IL MODELLO TCP/IP

ISO/OSI	*TCP/IP*	*protocolli*
Applicazione	Applicazione	
Presentazione		HTTP, FTP, Telnet
Sessione		
Trasporto	Trasporto	TCP, UDP
Rete	Rete	IP, ICMP, ARP
Collegamento Dati	Collegamento Dati	
Fisico	+ Fisico	IEEE 802.3, 802.5, 802.6, 802.11

Gli indirizzi IP

Per instradare correttamente i pacchetti, i router necessitano di informazioni riguardanti la tipologia della rete, necessita cioè di poter ***identificare in modo univoco*** ogni nodo della rete stessa. Ogni computer o dispositivo all'interno della rete è identificato da un indirizzo chiamato **IP address**. Nel caso in cui un host abbia connessioni multiple alla rete (due o più interfacce) come i router, ogni interfaccia ha un proprio indirizzo IP.
Gli indirizzi fino ad ora utilizzati secondo lo standard **IPV4** sono costituiti da quattro numeri decimali, variabili ciascuno da 0 a 255 del tipo: **192.168.39.6**. L'indirizzo è infatti a 32 bit ed ogni numero è rappresentato da un byte. Il numero massimo di indirizzi ottenibili 4294967296.
La struttura dell'indirizzo prevede che una prima parte identifichi l'indirizzo di rete ed una seconda l'indirizzo di host, cioè la connessione alla rete del computer o del dispositivo:

IP address

Indirizzo di rete	**Indirizzo di host**

L'*indirizzo di rete* può essere rappresentato, a seconda della classe di appartenenza della rete, da uno, due o tre numeri (byte) iniziali dell'IP address. Così l'*indirizzo di host* dai restanti numeri dell'IP address.

Le **classi** più utilizzate vengono denominate *classe A*, *classe B* e *classe C*.
La classe di appartenenza è specificata dai primi bit dell'indirizzo, o più precisamente dalla posizione del *primo 0 dell'indirizzo*: se è il primo bit siamo in classe A, se è il secondo bit siamo in classe B, se invece è il terzo bit siamo in classe C e così via..

Classe A

è utilizzata per reti di grandi dimensioni, per esempio nelle grandi imprese internazionali, in quanto può indirizzare molti host.
Il numero di reti disponibili è 127 (7 bit).
Il numero di host indirizzabili sono 2^{24} (16M) essendo 24 il numero di bit dell'indirizzo di host disponibili.
Gli IP disponibili vanno da 1.0.0.0 a 127.255.255.255 (l'indirizzo 0.0.0.0 è riservato).

Classe B

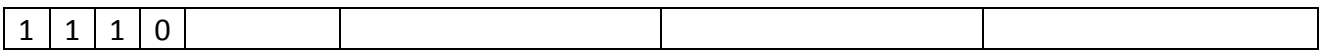
è utilizzata per reti di medie dimensioni, per esempio la rete di una azienda con molti uffici o di una università.
Il numero di reti disponibili è 16K (14 bit).
Il numero di host indirizzabili sono 2^{16} (64K) essendo 16 il numero di bit dell'indirizzo di host disponibili.
Gli IP disponibili vanno da 128.0.0.0 a 191.255.255.255.

Classe C

è utilizzata per reti di piccole e medie dimensioni.
Il numero di reti disponibili è 2M (21 bit).
Il numero di host indirizzabili sono 2^{8} (255) essendo 8 il numero di bit dell'indirizzo di host disponibili.
Gli IP disponibili vanno da 192.0.0.0 a 223.255.255.255.

Esistono anche altre due classi che generalmente sono riservate e non utilizzabili:

Classe D



per *multicast address*, cioè utilizzate dai router per indirizzamenti contemporanei di un sottoinsieme di host di una rete.
Gli IP disponibili vanno da 224.0.0.0 a 239.255.255.255.

Classe E

1	1	1	1	0				

è una classe riservata ad scopi sperimentali ed usi futuri.
Attualmente non ci sono applicazioni per gli indirizzi IP di classe E.
Gli IP disponibili iniziano da 240.0.0.0.

