Internet: dietro le quinte

Oltre a Web, email e chat, Internet offre molti strumenti per orientarsi e risolvere problemi pratici. Scopriamo come usare al meglio risorse accessibili a tutti grazie a software potenti ma semplici

a cura di GABRIELE FAVRIN (gabrielef@publishart.it)

Prima di tutto è necessario approfondire i concetti alla base del funzionamento della Rete. Niente paura, questo non è un trattato tecnico ma solo un'introduzione utile per comprendere al meglio le possibilità offerte da Internet.

Fondamenti di Internet: l'indirizzo IP

Uno dei cardini della Rete è l'indirizzo IP, ovvero un insieme di quattro valori fra 0 e 255 separati da punti, ad esempio 212.17.220.131. Questo è l'indirizzo IP del sito "www.programmazione.it". Sulla corrispondenza fra nome e numero torneremo più avanti, per ora ci basta sapere che quando visitiamo quel sito ci colleghiamo al relativo IP.

Ogni sistema collegato ad una rete in tecnologia TCP/IP (Internet ma anche le reti aziendale o casalinghe) ha un proprio IP univoco, diverso cioè da tutti gli altri presenti nella stessa rete. L'IP è paragonabile ad un numero telefonico e svolge la stessa funzione, consente cioè il collegamento diretto ad un sistema specifico. Tutto in Rete si basa sull'IP, anche se generalmente non lo vediamo. Quando navighiamo sul Web, preleviamo la posta o scarichiamo un file via FTP, stiamo sempre e comunque effettuando collegamenti ad indirizzi IP.

Gli IP si dividono in due categorie: IP pubblici ed IP privati. Normalmente gli utenti Internet hanno tutti un IP pubblico, ovvero raggiungibile da chiunque. Ne consegue che se un utente installa un server Web sul proprio computer chi conosce il suo IP potrà

Tutte le informazioni sull'intestatario di un IP sono a portata di mano grazie all'interfaccia Web dei tre registri whois:
http://www.ripe.net/db/whois/whois.html
http://www.arin.net/whois/index.html
http://www.apnic.net/apnic-bin/whois.pl

collegarsi direttamente a lui. Al contrario gli indirizzi IP privati non sono raggiungibili da Internet e vengono usati per collegare fra loro macchine appartenenti a reti locali.

Mentre chi gestisce una rete locale può scegliere arbitrariamente gli IP di cui servirsi, ovviamente entro i limiti degli indirizzi destinati a tale scopo, l'assegnazione degli IP Internet pubblici spetta ad alcune organizzazioni internazionali che operano secondo precise regole tese ad evitare sprechi e coordinare l'interconnessione fra le diverse reti. Nel dettaglio, ogni azienda può richiedere gli indirizzi di cui ha effettivamente bisogno per svolgere la propria attività. Chi offre servizi Web dispone di uno o più IP per le proprie macchine, mentre i grandi provider generalmente riservano quantità di IP molto ampie e diventano a loro volta punti di riferimento per chi necessità di IP. Per esempio tutti gli IP che iniziano per 62.98 e 212.141 sono di Wind. Considerando che un indirizzo è composto da quattro valori e che ogni valore va da 0 a 255, ne consegue che Wind dispone per i propri clienti (privati e aziende) di migliaia di possibili indirizzi.

Per ogni indirizzo pubblico vengono inserite diverse informazioni all'interno di uno speciale registro denominato senplicemente whois ("chi è"). Tali informazioni identificano l'azienda che ha riservato quell'indirizzo ed i responsabili da contattare in caso di problemi tecnici o amministrativi. Il registro whois è consultabile da chiunque effettuando un collegamento telnet, tramite Web o con un software apposito.

Ricapitolando: a tutti i sistemi accessibili da Internet corrisponde almeno un indirizzo IP pubblico. Gli indirizzi IP sono assegnati da apposite autorità di rete che mantengono un registro tramite cui è possibile sapere a chi appartiene l'indirizzo, chi contattare in caso di problemi e spesso anche diverse altre informazioni fra le quali la località in cui si trova il sistema e l'uso a cui è destinato.

