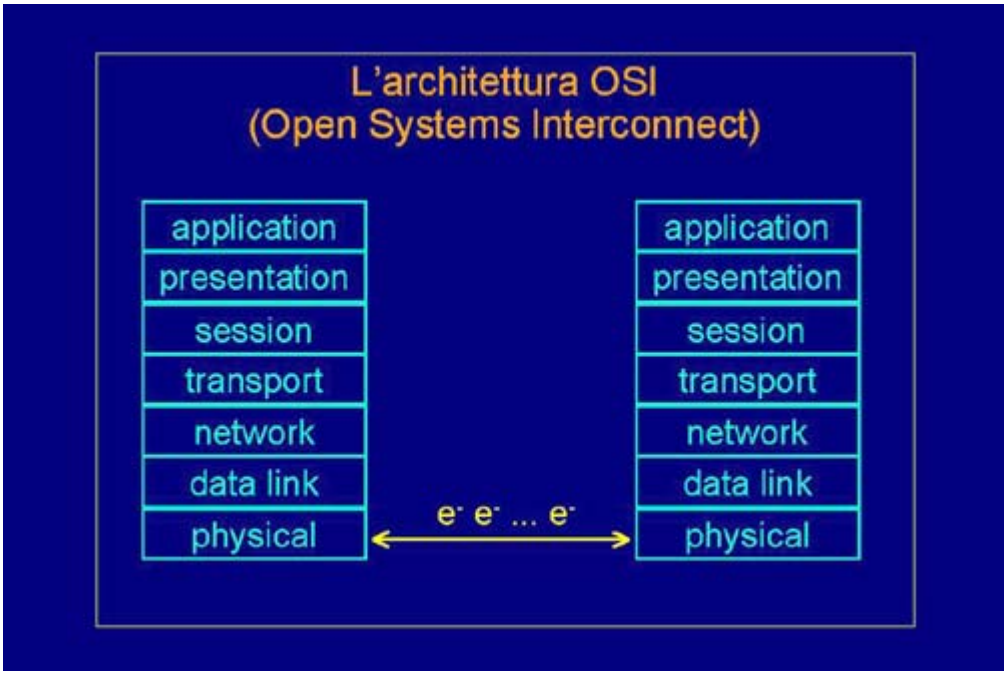
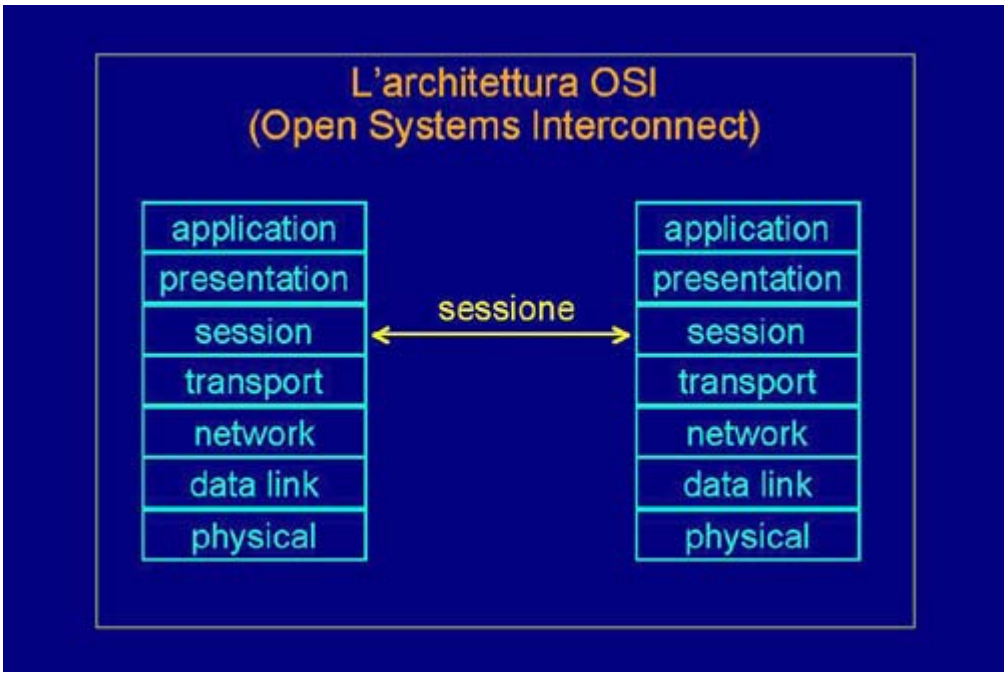
L'architettura di rete TCP/IP
OSI: Fisico - Data link