Segmentazione della rete in sottoreti (subnetting)

Per poter meglio sfruttare la disponibilità degli IP, ed evitare che tanti restino inutilizzati, è possibile modificare in parte la struttura dell'indirizzamento utilizzando le **sottoreti** (*subnet*).
La creazione delle sottoreti è ottenuta suddividendo la parte host dell'IP in due parti:
la parte di *subnetting* e la parte di *host*.

Indirizzo di rete	Indirizzo di subnetting	Indirizzo di host

Per decidere in modo più veloce la destinazione dei messaggi verso i computer della rete si usano le **subnet mask** (*maschere di sottorete*) per indicare ai router della rete cosa controllare negli indirizzi IP per individuare la sottorete di appartenenza.
Queste maschere sono indirizzi a 32 bit simili agli indirizzi IP ed indicano quali bit devono essere controllati all'interno dell'IP e quali no. Dove il bit della maschera vale 1 significa che il router deve controllare il corrispondente bit dell'IP, dove vale 0 questo controllo non è necessario.
Se ad esempio consideriamo un indirizzo IP di classe B dove sono destinati alla sottorete otto dei sedici bit dell'indirizzo di host, la subnet mask vale :

255.255.255.0 che in binario è 11111111.11111111.11111111.00000000

il quale indica che sono determinanti per l'individuazione della sottorete i primi tre numeri dell'IP.
Per far questo il router compie un **AND logico** tra la *subnet mask* e *l'indirizzo IP*.
Il risultato è la rete di appartenenza.

La *subnet mask* è fondamentale perché permette di determinare la sottorete di destinazione, cioè se un IP fa parte della rete locale o va ricercato in una rete remota.
Lo stack TCP/IP di un host esegue, durante l'inizializzazione, un'operazione di AND fra il numero IP e la sua maschera di sottorete. Quando un pacchetto viane inviato in rete, il suo IP destinatario viene sottoposto anch'esso alla stessa operazione. Se i risultati dei due processi sono uguali significa che il destinatario appartiene alla rete locale, altrimenti il pacchetto viene inviato al router che provvede a smistarlo ad una rete remota.

Indirizzi IP privati

Anche se gli indirizzi IP nascono per essere univoci sulla rete internet, alcuni di essi sono considerati **privati** (*non pubblici*) secondo la documentazione RFC 1918 e quindi riservati per l'indirizzamento degli host di una rete interna.

Classe di indirizzi IP	Intervallo di indirizzi Privati
Classe A	Da 10.0.0.0 a 10.255.255.255
Classe B	Da 172.16.0.0 a 172.31.255.255
Classe C	Da 192.168.0.0 a 192.168.255.255

Indirizzi IP riservati

Alcuni indirizzi IP sono invece riservati alla rete e quindi non possono essere utilizzati per indirizzare dispositivi di rete.
Si tratta degli **indirizzi di rete** (es 192.168.0.0) e degli **indirizzi di broadcating**, che sono indirizzi utilizzati per indirizzare contemporaneamente tutti i dispositivi della rete (es 192.168.255.255).
Allo stesso modo quando si utilizzano sottoreti si escludono gli indirizzi che hanno il valore binario di tutti 0 o tutti 1, sia per gli indirizzi di sottorete che per gli indirizzi di host. Quindi nella progettazione occorre considerare che il numero degli host indirizzabili con *n* bit è $n=2^n-2$.

Indirizzi IPV6

Per sopperire ad esigenze di poter supportare milioni di host e non preoccuparsi di eventuale spreco dello spazio di indirizzamento, oltre che per ridurre le tabelle di routing ed aumentare la sicurezza, si sta introducendo il nuovo indirizzamento IPV6 che prevede *otto* gruppi di *quattro* cifre esadecimali separate dai due punti:

8000:0000:0000:0000:57A5:88DF:123A:990E

Per abbreviare l'indirizzo è possibile, dati i tanti probabili 0, inserire una coppia di due punti ::
8000::57A5:88DF:123A:990E

Un campo apposito dell'*header* del pacchetto indica la versione di IP e permette ai router di sapere con quale IP deve operare.
Per quanto riguarda la sicurezza, IPV6 è predisposto per lavorare con campi crittografati e nel preambolo di autenticazione fornisce un meccanismo con il quale chi riceve un pacchetto può essere sicuro dell'identità del mittente.
I nuovi protocolli e le nuove applicazioni vengono sviluppate con le due versioni di indirizzi e si prevede che IPV4 potrà essere abbandonato entro pochi anni.