Ancora sulle basi di Internet: i domini

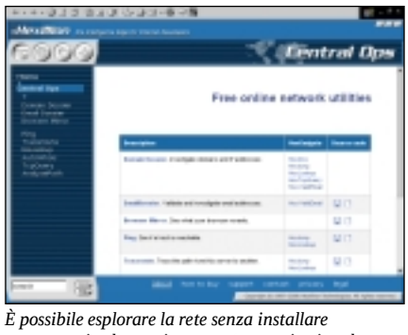
Sinora abbiamo parlato di numeri, eppure quando navighiamo non abbiamo quasi mai a che fare con gli IP: tutto ciò che vediamo sono nomi come "www.programmazione.it" o "www.cnn.com". Lo scopo di tali nomi è quello di semplificare l'accesso alle risorse da parte degli... umani. Ciò vale sia per una rete personale composta da due o tre macchine (ad esempio "pc1", "pc2", "mac1"), sia per Internet. Tanto per chiarire: per leggere le ultime notizie quale sito vi viene in mente? "www.cnn.com" oppure "64.236.24.4"? Eppure sono esattamente la stessa cosa!

Agli albori di Internet, quando la rete si "estendeva" attraverso pochi istituti di ricerca, tutti i sistemi collegati scambiavano quotidianamente le informazioni sulle corrispondenze IP/nome condividendo un file denominato "hosts". Con la progressiva crescita di Internet l'uso del solo file hosts è diventato poco pratico, visto che ogni sistema doveva immagazzinare e condividere una mole di dati sempre maggiore. Si è così giunti alla creazione di una nuova infrastruttura, il Domain Name Server (DNS), relegando il file hosta all'uso nel contesto delle reti locali (lo si può tuttora trovare in quasi tutti i sistemi operativi).

Chiunque si colleghi a Internet ha sentito parlare dei DNS e tutti, durante la navigazione, se ne servono. Il software che gestisce il protocollo TCP/IP può aprire collegamenti solo con indirizzi numerici, quindi per ogni accesso ad un sito viene chiesto al server DNS a quale indirizzo IP corrisponda quel nome. Esiste una rete mondiale di server DNS che scambia costantemente i dati secondo precisi protocolli e scadenze.

I DNS, come dice il nome, gestiscono i "nomi a dominio" o più semplicemente domini. Ogni dominio è strutturato secondo una precisa gerarchia che vede differenti organizzazioni responsabili della gestione delle diverse componenti del dominio stesso. Prendiamo come esempio il solito "www.programmazione.it" e scomponiamolo: il dominio principale è ".it" ed è un dominio di primo livello, per l'esattezza quello assegnato all'Italia e gestito autonomamente da un'apposita autorità (il NIC, http://www.nic.it). Ci sono parecchi altri domini di primo livello: i famosi ".com" (domini commerciali), ".org" (organizzazioni no-profit), ".edu" (isituazioni accademiche americane), ecc. Esistono poi domini per quasi tutte le nazioni del mondo.

Tornando al nostro esempio, dopo il suffisso ".it" troviamo "programmazione", il cosiddetto "dominio di secondo livello". Tale tipologia di domini può essere registrata da chiunque rivolgendosi ad uno dei numerosi "registar" accreditati presso l'ICANN. Il "www", infine, è un sottodominio impostato arbitrariamente dal proprietario del dominio. Una caratteristica interessante dei sottodomini è che possono essere usati per indicare macchine differenti all'interno di uno stesso



È possibile esplorare la rete senza installare programmi sul proprio computer grazie ai tool gratuiti offerti sul sito ***http://www.hexillion.com/utilities/***

CHI SEI?

