Internetworking: connessione fra reti

"Stack" di protocolli TCP/IP

TPC, **IP** e molti altri protocolli utilizzati nella "rete delle reti" Internet costituiscono un'architettura di rete stratificata, simile a quella del modello OSI. Dato che l'inizio del loro sviluppo risale a prima che gli standard ISO/OSI fossero promulgati, IP e TCP li hanno in parte ispirati. Vista la struttura "a catasta", tutti insieme vengono di solito definiti come lo "stack" di protocolli TCP/IP; in altri casi li si trova definiti come la "Internet protocol suite".
TCP e IP nascono come protocolli portanti della rete di internetwork ARPAnet, commissionata dal Dipartimento della Difesa USA (agenzia DARPA) a partire dal 1968. Il loro sviluppo iniziale era orientato alla connessione su aree estese e geografiche, ma furono impostati con servizi di basso livello di tipo connectionless, per questo si rivelarono adatti anche alle reti locali. TCP e IP furono sviluppati nel Sistema Operativo Unix ed adottati nella sua versione "Berkeley", distribuita gratuitamente, che divenne subito standard di fatto. TCP/IP diventò perciò la modalità di collegamento in rete locale di tutti i sistemi Unix.
Il gruppo di protocolli che fa riferimento a TCP/IP si può stratificare in diversi livelli:

<table>
<tr><th>Strato TCP/IP</th><th colspan="6">Protocolli Internet</th><th>Livello OSI</th></tr>
<tr><td rowspan="2">Application (Servizi per le applicazioni)</td><td>FTP</td><td>Telnet</td><td>SMTP</td><td>HTTP</td><td>NNTP</td><td rowspan="2">NTP</td><td>7 Application</td></tr>
<tr><td></td><td></td><td></td><td></td><td></td><td>6 Presentation</td></tr>
<tr><td rowspan="2">Host to host transport</td><td colspan="5" rowspan="2">TCP</td><td rowspan="2">UDP</td><td>5 Session</td></tr>
<tr><td>4 Transport</td></tr>
<tr><td>Internetwork</td><td colspan="6">IP</td><td>3 Network</td></tr>
<tr><td rowspan="2">Network access (di solito non è specificato da standard Internet)</td><td colspan="3">DLL (LLC + MAC)[1]</td><td colspan="3">PPP[2]</td><td>2 DLL</td></tr>
<tr><td colspan="3">Fisico</td><td colspan="3">RS 232[3] + modem[4]</td><td>1 Physical</td></tr>
</table>

Disegno: "stack" TCP/IP confrontato con ISO-OSI

Il livello di internetwork corrisponde di fatto al livello 3 del modello OSI, e viene realizzato con IP (Internet Protocol).
Il livello di trasporto fra le stazioni (Host to host transport) assorbe le funzionalità il livello 4 (sessione) ed alcune delle funzioni che sono ascrivibili al livello 5 (trasporto) e fornisce un canale di comunicazione da stazione a stazione ("end to end") fra due applicazioni. I principali protocolli di questo livello sono TCP e UDP. TCP è connection oriented, con consegna dei messaggi garantita ed affidabile. UDP è un servizio connectionless, più efficiente di TCP, che è usato se non interessa il controllo e la rimozione degli errori.
Il livello di servizio alle applicazioni include, oltre che alcune funzioni ascrivibili al livello 5, le funzionalità di più alto livello, tipiche degli strati 6 e 7 di OSI e che sono realizzate dai "famosi" protocolli di Internet quali HTTP, SMTP, FTP, alcuni dei quali sono indicati nel disegno "stack TCP/IP". Le funzioni che sono fornite sono strettamente dipendenti dal protocollo che viene utilizzato. Esistono moltissimi di questi protocolli, che hanno avuto diversa fortuna.

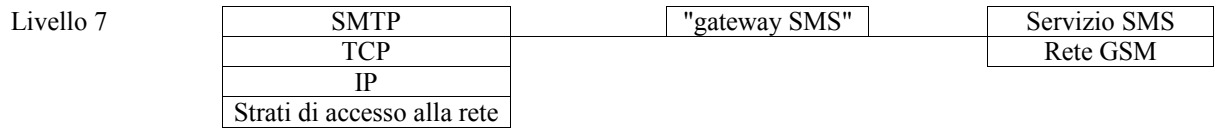
IP (RFC791 STD 5)

Internet Protocol è un protocollo di livello di rete (terzo livello OSI) di tipo connectionless. Fu specificato per la prima volta nella RFC791, del Settembre 1981. La versione di IP più utilizzata attualmente è la quattro (IPv4), la versione più recente "ratificata" dalla **ISOC** (**I**nternet **Soc**iety) è la 6 (Ipv6, RFC1883).
Essendo stato pensato per le WAN utilizza il minor numero possibile di richieste broadcast. Infatti il broadcast diretto fra le stazioni viene sempre impedito dai router fra LAN diverse collegate con IP ed è limitato alle sole stazioni che risiedono sulla stessa LAN (dominio di broadcast). L'unico tipo di "broadcast" a livello di internetwork che IP utilizza è quello, utilizzato dal protocollo **RIP** (**R**outing **I**nformation **P**rotocol), tramite il quale i router si scambiano informazioni relative all'instradamento. Come già accennato, IP realizza una trasmissione di tipo "best effort", perciò può essere impiegato con efficacia anche nelle reti locali.
In una spedizione "best effort" la rete fa tutto il possibile per fare in modo che il pacchetto di dati raggiunga il suo destinatario, ma non effettua alcun tipo di controllo, demandando agli strati di software superiori il problema della rilevazione e della correzione degli errori. Ciò è tipico delle LAN, sulle quali c'è un tasso d'errore piuttosto basso e l'alta velocità di trasmissione permette la ritrasmissione senza grossi "costi" delle informazioni corrotte.
IP non ha perciò meccanismi di rilevazione e correzione degli errori, la rilevazione e la notifica degli errori è affidata ad un protocollo particolare, detto ICMP (**I**nternet **C**ontrol **M**essage **P**rotocol, RFC792 STD 5), che può essere considerato un protocollo "ancillare" di IP e che stabilisce il modo tramite il quale due stazioni si comunicano a vicenda gli eventuali errori avvenuti nella comunicazione. La correzione degli errori commessi, se interessa, è effettuata per mezzo della ritrasmissione ed è affidata agli strati superiori dello "stack".

1 Si tratta di uno standard IEEE
2 Standard Internet
3 Standard EIA
4 Standard ITU-T

IP trasmette un pacchetto di dati che porta un indirizzo del destinatario ed uno del mittente. Questo pacchetto viene inoltrato nella rete senza accertarsi della sua consegna, in questo è analogo ad un telegramma "senza ricevuta di ritorno" e per questo viene detto "datagramma".
IP è un protocollo di internetworking, cioè collega reti che potrebbero essere autonome, diverse nei mezzi di trasmissione, nel metodo di accesso e nel frame di livello 2, occupandosi di far giungere il datagramma fino alla rete di destinazione, ed effettuando l'instradamento lungo un percorso stabilito, che permette di giungere a destinazione anche quando c'è la possibilità di arrivarci con percorsi diversi. Usando IP ogni dispositivo coinvolto nel trasporto del pacchetto è in grado di decidere quale strada esso deve prendere ogni volta che ci sono diramazioni. Peraltro IP non è un protocollo di scoperta del percorso, quindi usandolo non si è in grado di stabilire il miglior percorso per giungere a destinazione; ciò significa che la decisione ai "bivi" verrà presa sulla base di "tabelle di routing", contenute nel router, che non sono gestite con IP, ma con protocolli diversi.

Host, gateway, internet, datagramma
Diamo alcune definizioni del "gergo IP".
Una internet (notare la i minuscola) è un insieme di reti, per esempio reti locali, interconnesse con protocollo IP. Si noti invece che la Internet (I maiuscola) è la rete mondiale che collega milioni di internet IP. Internet, per alcuni servizi, è in grado di collegare anche reti non IP, con le quali effettua uno scambio a livelli più alti nel modello OSI.
Un router viene chiamato spesso anche "**gateway**" (cancello). Mentre il primo termine pone l'accento sulle funzionalità di instradamento del sistema, il secondo evidenzia la sua funzione di interfaccia fra reti eterogenee, di sistema che fa da "ponte" fra due mondi e tramite il quale si ha accesso ad altre reti.
È bene notare che il termine gateway può essere ambiguo, perché nella documentazione Internet viene usato al posto di "router" mentre in tutte gli altri contesti, in particolare in OSI, viene utilizzato per indicare un dispositivo che opera a livello 6 o 7 del modello (p.es. un "gateway" di posta elettronica fra Internet e la messaggistica SMS della telefonia GSM).



Di solito un computer in rete viene detto "**host IP**" ("ospite"). In realtà il termine host è usato più in generale, indicando una scheda di rete, un computer od un router (gateway) che è visibile su una internet e, come tale, possiede un indirizzo IP. In questo senso sarebbe più chiaro usare in luogo di "host" il termine "interface", che fa capire meglio che ogni scheda di rete dovrebbe avere il suo indirizzo IP, in particolare quando c'è più di una scheda sullo stesso computer.

L'elemento "atomico" della comunicazione IP, il pacchetto che viene spedito in rete, viene detto "datagramma IP".

Indirizzi IP
L'indirizzo IP è un indirizzo "di rete", nel senso che viene utilizzato dallo strato "network" della rete ed è diverso dall'indirizzo MAC.
IPv4 usa indirizzi a 32 bit, che corrispondono a 4 Giga Indirizzi (circa quattro miliardi). Questo spazio sembra molto grande ma in realtà in Internet è vicino all'esaurimento, dato che molti degli indirizzi vanno "sprecati", per il modo con il quale vengono assegnati. Per questo in IPv6 è stato aumentato il numero dei bit dell'indirizzo, portandolo a 128 (RFC1752), pur assicurandosi di mantenere una certa compatibilità con le precedenti versioni.
In forma "scritta" l'indirizzo IP v4 viene visualizzato con quattro numeri decimali separati da punti. Ciascuno dei numeri rappresenta 8 bit dell'indirizzo e perciò può essere compreso fra 0 e 255. Il byte più significativo dell'indirizzo è quello scritto alla sinistra del numero (p.es. 126.3.12.9).

Dato che IP è connectionless ogni pacchetto spedito deve poter viaggiare indipendentemente da tutti gli altri, esso deve perciò contenere l'intero indirizzo IP di mittente e destinatario.

Classi di indirizzi IP
L'indirizzo IP deve bastare per raggiungere, da un host qualunque in una qualunque rete locale, un altro un host qualunque. Ogni nodo della rete complessiva, vedendo un indirizzo di destinazione, deve essere in grado di stabilire se il destinatario è nella stessa rete locale o in un'altra rete. Se i due soggetti sono nella stessa rete il pacchetto verrà trasmesso con le normali tecniche "da rete locale", che abbiamo già visto. Qualora invece i due soggetti siano su reti diverse il pacchetto dovrà essere passato ad un router, che si arrangerà a spedirlo verso la sua destinazione finale.
Illustriamo ora il concetto di "classe" di indirizzi IP che, pur essendo superato dall'evoluzione dell'Internet, ne ha costituito la base per quel che riguarda il routing.
Dato che il pacchetto è "solo" nel suo viaggio nella rete, la struttura stessa dell'indirizzo IP deve indicare quale è la rete cui appartiene la stazione di destinazione.
L'indirizzo IP a 32 bit si può dividere in due parti: Indirizzo di rete - Indirizzo di host. Questa suddivisione viene fatta byte per byte e l'indirizzo può assumere la forma rete.host.host.host, rete.rete.host.host o rete.rete.rete.host. La distinzio-

ne fra questi tipi di indirizzo avviene considerando i primi bit dell'indirizzo IP, che specificano il formato del resto dell'indirizzo e la sua "classe".
Se il primo bit dell'indirizzo (il bit più significativo dei 32) è zero, l'indirizzo IP viene detto di "**classe A**". In questo caso i sette bit successivi al primo, che concludono il primo byte, indicano la rete; i 24 bit successivi, che concludono l'indirizzo, indicano la stazione all'interno della rete. Il formato dell'indirizzo è dunque del tipo rete.host.host.host.
Le reti di classe A sono poche e molto vaste, possono cioè comprendere molti computer (teoricamente fino a circa 2^{24} = 16777216). Le reti di classe A hanno il primo byte che va da 0 a 01111111b e quindi potrebbero essere al massimo 2^7 - 1 = 127, anche se non tutti i numeri possono essere usati (vedi dopo).
Se i primi due bit dell'indirizzo IP sono 10b, la rete è di classe B. In questo caso l'indirizzo della rete è dato dagli altri bit che completano i primi due byte , cioè da 14 bit. I due byte finali sono l'indirizzo dell'host. Le reti di tipo B hanno indirizzi del tipo rete.rete.host.host; hanno i primi due byte che vanno da 8000h a CFFFh e perciò possono essere, in linea di principio, CFFFh - 8000h = 4FFFh = 20479, ciascuna con un massimo di circa 65536 stazioni, sempre con l'avvertenza che alcuni numeri sono "vietati".
Se i primi 3 bit dell'indirizzo sono 110b la rete è di classe C ed è identificata dal resto dei primi tre byte dell'indirizzo (21 bit). Solo l'ultimo byte serve per indicare l'host (rete.rete.rete.host). Le reti di classe C possono essere numerosissime (circa DFFFFFh - C00000h = 1FFFFFh = 2097151), ma possono avere relativamente poche stazioni (circa 256).
Se i primi 4 bit dell'indirizzo sono 1110b (classe D) l'indirizzo non identifica una rete, ma un gruppo di multicast. Il datagramma non è diretto ad un solo host, ma ad un insieme di host.
La classe E, con indirizzi che iniziano con 1111b, è riservata per scopi futuri e per sperimentazioni.