I nomi a dominio

Con il sistema fin qui visto per raggiungere un computer della rete occorre conoscere il suo indirizzo IP. Con l'introduzione dei nomi di dominio si crea una codifica che prevede un nome invece di un numero.
L'indirizzo diventa del tipo:
computer.sottorete.rete.zona
es *pc5.gruppo1.host.it* con i caratteri in minuscolo e senza spazi.
La prima parte indica il nome del computer, la rimanente, detta ***dominio***, individua l'ente, l'azienda o l'organizzazione a cui il computer è collegato (spesso l'indicazione della sottorete non è presente nell'indirizzo).
Un indirizzo internet ha quindi una struttura gerarchica di dominio e sottodominio concatenati con il punto dove ogni gruppo di caratteri indica un *livello inferiore* rispetto a quello che sta *alla sua destra* dopo il punto. La *zona* dell'indirizzo è detta **dominio di livello alto** (*TLD*) e può essere geografico od organizzativo.
Questo sistema di gestione dei nomi di dominio è denominato **DNS** (*Domain Name System*) che oltre a fornire la **mappatura** degli indirizzi IP stabilendo la corrispondenza tra indirizzo numerico e indirizzo simbolico, utilizza i database di nomi simbolici (**URL**) distribuiti sui vari servers collegati alla rete internet.
Nel linguaggio informatico **risolvere un nome in un indirizzo IP** significa ritrovare l'indirizzo che corrisponde al nome di un computer. Il DNS è un servizio fornito dal *livello applicativo* del modello TCP/IP. La documentazione ad esso relativa è contrassegnata con **RFC 1034**.
Gli enti internazionali per l'assegnazione di un nome a dominio sono:
- **Internet Society** (www.isoc.org)
- **ICANN** (www.icann.org)
- **CNR** (www.nic.it/RA) per il .it

Il protocollo IP (Internet Protocol)

E' un protocollo di trasmissione del *livello network* di tipo **non connesso**, quindi senza *conferma*, che riceve i dati dal *livello transport* e li incapsula in pacchetti di dimensione massima di 64 Kbyte e successivamente li instrada verso i livelli inferiori, per poi riassemblare i *frame* in ricezione dal *livello over IP*.
La documentazione specifica per il protocollo IP è contrassegnata con la sigla **RFC 791**.