Prima o poi sarà capitato a tutti: durante la navigazione il firewall insorge gridando che qualcuno sta cercando di penetrare nel nostro computer. Come unico indizio ci viene fornito un indirizzo IP. Chi è? Come possiamo dirgli di smettere? Nella maggior parte dei casi, almeno per quanto riguarda gli utenti privati, queste segnalazioni riguardano banali "scan port", ossia tentativi di vedere se un computer ha delle "falle" da cui entrare. Lo "scan port" in sè non è un atto criminale, anzi può essere utile per controllare la sicurezza dei propri computer o di quelli di amici. Il problema nasce quando qualcuno ne abusa, effettuandolo su indirizzi altrui, magari insistentemente. In ogni caso abbiamo il diritto di capire da dove proviene ed eventualmente esprimere il nostro disappunto al provider la cui rete è usata per queste azioni. Per farlo dobbiamo innanzitutto prendere nota dell'indirizzo IP da cui parte il tentativo di accesso ed interrogare i tre registri whois esistenti: RIPE per gli indirizzi europei, mediorientali e nordafricani, ARIN per il contenente americano ed il sud Africa e APNIC per l'Asia. Tali registri sono accessibili anche via Web. Nel caso all'IP corrisponda un dominio è possibile reperire informazioni anche interrogando in merito i DNS tramite lo strumento nslookup.
Se queste operazioni appaiono troppo macchinose ci si può appoggiare ad un sito Web come **http://www.hexillion.com/utilities/** oppure ad un software apposito, ad esempio l'ottimo Visual Route. Così facendo sarà il computer a "faticare" per noi, andando a reperire tutte le informazioni possibili dalle varie fonti. Dai risultati di queste analisi spesso è possibile capire con chi si ha a che fare. Gli amministratori di rete più solerti inseriscono nei registri whois informazioni sulla finalità di uno specifico indirizzo. Con un po' di allenamento si impara a distinguere rapidamente fra connessioni analogiche (le cosiddette "dial up"), xDSL o sistemi aziendali sempre attivi.
Una volta scoperto a chi appartiene l'IP del disturbatore il passo successivo sarà l'invio di una email al servizio di segnalazione abusi del relativo provider. Se abbiamo a che fare con l'utente di un provider sarà sufficiente inoltrare il messaggio ai gestori del dominio. Al contrario, se l'analisi del registro whois fa pensare che l'"attacco" parta da un server aziendale, per sicurezza sarà bene contattare anche i proprietari dell'IP o in generale chi fornisce connettività a quello specifico indirizzo. Limitandoci a scrivere all'eventuale dominio collegato all'indirizzo rischieremmo infatti di fare un buco nell'acqua: se il comportamento scorretto parte proprio dall'amministratore del server oppure se la macchina è caduta in mano a pirati informatici è improbabile che la nostra email venga presa in considerazione. Ma torniamoo al caso più comune, quello cioè di un utente che si "diverte" a curiosare fra gli indirizzi altrui. Non dobbiamo aspettarci che il provider ci fornisca informazioni su chi ci ha disturbati: la legge sulla privacy lo vieta a meno che a chiederle non sia la magistratura nell'ambito di una inchiesta. In ogni caso è probabile che la persona riceva, direttamente dal provider, una diffida al proseguire azioni ritenute di disturbo.
In effetti, e visti i risultati, attuare tutta questa procedura per un banale "scan port" forse è eccessivo, visto poi che il firewall che lo ha segnalato ci protegge anche dai possibili rischi. D'altra parte con lo stesso sistema è possibile capire a chi segnalare un utente che in chat si comporta in maniera scorretta nei nostri confronti. Naturalmente non ci riferiamo alle comuni zuffe ma a minacce o ad altri comportamenti punibili dal codice penale. L'utilizzo intenso dei registri whois e di nslookup è anche una pratica comune per chi si occupa di lotta allo spam, tanto che sull'argomento esiste un'articolata letteratura. Rimandiamo gli interessati al sito **http://www.collinelli.net/antispam/**.

L'IMPORTANZA DEL... PING!

Situazione tipo: ci hanno appena attivato una fiammante linea ADSL, finalmente possiamo restare collegati per tutto il tempo che vogliamo. Da bravi estimatori dei vari Quake3, Unreal, ecc, come resistere al fascino di lanciarci in una sfrenata sfida online? Un amico straniero, collegato ancora con il modem analogico, ci invita su un non meglio identificato server finlandese che promette faville. Trenta secondi e senza neppure accorgerci del perchè ci ritroviamo colpiti! Una, due, dieci volte. Perchè? Eppure la nostra linea è molto più veloce di quella dell'avversario!
Qual è il mistero che può annullare la differenza di prestazioni fra ADSL e modem analogico? Cosa può rallentare una partita a Quake3, una transazione o una chat? La risposta si chiama ping, o per l'esattezza tempo di risposta al ping. Come già detto, il valore restituito dal ping indica il tempo intercorso fra la spedizione del nostro messaggio e la ricezione della risposta da parte del server. Più alto è il tempo di risposta al ping più lenta sarà l'interazione fra noi e il server. Nel caso dei giochi online, con l'evoluzione del fenomeno, i programmatori hanno lavorato per ridurre al minimo la quntità di dati scambiati puntando nel contempo tutto sui tempi di risposta. Per fare un esempio concreto: quando in Quake3 spariamo ad un avversario il gioco invia la nostra azione al server e attende risposta. Vedremo se il colpo è andato a segno solo quando il server invierà la relativa informazione. Lo stesso vale per ogni azione: dal camminare al correre al raccogliere un'arma... È chiaro quindi, tornando all'esempio, che se il nostro avversario ha un tempo di risposta al ping più basso del nostro, potrà muoversi molto più agevolmente di noi anche se la sua linea è più lenta. È per questo che il comando ping rappresenta uno strumento diagnostico tutt'altro che banale o riservato ai soli amministratori di rete. Servirsi regolarmente del ping per scegliere il server a cui collegarsi, per un gioco ma anche per applicazioni più serie, permette di operare nelle condizioni migliori.
Ma cosa determina un tempo di ping alto? Non è solo un problema di rete congestionata o di lunghe tratte fra noi e il server che ci interessa. Anche il tipo di collegamento a Internet influisce sui tempi di risposta. Attualmente le connessioni ISDN hanno il tempo di ping più basso (ecco perchè molti videogiocatori se ne servono, a fronte degli alti costi). Seguono le ADSL e come fanalino di cosa i modem analogici.
Per l'ADSL comunque il problema è più complesso: in Italia vengono attivate quasi esclusivamente connessioni in modalità "interleaved", una soluzione che prevede maggiori controlli sui dati in transito per compensare la qualità spesso pessima dei cavi telefonici. Purtroppo ciò si traduce anche in tempi di ping nettamente più elevati. Esiste anche una modalità denominata "fast" che, a fronte di minori controlli, offre tempi di ping molto bassi. Attualmente nessun provider la offre, ma pare che Telecom Italia la stia sperimentando su alcune nuove attivazioni del suo servizio Alice.
In ogni caso il fattore discriminante resta il server remoto: più è lontano ed è lento, minori prestazioni possiamo aspettarci per attività fortemente interattive. Un motivo in più per avere sempre il comando ping a portata di mano!