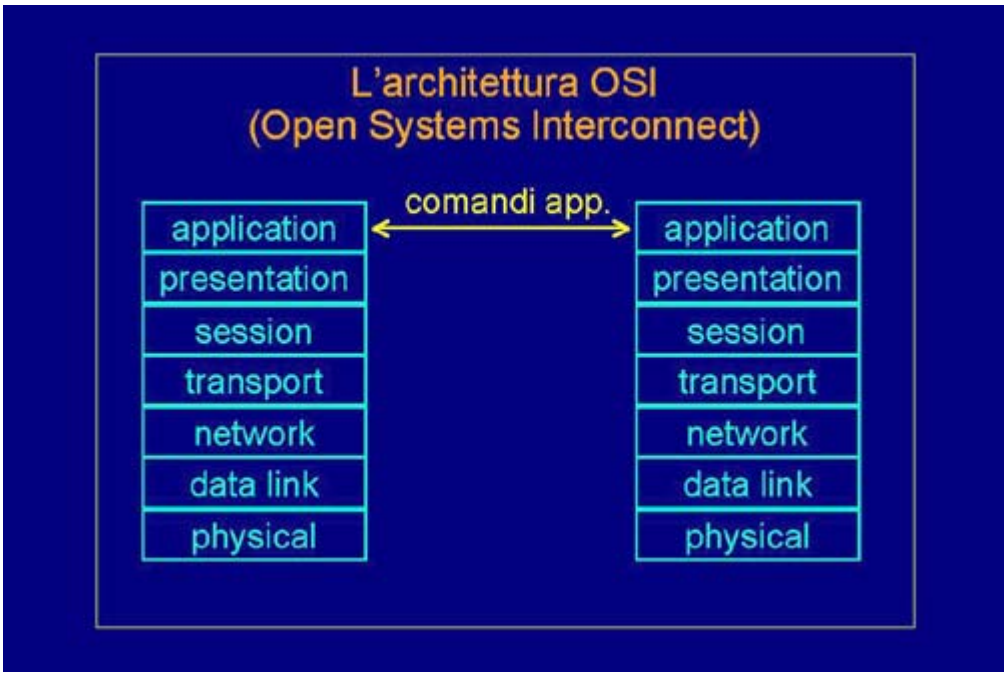
Per poter rendere sicura una rete bisogna prima aver capito molto bene in quale modo funziona. Ecco quindi che in questa breve lezione parleremo dei meccanismi di funzionamento delle reti, concentrandoci in particolare sulle reti TCP/IP che oggigiorno sono quelle più utilizzate. In generale il modello a cui obbedisce il funzionamento di una rete di calcolatori è quello definito dall'architettura OSI, che significa interconnessione di sistemi aperti. OSI è un modello che descrive quali sono i vari livelli di astrazione e a volte anche di implementazione in cui due calcolatori colloquiano. Il primo è il cosiddetto "livello fisico". A questo livello due calcolatori sono in comunicazione scambiandosi dati secondo un contenuto fisico appropriato. Ad esempio due calcolatori, collegati tramite una rete Ethernet o ISDN, possono trasmettersi dati scambiandosi in realtà degli elettroni, ossia delle correnti o delle tensioni. Il "livello fisico" serve per trasmettere fisicamente i dati forniti dal livello 2, detto "data link", di trasmissione dei dati. A livello "data link" noi non trattiamo più col formato fisico dei dati inteso come elettroni o fotoni, ma con bit logici, quindi zeri e uni.

OSI: Network - Trasporto - Sessione



Questi bit logici a loro volta vengono utilizzati per formare i cosiddetti pacchetti di rete. Infatti il livello 3 di trasmissione è chiamato il "livello rete" ed è il primo in cui ci si rende completamente indipendenti dal substrato di trasmissione. È detto "end to end": dall'indirizzo del mittente a quello del destinatario ignorando quale sia il cammino intermedio. Ci penserà l'infrastruttura di rete a trasmettere i dati, sottoforma di pacchetti, dalla macchina che ha indirizzo numero uno alla macchina che ha indirizzo numero due. I pacchetti di rete servono a creare dei canali logici che appaiono a livello 4, il cosiddetto "livello di trasporto", in cui due calcolatori sono collegati da un canale virtuale o da una comunicazione logica di tipo messaggio. I canali logici sono delle sorti di oleodotti dentro cui transitano i bit invece che il petrolio. Bisogna però decidere quali sono le regole per costruire un oleodotto; questo in termini di calcolatori viene deciso a livello 5 ossia: il "livello di sessione".

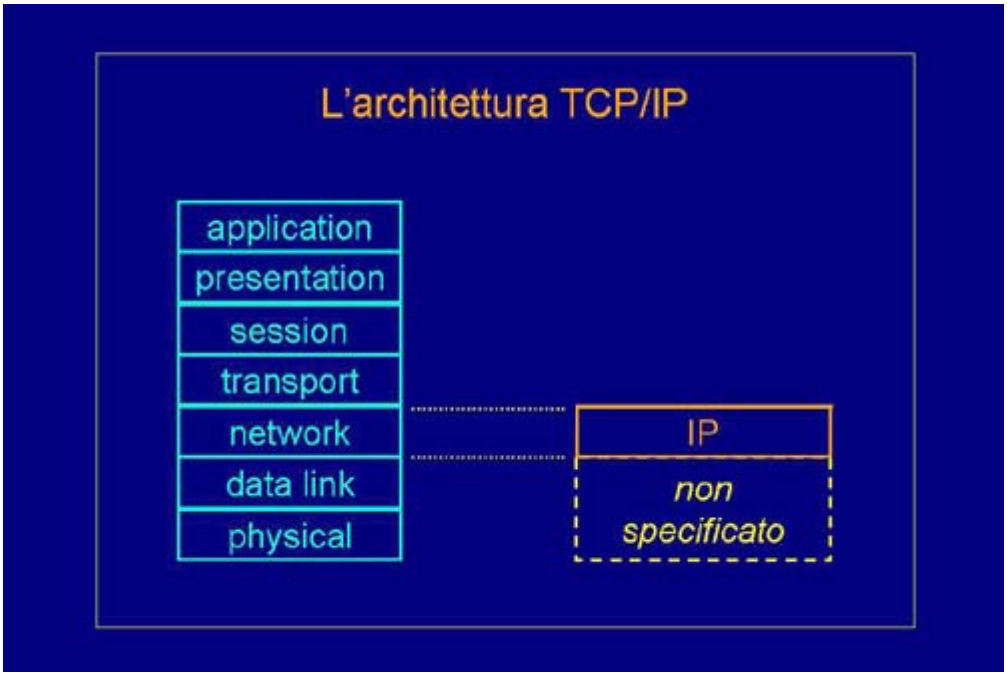
OSI: Presentazione - Applicazione



Sopra la sessione esistono ancora altri due livelli. Il "livello presentazione" è quello che effettua la trasformazione del formato dei dati, per adattarli al tipo di codifica che viene utilizzato tra due