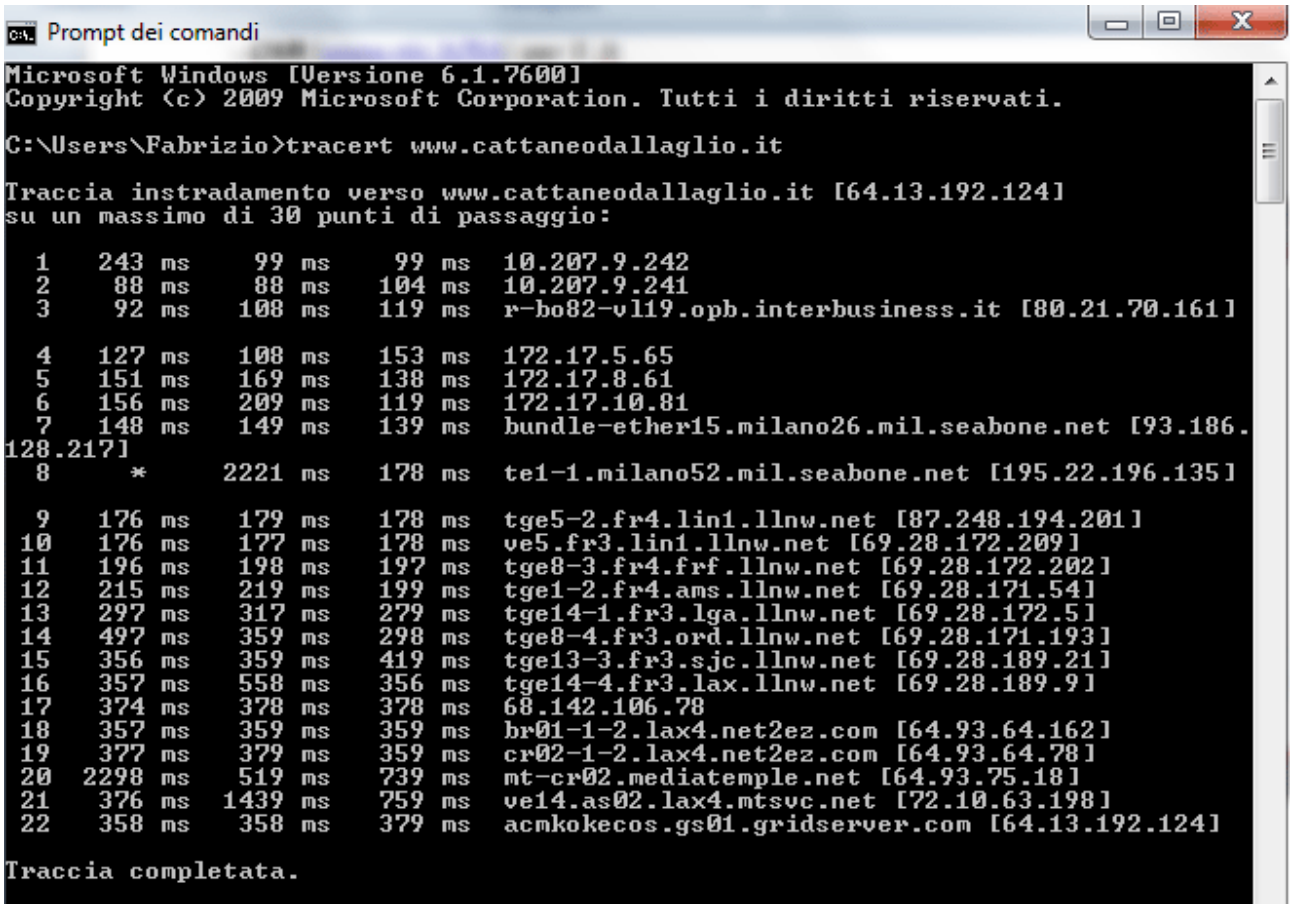
Pacchetto (datagramma) IPv4

Header	Packet fragmentation	TTL protocol	Source IP address	Destination IP address	Options	Data