In sintesi gli indirizzi IP sono così suddivisi:

primi bit	Classe dell'ind.	Significato dell'indirizzo	Primo byte indirizzo (decimale)
0	Classe A	rete.host.host.host	0 .. 126
10	Classe B	rete.rete.host.host	128 .. 191
110	Classe C	rete.rete.rete.host	192 .. 223
1110	Classe D	N.A. (non applicabile)	224 .. 239
1111	Classe E	N.A. (non applicabile)	240 .. 255

Per rinforzare il concetto che l'indirizzo IP (di livello 3) è cosa del tutto diversa dall'indirizzo MAC, si pensi a queste due considerazioni:
- Più schede di rete nella stessa macchina possono avere lo stesso indirizzo IP.
- Una scheda di rete può avere più di un indirizzo IP

Indirizzi IP particolari
Gli indirizzi di rete o di host con tutti uno o tutti zero non identificano una rete o un host specifico ma hanno un significato particolare.
L'indirizzo composto da tutti 0 nella parte di host (detto "network number) significa "tutta questa rete"; è usato dal router per indicare, nelle sue tabelle, tutta la rete relativa. P.es., l'indirizzo 192.168.13.0 non può essere assegnato ad alcun host e significa "tutta la rete in cui i primi tre Byte sono: 192.168.13"
I datagrammi che hanno indirizzo di destinazione con tutti 1 nella parte di host sono destinati a tutti gli host di quella rete locale, ovverosia sono datagrammi di broadcast nella sottorete. Per esempio un indirizzo del tipo <IndirizzoDiRete>.<Tutti 1> fa un broadcast in tutta la rete locale che ha <IndirizzoDiRete> come sua parte di rete.

La RFC1918, stabilisce alcuni indirizzi "privati", che sono speciali perché i loro datagrammi non vengono mai propagati dai router al di fuori della rete locale. Questi indirizzi IP sono quelli che vanno usati nelle reti locali, anche se esse non hanno accesso a Internet. Il loro uso garantisce infatti che, se e quando la rete verrà collegata ad Internet, essa non interferirà, dato che i datagrammi scambiati fra gli indirizzi già assegnati con numeri IP "privati" rimarranno confinati all'interno della rete locale.
Gli indirizzi privati sono:
Classe A: 10.0.0.0 - 10.255.255.255 (una rete di classe A)
Classe B: 172.16.0.0 - 172.31.255.255 (15 reti di classe B)
Classe C: 192.168.0.0 - 192.168.255.255 (255 reti di classe C)

127.0.0.0 non è una normale rete di classe A, perché viene usata come indicazione di "loopback". I pacchetti spediti alla rete 127 in realtà tornano indietro subito al mittente, senza interessare di fatto le altre stazioni.
Tipico per questo uso è l'indirizzo 127.0.0.1, detto anche "localhost" o "local loopback" (lo). L'indirizzo di loopback viene usato per far funzionare lo stack IP anche sui computer che non sono connessi ad alcuna rete, oltre che per scopo diagnostico.

Indirizzi Ipv6
Gli indirizzi IPv6 sono numeri di 128 bit, che dovrebbero bastare per sempre. Con 128 bit di indirizzo si possono avere 280 milioni di miliardi di indirizzi unici ogni metro quadrato della superficie della terra (pure troppo?).
Per scrivere gli indirizzi IPv6 si usa una notazione analoga a quella degli indirizzi MAC, considerandoli numeri da 128 bit e rappresentandoli in esadecimale separati da ":" ogni quattro cifre esadecimali (16 bit).

Per esempio:
FEDC:BA98:7654:3210:FEDC:BA98:7654:3210 (che ha 32 cifre e 39 caratteri). Si può semplificare un poco omettendo gli zeri non significativi; per esempio:
1080:0:0:0:8:0800:200C:417A
che si può semplificare ulteriormente in questo modo:
1080::8:800:200C:417A[5] (che ha "solo" 21 caratteri)

Dato che il numero non può sempre essere semplificato, questo modo di scrivere l'indirizzo è piuttosto ingombrante, per cui ne è stato inventato un altro (RFC1924):
1. si rappresenta il numero di 128 bit in base 85 (urca!)
2. si associa a ciascuna delle cifre della base 85 il codice ASCII di un carattere in base alla tabella seguente, i cui valori sono attentamente pensati
3. ne esce una "scritta", apparentemente alfanumerica (in realtà è un numero di 128 bit rappresentato in base 85), che è l'indirizzo IP a 128 bit.

Dato che 2^{128} = 340282366920938463463374607431768211456, che corrisponde a circa 3,4 * 10^{38}, mentre 85^{20} = 38759531084514355873123178482055664062 5 (circa 3,8 * 10^{38}), è chiaro che, con questa rappresentazione, bastano 20 "cifre" base 85, invece che 32 in base 16 (39 caratteri), per scrivere un qualsiasi indirizzo IPv6 .

	0	***1***	***2***	***3***	***4***	***5***	***6***	***7***	***8***	***9***
0	0	1	2	3	4	5	6	7	8	9
10	A	B	C	D	E	F	G	H	I	J
20	K	L	M	N	O	P	Q	R	S	T
30	U	V	W	X	Y	Z	a	b	c	d
40	e	f	g	h	i	j	k	l	m	n
50	o	p	q	r	s	t	u	v	w	x
60	y	z	!	#	$	%	&	(	)	*
70	+	-	;	<	=	>	?	@	^	_
80	`	{	|	}	~					

Tabella: valore delle cifre "base 85" negli indirizzi IPv6

Esempio:
L'indirizzo IPv6 1080:0:0:0:8:800:200C:417A, diventa 21932261930451111902915077091070067066 in base 10 e convertito in base 85, per lunga divisione, è 4-68-70-46-66-12-63-31-61-19-4-37-53-75-0-58-57-65-34-51.
Facendo la corrispondenza con la tabella il risultato finale è:

4)+k&C#VzJ4br>0wv%Yp

La scelta della base 85 viene dal fatto che i codici ASCII utilizzabili sono 94^{6}, ma con la base 94 sarebbero comunque state necessarie 20 "cifre" per rappresentare il numero di 128 bit. Dunque si usano per rappresentare il numero solo 85 caratteri, quelli esclusi (p.es. ".", "[", "]", "/", "\", """) sono usati per altro scopo.

Routing IP

L'instradamento fra varie reti in una internet è realizzato al livello di IP. Le funzioni di router possono essere fatte sia da sistemi dedicati, fisicamente simili ad un hub ("stand alone" router), sia da normali computer, in genere server di rete, equipaggiati del giusto software e che dispongano dei dispositivi di accesso alla rete (schede di rete e/o modem, schede ISDN, frame relay, ATM, o quant'altro).
Un router dedicato si compone di una CPU, del relativo software, di una certa quantità di memoria e di diversi "port" ciascuno dei quali è collegato ad un dispositivo di "network access", come potrebbe essere una scheda Ethernet, un link geografico con il sistema telefonico, su ISDN o linea dedicata o anche un modem analogico su linea telefonica commutata. A ciascuno dei port di un router viene assegnato un diverso indirizzo IP. Il router deve decidere dove instradare ogni datagramma che riceve. Per farlo distingue tutti gli altri host in due gruppi: **host diretti** ed **indiretti**. Un host diretto è collegato ad una rete locale che termina un suo segmento nel router. Quindi un datagramma che debba raggiungere un host diretto è già nella rete di destinazione e non deve essere instradato su percorsi diversi. Il router raggiunge un host diretto semplicemente passando il pacchetto IP al primo degli strati sottostanti, che lo propagano in rete locale seguendo le regole MAC locali. Un host indiretto è collegato ad una rete diversa, per cui deve essere raggiunto passando

5 I doppi : possono essere messi una volta solo ed in un modo un po' strano, che omettiamo.
6 I codici ASCII sono 127, ma vanno esclusi i primi 32 caratteri non stampabili, e quello di codice ASCII 127, pure non stampabile)

attraverso un altro router che è collegato al nostro attraverso uno dei suoi port. Per decidere su quale port smistare il datagramma il router usa una tabella che risiede al suo interno e che è detta "**tabella di routing**" (routing table). La tabella di routing stabilisce attraverso quali port devono essere smistati tutti i tipi di indirizzo. Si fa notare che un singolo router non conosce necessariamente tutto il percorso che il datagramma deve fare per arrivare a destinazione, ma è interessato al solo salto ("**hop**") che va da sé stesso al prossimo router del percorso.
La parte dell'indirizzo del destinatario che ne indica la rete è tutto ciò di cui il router ha bisogno per stabilire cosa fare del datagramma. Se la parte di rete dell'indirizzo di destinazione è uguale a quella del router, il datagramma è già nella rete di destinazione e quindi sarà spedito, con le tecniche di "tipo broadcast" da rete locale, alla stazione di destinazione, senza passare per nessun altro router. Se la parte di rete dell'indirizzo di destinazione è diversa da quella del router il datagramma dovrà essere spedito ad un altro router, senza più interessarsene successivamente. L'altro router sarà più vicino alla destinazione e si occuperà del prossimo "salto" del datagramma verso la sua meta.
IP è un protocollo di routing ma non di scoperta del percorso, è in grado cioè di portare a destinazione un pacchetto utilizzando delle tabelle di instradamento, ma non di creare o modificare quelle tabelle. La compilazione delle tabelle potrebbe essere manuale, gestita dall'amministratore della rete, o automatica, gestita dal router stesso. Nel primo caso il routing sarà necessariamente statico mentre nel secondo i vari router in rete, o meglio quelli più "vicini" fra loro, dovranno usare un opportuno protocollo accessorio per scambiarsi delle informazioni sulla topologia e sulle prestazioni della rete ("metriche" della rete). In seguito useranno quelle informazioni per compilare e gestire le tabelle di routing. Esse vengono "calcolate" eseguendo algoritmi di ricerca operativa che permettono trovare il percorso più "breve".
Il routing dinamico, cioè la realizzazione di percorsi diversi secondo le condizioni della rete, è ovviamente possibile solo nel caso che i router siano in grado autonomamente di comunicare e di calcolare il percorso o almeno parte di esso. Esistono molti protocolli per lo scambio di informazioni fra i router e la scoperta del percorso ottimale, uno relativamente semplice, che viene spesso utilizzato, è RIP (**R**outing **I**nformation **P**rotocol) (RFC1723). Altri protocolli di routing sono BGP (**B**order **G**ateway **P**rotocol, RFC1771), e IDRP (**I**nter-**D**omain **R**outing **P**rotocol, che fa parte della "suite "OSI)
L'operazione tramite la quale un router comunica agli altri router gli indirizzi degli host che è in grado di raggiungere viene detta "advertizing" (pubblicità!).

Tabelle di routing

Una tabella di routing di esempio:

Rete di destinazione	Percorso (router cui spedire il datagramma)	Porta fisica del router	Tipo di porta
199.2.2.0	Collegamento diretto (rete di classe C)	2	Ethernet 0
130.215.0.0	Collegamento diretto (rete di classe B)	1	Token -ring 1
194.28.36.0	Collegamento diretto (rete di classe C)	5	Ethernet 2
10.0.0.0	130.215.24.9 (questo è l'indirizzo di un altro router)	3	Modem
0.0.0.0 (default)	130.215.24.56 (questo è l'indirizzo del "default gateway")	4	ISDN

Nella colonna "percorso" c'è l'indicazione che si tratta di una rete collegata direttamente oppure l'indirizzo IP di un router attraverso il quale fare il primo salto per avvicinarsi alla destinazione. Se un router trova la rete fra quelle della colonna "reti di destinazione" manda il datagramma al port corrispondente. Se non lo trova può fare due cose: non trasmettere più il datagramma ("packet drop") o trasmetterlo a quello che viene detto "default gateway" (se esiste). Il "default gateway" è un router "più importante" che si suppone abbia una maggiore conoscenza della rete e che abbia in passato già trovato un percorso per quella destinazione, avendo perciò l'indirizzo nella sua tabella.
Come si può notare nella tabella di esempio gli indirizzi sono scritti in forma abbreviata, utilizzando dei byte a zero. Infatti nelle tabelle di routing gli indirizzi che hanno la parte di host tutta a zero significano "tutti gli host di questa rete". Più abbreviati sono gli indirizzi, più piccola è la tabella di routing; se le tabelle di routing diventano troppo grandi il router può non essere in grado di instradare i pacchetti.
La tabella di routing deve di fatto contenere una voce per ogni rete raggiungibile, ciò con le abbreviazioni e attraverso l'entry "default", indicato dall'indirizzo 0.0.0.0, che individua tutte le reti diverse dalle altre indicate nella tabella.
In caso di guasto o di rallentamento eccessivo di uno dei link collegati alle porte del router una tabella come la precedente non ha modo di indicare un percorso alternativo. Forme più evolute di tabelle permettono di specificare degli indirizzi secondari, in pratica altri campi "percorso" sulla stessa "riga", ai quali verranno spediti i datagrammi solo nel caso di guasto del link principale. In altri casi invece il router usa un protocollo di scoperta del percorso non appena un numero di errori troppo grande indica che è in corso un malfunzionamento in uno dei suoi link.
Si noti ancora che il router viene visto dall'esterno come tanti indirizzi IP quanti sono i suoi port collegati.

Disegno: "una internet collegata a Internet"

Nel viaggio di un datagramma l'indirizzo IP di destinazione rimane sempre lo stesso, mentre l'indirizzo fisico che viene usato cambia ogni volta che il datagramma attraversa un router.