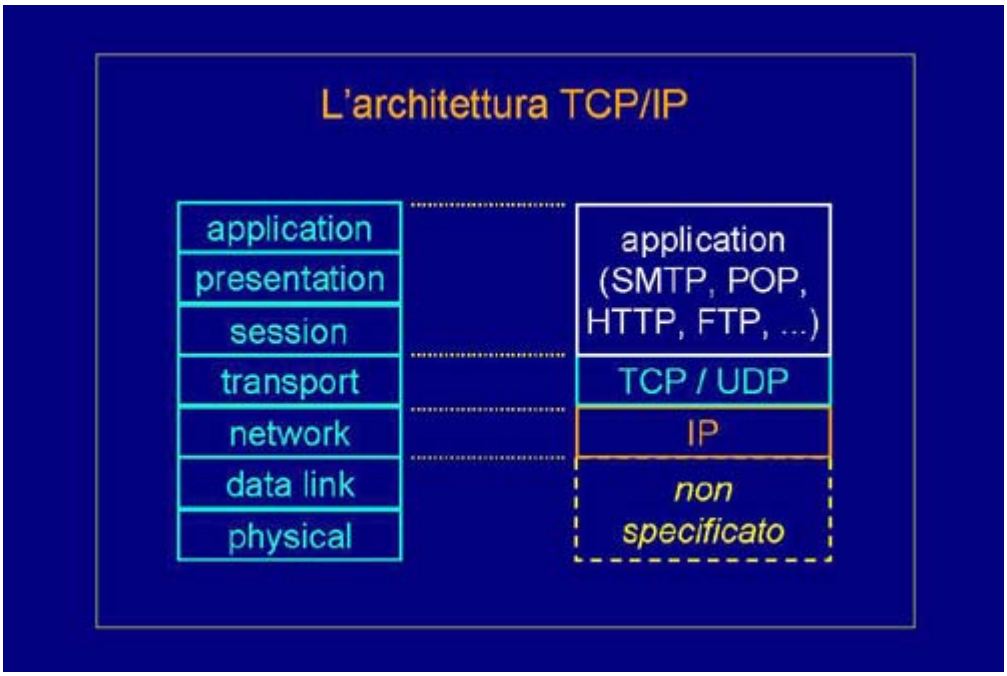
diversi sistemi che comunicano. Infine, a livello 7, si parla di "applicazioni": ossia tutti i dati che sono stati trasportati attraverso la rete sono serviti a creare dei comandi applicativi, a svolgere una qualche funzione. Dal punto di vista dell'utente questo è l'unico livello che interessa: tutti gli altri sono semplicemente ausiliari che servono a trasportare queste informazioni e a far funzionare una applicazione via rete. Questo è un modello teorico.

L'architettura TCP/IP 1



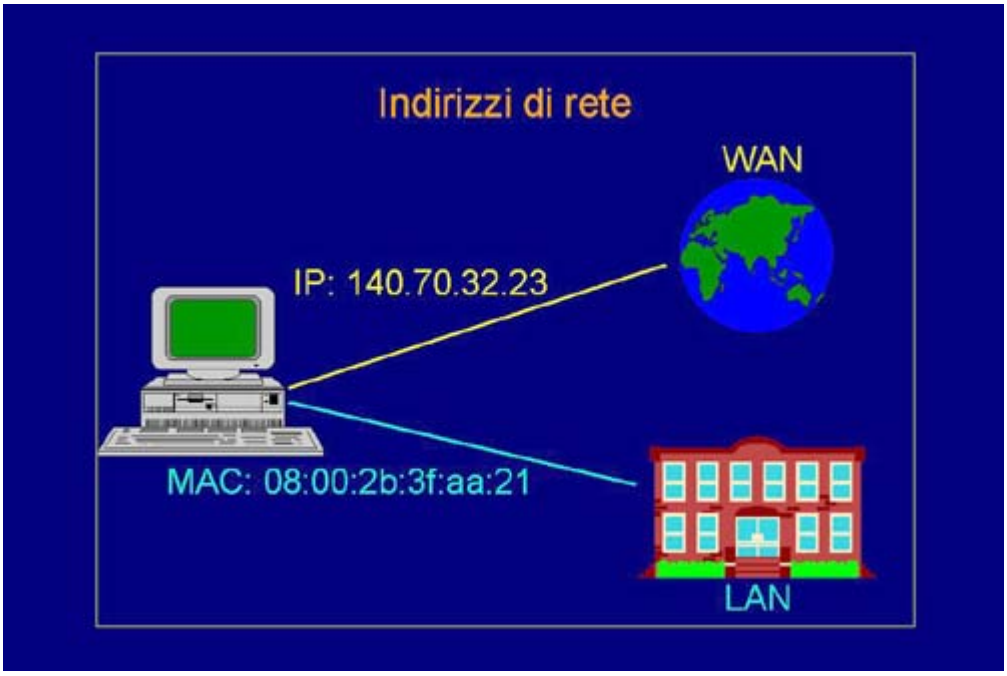
Vediamo adesso come nella realtà questo modello venga implementato dalla rete oggigiorno più utilizzata: la rete TCP/IP. Confronteremo tale architettura rispetto al modello logico OSI. La prima cosa, per cominciare, è che TCP/IP non specifica assolutamente alcun tipo di formato, protocollo o codifica per quanto riguarda i livelli bassi, ossia il livello fisico e il livello 2. Questo significa che qualunque sistema che sia in grado di implementare i livelli 1 e 2, in modo conforme a quello che i livelli superiori di TCP/IP si aspettano, può benissimo funzionare con tutti gli altri protocolli dello stack di rete. Il primo livello in cui TCP/IP è presente è il terzo, il livello rete. Questo è implementato dal protocollo IP (Internet Protocol): originariamente l'architettura TCP/IP è stata concepita per effettuare l'interconnessione di reti locali e solo recentemente è stata utilizzata anche come protocollo al loro interno.