dominio. Si possono quindi avere indirizzi come "www.programmazione.it" e "ql.programmazione.it" che danno accesso a macchine diverse, anche a livello di IP.

I DNS non sono utili soltanto per la mera navigazione. Per ogni dominio, infatti, offrono una serie di informazioni aggiuntive, come la scadenza dello stesso, l'ultimo aggiornamento, i sottodomini registrati, le macchine impiegate per gestirli e in taluni casi anche le coordinate geografiche di tali sistemi. Anche il registro whois, di cui abbiamo parlato riguardo agli IP, contiene informazioni sui domini. Purtroppo a seguito della liberarizzazione della vendita dei domini molte aziende hanno creato i propri archivi invece di utilizzarne uno centrale, finendo per rendere più difficoltosa la ricerca manuale di informazioni. Fortunatamente i programmi più recenti sanno accedere ai diversi archivi in maniera automatica.

È importante comprendere che dominio ed indirizzo IP possono non appartenere alla stessa entità. Chiunque (aziende, associazioni, privati...) può registrare un dominio, diventandone proprietario a tutti gli effetti, con tanto di dati anagrafici inseriti nel registro whois. Gli indirizzi IP, al contrario, sono generalmente assegnati ad un fornitore di connettività che li attribuisce ai propri clienti finali (che si tratti di utenti connessi via modem, aziende che necessitano di collegamenti dedicati, società di Web hosting, ecc), mantenendone però la proprietà.

Ecco quindi perchè, interrogando il registro whois del RIPE e immettendo prima l'IP e poi il dominio di programmazione.it, si otterranno risultati differenti: dal dominio possiamo conoscere "chi c'è" dietro a quel nome, mentre dall'IP è possibile sapere quale azienda fornisce loro la connettività.

Alcuni suggerimenti su come utilizzare le informazioni reperibili in merito ad IP e domini sono proposte negli approfondimenti di queste pagine.

Funzionamento (e malfunzionamento) della rete

Così come nei sistemi casalinghi, anche in Rete, a volte, si verificano dei guasti e alcuni computer smettono di funzionare. Può trattarsi di un server Web o di un computer di supporto a qualche attività. Quando ciò avviene è necessario capirlo rapidamente, tanto per gli umani, quanto per altri computer eventualmente collegati al sistema andato fuori uso. Lo strumento diagnostico principale, disponibile su tutti i sistemi operativi, è il comando ping. Scrivendo in linea di comando (su Windows è necessario aprire una sessione DOS o servirsi di un client grafico) "ping 212.17.220.131" otterremo una serie di messaggi a conferma che il server che risponde all'IP indicato è funzionante.