Gli indirizzi IP vanno assegnati con attenzione. Dato che è l'indirizzo che indica la rete tutti i computer sulla stessa rete locale devono avere la parte di rete dell'indirizzo uguale. Quindi se in una rete di tipo B le stazioni effettivamente pre-

senti sono 50, invece che ventimila, tutti gli indirizzi non utilizzati sarebbero sprecati, dato che un'altra rete locale dovrebbe avere comunque un indirizzo di rete diverso. Per ovviare a questo problema è stato introdotto il "subnetting".

Subnetting (RFC950 STD 5)

Per utilizzare con maggiore efficienza lo spazio degli indirizzi IPv4 si usa il "subnetting" (RFC950). Esso fa in modo che LAN diverse appaiano alle altre reti come se fossero una sola. Il subnettig permette di dividere la parte "host" dell'indirizzo IP in due parti: **subnet**, nella parte alta e host, nella parte bassa. Ciò permette di risparmiare indirizzi IP di rete e di limitare la dimensione delle tabelle che devono essere incluse nei router. Se si hanno molte reti con pochi computer ciascuna, invece di usare molti indirizzi di rete di classe C se ne può usare uno solo, magari di classe B, e fare le giuste netmask per separare le reti locali solo all'interno della rete più grande.

Per impostare i bit dell'indirizzo iniziale di host che diventano indirizzo di subnet e quelli che invece rimangono indirizzi di host si deve usare un numero di 32 bit detto "netmask" (maschera di sottorete). I bit della netmask dove c'è 1 corrispondono all'indirizzo di subnet, mentre gli altri rimangono indirizzi di host.

Per esempio: l'indirizzo 140.2.0.0 corrisponde ad una rete si tipo B, cioè rete.rete.host.host. Introduciamo, in tutti gli host della rete, la netmask 255.255.255.0. La rete di tipo B è di fatto suddivisa in 255 sottoreti. Il significato dei primi due byte dell'indirizzo non cambia in conseguenza dell'introduzione della netmask. La parte di host invece assume due significati. Il terzo byte è il numero di subnet (una delle 255 possibili), mentre l'ultimo byte è l'indirizzo all'interno della subnet.

Segue un altro esempio, un po' più complicato, con una rete di tipo A.

Un indirizzo IP di tipo A (102.81.15.6):

0	1	1	0	0	1	1	0	0	1	0	1	0	0	0	1	0	0	0	0	1	1	1	1	0	0	0	0	0	1	1	0
Indirizzo di rete								Indirizzo di host																							

Una netmask (255.255.240.0):

1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	0	0	0	0	0	0	0	0	0	0	0	0

L'indirizzo IP con subnetting (la maschera divide l'indirizzo di host in subnet e host):

0	1	1	0	0	1	1	0	0	1	0	1	0	0	0	1	0	0	0	0	1	1	1	1	0	0	0	0	0	1	1	0
Indirizzo di rete								Indirizzo di subnet												Indirizzo di host											

Network address: 102 ; Subnet address: 1296 (max numero di subnet: 2^{12} = 4 Mega) ; Host address: 3846 (max numero di host: 2^{12} = 4 Mega)

Quando un host vuole inviare un pacchetto IP fa l'AND bit per bit fra la netmask e il proprio indirizzo. Se esso è diverso dall'AND fra netmask e indirizzo del destinatario assume che le due stazioni NON siano sulla stessa rete locale, a dispetto del fatto che l'indirizzo di rete è lo stesso.

Perciò, se i due PC sono connessi alla stessa subnet, l'host può spedire il datagramma direttamente; altrimenti lo deve passare ad un router.

Il funzionamento di questo primo livello di routing, effettuato da ogni host in una subnet, è descritto anche dal seguente pseudocodice:

```
IF ((IPmittente AND netmask) = ((IPdestinatario AND netmask)) THEN
    Spedisci il pacchetto alla rete locale
ELSE
    Spedisci il pacchetto al router
ENDIF
```

In sintesi con questo meccanismo da Internet è possibile vedere una rete "grossa" indistinta, che corrisponde al normale indirizzo di rete. In verità all'interno della rete si può distinguere fra sottoreti diverse applicando la netmask. Un provider Internet potrà acquistare un certo numero di indirizzi IP della stessa rete e suddividerli fra i suoi clienti facendo in modo che essi utilizzino la giusta maschera.

Per non dare problemi tutti i computer della stessa rete devono avere la stessa maschera per definire le sottoreti.

Broadcast nella sottorete

Come nel caso delle reti in generale l'indirizzo di broadcast nella sottorete è quello con tutti 1, naturalmente nella parte di sottorete. L'indirizzo con tutti 1 in tutta la parte di rete viene inteso come broadcast in tutte le sottoreti.

In sintesi l'indirizzo composto da <IndirizzoDiRete> <IndirizzoDiSottorete> <Tutti 1> fa il broadcast nella sottorete indicata, mentre, come già visto, un indirizzo composto da <IndirizzoDiRete> <Tutti 1> <Tutti 1> effettua il broadcast in tutta la rete, cioè verso tutte le subnet della rete (se ciò non viene bloccato dal router!).

Un problema che si può presentare con reti immense come l'Internet è quello delle dimensioni delle tabelle di routing. Se lo spazio degli indirizzi IP viene sempre più "spezzettato" in gruppi non contigui di indirizzi assegnati a provider diversi le tabelle non possono contenere indirizzi semplificati e devono avere un gran numero di entry, crescendo in modo abnorme. Se le tabelle di routing dei gateway "chiave" dell'Internet divenissero troppo grandi, alcune parti della rete potrebbero trovarsi "isolate".

*CIDR (**C**lassless **I**nter**d**omain **R**outing, RFC1518)*
Per ovviare a questo problema è stato inventato un protocollo di routing "senza classi", che permette di ridurre drasticamente le tabelle di routing dei router "importanti" facendo delle assunzioni sulla posizione geografica degli host. Se si fa in modo che, per esempio, tutti gli host che hanno un indirizzo che inizia per 194 stiano fisicamente in Europa, allora i router che sono negli USA manderanno tutti i datagrammi che iniziano per 194, indipendentemente dal resto dei byte e quindi anche indipendentemente dalla classe, verso il router più vicino all'Europa con il quale sono in contatto. Le autorità che assegnano gli indirizzi IP fanno in modo che sia rispettata una struttura che permette il funzionamento di CIDR. La RFC1519 spiega come devono essere assegnati gli indirizzi CIDR.
Attualmente la gran parte delle reti si connette ad Internet in un solo punto. Raramente ci sono "bivi", con due strade diverse, ed i router che hanno più di due instradamenti diversi sono pochi; di solito quelli dei provider "importanti" ("transit networks"), quelli di dorsale, che gestiscono il traffico di decine di provider "normali". Data questa caratteristica della Rete, si può dire che essa ha una topologia fortemente "gerarchica", molto simile ad un albero, sia pur con le dovute, significative, eccezioni (vedi figura: "architettura dell'Internet").
Questa gerarchia viene sfruttata riproducendola nell'assegnazione degli indirizzi e facendo in modo che l'indirizzo contenga un'indicazione sulla topologia, in particolare sul posto dove l'host è situato. Come vedremo questo contribuisce a diminuire drasticamente la dimensione delle tabelle di routing, a "risparmiare" indirizzi IP ed a rendere più rapide le operazioni di routing.

Con CIDR cambia il punto di vista sul routing IP. L'indirizzo rimane lo stesso, ma i router memorizzano sempre, per ogni riga della tabella di routing, assieme all'indirizzo IP della rete, anche una maschera.

CIDR è in qualche modo un netmasking "generalizzato", di lunghezza variabile. Dato che con CIDR si "aggregano" molte reti di classe C o B in reti più "grandi", viene anche detto "supernetwork".

Per dividere la parte di rete e di host di un indirizzo CIDR non si fa più uso del concetto di classe ma di quello di "prefisso". Un "prefisso" è l'analogo CIDR dell'indirizzo di rete "con classi" (classful). Un prefisso è un numero costituito da alcuni dei primi bit di un indirizzo IP; può essere grande da uno a 32 bit e viene individuato con una maschera, del tutto analoga ad una subnet mask.
La distinzione fra indirizzo di rete e indirizzo di host, che con il concetto di classe era "limitata" ai confini dei byte, ora può essere effettuata in ogni bit dell'indirizzo. In questo modo la divisione degli indirizzi diviene molto più flessibile ed è facile realizzare una struttura gerarchica degli indirizzi che tenga conto anche della topologia della rete. Ciò si ottiene in modo molto semplice, associando ad ogni indirizzo anche la sua netmask ed estendendo le tabelle di routing con la relativa maschera.

Quando un router "propaganda" ("advertise") ad altri router la sua connessione con una rete non indica solo l'indirizzo IP, ma una coppia di numeri: un indirizzo IP ed una netmask, che indica quale è la parte di rete e la parte di host.
Al posto della netmask può comunicare solamente il numero di bit che costituiscono il prefisso (ricordo che in una netmask ci sono tutti uno nella parte più significativa seguiti da tutti zero da un certo punto in poi).
Questi due modi di vedere gli indirizzi CIDR corrispondono a due notazioni (modi di scrivere) gli indirizzi.
Si può scrivere la coppia indirizzo netmask, in questo modo:

IP-address ::= { <Network-prefix>, <Host-number> }

Per scrivere gli indirizzi CIDR che i router devono trasmettersi si usa la seguente notazione:

<Indirizzo> / <Numero di bit di prefisso>

<Indirizzo> è un normale indirizzo IP, eventualmente abbreviato con l'uso degli zeri nella parte "di host".
<Numero di bit di prefisso> è il numero dei bit che servono per il routing, cioè quello che, nella denominazione "delle classi", verrebbe detto indirizzo di rete. Dato che essi stanno all'inizio dell'indirizzo (sono, appunto, un prefisso) corrispondono ad una maschera con tutti 1 a sinistra fino al bit indicato, poi tutti 0.

Vediamo un esempio, in cui si indica l'indirizzo ed una maschera che individua la parte "di rete" cioè il prefisso:

198.128.0.0 / 255.128.0.0

oppure, ed è la notazione più frequente, si può scrivere l'indirizzo, seguito da una barra ed il numero di bit del prefisso:

198.128.0.0 /9
che dice che il prefisso è lungo 9 bit. A dispetto del fatto che sembrerebbe una rete di tipo C, con 254 host al massimo, questa rete ha fino a 1 Mega stazioni (un po' più di un milione).

Da quanto detto precedentemente consegue che la classe non ha più senso ed i primi tre bit di un indirizzo IP non ci fanno più distinguere fra parte di rete e di host. Essi sono significativi solo per le reti di classe D ed E, che non cambiano con l'introduzione di CIDR.

Il passaggio fra un continente e l'altro è un confine naturale che corrisponde anche ad un confine nella topologia della Rete e nel modo di gestirla. Per usare la divisione dei continenti come modo di semplificare il routing in ogni area geografica esiste un organismo di assegnazione degli indirizzi IP, detto registry primario che dispone di un vasto numero di indirizzi da distribuire.
L'organismo che sovrintende a tutte le operazioni relative agli indirizzi è la IANA (Internet Assigned Numbers Association, http://www.iana.org/), il suo "braccio commerciale" la ICANN (Internet Corporation for Assigned Names and Numbers, http://www.icann.org/). Gli organismi che gestiscono gli indirizzi nei continenti attualmente, emanazione diretta della IANA, sono tre:
ARIN (**A**merican **R**egistry for **I**nternet **N**umbers) (http://www.arin.net/), per le Americhe, **RIPE NCC** (**R**éseaux **IP E**uropéens, **N**etwork **C**oordination **C**entre) (http://www.ripe.net) per l'Europa, il Medio Oriente e l'Africa, **APNIC** (**A**sia-**P**acific **N**etwork **I**nformation **C**enter) (http://www.apnic.net/) per l'area dell'Asia e dell'Oceania.
I registry continentali distribuiscono i loro indirizzi, con le opportune maschere, a provider nazionali di dimensioni molto grandi, come quelli che gestiscono la dorsale di Internet in Italia. Date le loro dimensioni essi possono acquistare molte migliaia di indirizzi IP aggregati. In Italia questi provider sono una decina. A loro volta essi rivendono gli indirizzi ad altri provider più piccoli ed eventualmente agli utenti finali.
I provider più grossi usano nelle loro tabelle indirizzi con prefissi più corti, mentre il loro clienti useranno gli stessi indirizzi con prefissi più lunghi, ottenendo reti con un minor numero di host.

Con CIDR cambia in qualche modo il modo di ottenere gli indirizzi IP. Mentre prima "chiunque" poteva avere il suo numero IP rivolgendosi direttamente alla IANA, ora ci si deve rivolgere necessariamente ai provider, che affittano i loro numeri e mantengono lo schema gerarchico che garantisce la semplificazione del routing tramite CIDR.

Esempio:
193.0.0.0 /8 è una rete europea CIDR; tutti i percorsi pubblicizzati dai router come 193.0.0.0 /8 vengono instradati verso l'Europa.