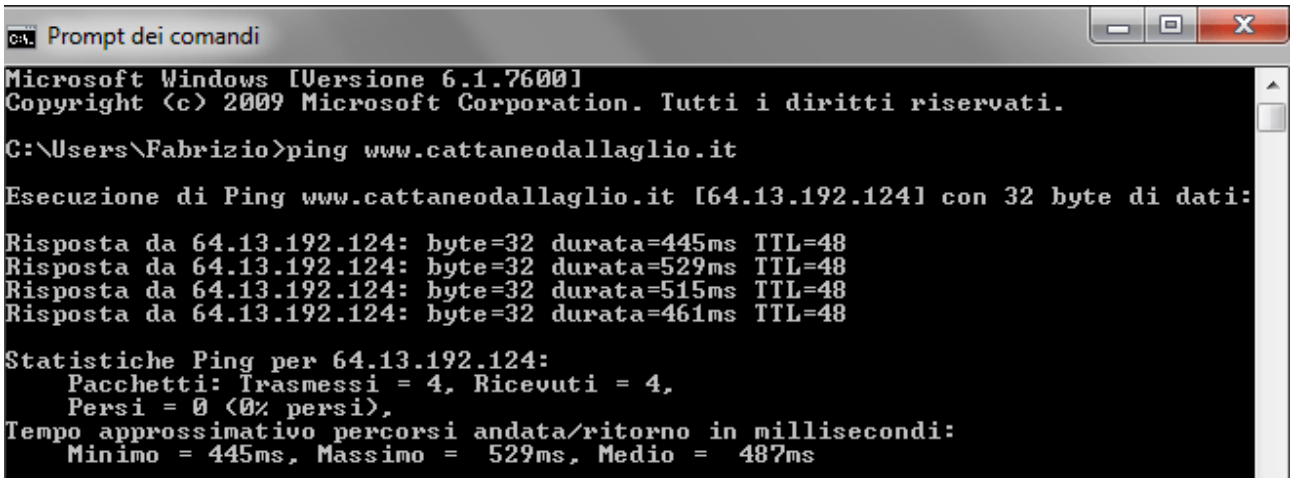
Il protocollo ICMP

E' anch'esso un protocollo di trasmissione del *livello network* che è alla base di importanti servizi come i comandi del prompt **tracert** e **ping**.

Il ***tracert*** attiva il servizio *traceroute* che permette di rilevare l'instradamento verso un IP.



Il comando ***ping*** permette di verificare la raggiungibilità di qualunque host, sia nella rete locale che in internet.



Il protocollo ARP

Il protocollo **ARP** (*Address Resolution Protocol*) è un protocollo di livello network che consente di determinare l'indirizzo fisico MAC delle schede nel caso sia noto solo l'indirizzo IP.
La documentazione specifica per questo protocollo è contrassegnata con la sigla **RFC 1180**.
Quando un host deve spedire un pacchetto a un destinatario di cui non conosce il MAC address, spedisce in broadcasting un messaggio in cui chiede quale sia l'host con quell'indirizzo IP.
L'host cercato rimanda quindi il proprio indirizzo fisico permettendo quindi l'associazione con l'IP.

Instradamento

L'instradamento è compito dei *router* che quando riceve un pacchetto verifica l'indirizzo di destinazione. Se corrisponde alla sua scheda LAN inizia il processo di **forwarding** per stabilire su quale linea deve essere instradato il pacchetto.
Per poter scegliere tra linee differenti occorre sapere quale sia il percorso migliore in base alla valutazione di alcuni parametri.
Questi parametri sono il **numero di hop**, cioè il numero di nodi intermedi da attraversare prima di giungere a destinazione, ed il **costo**, inteso come l'inverso della velocità della linea utilizzata.
L'instradamento avviene quindi attraverso **algoritmi di routing** che possono essere *statici* o *dinamici* a seconda che le **tabelle di routing** nel router siano inserite manualmente da un operatore o siano aggiornate in modo automatico dal router stesso.
Gli algoritmi di routing possono prevedere anche più di una linea (percorso) per raggiungere un host.

I protocolli del *livello Transport*

Il protocollo TCP

Il *protocollo TCP* ha il compito di trasmettere in modo affidabile i dati tra due nodi della rete.
TCP crea una **sessione orientata alle connessioni** tra i due host.
La fase iniziale della trasmissione (**handshaking**) prevede che il client richiedente invii al server un segmento specificando la porta che intende usare ed il suo *Numero di Sequenza Iniziale* (**ISN**).
A questo fa seguito una risposta del server che invia a sua volta un segmento contenete il suo ISN ed un segnale di riconoscimento dell'ISN del client (**acknowledgement**).
Quindi il client da inizio alla sessione.

Segmento TCP

Numero porta sorgente **Numero porta destinazione**	**Numero sequenza**	**Numero acknowledge**	**Campi opzionali**	**Dati**

Numero di porta

I numeri di porta, che sono fissati a livello internazionale, servono per indicare al *livello Application* il protocollo da utilizzare:

Porta	***Protocollo***
20, 21	FTP (*File transfer Protocol*) dati sulla porta 20, controllo sulla porta 21
23	TELNET
25	SMTP (*Simple Mail Transfer Protocol*)
53	DNS (*Domain Name Server*)
70	GOPHER
79	FINGER
80	HTTP (*Hyper Text Transfer Protocol*)
110	POP3 (*Post Office Protocol, versione 3*)
119	NEWS
194	IRC (*Internet Relay Chat*)
443	HTTPS (*Secure Hyper Text Transfer Protocol*)

L'utilizzo del concetto di numero di porta, permette di poter eseguire più applicativi contemporaneamente (*multiplexing*).
La documentazione specifica per il protocollo TCP è contrassegnata con la sigla **RFC 0793**.