Ma come funziona il ping? Se leggendo il termine "ping" avete pensato al ping pong siete sulla buona strada: il ping invia un messaggio ad un server e aspetta una risposta, detta proprio "pong". Se la risposta non arriva entro un preciso lasso di tempo significa che la macchina non sta funzionando. Se arriva è possibile anche calcolare il tempo intercorso fra l'invio del ping e la ricezione del pong. Tale dato fornisce informazioni utili sulle prestazioni che ci si possono aspettare da quel server. Nel riquadro "L'importanza del ping" è spiegato come il tempo di risposta al ping si riflette su varie attività online.

Va detto che oggigiorno, per esigenze di sicurezza, non tutte le macchine rispondono al ping. Questo può creare dei problemi agli utenti che desiderano semplicemente valutare la bontà di una connessione o verificare se un proprio interlocutore è ancora online anche se non risponde in chat. D'altro canto il ping può essere strumentalizzato al fine di danneggiare un sistema altrui. Ecco quindi che certe scelte, penalizzanti per alcuni, possono rendersi necessarie, almeno da parte degli amministratori di rete.

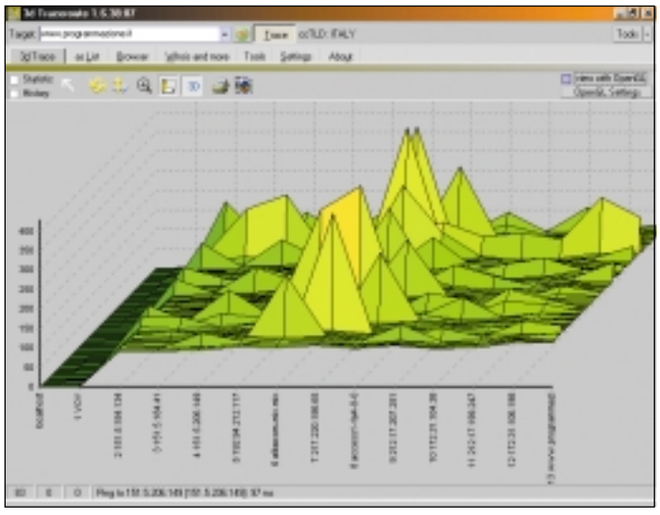
A proposito di sicurezza, la leggenda vuole che il ping nasca come strumento per identificare rapidamente i sistemi sopravissuti ad un attacco nucleare. Bisogna infatti ricordare che Internet poggia sulle basi poste da ARPANET, (Advanced Research Projects Agency Network), un progetto creato in ambito militare alla fine degli anni sessanta, quindi in piena guerra fredda.

Il fatto che la Rete sia stata pensata per sopravvivere ad attacchi dalla capacità distruttiva devastante anche in termini di risorse informatiche, ci porta a compiere un altro passo importante nella comprensione dei meccanismi alla base del suo funzionamento. Vedremo ora come avviene la comunicazione fra i sistemi in rete.

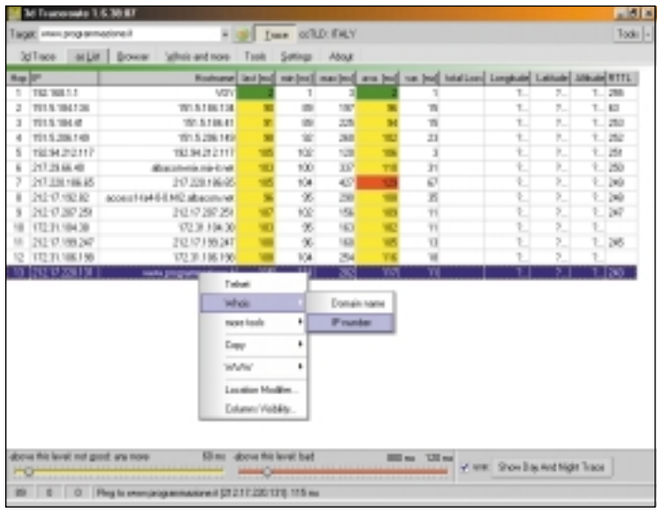
Osservando una rete casalinga composta da due o tre computer potremmo pensare che la comunicazione fra le diverse macchine sia sempre diretta. Ma se accediamo al sito "www.cnn.com" stiamo dialogando direttamente con il computer della CNN? Niente affatto. I nostri dati, sia in ricezione che in invio, vengono spezzettati ed incapsulati all'interno di "pacchetti" che sono poi veicolati attraverso un gran numero di altre macchine.