L'architettura TCP/IP 2



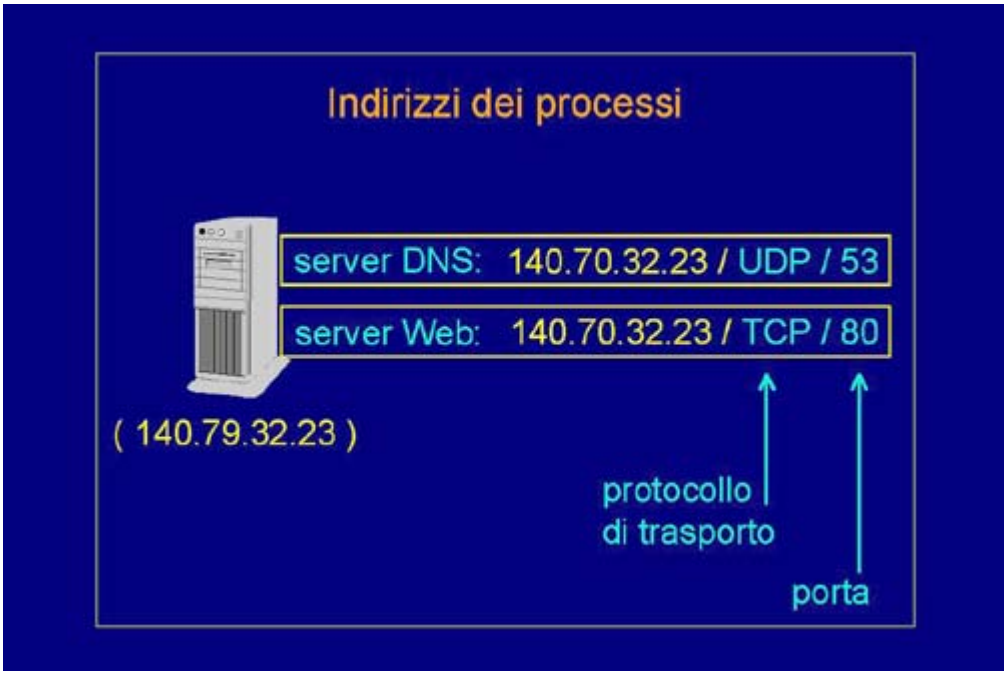
TCP/IP ha anche specificato dei protocolli per quanto riguarda il livello di trasporto. In particolare due sono i principali protocolli a livello 4: il TCP, che offre un canale logico virtuale appoggiato sopra IP, e il protocollo UDP, che utilizza invece dei messaggi di tipo datagram per consegnare messaggi "end to end" all'interno della rete. TCP/IP non frammenta ulteriormente la trasmissione ai livelli superiori ma ingloba tutto quanto in un unico livello applicativo. Questo significa che ciascuna applicazione deciderà autonomamente quali tipi di sessione, di formato dati e di comandi applicativi utilizzare. Quindi, in questo senso, esistono dei protocolli unici che specificano insieme tutti e tre i livelli. Ad esempio, il protocollo SMTP è quello utilizzato per la trasmissione dei messaggi di posta elettronica, il POP è quello utilizzato per trasmettere i messaggi che sono depositati nella casella postale fino alla postazione di lavoro dell'utente e così via. Quindi diciamo che, in generale, TCP/IP è un insieme di protocolli più semplificato rispetto al modello teorico OSI, avendo in questo modo il vantaggio di risultare più veloce, più leggero e più facilmente gestibile nelle reti reali.

Indirizzi di rete



Affinché due calcolatori possano funzionare e comunicare attraverso una rete, a ciascuno di essi deve essere dato un indirizzo. Esistono però svariati tipi di indirizzi: in particolare se il nostro calcolatore è collegato all'interno di una rete locale, quella che normalmente si chiama una Lan, dovrà avere un indirizzo che lo contraddistingue nei confronti delle apparecchiature che costituiscono tale la rete. Ad esempio qui vedete indicato un indirizzo su 48 bit tipico delle reti Ethernet. Se però il nostro calcolatore desidera anche comunicare attraverso una rete geografica, quale ad esempio la rete internet, avrà bisogno anche di un indirizzo univoco a livello mondiale. Siccome non è certo che il nostro destinatario utilizzi il medesimo tipo di tecnologia che utilizziamo noi, e soprattutto perché la tecnologia delle reti locali non può essere utilizzata anche per coprire distanze geografiche, bisognerà fornire un altro tipo di tecnologia di interconnessione e anche un altro tipo di indirizzo. Ecco quindi che per i collegamenti in rete geografica il medesimo nodo di elaborazione verrà identificato con un altro indirizzo. All'interno della rete TCP/IP si usano gli indirizzi IP che sono indicati con quattro gruppi numerici ognuno dei quali può variare da 0 a 255, perché in realtà sono indirizzi su 32 bit e quindi ognuno di questi gruppi, separati da punti, corrisponde a 8 bit.