195.103.0.0/16 è una route italiana di 64 k host (interbusinnes)

Quando è stato sviluppato CIDR (1993) gli indirizzi IP sono stati divisi in blocchi il più possibile contigui, assegnati ai vari gestori continentali in modo che indirizzi vicini fossero assegnati a nazioni vicine. Essi li ridistribuiscono a loro volta ai loro clienti, assicurando così che gli indirizzi IP contengano anche un'informazione sul posto dove si trova l'host che lo usa e che le tabelle di routing dei router "intercontinentali" contengano prefissi "piccoli", dando luogo ad un instradamento più efficiente ed tabelle piccole.
Le organizzazioni che già avevano indirizzi IP assegnati sono state incoraggiate a "restituirli" cambiandoli con indirizzi validi per il CIDR. In questo modo, nel corso del tempo, anche gli indirizzi attuali "con classi" vengono a mano a mano resi "senza classi" e "riciclati" al CIDR.
Ma ora sorge un problema. Come fanno i router a gestire indirizzi con e senza classi nella stessa internetwork, come è il caso di Internet? Il prefisso 192.0.0.0 /8 è l'indirizzo CIDR di una rete di provider europei. Supponiamo che un'organizzazione situata in USA possieda da molti anni l'indirizzo della rete di classe C 192.28.12.0. Come fa un datagramma spedito a 192.28.12.28 ad arrivare in USA e non in Europa?
Il meccanismo è molto più semplice di quanto si possa pensare a prima vista.
Ogni router sceglie la destinazione scandendo la sua tabella di routing andando dagli indirizzi particolari a quelli generali.

Quindi se la tabella contiene:

192.28.12.0	mask 255.255.255.0 (*)	198.16.13.8 (Link verso USA)
192.0.0.0	mask 255.0.0.0	192.28.17.31 (Link verso Europa)

Consideriamo per esempio l'indirizzo 192.28.12.28, che appartiene alla rete USA. Entrambe le linee della tabella individuerebbero un percorso di routing per il datagramma, ma il router dà la priorità alla rete più particolare che trova, quella che ha il prefisso più lungo, cioè al link con USA. Per cui 192.28.12.28 viene instradato verso gli USA. Considerando invece l'indirizzo 192.28.21.7, che non fa parte della rete 192.28.12.0, l'unica riga della tabella che dà luogo ad un instradamento è quella che conduce in Europa.
Naturalmente se la rete 192.28.12.0 fosse stata in Europa la prima riga della tabella sarebbe stata del tutto inutile e si sarebbe potuta omettere. Questo ci spiega quanto sia importante usare indirizzi CIDR per ridurre la dimensione delle tabelle dei router "chiave" dell'Internet, ma anche come ciò non sia "obbligatorio", dato che la rete funziona ancora anche con gli indirizzi con classe ("classfull").

Aggiornamento delle tabelle di routing
RIP2 (RFC1723, RIP è in RFC1058 ora "Historical"), OSPF (v.2 RFC1583), BGP (v.4 RFC1771), EGP (RFC904 STD 18, ora "Historical")

NAT o IP Masquerading
Network Address Translation, IP masquerading

IP Multicast
IP può sfruttare anche un tipo di spedizione in multicast: un singolo pacchetto può essere spedito a tutti i destinatari che appartengono ad un "gruppo di multicast". Un host può appartenere a più gruppi di multicast. Il multicasting sfrutta gli indirizzi di classe D, cioè quelli da 224.0.0.0 a 239.255.255.255 (il protocollo è descritto nella RFC1112). La IANA assegna specifici indirizzi multicast a protocolli od applicazioni che ne fanno uso (RFC1700 STD0002).
Mentre il multicast ha senso su una LAN, è difficile da realizzare o del tutto improponibile su reti geografiche, anche se sforzi recenti vanno nella direzione del miglioramento delle prestazioni del multicasting anche sulla Internet. Ciò in particolare per minimizzare lo "spreco" di banda nelle trasmissioni "live" di video e audio, oggi molto di moda.
Per registrare e mantenere i gruppi di multicast il software deve usare il protocollo IGMP (Internet Group Managment Protocol, RFC1112 STD 5). Analogamente a quanto succede per il routing, IP è in grado di trasportare datagrammi in multicast, ma non di gestire il multicasting.

Il datagramma IP

Il datagramma IP è di lunghezza variabile, la sua lunghezza minima è di 20 , la massima è di 64 kByte ; il datagramma viene anche detto PDU (**P**rotocol **D**ata **U**nit).

Datagramma IP

Versione (4)	L. header (4)	Tipo di Servizio (8)	Lunghezza totale (16)	
Identificatore (16)			Flag (3)	Offset del frammento(13)
Tempo di durata (8)		Protocollo (8)	Checksum dell'header (16)	
Indirizzo IP origine (32)				
Indirizzo IP destinazione (32)				
Opzioni (Variabile)				Riempimento (per allineare a 32 bit)
DATI (Variabile, multiplo di 32 bit)				

Figura: Il datagramma IP, mostrato con allineamento a 32 bit

Descrizione dei campi:
Versione
(campo di 4 bit) il formato del datagramma può cambiare con l'evolvere delle versioni di IP, la prima cosa da sapere è perciò il numero di versione del programma che lo ha generato.
Lunghezza dell'intestazione (IHL: Internet Header Lenght)
(campo di 4 bit) è misurata in parole di 32 bit (4 byte). La lunghezza massima dell'header è perciò di 64 byte (2^4 * 4). L'header non può essere di lunghezza qualsiasi; essa deve essere un multiplo di 4. Ciò significa che potrebbe dover essere necessario aggiungere qualche byte all'header. Se non ci sono opzioni la lunghezza dell'header è di 20 byte, perciò c'è 5 nel campo lunghezza.
Tipo di servizio (TOS: Type Of Service)
(campo di 8 bit) se la rete sottostante è in grado di supportarne le funzionalità, in questo campo si può specificare la qualità del servizio (QOS) desiderata, in particolare si possono richiedere: il ritardo di transito nei router, la priorità, l'affidabilità della trasmissione. Alcune RFC specificano l'utilizzazione di questo campo nel trasporto di dati realtime.
Lunghezza totale del datagramma in Byte
(campo di 16 bit) comprende l'header ed i dati. Dato il numero di bit di questo campo il datagramma può essere lungo al massimo 64 kByte . Questa grandezza comprende l'header ed i dati.
Identificatore
(campo di 16 bit) serve per distinguere fra i vari pezzi di un messaggio di livello superiore che si sono dovuti frammentare in diversi datagrammi IP. In pratica è il numero del datagramma nella sequenza che deve ricostituire il messaggio originale.
Flag
(3 flag) il primo di questi flag (MF: More Fragments) determina se questo è l'ultimo frammento di un datagramma frammentato, l'altro (DF: Don't Fragment) indica se il datagramma può essere frammentato (p.es. nel passare attraverso una LAN potrebbe essere diviso in diversi frame, questo flag può impedire questa suddivisione). Il terzo flag non è usato ed è lasciato a 0.

Offset
(campo di13 bit) è lo spostamento, misurato in unità di 8 byte, dei dati contenuti nel pacchetto IP corrente, rispetto all'inizio del messaggio originale, passato dal protocollo superiore. In pratica per ottenere l'offset del byte in cui scrivere nel buffer di memoria dell'host ricevente, si aggiungono 3 bit nulli a destra di questo numero di 13 bit.
*Durata massima (TTL: "**T**ime **T**o **L**ive")*
(campo di 8 bit) un numero che rappresenta il "tempo" che è intercorso fra la partenza del datagramma ed il suo arrivo nel router che lo sta elaborando. Viene inizializzato con un valore diverso da zero. Ad ogni passaggio in un router esso toglie uno al valore di questo campo. Quando questo valore giunge a zero, il pacchetto viene giudicato "perduto", perché è scaduto il tempo che gli era stato assegnato per arrivare a destinazione, e non viene più propagato dal router. Se un router trova che il campo TTL è nullo lascia cadere il datagramma e dà comunicazione al mittente del fatto, spedendogli un messaggio ICMP. Dunque il campo TTL, alla partenza del datagramma, è il numero massimo di salti ("hop") che il datagramma può fare per giungere a destinazione.
Protocollo
(campo di 8 bit) è un codice che specifica il protocollo di trasporto che utilizza questo datagramma, cioè il protocollo di livello superiore che ne ha richiesto la trasmissione;
Alcuni codici di protocolli sono:

Decimal	Keyword	Protocol
0		Reserved
1	ICMP	Internet Control Message
2	IGMP	Internet Group Management
3	GGP	Gateway-to-Gateway Protocol
4	IP	IP in IP (encapsulation)
5	ST	Stream
6	TCP	Transmission Control Protocol
..		
17	UDP	User Datagram Protocol
..		

La tabella intera, "Assigned Internet Protocol Numbers", in RFC1700 (1995), ha circa 100 numeri assegnati.
Header checksum
(campo di 16 bit) è una somma di controllo dell'header. Usa un algoritmo semplice e molto veloce da eseguire, di una certa sensibilità, anche se non come un CRC. Serve ad evidenziare errori di trasmissione nel solo header del pacchetto, non nella parte di dati, che viene quindi consegnata senza controllo di congruenza.
Indirizzo IP origine
(campo di 32 bit) cosa dire?
Indirizzo IP destinazione
(campo di 32 bit) idem
Opzioni
il campo opzioni è di dimensione variabile, può non esserci come prendere parecchi byte (fino a 40). Ogni opzione è preceduta dalla sua lunghezza, così che essa può essere diversa in ogni datagramma. Le opzioni servono per la gestione del protocollo e per la diagnostica dei collegamenti.
Riempimento ("padding")
l'algoritmo per calcolare il checksum prevede che il numero di bit coinvolti sia un multiplo di 32. Data la lunghezza variabile dei campi precedenti e visto che l'header deve avere lunghezza multipla di 32 bit, è necessario riempire il datagramma, con questo campo, fino al primo multiplo di 4 byte.
I campi fino al precedente fanno tutti parte dell'header del pacchetto IP.
Dati ("payload")
campo di lunghezza variabile che contiene i dati, trasportati per conto del protocollo di livello superiore. Quindi questo campo potrebbe essere p.es. un "frame" TCP (che viene detto "segmento" TCP).

Si noti che, non essendo verificato il contenuto dei dati, non esiste un trailer con un checksum per la verifica dei dati.
Se due host che devono comunicare attraverso una rete IP sono entrambi sulla stessa rete Ethernet, il datagramma IP viene "incapsulato" in un frame Ethernet, al posto che compete al campo dati.
Qualora un router verificasse, tramite il campo "header checksum", che l'intestazione del datagramma IP è corrotta, l'unica azione che può fare è non propagarlo ulteriormente ad altri gateway o all'host locale di destinazione. L'azione viene detta "packet drop": il router "lascia cadere" il pacchetto. Infatti l'indirizzo di destinazione potrebbe essere corrotto e si correrebbe il rischio di spedire il datagramma ad una stazione che non c'entra nulla con quella cui si dovrebbe spedire veramente. Se il pacchetto si ferma non giungerà mai a destinazione e sarà definitivamente perduto nel caso di UDP, oppure sarà rispedito a cura del protocollo di livello superiore, come accade, per esempio, in TCP.
Il router che deve effettuare un "packet drop" può comunicare l'evento al destinatario, in modo che esso possa adattare la sua velocità o, se riceve molte di questi avvisi in poco tempo, decidere che la destinazione non è raggiungibile.

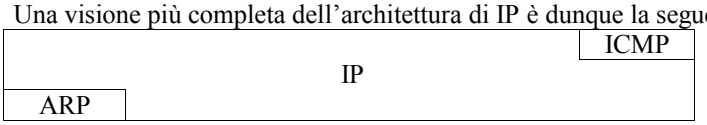
Frammentazione
Dato che un datagramma IP è lungo fino a 64 kByte, se lo si vuole far passare su una rete Ethernet, che ha un frame lungo al massimo 1514 byte, può essere necessario suddividerlo in unità più piccole. Quest'operazione si chiama "**frammentazione**" (fragmentation) e viene eseguita automaticamente dal software IP, quando esso ne rileva la necessità. Passando in molte reti eterogenee, il datagramma potrebbe essere frammentato più volte, l'offset contenuto nel relativo campo del datagramma fa comunque riferimento alla posizione nel datagramma originale passato dal protocollo di livello superiore dell'host trasmittente, prima che venisse effettuata la prima frammentazione. Ciò permette una semplice ricostruzione del datagramma alla ricezione. Per far ciò ogni frammento viene copiato in un buffer in memoria, alla locazione che ha per indirizzo la somma dell'indirizzo di inizio del buffer e dell'offset, che viene letto dal datagramma. Quando la trasmissione del datagramma è completa, IP cede il controllo del buffer al protocollo di livello superiore che l'aveva richiesto.

Disegno

ICMP (Internet Control Message Protocol)
Se si determina un errore durante la trasmissione di un pacchetto, se esso scade per limiti di "tempo" o di numero di router attraversati (TTL) o se se la destinazione indicata non è raggiungibile, il router che rileva l'errore spedisce indietro al mittente un datagramma IP, contenente dati di formato ICMP, che "spiegano", tramite codici, l'errore accaduto. ICMP serve solo a segnalare errori e non a correggerli. Esso svolge anche alcuni servizi generali ed un "primitivo" controllo del flusso full duplex delle due parti trasmettente e ricevente. Anche programmi diagnostici come Ping o Traceroute (vedi oltre) fanno uso di ICMP per il loro funzionamento.
I più comuni messaggi ICMP sono: "Destination unreachable": il router non ha strade che possano raggiungere l'indirizzo richiesto; "Echo" e "Echo Reply": si usano per il programma "ping"; "TTL exceeded": indica che il datagramma troppo "vecchio" è stato scartato dal router"; "Parameter Problem": problemi con l'header del datagramma; "Source Quench": spedito dal router al trasmittente per indicare che la rete è congestionata, utile per il controllo del flusso;
Dato che con le risposte ICMP dei router sono possibili attacchi a host in Internet che ne saturano il, oggi moltissimi router in Internet non emettono più messaggi ICMP.
Dato che con ICMP è possibile bloccare un server remoto, impedendogli di svolgere le sue funzioni[7], oggi la gran parte degli host su Internet non genera pacchetti ICMP in risposta ad errori o richieste. Per questo moltissimi host nella Internet non rispondono al "ping" (vedi oltre).