Generalmente il percorso è questo: la richiesta di visionare l'indice del sito CNN parte dal nostro computer e raggiunge il router (smistatore) locale del provider al quale siamo collegati. Da lì viene trasmessa ad altri smistatori interni alla rete del provider, fino ad uscire sulle grandi (e veloci) linee europee che conducono alle connessioni internazionali, realizzate tramite cavi sottomarini stesi a grandi profondità negli oceani. Superato il mare la nostra richiesta attraversa tutta la rete del fornitore di connettività della CNN, fino ad approdare al server di destinazione, che risponderà inviandoci il flusso di dati (sempre suddiviso in pacchetti), che percorrerà la strada inversa. Questa naturalmente è una semplificazione che non tiene conto di numerose possibili eccezioni, ad esempio connessioni privilegiate fra provider, ecc.

Questo sistema di comunicazione, solo apparentemente complesso, ha il pregio di sopravvivere ed adeguarsi sia alla crescita esponenziale della rete, sia ad improvvisi problemi tecnici. Senza arrivare ad un disastro nucleare, può capitare che una o più macchine cessino di funzionare o diventino irraggiungibili a causa di guasti alle linee, per



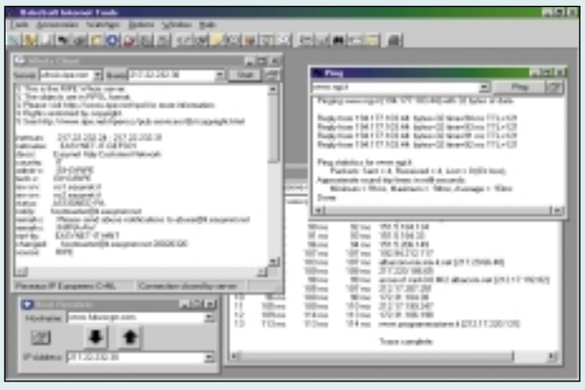
Un traceroute inusuale proposto dal programma 3DTraceroute. L'immagine è completamente navigabile e ruotabile!



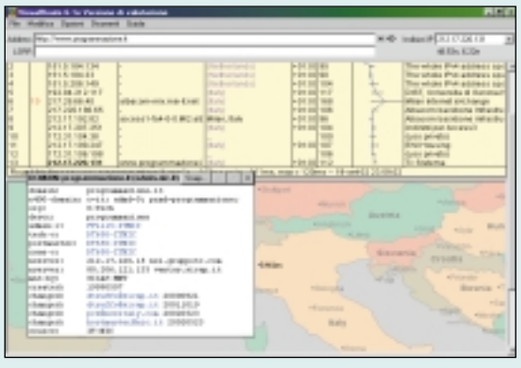
... lo stesso traceroute in una forma piu' riconoscibile. Notare il menu contestuale attivabile su qualsiasi host.

