di classe C contigue.

Logical IP subnet

LIS

Con la definizione di *Logical IP Subnet* si definisce un'entità amministrativa separata composta da un gruppo di nodi IP (*host* e **router**) collegati alla stessa rete ATM e appartenenti alla stessa IP *subnet*. Si tratta in definitiva di una rete fisica in cui gli *host* possono colloquiare direttamente tra loro senza passare attraverso *router*, ma utilizzando sistemi posti a livelli inferiori della pila **OSI** (o equivalente), quali **switch**, **bridge** e **hub**.

I requisiti necessari per appartenere a una LIS sono i seguenti:

- avere lo stesso **indirizzo** di *Net* e *Subnet*;
- essere configurati da una singola autorità amministrativa per la configurazione e gestione;
- essere collegati direttamente alla stessa rete ATM;
- ogni accesso tra LIS diverse deve avvenire attraverso un border *router*;
- avere un meccanismo di traduzione degli indirizzi da IP ad ATM (e viceversa);
- la rete di connessione deve essere a maglia completa.

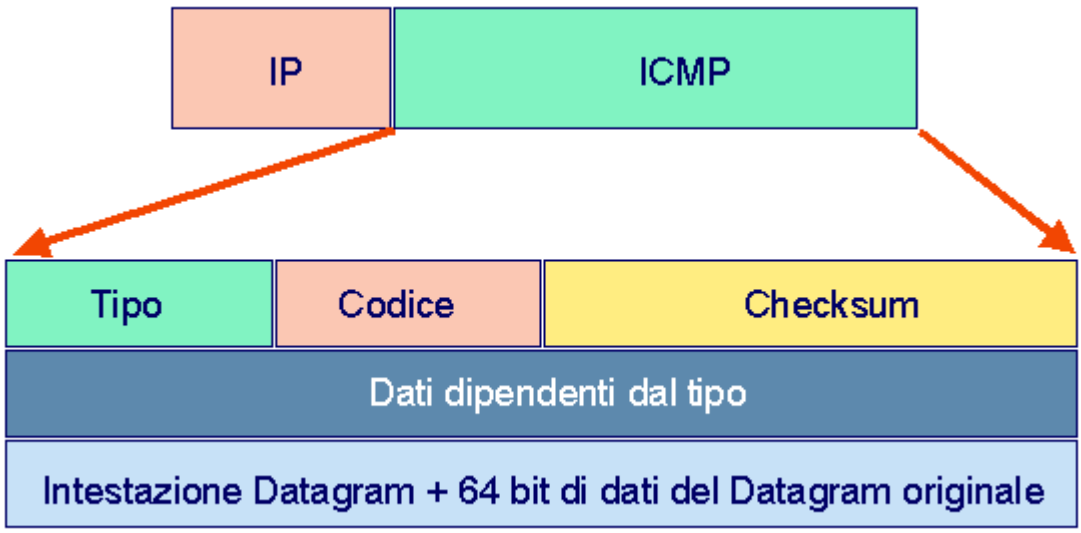
Protocolli correlati a IP e loro impiego

Il protocollo IP, impiega il corrispondente indirizzo per permettere ai *gateway* di prendere le decisioni di instradamento del datagramma. Tuttavia, affinché possano essere consegnati i dati nell'ambito di una rete locale, occorre fare riferimento all'indirizzo della stazione destinataria. Per tale motivo, e non solo, esistono altri protocolli che vengono tipicamente utilizzati nell'ambito delle reti e che possono essere considerati all'*Internet Protocol*:

- **ARP** (*Address Resolution Protocol*) e il corrispondente RARP (*Reverse Address Resolution Protocol*);
- **ICMP** (*Internet Control Message Protocol*).

Di questi due viene fornita una spiegazioni tecnica (e la loro motivazione all'uso) nelle sezioni loro dedicate.

Internet Control Message Protocol (ICMP)



IP non possiede meccanismi di indicazione o correzione degli errori, ma si affida a un modulo denominato *Internet Control Message Protocol* (ICMP) per la segnalazione degli errori sopravvenuti nel corso dell'elaborazione di un datagramma e per la generazione di messaggi amministrativi e di stato. ICMP risiede in ogni *computer host* o *router* come protocollo abbinato a IP. ICMP viene

utilizzato tra gli *host* o i *router* quando i datagrammi non possono essere consegnati, quando un *router* non ha sufficiente memoria temporanea per conservare ed inoltrare unità dati del protocollo, eccetera. ICMP comunica all'*host* se una destinazione è irraggiungibile; inoltre, gestisce o crea un messaggio per segnalare il superamento del tempo massimo di permanenza in rete (**TTL**) di un datagramma. Infine, ICMP esegue alcune funzioni di modifica per determinare se l'intestazione IP è errata o in altro modo inintelligibile.

Il protocollo ICMP è descritto in RFC 792 ed è incluso in tutte le implementazioni IP come un protocollo a basso livello che si appoggia direttamente su IP.

È utilizzato per la trasmissione dei messaggi di errore, di messaggi di controllo e misure di prestazioni, ma non specifica le azioni da intraprendere.

I messaggi viaggiano nel campo dati del *datagram* IP e vengono manipolati dal *software* IP, non dagli applicativi utente.