ARP: Risoluzione degli indirizzi fisici
ARP è un protocollo, indipendente da IP, che serve ad un host per sapere l'indirizzo MAC della stazione con cui deve comunicare tramite IP. Ogni host diretto, che deve comunicare su rete locale con un altro host sulla stessa rete, ha bisogno di sapere l'indirizzo MAC della stazione a cui deve spedire i datagrammi, per inserirlo nel frame fisico. A tal scopo tiene una tabella ("ARP cache") di corrispondenza fra gli indirizzi IP e quelli MAC (es. 143.111.100.3 -> 00:02:0A:20:5C:83). Quando un indirizzo MAC non è presente nella tabella l'host deve procurarselo facendo uso del protocollo **ARP** (**A**ddress **R**esolution **P**rotocol, RFC826 STD 37) . ARP prevede l'emissione di un frame Ethernet con campo il codice di ARP nel campo di tipo, in broadcast, a tutte le stazioni della rete locale (si ricorda che nella rete locale il broadcast non penalizza le prestazioni, come avverrebbe in un'internet). Il frame ARP contiene l'indirizzo IP del quale l'host in questione sta cercando l'indirizzo MAC. Tutte le stazioni sulla rete locale leggono il frame ARP; la sola stazione che riconosce in esso il suo indirizzo IP risponde, spedendo al richiedente un frame ARP di risposta, che contiene il suo indirizzo fisico. Da quel momento il poi l'host riempie la sua tabella ARP, che viene tenuta in RAM, e può conoscere subito l'indirizzo fisico da utilizzare per comunicare con quella stazione. Siccome l'indirizzo fisico di un computer può cambiare, per esempio se gli si cambia la scheda di rete, la cache ARP non deve contenere per sempre i suoi dati; per questo i valori della cache ARP vengono periodicamente cancellati e per avere accesso fisico le stazioni devono ricominciare un processo di risoluzione di indirizzi con ARP. Il frame ARP contiene, oltre all'indirizzo fisico della stazione, altre informazioni che specificano come è fatta la rete su cui è presente la stazione.
Alcuni tipi di rete non hanno bisogno di ARP, come esempio si può considerare ATM che, essendo connection oriented, non usa indirizzi fisici durante la sessione, ma solo durante la negoziazione iniziale del percorso. Lo stesso accade per collegamenti fisici punto - punto, *come* nel tratto da utente a provider nei collegamento a Internet, ove si usa PPP (Point to Point Protocol, vedi oltre).

Una visione più completa dell'architettura di IP è dunque la seguente:



Lo schema è disegnato così perché IP impiega ARP per risolvere i suoi problemi di indirizzo di basso livello. Solo per alcune funzioni è ARP che si interfaccia per conto di IP con i livelli più bassi della rete. Per questo ARP è stato disegnato a livello più basso di IP, ma non per tutta l'estensione dello strato IP.

7 Gli attacchi remoti volti a "bloccare" il computer bersagliato si chiamano RDoS (Remote Denial of Service)

Anche ICMP rimane nello stesso strato, pur essendo accessibile anche dai livelli superiori (infatti molti protocolli dei due strati superiori ne fanno uso), ma "un po' più in alto" di IP, dato che ICMP fa uso dei datagrammi che IP gli mette a disposizione.

RARP (Reverse ARP, RFC903 STD 38)

In alcuni casi un computer che non conosce il suo indirizzo IP, può determinarlo attraverso il protocollo RARP. Ciò può accadere nel caso di un computer senza disco, che deve caricare il suo Sistema Operativo dalla rete. Questo computer conosce il suo indirizzo MAC, dato che la scheda di rete glielo può comunicare, ma non l'indirizzo IP, perché esso è configurato nel suo Sistema Operativo, che non è ancora stato caricato. Usando RARP può ottenere da un altro host della rete il suo indirizzo IP e cominciare a scaricare dalla rete il Sistema Operativo, usando TCP/IP.

Esistono delle versioni di ARP e di reverse ARP anche per le reti DLL diverse da Ethernet, se p.es., IP risiede su frame relay, si usa InARP (InverseARP), che "mappa" il numero di circuito virtuale frame relay con l'indirizzo IP. Se la rete che si utilizza è ATM, ci sono ATMARP e ATMInARP, che stabiliscono la relazione fra l'indirizzo IP e il numero di canale o percorso virtuale ATM.

DHCP (port 68 UDP, RFC2131)

Dynamic **H**ost **C**onfiguration **P**rotocol permette di assegnare a richiesta tutti parametri di indirizzamento e routing locale utili ad un host IP.

Tramite DHCP si possono assegnare ad un host che ne fa richiesta:

- un indirizzo IP, preso fra un "pool" di indirizzi che il DHCP è configurato per distribuire
- una maschera di sottorete
- l'indirizzo del router di default (default gateway) per la rete dell'host
- il nome dell'host ed il suo dominio DNS (vedi oltre per DNS)
- indirizzi dei server DNS primario e secondario
- indirizzi di servizi di tempo (NTP), nomi (NIS), stampa (print server) ed altri

E' possibile che alcuni indirizzi IP possano essere riservati dal server DHCP ad alcune specifiche stazioni, riconosciute tramite il loro indirizzo MAC. In questo caso, quando una stazione con un certo indirizzo MAC farà richiesta DHCP, le verrà dato sempre lo stesso indirizzo IP.
DHCP usa UDP/IP in multicasting,
In una rete locale ci può essere un solo server DHCP. DHCP usa lo stesso port del precedente protocollo BOOTP, del quale è un'estensione. Bisogna dunque fare attenzione a che non ci siano un server DHCP ed uno BOOTP contemporaneamente abilitati nella stessa rete.
Il protocollo DHCP spedisce al client i parametri che esso richiede, per cui deve essere il client ad inoltrare per primo una richiesta, nella quale deve specificare cosa vuole. Se il client è stato appena riacceso ed aveva precedentemente un certo indirizzo dinamico, proverà a chiedere proprio quello. Sarà naturalmente compito del server accordare o rifiutare la richiesta.

"Lease" DHCP

Un server DHCP "affitta"[8] ad un suo client uno degli indirizzi che appartengono ad un suo "pool" di indirizzi.
Gli "affitti" (lease) valgono per un certo tempo. I tempi che vengono stabiliti sono i seguenti:

- renew time (tempo di rinnovo): il momento in cui il client comincia a ricontattare il server per ottenere il rinnovo dell'autorizzazione all'uso dell'indirizzo
- rebind time: stabilisce il momento in cui il client deve cominciare a cercare un qualsiasi server DHCP, perchè il lease sta per scadere e bisogna cercare un indirizzo in broadcast, anche da un server diverso da quello che ce l'ha dato precedentemente
- expire time: è il momento in cui l'indirizzo non vale più; da questo momento il client deve cessare l'utilizzazione dell'indirizzo.

Opzioni del client

Il client DHCP fa richieste al server di diverso genere:

- request (richieste): le richieste al server di particolari informazioni sulla rete
  - il server può fare la richiesta di uno specifico indirizzo o di un certo tempo di lease, che il server potrà accordare o negare.
- require (requisiti): le informazioni "obbligatorie" che il client deve acquisire. Se un server non darà tutte queste informazioni, nell'ordine specificato, il client non acquisirà l'indirizzo
- lease: richieste di indirizzi
  - lease fissi (fixed-address): si può configurare un lease con un indirizzo specifico
    - quando il client non trova un server prova tutti i server DHCP da cui ha avuto in passato un indirizzo che risulti ancora valido. Se non ne trova nessuno si può configurare per assumere un indirizzo fisso, in un lease che non finisce mai.

8 to lease = affittare

DNS: nomi per indirizzi

Un numero di 32 bit è ciò che serve e basta ad un host per conoscere e raggiungere un qualsiasi altro host in una internet. Per un essere umano l'indirizzo IP è però sconveniente, difficile da memorizzazione e da "leggere". Con Ipv6, che ha indirizzi a 128 bit, la cosa diventa impossibile.
Al posto dell'indirizzo IP i comuni mortali usano di solito un "nome", cioè una particolare stringa, che in qualche modo ricorda l'host e che deve essere associata automaticamente ad un indirizzo IP.
DNS (**D**omain **N**ame **S**ystem) è un protocollo di livello applicazione, che serve per associare indirizzi IP a stringhe identificative. Queste stringhe, che vanno sotto il nome di "nomi di dominio" (domain names), devono essere uniche per tutta la rete, nel senso che solo una "entità" della rete deve avere quel nome. Il nome di un'entità in rete può servire per identificare un host, un gateway, una persona, un programma, un file ma non ne specifica direttamente la posizione, al contrario dell'indirizzo. Per assicurare l'univocità dei nomi deve esistere un sistema di registrazione dei nomi di dominio. Esso fa riferimento in ultima analisi all'Internet Society, attraverso i diversi livelli di management della rete forniti dai vari provider d'informazione.
Per trovare quale indirizzo IP corrisponde ad un nome di dominio, ogni host può usare il DNS: "sistema dei nomi di dominio" (**D**omain **N**ame **S**ystem RFC1034,1035 STD 13). Il DNS è un database distribuito dei nomi che vengono associati a indirizzi IP. Il database DNS è costituito da "Resource Records" che, oltre ai nomi ed agli indirizzi IP contiene anche altre informazioni: nome, indirizzo ed e-mail dell'organizzazione che ha quel nome, nomi ed e-mail dei responsabili: tecnico, amministrativo e commerciale del dominio.
L'operazione di ricerca del nome nel DNS viene detta "DNS lookup".
Quando un qualsiasi host non sa l'indirizzo IP di un altro host cui deve spedire un datagramma, ma ne conosce il nome di dominio, fa una richiesta ad un particolare server (DNS Server), del quale conosce l'indirizzo. Il server DNS cerca in una sua tabella la corrispondenza fra il nome e l'indirizzo. Se la trova comunica l'indirizzo IP al richiedente, se non la trova propaga la richiesta ad uno o più altri server DNS di cui è a conoscenza, aiutandosi con il nome di dominio per decidere "a chi chiedere". Se il secondo server trova l'indirizzo lo comunica al primo, il quale a sua volta lo trasmette al richiedente e lo memorizza in una sua tabella che funge da "cache", per uso futuro. Il dato verrà tolto dalla cache solo quando nessuno lo richiederà per un certo periodo. Se l'indirizzo non viene trovato, la richiesta può essere ulteriormente propagata, ma non per molte volte.
Se, dopo un certo tempo dalla richiesta DNS, l'host non ha nessuna risposta, assume che il nome non sia valido, cioè che non abbia corrispondenza con un indirizzo IP. Se successivamente al tempo limite un server DNS "lontano" trova l'indirizzo, lo comunica al primo server. Dato che l'indirizzo viene mantenuto nella cache del primo server, ad un successivo tentativo di accesso allo stesso nome da parte dell'host sarà data, questa volta, una risposta positiva ed "immediata". Se un nome di dominio cambia indirizzo, il relativo responsabile ne pubblica il nuovo indirizzo in almeno un server DNS, cioè su quello che ha l'autorità per quel dominio, poi effettua una procedura di "pubblicizzazione" del nuovo indirizzo fra alcuni server importanti ("advertising"). Questo permette di modificare le tabelle di alcuni server della Rete.
Gli altri server DNS, che hanno ancora il vecchio indirizzo nelle loro tabelle locali dei DNS risponderanno alle richieste con il vecchio IP number. Di conseguenza gli host che fanno la richiesta non riusciranno a prendere contatto. Il server non aggiornato allora "chiederà in giro" ad altri server ed il giusto indirizzo si propagherà a mano a mano in tutto il DNS.
Da quanto detto consegue che l'unico indirizzo IP che è indispensabile conoscere in forma numerica è quello di un server DNS[9]; gli altri indirizzi IP che possono servirci possono essere cercati nel DNS. Ogni host IP ha al suo interno una piccola cache DNS: gli ultimi nomi usati hanno corrispondenza con l'indirizzo, per essi l'host non ha la necessità di fare alcuna richiesta al DNS.

Le comunicazioni con i server DNS utilizzano i servizi connection oriented di TCP, al numero di port 53 (vedi oltre).
Il protocollo DNS deve essere considerato un protocollo di livello applicazione.
La gestione del DNS è strettamente gerarchica, controllata dalla Internet Society per mezzo dell'InterNIC (**Inter**net **N**etwork **I**nformation **C**enter). L'InterNIC ha emanazioni nazionali in ogni paese. I NIC nazionali di solito delegano aziende commerciali alla gestione dei nomi. Chi vuole acquisire un nome di dominio deve rivolgersi a quelle aziende, spedire i dati per la registrazione, seguire una certa procedura burocratica e pagare il dovuto.
E' possibile registrare un nome entro un dominio di una certa nazione anche se il computer che ha il relativo IP non è fisicamente situato in quella nazione. Per esempio è possibile per un'azienda che mantenga i suoi server in USA registrare un dominio .it, mentre molte ditte italiane, con server in Italia, hanno dominio primario "USA" di tipo .com. Comunque il registry può richiedere delle condizioni, per esempio in Italia la registrazione di un nome di dominio .it è stata per lungo tempo riservata alle ditte che abbiano attività in Italia e vietata alle persone. E' stato anche necessario identificare personalmente il responsabile del nome di dominio (spedizione della fotocopia di un documento valido), ed una lettera di assunzione di responsabilità.