Indirizzi dei processi

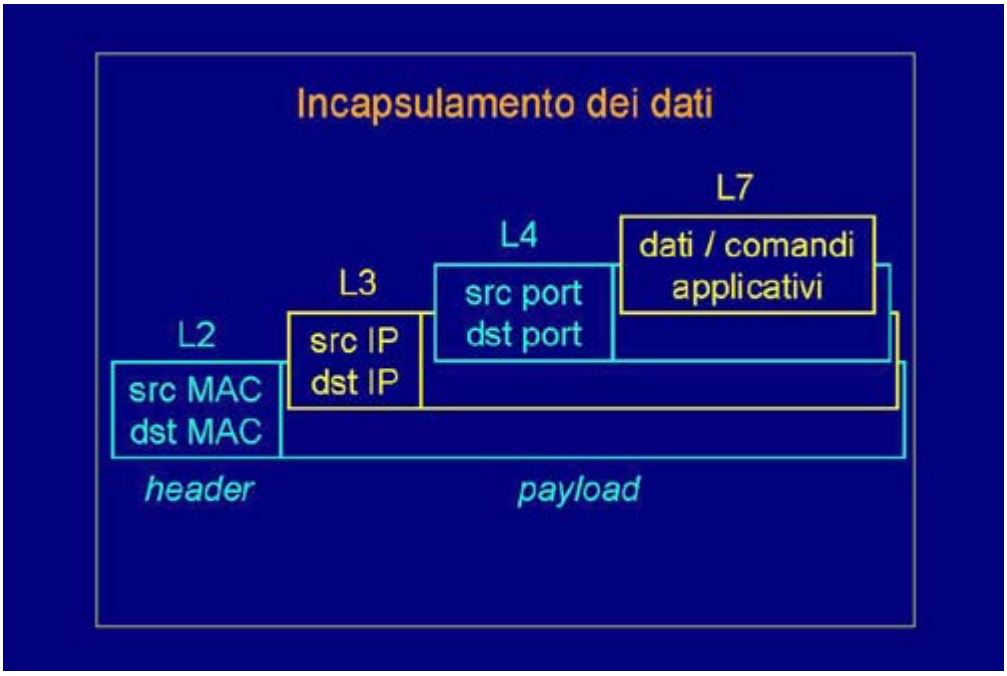


Ma all'interno di un unico nodo di elaborazione possono essere presenti più processi applicativi, tipicamente più servizi: i cosiddetti "server". Quando un'applicazione deve accedere ad uno di questi sevizi ha bisogno di venire a conoscenza, non soltanto dell'indirizzo di rete del nodo di elaborazione da cui il servizio è offerto, ma anche di indirizzare lo specifico processo. Ecco quindi che si parla anche di indirizzi dei processi. Ad esempio su questo nodo di elaborazione, che ha indirizzo IP 140.70.32.23, girano due processi: un server web e uno DNS. Per riuscire a distinguere questi server bisogna dare delle informazioni aggiuntive: il protocollo di trasporto con cui i dati verranno veicolati verso il nostro server e la particolare porta. La porta è una distinzione ulteriore che permette di riconoscere i vari processi attivi su un unico nodo di rete. Ecco allora che il nostro server web potrà essere identificato in base al suo indirizzo IP, al fatto che dialoga tramite il protocollo di trasporto TCP e alla porta 80, quella su cui tutti i server web normalmente sono in ascolto. Ovviamente un server diverso dovrebbe avere un indirizzo diverso. Infatti, il server DNS ospitato sulla medesima macchina (lo si nota perché ha lo stesso indirizzo IP), utilizzerà il protocollo di trasporto UDP, quindi un protocollo diverso da TCP, e una porta diversa, ad esempio la 53.

Incapsulamento dei dati 1

Quando si trasmettono dei dati, ogni livello di rete richiede che siano messi in un formato peculiare di quel livello. Questo vuol dire che i dati a livello applicativo vengono incapsulati in una serie di buste di livello successivo. Quindi, in realtà, i dati che sono trasmessi in rete sono soltanto in minima parte dati applicativi e per la maggior parte sono dovuti al meccanismo di trasporto. In particolare i dati, ad ogni livello, sono trasportati all'interno del cosiddetto "payload" (carico pagante), il quale è preceduto dall'"header" (intestazione), che dice, per quel particolare livello, chi sono il mittente e il destinatario. Ad esempio, a livello 2 l'header conterrà fra gli altri dati anche l'indirizzo di livello 2, il cosiddetto "MAC", del sorgente e quello del destinatario. Ma se questo pacchetto di livello due è stato originato fuori dalla nostra rete locale, vorrà dire che è stato generato da un pacchetto di livello 3. Ed ecco che a livello 3 il payload di livello 2 sarà in realtà scomposto in due parti: un payload di livello tre preceduto da un intestazione di livello 3, che fra gli altri dati conterrà anche gli indirizzi IP del mittente e del destinatario.