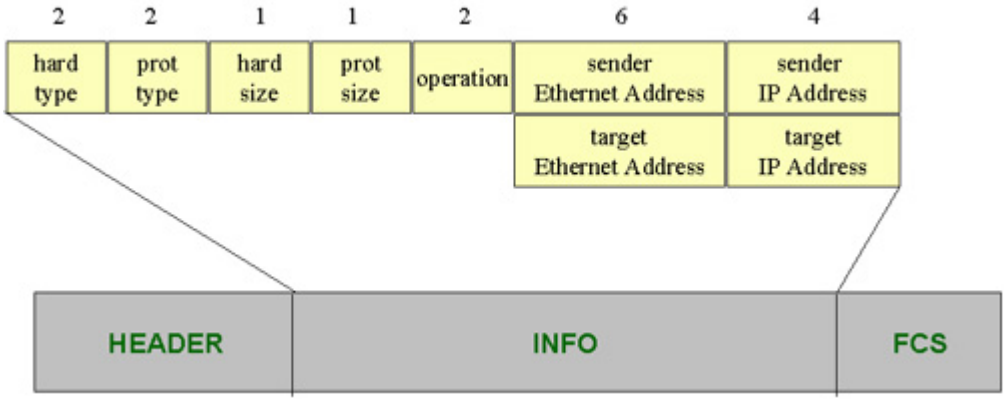
ICMP viene imbustato in IP, indirizzato con 1 nel campo *protocol*. Il formato del pacchetto ICMP prevede:

- tipo, indica un particolare messaggio ICMP (si veda la tabella seguente);
- codice, viene usato in alcuni messaggi ICMP per specificare alcune condizioni;
- **checksum**, per il controllo di errore; viene calcolato su tutto il pacchetto ICMP;
- la parte rimanente viene usata per trasmettere dei dati legati al particolare messaggio ICMP.

Come esempio, nella figura precedente è mostrato un pacchetto di ICMP, del tipo *error message*, in cui nella parte di dati è inclusa l'intestazione IP e altri 64 bit del pacchetto che ha generato l'errore.

Address Resolution Protocol (ARP) e Reverse ARP

Lo *stack* IP fornisce un protocollo per risolvere gli indirizzi. Il protocollo di risoluzione degli indirizzi (ARP) gestisce la traduzione degli indirizzi IP in indirizzi fisici e nasconde questi indirizzi fisici agli strati superiori. Generalmente, ARP funziona con tabelle di mappatura, definite *cache* ARP, che forniscono la mappatura tra un indirizzo IP e un indirizzo fisico. In una LAN, ARP prende l'indirizzo IP di destinazione e cerca l'indirizzo fisico corrispondente nella *cache* ARP: se lo trova lo restituisce al richiedente. Se l'indirizzo richiesto non viene reperito nella *cache ARP*, il modulo ARP effettua una trasmissione *broadcast* sulla rete: questa prende il nome di richiesta ARP (ARP *request*) e contiene l'indirizzo IP richiesto. Di conseguenza, se una delle macchine che ricevono la richiesta riconosce il proprio indirizzo IP nel messaggio di ARP, restituisce una risposta ARP (ARP *reply*) all'*host* richiedente. Il *frame* contiene l'indirizzo fisico dell'*host* interrogato. Quando riceve questo *frame*, l'*host* richiedente inserisce l'indirizzo nella propria *cache* ARP: i datagrammi che verranno successivamente inviati a questo particolare indirizzo IP potranno essere tradotti nell'indirizzo fisico accedendo alla *cache*.



Il protocollo ARP si appoggia direttamente sul livello *data link* e non su IP. Il pacchetto ARP è incapsulato nella PDU del livello *data link*, che potrebbe essere per esempio una trama *Ethernet*. La richiesta viene inviata all'indirizzo di *broadcast* di livello 2, perché deve essere elaborata da tutte le macchine; contiene inoltre l'indirizzo di livello 2 e quello di livello 3 della macchina sorgente; così la macchina che riconosce il proprio indirizzo di livello 2 sa a chi inviare il *reply*. Nel pacchetto di risposta vengono riempiti tutti i campi; importante è chiaramente l'indirizzo di livello 2 di chi invia il *reply*, che era l'informazione richiesta in partenza. Qualsiasi modulo ARP può avvalersi di un pacchetto ARP per aggiornare la propria *cache*: il modulo esamina l'indirizzo IP e l'indirizzo *hardware* del mittente per determinare se queste voci sono comprese nella propria *cache*. In questo modo, ottiene tutte le informazioni possibili sui dati. Il pacchetto ARP, oltre ai campi per gli indirizzi di livello 2 e 3 di sorgente e destinazione, contiene:

- *hard type*, specifica il tipo di indirizzo di livello 2; per indicare che l'indirizzo è di tipo MAC si usa il valore 1;
- *protocol type*, specifica il tipo di indirizzo di livello 3, si usa 0x0800 per indicare indirizzi IP;
- *hard size*, indica la lunghezza dell'indirizzo di livello 2;
- *protocol size*, indica la lunghezza dell'indirizzo di livello 3;
- *operation*, indica il tipo di comando ARP, 1 per ARP-*request*, 2 per ARP-*reply*.

A volte risulta utile risalire all'indirizzo IP a partire dall'indirizzo *Ethernet*; tali funzionalità sono assicurate dal Protocollo RARP (*Reverse Address Resolution Protocol*).