Nel DNS non sono contenuti solo indirizzi IP, ma anche altre informazioni quali il nome e l'indirizzo di posta elettronica del responsabili tecnico e legale del nome, nomi di "alias", ovverosia nomi equivalenti, che indicano lo stesso indirizzo IP.
I campi del database DNS sono:

9 In verità è possibile che esso venga richiesto per il trami te si un server DHCP, per cui, in questo caso non è effettivamente necessario conoscerlo. Ciò può accadere in reti locali dotate di server DHCP in casi di accesso ad Internet con un modem. In quest'ultimo caso il collegamento è quasi sempre da punto a punto, con il server del provider, che ha sempre la possibilità di comunicare l'indirizzo dei server DNS tramite DHCP.

Record A: associa i nome di dominio a uno o più indirizzi IP
Record PTR (pointer): associa l'indirizzo IP al nome di dominio (per il reverse lookup)
Record NS: elenca i server DNS relativi a questo nome di dominio. In questo server si troveranno i nomi DNS di livello inferiore a quello di questo nome di domino.
Record MX: indica il server di posta elettronica di questo nome di dominio.

Reverse lookup
Qualche volta può essere utile conoscere il nome associato ad un indirizzo IP. Se l'assegnatario del nome di dominio vuole che dal numero IP si possa trovare il nome di dominio corrispondente, fa un modo che venga compilata una particolare tabella di "reverse lookup". Se questo collegamento inverso esiste gli host possono chiedere al DNS il nome che corrisponde ad un indirizzo IP. Nel caso in cui ad un singolo indirizzo IP siano assegnati molti nomi il reverse lookup fornisce il principale.

Convenzioni per i nomi di dominio.
Vediamo un nome di dominio "inventato": parvulus.studio.ingmonti.it. Questo nome contiene informazioni scritte in ordine, che indicano la gerarchia di responsabilità nell'assegnazione dei nomi stessi.
Un dominio si può dividere in sottodominii, ciascuno dei punti nel nome indica un sottodominio.
Ogni nome di dominio deve essere unico; ci deve essere un meccanismo tramite il quale viene assicurata l'univocità dei nomi.
Nell'esempio ".it" è un dominio primario (top level domain), "ingmonti.it" è un nome di dominio primario. I domini primari sono pochi, e sono stabiliti dall'Internet Society, che li affida ad apposite organizzazioni, sparse nel mondo intero. I nomi del dominio ".it" sono gestiti in Italia dal NIS - GARR, un organismo costituito da centri di ricerca e università italiani. Il GARR lo dà in appalto ad un'Azienda (itNIC) che assegnerà, dietro richiesta, i nomi del dominio ".it", assicurandosi che siano unici.
Leggendo un nome da destra a sinistra si individuano i sottodominii. "ingmonti.it" è il nome di dominio che il GARR ha assegnato all'organizzazione o alla persona che ne ha fatto richiesta. Quest'ultima organizzazione quale gestisce i nomi che stanno a sinistra di "ingmonti.it". Il nome di dominio secondario "studio.ingmonti.it" è dunque assegnato dal proprietario di "ingmonti.it", mentre "parvulus.studio.ingmonti.it", assegnato da chi amministra "studio.ingmonti.it", è il nome del computer che contiene la scheda di rete che ha l'indirizzo IP contenuto nel DNS.
I nomi di dominio non servono solo a individuare indirizzi, ma anche servizi. P.es. se "parvulus" fa da server di posta elettronica ugo@parvulus.studio.ingmonti.it è l'indirizzo di posta elettronica dell'utente ugo, gestito dal programma server SMTP che risiede sul computer "parvulus".
Alcune macchine possono avere un nome di dominio anche senza essere collegate ad Internet in senso proprio, si pensi per esempio ai gateway di posta elettronica collegati a servizi telematici non Internet, come p.es. Compuserve.
Oltre a "it" ed agli altri ai dominii di nazione, da al (Albania) a zw (Zimbabwe), con l'indicatore a due lettere dato dallo standard ISO 3166, esistono altri domini primari:
.gov usato dalle agenzie del governo degli USA
.edu usato dalle università degli USA
.com usato dalle Aziende "commerciali" in USA e nel mondo
.mil (sempre meno) usato dai militari USA
.org usato da organizzazioni "no profit" varie
.net usato da organizzazioni varie che costituiscono o gestiscono delle "reti" all'interno della Rete.

In conseguenza delle ultime revisioni degli standard relativi ai nomi di dominio, sono stati recentemente introdotti altri nomi di dominio primari, fra i quali:
.eu per le organizzazioni e le persone che fanno riferimento all'Unione Europea
.firm per le ditte
.store per i magazzini "virtuali"
.web per i dominii che privilegiano siti WWW
.arts per i dominii culturali
.rec per i dominii di intrattenimento (recreation)
.info per i dominii che offrono servizi d'informazione

La tendenza attuale è di usare nomi di dominio "corti", per questioni "estetiche" e commerciali, per cui moltissimi nomi di dominio sono di primo livello e non mostrano la gerarchia della loro assegnazione.
Per conoscere i dati scritti nei record DNS si può usare i protocolli WHOIS (RFC954) o WHOIS++ (RFC1835), che vengono supportati dai server delle organizzazioni di registrazione dei nomi.

DNS dinamico (RFC2136)
Il protocollo, specificato nella RFC2136, permette di raggiungere anche gli host IP che abbiano un indirizzo IP dinamico, "affittato" a tempo da un server DHCP.
Il servizio DNS dinamico è offerto gratuitamente da alcune organizzazioni in rete. Per utilizzarlo ci si deve registrare sul sito del provider del DNS dinamico. Poi, se l'host che deve essere raggiunto è un computer, si deve fare in modo di cari-

care un programma che si attiva all'atto del collegamento ad Internet e spedisce al provider del servizio il nuovo indirizzo IP.
Il nome di dominio che si ottiene è un nome DNS di secondo livello, del tipo: <nome DNS dinamico registrato>.<nome di dominio del provider DNS dinamico>.<sigla di domino primario>.
Il protocollo del DNS dinamico è usato anche da alcuni dispositivi "standalone", quali i router wireless. Dato che tali apparecchiature sono già in grado di usare il DNS dinamico, in questo caso non sarà necessario installare un programma, ma solo registrare il nuovo nome e configurare l'apparecchiatura con il nome del fornitore del servizio di DNS dinamico.

IPSec SSL e VPN

!! TODO !!

TCP

Transmission Control Protocol è un protocollo che può essere classificato a livello di trasporto OSI (Livello 4) ma che fornisce anche diverse funzionalità attribuibili al livello di sessione (Livello 5). Le funzioni che rende disponibili sono:
- consegna assicurata ed affidabile
- controllo del flusso fra i punti finali (fra gli host)
- frammentazione e risequenziamento dei messaggi
- gestione di collegamenti fra programma e programma ("sessioni" fra i programmi)
- multiplexing (più sessioni per ogni host)
- comunicazione full duplex
- sicurezza
- priorità

Un collegamento con protocollo TCP è affidabile. Ciò significa che i dati trasportati da TCP sono verificati a destinazione e sono rispediti se non
prima di spedirsi i dati, i due soggetti della comunicazione devono iniziare una fase di connessione e negoziazione. A negoziazione terminata, cioè a sessione iniziata, si stabilisce fra i due host un collegamento che, dal punto di vista logico, simula un collegamento fisico da punto a punto.
I dati vengono passati a TCP, da parte dei protocolli di livello superiore, un byte alla volta, non a frame. In pratica TCP riceve dagli altri protocolli un flusso di Byte ("Byte stream[10]"), non strutturato e non necessariamente continuo nel tempo ("bursty"), che può avere interruzioni lunghe quanto si vuole e termina solo con la chiusura della sessione.
Questo fatto facilita la stesura del software. Il software che usa TCP funziona, dopo il collegamento, come se avesse a disposizione una "linea" virtuale con l'altro soggetto. E' facile riciclare, sopra TCP, programmi che erano stati scritti per funzionare sopra a reti molto diverse, come per esempio il software per la gestione dei terminali che comunicano con RS-232.
TCP raggruppa autonomamente i byte che gli vengono passati in pacchetti detti "segmenti", decidendone autonomamente anche la lunghezza. Quando ha ricevuto il numero di byte che ha stabilito, oppure quando ci sono byte in attesa da troppo tempo, TCP spedisce un segmento. Ogni segmento è autonomo, ed al suo interno i dati vengono numerati per byte a partire da un numero casuale stabilito in fase di negoziazione del collegamento. I segmenti spediti vengono controllati e "risequenziati" dal software dello stesso livello del computer ricevente, che ha anche modo di ottenere delle ritrasmissioni, se non ha ricevuto tutto il messaggio o l'ha ricevuto con errori. Quando il computer ricevente ha a sua volta dati da spedire include insieme ad essi anche informazioni di ritorno sullo stato della sua ricezione. In questo modo il trasmittente può sapere quali segmenti sono già arrivati a destinazione e se ci sono stati errori. Se il ricevente non ha dati da spedire trasmette comunque, con cadenza regolare, lo stato della sua ricezione, senza altre informazioni. Dunque il funzionamento è full duplex ed ogni segmento TCP può portare sia dati che informazioni di controllo, relativi ad entrambe le direzioni del flusso.
Il software TCP, essendo di alto livello, di solito non è implementato nel router, ma risiede nei computer host.
Si può far notare che, data la natura stratificata dell'architettura delle reti, TCP può funzionare anche sopra uno stack di protocolli che *non* comprenda IP; p.es. esistono implementazioni di TCP basate su X.400.

Port e socket

Per poter iniziare una sessione TCP bisogna conoscere, oltre all'indirizzo IP dell'host di destinazione, anche un altro numero, di 16 bit, detto "port". Esso identifica il programma, che gira sull'host di destinazione, con il quale si vuole comunicare. Una comunicazione TCP si stabilisce fra due programmi che si "trovano" usando il numero di port. La conoscenza della coppia (indirizzo IP, numero di port) permette di creare una terza entità, detta "socket" ("connettore"), che identifica univocamente uno dei due lati di un collegamento TCP. Quando una sessione TCP è attiva, essa è individuata dai due socket sui due host che sono in comunicazione.
Il programma che origina la comunicazione TCP, che viene detto "client" TCP, crea un socket "locale" e cerca di mettersi in comunicazione con un altro socket, sull'host remoto. Per questo deve indicare oltre all'indirizzo IP del destinatario anche il numero di port sul quale si vuole collegare. Dall'altro lato, l'applicazione che deve ricevere richieste di collegamento TCP, che viene detta "server", crea un socket che si "mette in ascolto" sullo stesso port. Quando "sente" una richiesta di collegamento può accettarlo e cominciare in questo modo una sessione TCP. Di solito il programma sul server crea un altro socket e realizza la sessione TCP utilizzando quest'ultimo. In questo modo il primo dei due socket sul server (il "listener") può continuare a rimanere in ascolto, continuando ad accettare anche altre richieste di connessione. Il server è dunque in grado di gestire contemporaneamente molte sessioni TCP, anche con lo stesso host e sullo stesso port (questa caratteristica viene detta "multiplexing" TCP).
Quale sia l'host che contiene i socket con cui il server si collega non importa; si può stabilire una sessione TCP fra due socket sullo stesso computer, come fra host in parti opposte del mondo.
In Internet alcuni port sono assegnati dagli standard alle particolari applicazioni che realizzano i protocolli di livello superiore. I port di questo tipo sono detti "porte conosciute" (well known port numbers) ed hanno avuto per molto tempo un numero inferiore a 256, successivamente sono stati espansi da 0 a 1023. Essi sono pubblicati nello standard Internet

10 Stream significa "corrente" (the Gulf Stream è la corrente del Golfo (del Messico))

STD 0002, p.es. RFC1700 (STD0002). I port sopra al 1000 sono di solito relativi ad applicazioni particolari, non standard, oppure non sono usati.
I "well known port numbers" dei più importanti protocolli Internet (e non Internet (vedi p.es. 666)):

Nome	N. di port	Descrizione
echo	7	Echo: il server risponde rispedendo i caratteri che gli vengono spediti
discard	9	Discard: il server getta via i dati che gli vengono spediti
Daytime	13	Daytime: vengono restituiti il giorni e l'ora attuale
qotd	17	Quote of the Day: il server restituisce il "motto del giorno"
ftp-data	20	File Transfer Protocol [Default Data]: canale per il trasferimento dei dati
ftp	21	File Transfer Protocol [Control]: canale per il controllo del server
telnet	23	Telnet: collegamento da terminale per computer multiutente
Smtp	25	Simple Mail Transfer Protocol: protocollo per la spedizione della posta elettronica
Time	37	Time
nicname	43	Protocollo WhoIs per interrogare il database DNS
domain	53	Domain Name Server: server DNS
bootps	67	Bootstrap Protocol Server (usato dal server DHCP)
bootpc	68	Bootstrap Protocol Client (usato dal client DHCP)
gopher	70	Gopher: vecchio protocollo per accesso ad informazioni "collegate", precedente ad HTTP
finger	79	Finger: comunica quali sono gli utenti attualmente collegati ad un sistema Unix
www-http	80	World Wide Web HTTP, HyperText Transfer Protocol: protocollo per la trasmissione di contenuti multimediali "collegati" in ipertesti
kerberos	88	Kerberos: protocollo per l'autenticazione degli utenti
pop2	109	Post Office Protocol - Version 2: per scaricare i messaggi di posta elettronica
pop3	110	Post Office Protocol - Version 3: per scaricare i messaggi di posta elettronica
sunrpc	111	SUN Remote Procedure Call: per l'esecuzione remota di software nelle architetture distribuite
auth	113	Authentication Service
audionews	114	Audio News Multicast
sqlserv	118	SQL Services: per l'accesso a server di database con linguaggio SQL
nntp	119	Network News Transfer Protocol: per la gestione dei "newsgroup"
ntp	123	Network Time Protocol: per sincronizzare gli orologi degli host
statsrv	133	Statistics Service
netbios-ns	137	NETBIOS Name Service: spedisce i nomi dei computer nelle reti Microsoft
netbios-dgm	138	NETBIOS Datagram Service: incapsula i dati NetBIOS su TCP, spedizione non affidabile
netbios-ssn	139	NETBIOS Session Service: sessione affidabile NetBIOS su TCP (NetBIOS over TCP)
iso-tp0	146	ISO-IP0
iso-ip	147	ISO-IP
snmp	161	Simple Network Management Protocol: per gestire da remoto i dispositivi di rete
snmptrap	162	SNMPTRAP: per gestione SNMP
send	169	SEND
print-srv	170	Network PostScript: stampa con stampanti Postscript
srmp	193	Spider Remote Monitoring Protocol
irc	194	Internet Relay Chat Protocol: per fare chiacchiere in Internet
ipx	213	IPX (Novell Netware): per servizi di basso livello Netware incapsulati su TCP
ldap	389	Lightweight Directory Access Protocol: per gestire "unitariamente" gruppi di server e di utenti
netware-ip	396	Novell Netware over IP: per servizi Netware incapsulati su TCP
ups	401	Uninterruptible Power Supply: perchè i gruppi di continuità (UPS) abbiano modo di avvertire i computer che la corrente è saltata
microsoft-ds	445	Microsoft-DS
whoami	565	Whoami: identifica l'utente
ipcserver	600	Sun IPC server: per servizi di rete nelle stazioni server
doom	666	Doom Id Software: programma sparatutto in prima persona
kerberos-adm	749	kerberos administration

La tabella intera, "WELL KNOWN PORT NUMBERS", in RFC1700 (dell'anno 1995) è lunga circa 15 pagine.