Incapsulamento dei dati 2

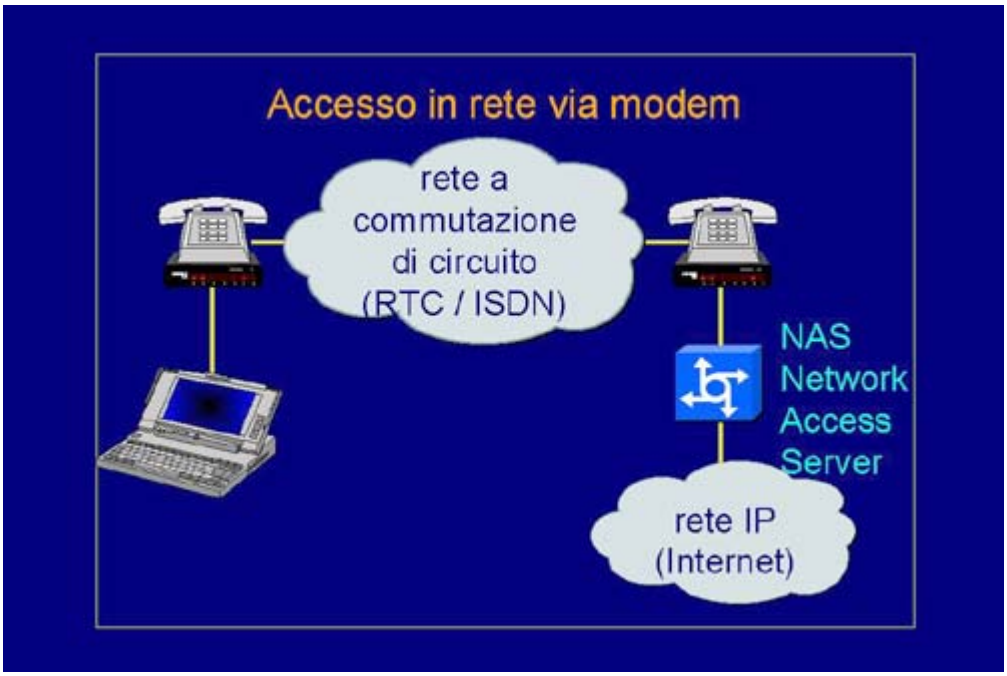


Questo gioco di scatole cinesi prosegue e, ad esempio, il livello 4 specifica che il mittente che aveva questi indirizzi "MAC" e IP era un processo situato in una certa porta. Analogamente il livello 4 specificherà qual è la porta del destinatario. A livello di payload utilizza direttamente i dati o i comandi applicativi che sono stati forniti dal livello 7.

Accesso in rete via modem 1

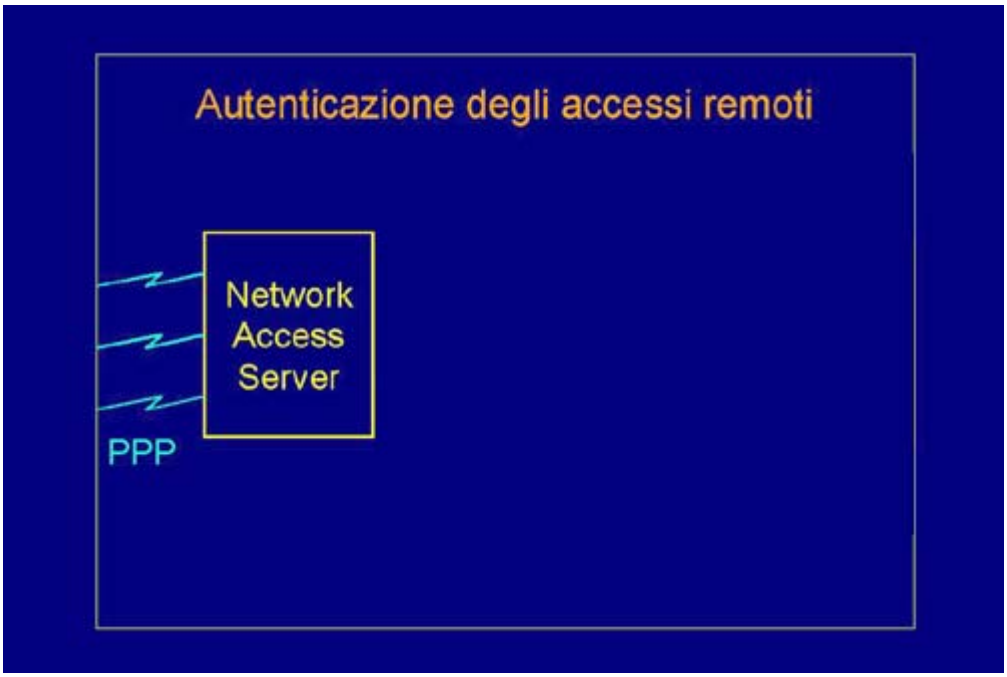
A questo punto consideriamo quali sono le possibili modalità per accedere in rete. Se una persona dispone di un personal computer a casa, o un portatile, tipicamente non è attaccato direttamente ad una rete locale. Per accedere alla rete geografica, quindi, utilizzerà un modem: una apparecchiatura di telecomunicazione che serve a trasformare i bit forniti dal computer in un segnale adatto alla trasmissione su una rete a commutazione di circuito. Per esempio: la normale rete telefonica commutata, su cui tutti facciamo le nostre normali telefonate, o la rete ISDN, che è la rete numerica integrata nei dati e nei servizi.

Accesso in rete via modem 2



Dall'altra parte ci sarà un'apparecchiatura analoga: ossia un altro modem in grado di decodificare i segnali telefonici e trasformarli in binari. Questi segnali binari verranno forniti a quello che si chiama un NAS (Network Access Server) ossia un nodo che ha proprio il compito di decidere se, in quale misura e come, i dati che arrivano dalla rete telefonica possono essere trasformati in dati appartenenti a una rete di tipo IP. Quindi, per collegarsi tramite un normale computer portatile o un computer casalingo a una rete geografica, occorre disporre a casa nostra di un modem che effettuerà la traduzione da bit ad impulsi fonici. Da parte del ricevente ci dovrà essere, oltre a un modem che effettuerà la demodulazione da impulsi fonici a bit, anche un'apparecchiatura che sarà attaccata in modo permanente alla rete geografica a cui vogliamo collegarci.