PROGRAMMI SEGNALATI

Come accennato, i principali programmi necessari per analizzare la rete sono già disponibili in tutti i sistemi operativi.
Spesso però si tratta di programmi da utilizzare tramite linea di comando (una shell su Linux e MAC OS X oppure una sessione DOS su Windows 9x) inserendo parametri oscuri e reperendo autonomamente i server da interrogare. Per ovviare al problema negli anni sono stati sviluppati altri prodotti, dai semplici "front end" a vere e proprie implementazioni grafiche. Fra i titoli più interessanti c'è senza dubbio McAfee Visual Trace per Windows, versione commerciale del famoso shareware "NeoTrace".
La caratteristica saliente del prodotto è la visualizzazione del traceroute sul planisfero! In pratica è possibile "vedere" sia dove si trova un server, sia il percorso che i nostri pacchetti fanno per arrivarci, con relativi tempi di ping.
http://www.neoworx.com/. Un altro prodotto simile è Visual Route, disponibile per ben cinque sistemi operativi: Windows, Solaris, Linux, FreeBSD e MAC OS X. Visual Route è caratterizzato da un'ampia interfaccia (troppo ampia per uno schermo da 800 x 600!) divisa in due: nella parte superiore trova spazio la tabella del traceroute, mentre in quella inferiore c'è il planisfero zoomabile, pur se non con la stessa facilità di McAfee Visual Trace. Il pregio di questo programma è l'accessibilità dei dati: basta cliccare sui dati proposti a video per ottenere maggiori informazioni senza dover scavare fra whois, nslookup e quant'altro. Un clic sul dominio e sapremo a chi appartiene, uno sulla colonna "rete" e conosceremo il proprietario dell'IP e via dicendo...
http://www.visualware.com.
Altro titolo molto interessante, anche perchè gratuito, è 3DTraceroute (per tutte le versioni di Windows). Si tratta di un programma in grado di visualizzare il traceroute come grafico tridimensionale. 3DTraceroute offre anche ping, whois, nslookup e molto altro. Sarebbe perfetto se non fosse per l'interfaccia grafica un pò troppo personalizzata scelta dall'autore. Bella ma può anche disorientare...
http://www.hlembke.de/prod/3dtraceroute/. Meno spettacolare dei prodotti citati finora ma altrettanto comoda è la suite "Internet Tools" di OstroSoft (**http://www.ostrosoft.com/ostronet.html**). Si tratta di un insieme di funzioni utili, da ping a traceroute, da whois a nslookup, ecc. Il tutto integrato in un unico programma che offre la classica interfaccia multifinestra di Windows.
Un altro prodotto degno di nota per i sistemi Windows è la suite Essential Net Tools che offre anche funzioni specifiche per chi utilizza la condivisione di file e stampanti all'interno di una rete locale.
http://www.tamos.com.
Per gli utenti Macintosh segnaliamo AGNetTools e WhatRoute.
Entrambi offrono le funzioni più importanti: ping, traceroute, informazioni sui domini, ecc. Il primo è shareware ed è stato creato appositamente per MAC OS classic, mentre il secondo, gratuito, funziona anche su MAC OS X.
Per i sistemi Unix esiste un gran numero di programmi per l'analisi della rete. Purtroppo molto di questo software può essere usato solo da linea di comando.
Fra i programmi dotati di interfaccia grafica segnaliamo X-Traceroute (**http://www.dtek.chalmers.se/~d3august/xt/index.html**) che visualizza il traceroute su un'immagine rotante della terra: forse non proprio pratico ma certamente spettacolare!
Altri titoli validi sono KTroute e Gnetutil.KTroute, per l'ambiente grafico KDE, è un'implementazione di traceroute caratterizzata dalla presenza di opzioni avanzate che normalmente passano inosservate all'utente medio che usa il programma da linea di comando. **http://sourceforge.net/projects/ktroute/**.
Gnetutil, infine, è un semplice frontend per gli utenti dell'ambiente Gnome che consente di utilizzare i comandi traceroute, host, ping e finger tramite interfaccia grafica. **http://savage.iut-blagnac.fr/projets/developpement/gnetutil/**.
Ricordiamo che i programmi citati, quando possibile, sono stati inseriti nel CD-ROM allegato alla rivista.



La suite Internet Tools di OstroSoft al lavoro: ping, traceroute, whois, ecc, tutto a portata di mano e comodamente raggruppato nella finestra del programma.

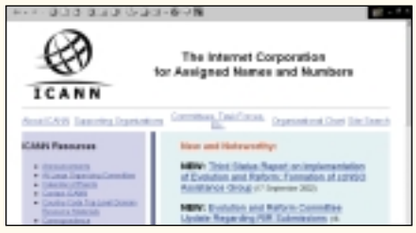


Il traceroute secondo Visual Route con in primo piano le informazioni sul dominio del server analizzato. La mappa in basso non mostra il percorso perchè raramente gli amministratori di rete italiani immettono le informazioni geografiche nei registri whois.

RISORSE

1 Il RIPE è uno dei tre enti che assegnano gli indirizzi IP. Dal sito **http://www.ripe.net** si possono conoscere molti dettagli circa l'organizzazione della rete e le procedure di assegnazione di un indirizzo in Europa.

2 IANA (Internet Assigned Numbers Authority) è l'organismo che coordina e documenta le procedure di assegnazione domini ed indirizzi a livello dell'intera Rete. Il sito **http://www.iana.org** è una vera miniera di informazioni per chiunque sia interessato all'argomento.



3 L'ICANN (Internet Corporation for Assigned Names and Numbers) è l'organizzazione responsabile della definizione dei domini di primo livello (".com", ".net", ".org", ".info", ecc). Per sapere come opera e quali sono i domini oggi disponibili e quelli previsti per il futuro si può visitare **http://www.icann.org**.

4 IETF è l'acronimo di Internet Engineering Task Force. Si tratta di una comunità internazionale di sviluppatori e ricercatori che opera per l'evoluzione e lo sviluppo di Internet. Se leggendo queste pagine è nato in voi un maggiore interesse per il funzionamento della Rete, sul sito **http://www.ietf.org** troverete, fra le altre cose, gli "RFC", ossia la "bibbia" della Rete.