Il protocollo UDP

Il *protocollo UDP*, a differenza del TCP, non necessita di connessione non stabilendo alcuna sessione di comunicazione limitandosi ad inviare i pacchetti sulla rete senza richiesta di conferma di avvenuta ricezione.
E' utilizzato dalle applicazioni che inviano piccole quantità di dati e che ripetono spesso l'invio nel tempo, oppure nello streaming audio e video dove è necessaria un'alta velocità di trasferimento.
La documentazione specifica per il protocollo TCP è contrassegnata con la sigla **RFC 0951**.

I protocolli del *livello Application*

Il protocollo Telnet

Telnet è un protocollo che permette di collegarsi ad un altro computer in remoto, connesso in rete, ed agire, dopo autenticazione, come se stesse direttamente lavorando su quell'elaboratore, attraverso la sua tastiera e visualizzando sullo schermo le risposte.
La documentazione si trova nell'**RFC 0854**.

Il protocollo FTP

Il **protocollo FTP** (*File Transfer Protocol*) serve per trasferire files tra due host. Con *client FTP* si indica l'host che richiede la sessione FTP mentre con *server FTP* l'altro host a cui ci si connette.
L'FTP utilizza due connessioni: la prima (**connessione di controllo**) serve al client per inviare comandi al server e ricevere risposte, mentre la seconda (**connessione dati**) viene stabilita successivamente quando inizia il trasferimento dei files.
La documentazione si trova nell'**RFC 959-2228-2640**.

Il protocollo SMTP

Il **protocollo SMTP** (*Simple Mail Transfer Protocol*) è l'applicativo TCP/IP che permette di inviare *posta elettronica* agli utenti della rete. Questo protocollo è stato studiato per funzionare anche nelle condizioni di maggior traffico sulla rete e quindi è stato progettato per una trasmissione il più possibile compatta.
Ogni utente è identificato da un indirizzo di posta elettronica (***utente@gestoredelservizio***) e non è richiesta alcuna autorizzazione per l'invio di un messaggio.
La documentazione si trova nell'**RFC 2821**.

Il protocollo POP3

Il **protocollo POP3** (*Post Office Protocol*) è definito per la lettura della posta elettronica che rimane disponibile all'interno della **casella postale** (*mailbox*) fino alla sua rimozione.
Per procedere alla lettura è necessario procedere alla identificazione dell'utente (*authorization state*) durante la quale occorre fornire l'identificativo dell'utente.
La documentazione si trova nell'**RFC 1939-1957-3206**.

Il protocollo HTTP

Il **protocollo HTTP** (*Hyper Text Transfer Protocol*) definisce un metodo di interazione client/server ottimizzato per lo scambio di messaggi brevi e veloci.
La connessione dura solo il tempo strettamente necessario per la trasmissione ed in quindi viene chiusa.
Nel protocollo HTTP le risorse della rete sono identificate con un indirizzo simbolico detto **URL** (*Uniform Resource Locator*). I documenti sono organizzati in forma ipertestuale e sono scritti in **linguaggio html** (*Hyper Text Markup Language*) che utilizza **tag** (*marcatori*) interpretabili dal programma visualizzatore (***browser***) per formare le pagine grafiche di internet.