Altri numeri di port, oltre il 1023, usati da particolari applicazioni ma non assegnati ufficialmente da IANA; sono pubblicati in RFC1700.

Affidabilità delle comunicazioni in TCP

Trasmissione a finestra mobile
TCP è stato sviluppato per le reti geografiche; deve perciò poter operare su reti che hanno lunghi tempi di latenza. In generale per assicurare l'affidabilità si potrebbe pensare di attendere conferma del ricevimento corretto di ogni pacchetto

prima di spedire il pacchetto successivo. In questo modo la rispedizione dei pacchetti danneggiati sarebbe rapida e facile, perché potrebbe avvenire subito. Dati i lunghi tempi di latenza delle reti geografiche, questo non è neppure pensabile in TCP. I segmenti vengono perciò spediti utilizzando un meccanismo abbastanza strano, detto "trasmissione a finestra mobile" ("sliding window transmission"). Con questo meccanismo è anche possibile effettuare il controllo del flusso fra i due host.
Il principio ispiratore della trasmissione a finestra di scorrimento è quello di continuare a spedire dati anche se non si sa se i precedenti sono stati ricevuti. Il destinatario spedirà periodicamente, a suo piacimento, informazioni di ritorno, che specificano quali dati sono giunti a destinazione correttamente. In base a queste informazioni il mittente sarà in grado di stabilire cosa fare.
TCP numera individualmente ogni byte trasmesso e ricevuto. Tutto funziona come se i due socket che comunicano avessero a disposizione due "buffer virtuali" di 4 Gbyte nei quali mantengono tutti i byte del flusso di dati da spedire ("data stream"). Mantengono inoltre lo stato di tre "puntatori" di 32 bit, che indicano in ogni istante fino a che punto del "buffer" ("stream") si è giunti nella trasmissione dei dati e nella loro ricezione.
Il primo di questi puntatori indica il byte prima del quale tutti i dati sono stati già **correttamente ricevuti** dal destinatario. Il secondo puntatore indica il byte prima del quale tutti i dati sono stati già **spediti,** il terzo puntatore indica i dati che **possono essere spediti**.
Disegno

Il destinatario include l'indicazione del punto cui è giunta la ricezione del messaggio ogni volta che spedisce un segmento al mittente. Infatti nel segmento TCP è previsto un campo proprio per questo scopo (numero di conferma, vedi oltre). Il mittente potrà così controllare se i dati che ha già spedito sono arrivati senza essere stati corrotti. Se non arriva conferma entro un certo tempo limite il mittente assumerà che i dati non arriveranno più e provvederà autonomamente, senza attendere alcun messaggio esplicito di errore, alla rispedizione di tutti i dati per i quali non ha ancora notizia del ricevimento corretto. Il mittente aggiorna il suo puntatore ai "ricevuti" quando aumenta il numero di conferma che gli giunge. In questo modo viene limitata la spedizione di messaggi di controllo sulla rete geografica. Si evidenzia come, usando questo meccanismo di ritrasmissione, possa darsi che il mittente decida di rispedire dei dati che non sono ancora arrivati ma che arriveranno in seguito. C'è perciò la possibilità di spedizioni "doppie", se un segmento arriva dopo che il trasmittente lo ha già ritrasmesso.
Per questo il software TCP sull'host ricevente avrà anche il compito di individuare e scartare eventuali segmenti "doppi".
Il secondo puntatore, relativo ai dati già spediti, non dipende dal destinatario. Il mittente lo aggiorna all'atto della spedizione di ogni segmento e rappresenta il numero di byte spediti durante la connessione. La differenza fra il primo ed il secondo puntatore dipende dalla velocità corrente della rete.
L'ultimo puntatore serve per il controllo del flusso. Il destinatario, a seconda dello stato di riempimento del suo buffer di ricezione e delle condizioni di carico della sua CPU, può aumentare o diminuire la velocità di spedizione dei segmenti utilizzando un campo apposito del segmento TCP (finestra di trasmissione). La finestra di trasmissione è la distanza fra il primo ed il terzo puntatore. Rappresenta il numero di byte che il destinatario autorizza a spedire. Il mittente potrebbe averne già spediti un certo numero, se il primo ed il secondo puntatore sono diversi, ma comunque non spedirà i byte dall'ultimo puntatore in poi. Se il secondo ed il terzo puntatore verranno a coincidere la trasmissione si fermerà, in attesa che il ricevente dìa una finestra abbastanza ampia. Anche a trasmissione "interrotta" sarà comunque possibile inviare qualche segmento facendo uso di un flag del frame che permette di specificare che il segmento è "urgente".
Da quanto descritto si può capire come questo originale meccanismo sia volto a minimizzare il traffico in rete dovuto ai messaggi di acknowledge e di controllo del flusso. Questi messaggi nella maggior parte dei casi vengono spediti insieme ai normali dati che il destinatario deve mandare al mittente nel corso del loro colloquio e quindi non occupano banda inutilmente. Lo svantaggio è che c'è una certa probabilità di rispedire anche segmenti che giungono a destinazione non errati.
Dalla descrizione del meccanismo di spedizione emergono due considerazioni. La prima è che la lunghezza del segmento TCP è molto importante per l'efficienza della trasmissione. Essa viene negoziata all'atto della connessione, in base alle caratteristiche della rete sottostante. Se entrambe le stazioni sono in LAN dovrebbero scegliere come lunghezza del segmento TCP la lunghezza del frame della rete. La seconda considerazione è l'importanza che assume la lunghezza dell'intervallo di tempo che il mittente attende prima considerare persi i dati che ha già spedito (soglia di ritrasmissione). Questa dipende dal tempo di latenza della rete, che può essere molto variabile nel corso di una sessione, specie in Internet. Ne consegue che la soglia di ritrasmissione deve variare durante il collegamento e che l'algoritmo che decide queste variazioni è molto importante, non solo per l'efficienza del collegamento fra i due host, ma per tutta la globalità di ogni rete TCP/IP, Internet inclusa.
La suddivisione del flusso di dati in segmenti ed il momento della spedizione del segmento sono responsabilità del software TCP, che di solito non distingue fra i tipi di traffico. Questo potrebbe dare problemi nel caso di dati in tempo reale, che devono essere spediti subito, pena la loro "scadenza". Per ovviare almeno in parte a questi problemi, TCP prevede anche un meccanismo per "forzare" la spedizione dei dati non ancora spediti. Quando il protocollo di livello superiore ne ha bisogno, può quindi ordinare di spedire i dati "in sospeso", senza aspettare che TCP accumuli i byte per concludere il segmento o passi un tempo superiore al limite. Il meccanismo per forzare la spedizione viene detto "push" del buffer.

I segmenti "push" possono essere letti immediatamente dal ricevente in quanto non entrano nella finestra mobile a tre puntatori precedentemente descritta. A questo proposito è presente un campo specifico nel "frame" TCP.

La soglia e la finestra di ritrasmissione
Se la soglia di ritrasmissione è troppo grande, il collegamento TCP è potenzialmente più "lento" perchè ci si accorge tardi degli errori e bisogna ritrasmettere troppi dati.
Se la soglia è troppo piccola aumenta il traffico in rete dovuto agli acknowledge del ricevente e si possono generare delle congestioni.

Congestione in TCP/IP
Controllo "end to end"
Nelle comuni reti IP la gestione della congestione non è compito di IP, ma è interamente demandata ai protocolli di livello superiore. Un router IP "normale" riconosce la congestione solo quando ha il suo buffer (coda dei pacchetti) completamente pieno. In tal caso non può far altro che scartare il pacchetto ("packet drop") e non propagarlo ad altri rami della rete.
Come già visto TCP ha una forma di controllo del flusso di tipo "end to end", perchè riguarda il mittente ed il destinatario dei segmenti TCP e non i nodi intermedi della rete (router).
Alla creazione di un collegamento, TCP comincia a trasmettere lentamente ed aumenta gradatamente la velocità di trasmissione ("slow start"), fino a che non osserva che alcuni pacchetti cominciano a "perdersi".
Se TCP rileva pacchetti persi, passa in modo "congestion avoidance": subito comincia a trasmettere molto più lentamente (diminuisce il valore della finestra di trasmissione), in modo da alleviare la congestione, poi ricomincia ad aumentare gradatamente la velocità, fino a che rileva nuovamente delle perdite di pacchetti.
Il software TCP nell'host di destinazione assume che la rete è congestionata rilevando che alcuni pacchetti non giungono a destinazione. Si considera che si sono persi dei pacchetti quando si ricevono 3 numeri di conferma (ACK) uguali, oppure se scatta il tempo di soglia per la ritrasmissione.
Sui meccanismi di gestione della congestione è stata emessa la RFC2001: "TCP Slow Start, Congestion Avoidance ..". Il meccanismo di TCP per la riduzione della congestione è piuttosto debole ed in alcuni casi particolari "controproducente", per cui sono stati studiati protocolli più efficaci, alcuni pubblici e specificati in RFC, altri proprietari, usati in router non standard.
Questi nuovi protocolli prevedono che i router rilevino la congestione "in anticipo", quando è più facile porvi rimedio. Infatti la congestione ha esiti drammatici quando il buffer del router è pieno; in tal caso il router non può far altro che scartare tutti i pacchetti; gli host allo scadere dei loro tempi di ritrasmissione cominceranno a ritrasmettere i pacchetti persi che verranno nuovamente scartati dal router, ed il fenomeno della congestione potrebbe facilmente peggiorare.
E' dunque importante che i router comincino "presto" a fare qualcosa contro la congestione. A questo scopo usano semplici tecniche "statistiche" che, monitorando nel tempo lo stato del buffer, permettono di rilevare l'inizio della congestione ben prima che essa arrivi a saturare il buffer.
Quando il router si accorge di una congestione incipiente, comincia a scartare alcuni pacchetti a caso. Il software TCP degli host che dovrebbero ricevere i pacchetti scartati inizia a rallentare la trasmissione, in accordo il con meccanismo di controllo del flusso "end to end" di TCP, appena descritto. Gli host hanno dunque il tempo di rallentare prima che la congestione del router si faccia drammatica.
La probabilità del packet drop casuale è tanto più alta quanto più aumenta il riempimento del buffer.
Questo meccanismo è del tutto compatibile con il controllo del flusso di TCP; il software TCP e IP non deve perciò essere cambiato.
Controllo della congestione con notifica esplicita
Una tecnica alternativa, più efficace e che però richiede la modifica dei protocolli IP e TCP, prevede l'intervento attivo del router.
Quando il router rileva l'inizio di una congestione, non scarta pacchetti a caso, ma li spedisce comunque, "marcandoli" nella intestazione con informazioni che indicano agli host il suo stato di congestione. Se gli altri router e, soprattutto, l'host di destinazione sanno "leggere" questa "marcatura" sono in grado di rallentare in modo più mirato, sotto la "direzione" del router congestionato. Questo meccanismo, noto come "Explicit Congestion Notification", è specificato nella RFC 2884. E' evidente che la sua implementazione richiede modifiche al software TCP/IP degli host coinvolti.