5 In queste pagine abbiamo accennato ad ARPANET, la rete militare antenata della Internet moderna. Per sapere come è nata e conoscere quindi le origini della Rete che tutti noi usiamo si può consultare l'interessante storia narrata su **http://www.dei.isep.ipp.pt/docs/arpa.html**.

6 Per chi proprio non mastica l'inglese un sito tutto italiano (**http://www.nic.it**) dove trovare le regole di assegnazione dei domini ".it" e molto altro materiale sulla Rete.

esempio dopo una calamità naturale. Bene, i vari smistatori sono in grado di cercare tratte alternative qualora quella utilizzata diventi inservibile. Ciò significa che sarà quasi sempre possibile accedere ad un sito, anche se il suo collegamento principale è venuto meno.

Noi in quanto utenti finali non percepiamo il passaggio dei dati attraverso differenti sistemi, nè possiamo intervenire sul percorso dei nostri pacchetti. Tuttavia ci è posssibile verificarlo, per valutare la qualità dei collegamenti del nostro provider o per cercare di capire come mai, nonostante la nostra fiammante linea ADSL, un sito vada così lento. Per compiere questa operazioni si utilizza un programma di nome traceroute, presente di serie su quasi tutti i sistemi operativi, seppur in forma testuale. Scrivendo il comando "traceroute www.programmazione.it" ("tracert" su Windows 95/98), ci verrà mostrato il percorso fra noi ed il server specificato. Ma come funziona? Traceroute (letteralmente "traccia il percorso") utilizza un metodo piuttosto ingegnoso per identificare i sistemi attraverso cui passano i nostri dati. Tutti i pacchetti trasmessi in rete affiancano al contenuto vero e proprio (parti di pagine Web, messaggi email, ecc), alcune informazioni di servizio fra cui il cosiddetto TTL ("Time To Live", cioè tempo di sopravvivenza). Si tratta di un valore che viene scalato di 1 ad ogni passaggio attraverso un sistema intermedio.

In certe condizioni può capitare che due o più smistatori inizino a palleggiarsi un pacchetto se non sanno più dove spedirlo, magari a causa di una configurazione errata o di un guasto improvviso e non ancora rilevato al sistema di destinazione. Se non esistesse il TTL il pacchetto continuerebbe a "rimbalzare" a tempo indeterminato, impegnando le macchine e lasciando l'utente in attesa di una risposta destinata a non arrivare mai. Grazie al TTL, invece, dopo un certo numero di passaggi il sistema che si trova in mano il pacchetto può capire che è tempo di eliminarlo invece di instradarlo nuovamente. In tal caso viene anche inviata una "notifica" al mittente in cui lo si informa che l'IP con cui cercava di comunicare è irraggiungibile.

Ma cosa c'entra questo con il traceroute? Semplicemente, traceroute cerca di collegarsi al sistema specificato utilizzando pacchetti di cui manipola il valore di TTL per accorciarne la vita. Il primo tentativo avviene con TTL pari a 1: lo smistatore che lo riceve annulla il pacchetto e ne informa il mittente, ossia il nostro traceroute, che quindi visualizza il nome del primo sistema intermedio. Poi traceroute prosegue, inviando altri pacchetti cui a mano a mano aumenta la durata della vita (ossia il numero massimo di sistemi attraverso cui possono passare), fino ad arrivare al server di destinazione.

Analogamente al ping anche traceroute mostra il tempo intercorso fra l'invio del pacchetto e la sua riecezione da parte di una macchina, solo che in questo caso risulta più evidente il tempo che il pacchetto ha passato viaggiando tra i vari sistemi intermedi. Un tempo di risposta elevato su un determinato smistatore aiuta a individuare i "colli di bottiglia" e capire se la colpa di una navigazione lenta è della rete del nostro provider, di una tratta internazionale o dei sistemi a cui è collegato il server che ci interessa raggiungere.

Talvolta può capitare che il percorso verso un server cambi da un minuto all'altro. Quando questo avviene significa che uno smistatore ha rilevato un problema e ha attivato una "rotta" alternativa. Meraviglie di Internet!

Conclusioni

Il funzionamento di Internet è molto complesso e con questo articolo non pretendiamo certo di illustrarlo completamente.

Tuttavia riteniamo che conoscere concetti come l'IP o il dominio ed essere in grado di reperire informazioni aggiuntive sui vari sistemi consenta di risolvere al meglio i vari problemi che si possono incontrare durante la navigazione, nonchè di soddisfare qualche curiosità...