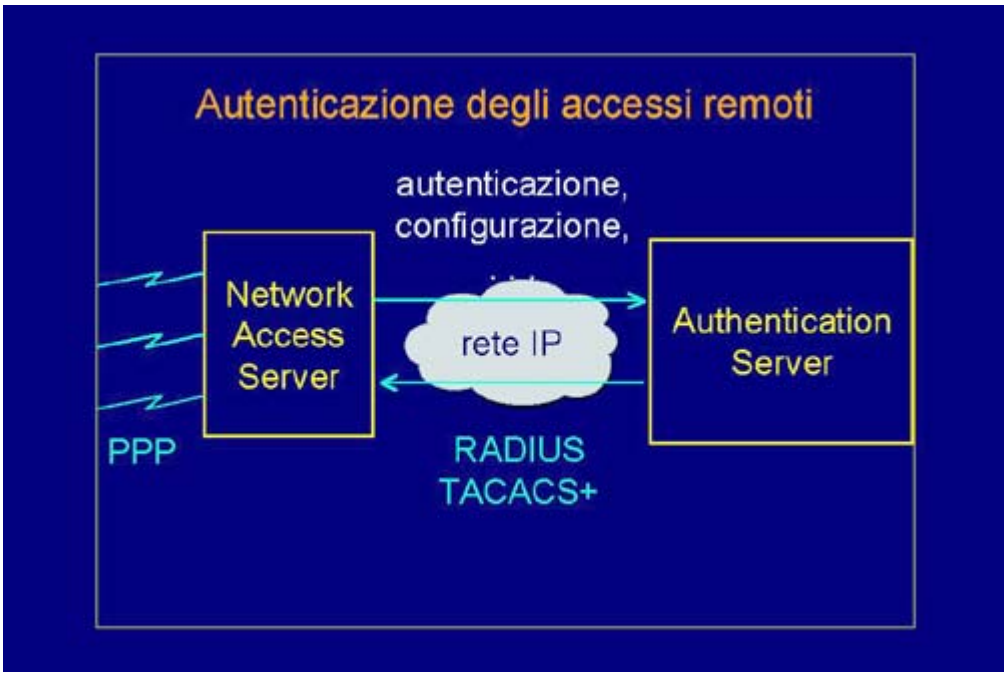
Autenticazione degli accessi remoti 1



Ovviamente bisogna evitare che delle persone non autorizzate possano collegarsi alla rete geografica. Per questo motivo, normalmente, il nostro Network Access Server dispone di un elenco di persone abilitate ad utilizzare la rete. Questo tipo di identificazione viene normalmente veicolato

tramite un canale cosiddetto PPP. Il “Point to Point Protocol” è un protocollo standard di livello 2, da utilizzarsi su reti commutate, che serve a veicolare protocolli di livello superiore.

Autenticazione degli accessi remoti 2



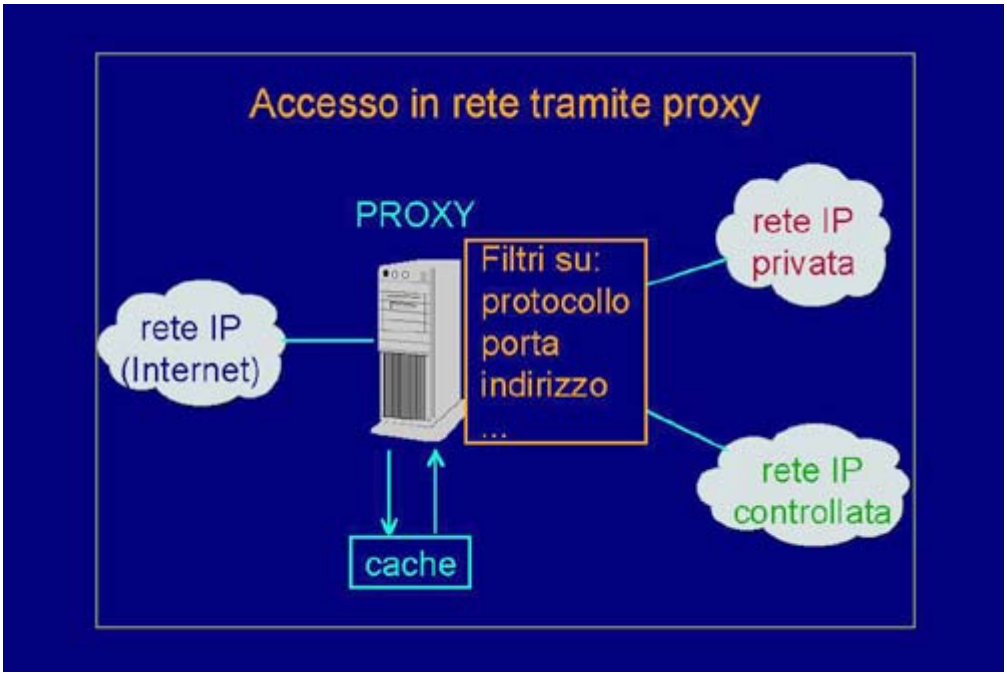
Il NAS può decidere lui stesso di concedere al chiamante l'accesso alla rete, ma solitamente dialoga, tramite una rete IP locale, con un server che fornisce i servizi di autenticazione, di configurazione e per esempio di logging, per più NAS. Il NAS dialoga con l'authentication server tramite dei protocolli specifici. Il protocollo RADIUS, il TACACS o TACACS PLUS sono attualmente quelli più utilizzati per effettuare l'autenticazione degli accessi remoti, ossia verificare se un utente che sta chiamando un certo numero telefonico ha diritto oppure no a collegarsi alla rete geografica.