Il *client* (browser), alla richiesta di un url, apre una connessione con l'host alla porta 80 (porta di default)
Il *server* invia quindi la risposta della pagina html e chiude la connessione.
La risposta del server comprende anche un **codice di stato** di tre cifre, il cui significato è rivolto al browser, del tipo:

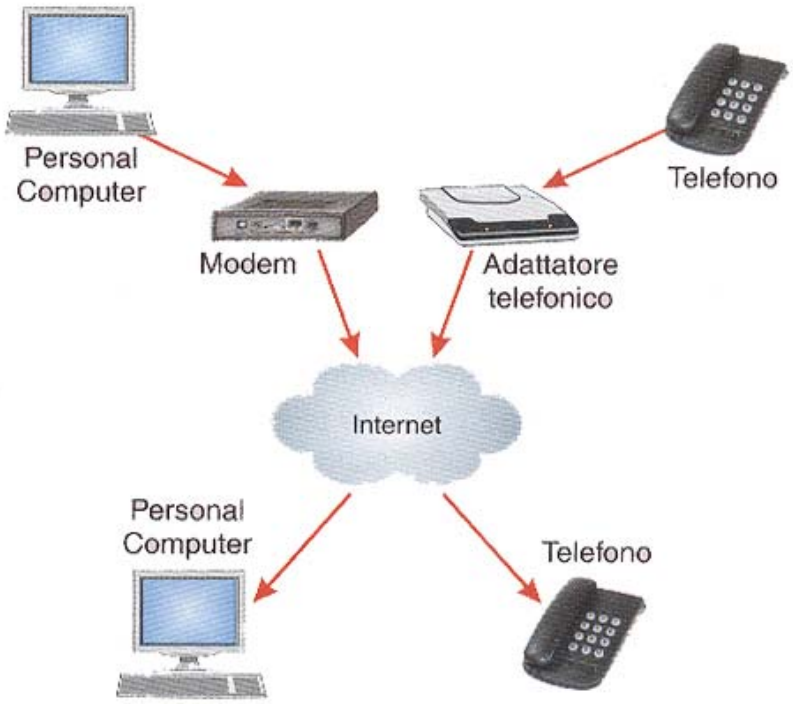
200 OK	La richiesta è stata processata ed i dati vengono spediti
204 No Content	La richiesta è stata processata ma non ha avuto risposta
301 Moved Permanently	Il file specificato è stato permanentemente spostato in un altro sito
403 Forbidden	Il client non è autorizzato a ricevere i dati richiesti
404 Not Found	I dati specificati nell'url non sono stati trovati

Per garantire la *sicurezza delle transazioni* si usano protocolli sicuri come **HTTPS** e **SSL**.
HTTPS è del tutto simile all'HTTP ma utilizza per la trasmissione la porta 443 anziché la 80 e interpone tra il *livello Transport* ed il *livello Application* un livello per la **autenticazione** e la **crittografia** rappresentato del protocollo SSL.
Questo protocollo garantisce la sicurezza attraverso la crittografia, scambiando la **chiave** alla base dell'*algoritmo di crittografia* nella fase preliminare di handshaking.
Il browser segnala che è stata richiesta l'attivazione del protocollo HTTPS e lo segnala nella barra degli indirizzi.
La documentazione si trova nell'**RFC 2616**.

La comunicazione *Voice over IP*

Telefonia in internet

Si tratta a differenza delle altre comunicazioni di un servizio in *tempo reale*, perché nella comunicazione vocale non è tollerato ritardo.



La differenza rispetto alla telefonia tradizionale consiste nel fatto che la telefonia **VoIP** funziona con la tecnica della ***commutazione di pacchetto*** e non a *commutazione di circuito*.
La commutazione a circuito non subisce ritardi, mentre nella gestione dei pacchetti si può manifestare, sia durante i campionamenti della voce e sia durante la ricomposizione di questi da parte del protocollo IP destinatario.
Ci sono due fondamentali caratteristiche che determinano la qualità di una connessione telefonica su internet:

- La **latenza**, cioè la somma dei vari ritardi oltre ai tanti nodi che i pacchetti devono attraversare
- La **qualità della comunicazione**, che rispecchia la fedeltà della riproduzione della voce nella telefonata

TCP/IP non garantisce in sostanza agli utenti la trasmissione di un certo numero di dati in un preciso periodo di tempo perché le prestazioni della rete possono cambiare di momento in momento: a volte i dati sono trasmessi immediatamente ed a volte non vengono trasmessi affatto.
Questi problemi di ritardo si manifestano sotto forma di **eco** quando i ritardi superano i 50mS ed in questo casi subentrano *cancellatori di eco*.