Il segmento TCP

Segmento TCP

<table>
<tr><td colspan="3">Porta Origine (16)</td><td colspan="2">Porta Destinazione (16)</td></tr>
<tr><td colspan="5">Numero di sequenza (32)</td></tr>
<tr><td colspan="5">Numero di conferma (acknowledge) (32)</td></tr>
<tr><td>Offset Dati (4)</td><td>Riservati (6)</td><td>Flag (6 da 1 bit)</td><td colspan="2">Finestra di ricezione (16)</td></tr>
<tr><td colspan="3">Checksum (16)</td><td colspan="2">Puntatore alla fine dei dati urgenti (16)</td></tr>
<tr><td colspan="4">Opzioni (Variabile)</td><td>Riempimento (per allineare a 32 bit)</td></tr>
</table>

DATI (Variabile)

Come già detto i numeri di porta servono per identificare i socket che sono collegati tramite TCP.
Numero di sequenza (32 bit)
Specifica il numero, all'interno del data stream TCP, del primo byte dei dati contenuti in questo segmento. Il numero dal quale tutto comincia viene assegnato a caso all'inizio della connessione (per problemi di sicurezza).
Numero di conferma (acknowledge) (32 bit)
E' il numero del byte prima del quale il ricevente ha avuto i dati ed ha verificato con il checksum che sono corretti.
Offset dati (4 bit)
E' la lunghezza dell'header, che deve essere sempre allineata a 32 bit. Per questo è di soli 4 bit, altri 4 sono aggiunti a destra e sempre a zero. Naturalmente alla fine dell'header ci sarà il campo dei dati e quindi la lunghezza dell'header è anche l'offset del primo byte di dati, rispetto all'inizio del segmento. Visto che il numero a 8 bit massimo ottenibile con questo campo è 11110000b (240), l'header può essere lungo al massimo 240 Byte.
Riservato (6 bit)
I sei bit di questo campo sono stati riservati per uso futuro.
Flag (6 flag)
Questi flag, che non descriviamo, indicano lo stato della trasmissione, il fatto che il segmento è di tipo "speciale" o l'occorrenza di alcuni eventi particolari relativi alla trasmissione, fra i quali la spedizione "urgente" o "push".
Finestra di ricezione (16 bit)
E' il numero di byte che il ricevente è disposto ad accettare in ingresso (si noti che è riferito al campo "Numero di conferma", dato che il ricevente non può certo sapere quanti sono i byte che gli sono stati trasmessi ma che non sono ancora arrivati!).
Checksum (16 bit)
A differenza del caso IP, comprende sia l'header che i dati
Puntatore ai dati urgenti (16 bit)
Indica il byte in cui sono depositati i dati che non rispettano il meccanismo della finestra di scorrimento, perché sono urgenti (p.es. i segmenti spediti con la modalità "push" accennata precedentemente).
Opzioni e riempimento (numero variabile di bit)
Analogamente al caso del datagramma IP le opzioni servono a casi particolari e ad implementare future modifiche al protocollo. I byte di riempimento allineano l'header in modo che abbia una lunghezza multipla di 32 bit (operazione di "padding").
Dati (numero variabile di bit)
Il "payload" (carico pagante!) del livello superiore.
C'è da notare che nel segmento TCP non c'è nessun indirizzo IP. Infatti quello è un problema dello strato inferiore!

UDP

La funzione principale di UDP è aggiungere un numero di port al datagramma IP, in modo che si possa formare un socket e si possano contattare molti programmi che usano UDP sullo stesso socket (multiplexing).
UDP è più veloce nel suo funzionamento rispetto a TCP, visto che non necessita della fase di negoziazione iniziale del collegamento, inoltre, dato che non deve gestire l'affidabilità, ha un numero inferiore di campi per la gestione del protocollo e quindi è più efficiente di TCP nell'utilizzare la banda del canale di comunicazione.

Il datagramma UDP

Porta Origine (16)	Porta Destinazione (16)
Lunghezza del datagramma (16)	Checksum (16)
DATI (Variabile)	

A internet, the Internet

TCP/IP può funzionare magnificamente anche in una rete, locale o geografica, la cui infrastruttura hardware non abbia alcun punto di contatto con la "madre di tutte le reti" Internet. In questo caso la rete è una "generica" internet.
In una internet abbiamo libertà assoluta di scelta degli indirizzi IP, dei router e dei protocolli di più alto livello da utilizzare. Ciò non è più vero se vogliamo collegare anche un solo computer che usa TCP/IP all'Internet, con la I maiuscola, che è unica.

Organizzazione di Internet

Se si interconnette un'internet all'Internet, emergono una serie di problemi per la cui soluzione esistono diverse organizzazioni internazionali. Il primo problema che si pone è quello della scelta degli indirizzi IP. Dato che l'indirizzo IP deve bastare, da solo, per raggiungere il relativo host è chiaro che se, in tutta l'Internet, due host hanno lo stesso indirizzo, la rete non può consegnare i datagrammi regolarmente.
Per evitare che host connessi alla Internet abbiano lo stesso indirizzo IP esiste una complessa organizzazione internazionale, che fa capo alla Internet Assigned Numbers Authority (IANA). La IANA, il cui controllo è recentemente passato alla ICANN (**I**nternet **C**orporation for **A**ssigned **N**ames and **N**umbers), assegna "lotti" di indirizzi IP con prefisso 8, a organizzazioni internazionali, che presiedono all'assegnazione degli indirizzi a livello "super-continentale" ("Regional Address Registries"), che sono a loro volta delegate ad assegnare ad altri i numeri IP che ricevono "in gestione" ("Local Registries"). Si determina così una scala gerarchia di organizzazioni che provvedono ad assegnare indirizzi univoci ad ogni host della Rete.
Del tutto analoga è l'organizzazione per l'assegnazione dei nomi di dominio, che fa capo a "registries" i cui compiti sono: assicurare l'univocità dei nomi all'interno dei dominii, effettuare la prima scrittura dei nuovi nomi in un particolare server DNS ("authoritative server", il server che ha l'autorità sul nome di dominio) e fare in modo che la nuova inserzione sia propagata in molti altri server DNS.
Per emettere standard comuni e guidare lo sviluppo della Rete in modo non del tutto caotico esistono altre organizzazioni. Tutte fanno capo alla Internet Society.
Internet Society (ISOC) (http://www.isoc.org/)
La Internet Society è un ente non governativo a base USA, che raccoglie esperti di Internet, alcuni anche come rappresentanti dell'utenza, con elezione in Internet. La ISOC coordina i diversi gruppi che sono interessati allo sviluppo di Internet.

Organismi per l'assegnazione dei numeri e dei nomi di dominio

Regional registries:
AfriNIC per l'Africa
APNIC per la regione Asia/Pacifico
ARIN per la regione Nord Americana
LACNIC per la regione Latino Americana (Centro e Sud America e qualche isola dei Caraibi)
RIPE NCC per l'Europa, Medio Oriente ed Asia Centrale (russa)
Local registry per l'Italia:
NicIT http://www.nic.it/

Organismi di sperimentazione e normalizzazione

IAB (Internet Architecture Board) (http://www.iab.org/iab/). E' un gruppo tecnico della ISOC, che presiede alla pubblicazione degli standard e delle RFC (vedi oltre). La IAB definisce l'architettura complessiva di Internet, dando indicazioni strategiche e controllo generale alla IETF (vedi oltre).
l'IESG (Internet Engineering Steering Group) è "alla guida" di Internet dal punto di vista tecnico. Gestisce il coordinamento tecnico delle attività della IETF. E' responsabile di tutte le azioni da intraprendere per l'emissione di standard Internet, inclusa l'approvazione finale dei documenti.
IETF (Internet Engineering Task Force) E' l'organismo responsabile dello sviluppo dei protocolli.
IRTF (Internet Research Task Force) Si occupa della ricerca e delle altre questioni più avanzate nel campo delle tecnologie di rete.

Organismi di gestione

IANA (Internet Assigned Numbers Authority) (http://www.iana.org/iana/)
Inizialmente era un'associazione fra "utenti" importanti dell'Internet, successivamente ha delegato i suoi poteri alla ICANN (Internet Corporation for Assigned Names and Numbers, http://www.icann.org/), un'azienda USA (corporation) di tipo no profit. Ha la responsabilità dell'unicità, in tutta la Internet, di ogni indirizzo IP, dei nomi di dominio e di altri numeri "importanti".

InterNIC (Internet Network Information Center) (http://www.internic.net/)
E' un servizio del Dipartimento del Commercio USA. Gestisce il database DNS, accessibile con il protocollo WhoIs, ed il processo di registrazione dei nomi del dominio primario .com, quello che ha il maggiore valore "commerciale". Delega la gestione a molte aziende, in molti paesi del mondo. Organismi analoghi ("NIC nazionali") sono presenti in ciascuno dei paesi che hanno un dominio primario con estensione "nazionale" (p.es. .it, .fr, .de, .uk ..).

RFC (Request For Comment)
In linea di principio sono normali pubblicazioni, come potrebbero essere gli articoli di una rivista scientifica. Esse sono sottoposte dall'Autore alla IAB, che decide di pubblicarle se sono d'interesse generale. Alcune RFC assumono però lo stato di standard, seguendo la normale procedura per la formazione del consenso: emissione di una bozza, discussione "pubblica" (anche su Internet!), raccolta dei commenti, modifiche, ratifica finale da parte dell'IESG. L'Autore può essere chiunque, naturalmente avranno più peso le persone note nel mondo di Internet e le case produttrici importanti.

A differenza delle norme di tutti gli altri organismi di normazione, tutte le RFC sono disponibili al pubblico in modo gratuito, anche se non è detto che ciò continui a valere anche per il futuro.
In Italia le RFC si possono trovare in ftp://ftp.nic.it/rfc/; un altro sito, che ha un motore di ricerca testuale completo è: http://www.faqs.org/rfcs/.
RFC STD: Norme Internet
Tutte le norme Internet sono RFC, mentre non è assolutamente vero il contrario.
Le norme Internet sono di diversi tipi, in base al livello cui sono giunte nella loro "storia" come standard.
RFC1796 chiama la "storia" di uno standard Internet "Standards Track" e distingue le norme in: "Proposed Standard", che è il documento iniziale che l'Autore chiede che diventi Standard, "Draft Standard", che è il documento in bozza durante la discussione e che può subire diverse revisioni, "Internet Standard" che è il documento finale ratificato.
Le RFC che sono anche standard Internet accettati hanno una seconda indicazione, si leggono perciò così: RFCXXXX (STDYYYY), spesso però la seconda indicazione viene omessa, generando confusione. Il numero YYYY fa riferimento al protocollo di cui si tratta, mentre il numero XXXX fa riferimento al solo documento. Un protocollo potrebbe essere descritto in molte RFC.
Per esempio STD0001 "INTERNET OFFICIAL PROTOCOL STANDARDS" è uno standard che comprende l'elenco corrente di tutti gli standard Internet validi e delle RFC ad essi associate. Un esempio di STD0001 è RFC2000 (STD0001) del Febbraio 1997, che rende obsoleta RFC1920 (STD0001) del Marzo 1996.
Altri tipi di RFC
Esistono altre categorie di RFC, che riguardano documenti che non sono, e non saranno mai, norme Internet. Essi sono: Informational (FYI: For Your Information), Experimental, o Historic, che riguarda vecchie norme superate da nuove RFC (denominazioni da RFC1796).

Accesso alla Rete

L'ISP
Contratti a tempo, a traffico, senza limiti. Fattori che ne determinano le prestazioni. Servizi (protocolli supportati, hosting, collegamento di reti, ..)

Accesso a bassa velocità via PSTN commutata e modem analogici
Accesso in area urbana su linea commutata costo della tariffa urbana a tempo
Accesso con modem, max velocità 56 kbit/s

Accesso a media velocità con tecniche digitali via ISDN
Costi fissi maggiori, costi a tempo analoghi alla PSTN
Accesso con scheda ISDN, min velocità 128 kbit/s, banda "aggregabile" usando più linee ISDN
Esistono router ISDN che sono in grado di instradare su Internet via ISDN il traffico con le reti locali ad esso collegate. Spesso questi router sono in grado di affasciare più linee telefoniche chiamando automaticamente quando c'è maggiore richiesta di traffico.

XDSL

Accesso ad alta velocità con linee dedicate
Le linee dedicate possono esser analogiche (con sigla italiana: CDA Circuito Dedicato Analogico), se la velocità da assicurare è bassa e quello che importa è il collegamento senza interruzione (si pensi per esempio ad un terminale Bancomat, che deve sempre stare in contatto con la centrale operativa, ma non ha certo bisogno di grande velocità di trasferimento.
Per i collegamenti Internet più spesso la linea dedicata da affittare dall'Azienda telefonica è di tipo numerico (CDN Circuito Dedicato.
Su CDN si usano tipicamente apparecchiature di network access di tipo ISDN, "frame relay" o ATM, standard sofisticati cui accenneremo in seguito. Una porta del router che si utilizza può dunque avere una interfaccia frame relay o ATM, per collegarsi ad alta velocità con il backbone Internet nazionale.

Condivisione dell'accesso a Internet
Condivisione degli indirizzi IP (NAT: Network Address Translation) (tipica funzione dei router).
Proxi router
Permette a tutti i computer che stanno su una rete locale di collegarsi su Internet con un solo indirizzo IP. Svolge anche una funzione di cache, prelevando dalla sua memoria le ultime pagine cui ha fatto accesso,
Tiene traccia dei collegamenti effettuati e permette di filtrare certi indirizzi, certi domini o i pacchetti di certi protocolli, cui si può impedire di attraversarlo.

QoS, Voice over IP (VoIP)
"Commutazione e segnalazione" per VoIP

Il protocollo ITU-T H.323, sviluppato per la teleconferenza, viene usato per "telefonare" in Internet.
Un server H.323 contiene l'associazione fra il nome dell'utente ed il suo attuale indirizzo IP ed è in grado di metterlo in contatto con altri utenti che interrogano il server.
In questo senso fa la funzione sia dell'elenco telefonico che della centralina di commutazione.
H.323 RFC3508

Esistono gli standard IP Precedence e Diff Serv (Differentiated Services) che, usano l'intestazione dei datagrammi IP (in particolare il campo TOS) per contenere informazioni sulla priorità, per distinguere fra i diversi tipi di traffico ed assegnare ad essi la larghezza di banda necessaria.

SIP session initiation protocol e SIPS secure session intitiaion protocol sono nella RFC3261.