Autenticazione dei canali PPP

Esistono due modalità base con cui l'utente può veicolare la propria autenticazione all'interno di un

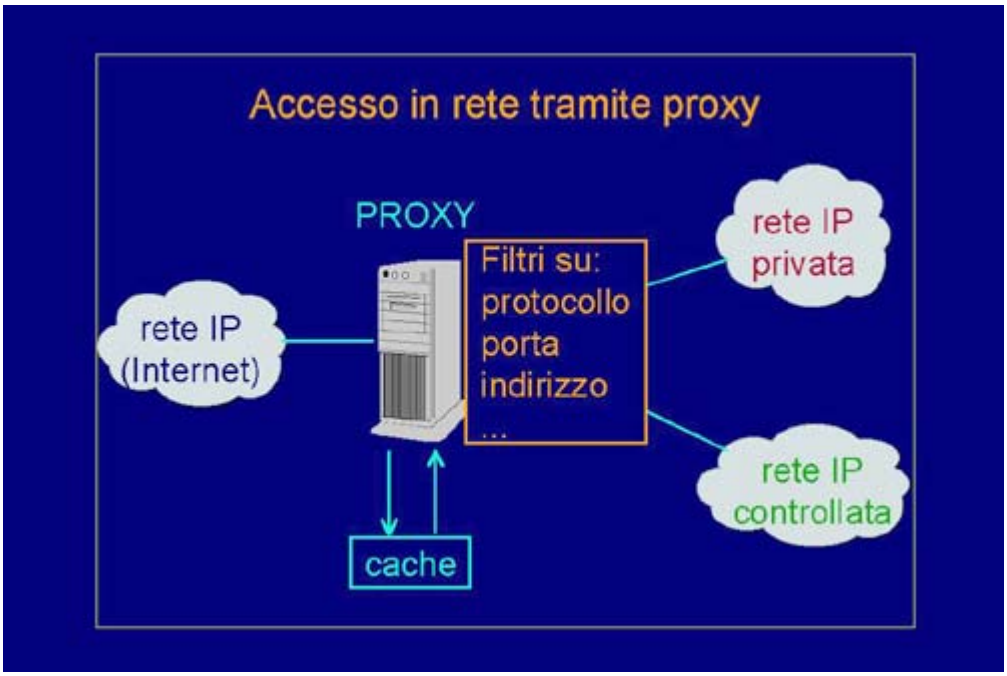
canale di tipo PPP. La prima modalità è quella chiamata PAP (protocollo di accesso tramite password). Il sistema PAP invia lo "user name" e la "password" dell'utente, in chiaro, sul canale. È quindi intuibile che è un sistema fortemente sconsigliabile se qualcuno può avere accesso alla linea telefonica. Ad esempio, un fasullo operaio dei telefoni che finge di correggere un guasto nella centralina o comunque qualcuno che possa attaccarsi alla rete telefonica. Per evitare questo genere di attacchi è consigliabile non usare gli stessi "user name" e "password" che già sfruttati per l'accesso ad altri tipi di sistemi, ma usarne uno specifico solo per l'accesso alla rete. Cosa ancora migliore sarebbe evitare il protocollo PAP utilizzando quello alternativo che si chiama CHAP: è un protocollo che si basa su una sfida (challenge) simmetrica basata sulla "password". Quindi, l'utente ha sempre assegnato uno "user name" e una "password" per entrare in rete, ma la seconda non viene visualizzata e non viene trasmessa attraverso la linea telefonica. Di per se è un protocollo che sarebbe altamente preferibile ma purtroppo la maggior parte degli Internet Service Provider non lo implementano quasi mai e quindi permettono che esista questa debolezza che potrebbe essere facilmente cancellata.

Accesso in rete tramite proxy 1



Nel caso, invece, che il nostro nodo di elaborazione sia già collegato ad una rete locale, tutta questa parte non ha bisogno di essere effettuata, perché normalmente significa che la nostra macchina è autorizzata a collegarsi a tale rete. In questo caso, spesso, per vari motivi viene istituito un filtro di controllo in uscita, quando i nostri dati devono uscire dalla rete locale e navigare all'interno della rete geografica. Questo normalmente viene fatto con quello che si chiama un PROXY. Questo è lo schema di un PROXY. Supponiamo di avere una rete IP esterna e delle reti IP interne. Noi potremmo avere una rete IP privata, in cui non vogliamo che i nostri utenti escano né che siano raggiunti dalla rete internet, oppure una rete IP interna di tipo controllato, in cui vorremmo sottoporre a controllo le azioni che i nostri utenti fanno.

Accesso in rete tramite proxy 2



In entrambi i casi queste reti non escono, non sono collegate direttamente in internet ma sono collegate tramite un PROXY, il quale svolge varie funzionalità. Ad esempio, è in grado di effettuare dei filtri in base al protocollo, alla porta o all'indirizzo sia del mittente che del destinatario dei pacchetti. Inoltre, nel caso che la linea che collega le nostre reti locali con la rete esterna sia a bassa prestazione, per esempio una linea ISDN a 64Kbit al secondo, per motivi di prestazioni molto spesso il PROXY ha anche funzioni di cache. Una volta che ha trasferito dei dati per conto di un utente, se ne fa anche una copia all'interno di una cache locale (dischi locali). Se per caso lo stesso utente o un altro utente della rete interna richiederà gli stessi dati, lui non andrà più a riprenderseli sulla rete geografica ma li estrarrà dalla cache e li fornirà a chi li ha richiesti, ottimizzando in questo modo anche le prestazioni Quindi un PROXI è un sistema che ha una doppia funzionalità: da una parte può essere utilizzato per migliorare le prestazioni di una rete tramite il meccanismo di caching, dall'altra parte può avere una funzionalità di controllo sugli utenti, sui nodi e sui protocolli che possono collegarsi tra la rete interna e la rete geografica.