- DNS

Il DNS, ovvero Domain Name System è il servizio che permette di associare un indirizzo IP ad una URL (Uniform Resource Locator), l'indirizzo web ad esempio richiedendolo ai server specializzati che gestiscono il database distribuito.

Se il server interrogato non ha l'informazione richiesta è comunque in contatto con altri DNS Server che possono fornirla.

In Linux la configurazione di quale DNS server interrogare viene mantenuta nel file /etc/resolv.conf che ha questa struttura:

paolo@kubuntu:~$ cat /etc/resolv.con

fsearch localdomainnameserver 151.99.125.1nameserver 212.216.112.112

- File HOSTS

/etc/hosts è un semplice file di testo che contiene nomi di host ed indirizzi.

Quando un computer cerca di connettersi ad un altro, prima di effettuare una richiesta ad un server DNS cerca nel file /etc/hosts se ha già l'informazioneche gli serve.

Questo può servire per assegnare degli alias a livello locale, per indirizzare a computer locali connessi in LAN, per memorizzare gli indirizzi usati di frequente riducendo la necessità di effettuare richieste esterne, oppure per esigenze di sicurezza.

Ad esempio per bloccare un sito porno www.sitoporno.com si può aggiungere al file hosts la seguente riga:

127.0.0.1 www.sitoporno.com

- INTERFACES

Il file di testo /etc/network/interfaces contiene la configurazione della rete.

Se viene impostato, al successivo riavvio del pc la rete sarà configurata automaticamente.

Dopo avere modificato manualmente la configurazione, per applicarla lanciare il comando:# /etc/init.d/networking restart

- DHCP

Oltre che manualmente è possibile effettuare la configurazione della rete in modo automatico mediante i servizi offerti da server DHCP (Dynamic Host Configuration Protocol) impostando correttamente il file /etc/network/interface oppure tramite il comando dhclient che invia in modalità broadcast una richiesta alla quale il server risponde con l'offerta di un indirizzo IP.

Se l'offerta viene accettata il pc si configura automaticamente anche con gli altri parametri previsti (DNS server primario e secondario, gateway, proxy)

- Configurare Modem ALICE

Per configurare una connessione tramite modem ADSL con scheda ethernet si usa il programma pppoeconf.

Dopo aver configurato la scheda di rete, aprite una shell e lanciate il comando: sudo pppoeconf

Basta rispondere alle domande (scheda Ethernet da usare, nome utente e password, abilitazione della connessione all'avvio) per configurare la connessione, attiva di default.

Per disabilitare e riattivare al connessione usare rispettivamente i comandi: poff nome-connessione pon nome-connessione

- PING

Ping è un programma disponibile sui principali sistemi operativi che misura il tempo, espresso in millisecondi, impiegato da uno o più pacchetti ICMP (Internet Control Message Protocol) a raggiungere un altro computer o server in rete (sia essa Internet o LAN) ed a ritornare indietro all'origine.

E' utilizzato per effettuare test diagnostici delle connessioni.

Tecnicamente ping invia un pacchetto ICMP di echo request e rimane in attesa di un pacchetto ICMP di echo response in risposta.

Solitamente infatti la parte di sistema operativo dedicata alla gestione delle reti (stack di rete) è programmata per rispondere automaticamente con un pacchetto echo response alla ricezione di un pacchetto di echo request, anche se non è infrequente trovare server che non rispondono al ping per presunti motivi di sicurezza. (attacco DDOS)

- TRACEROUTE

Traceroute è il programma che permette di individuare il percorso che i pacchetti di rete effettuano per giungere a destinazione.

Permette di effettuare trobleshooting ed analisi di rete.

paolo@kubuntu:~$ traceroute www.solution.it

- NETSTAT

In ogni pc sono attivi servizi che utilizzano, sia in entrata che in uscita, delle connessioni per comunicare con altri host, od anche solo per comunicare fra processi locali.

Per avere lo stato delle connessioni instaurate si utilizza il comando netstat che utilizzato con le opportune opzioni da tutte le informazioni necessarie.

paolo@kubuntu:~$ netstat -naptu

- TCPDUMP

Tcpdump è un programma per il debug delle reti di computer che funziona sotto riga di comando. Consente all'utente di intercettare e visualizzare TCP/IP e altri pacchetti che vengono trasmessi o ricevuti attraverso la rete.

paolo@kubuntu:~$ sudo tcpdump -i eth0

- WHOIS

Whois è un comando che interroga il database dell'autorità che assegna i nomi di dominio per mostrare le informazioni relative.

Serve ad identificare il proprietario di un sito o la sottorete assegnata.

E' un comando solitamente utilizzato in fase di analisi di una rete.

paolo@kubuntu:~$ whois www.solution.it

- wireless

Per configurare una scheda di rete wireless servono alcune informazioni in più rispetto a quanto serva per una scheda ethernet.

Oltre ad indirizzo IP, netmask, gateway, server DNS si deve conoscere anche il nome della rete wireless (ESSID) e la eventuale chiave WEP/WPA. Il comando iwconfig senza parametri visualizza le schede di rete wireless installate nel sistema.

- iwconfig

Il comando iwconfig serve a configurare una scheda wireless correttamente installata.

I comandi vanno dati con i privilegi di root.

ifup [nome scheda]

iwconfig wlan0 mode managed

iwconfig wlan0 channel 11 (se necessario impostare un canale)

iwconfig wlan0 essid [networkname]

iwconfig wlan0 key [chiave Hex]

A questo punto va impostata la configurazione dell'indirizzo IP, del gateway e del server DNS come già visto per unascheda ethernet.

- sicurezza wi-fi

La rete Wi-Fi di per se è insicura dato che gli apparati escono di fabbrica senza le misure di sicurezza attivate e che raramente gli utenti conoscono i rischi e tanto meno le semplici operazioni per porvi almeno in parte rimedio.

Per rendere sicura una rete wireless esistono varie tecniche, nessuna di esse è sicura al 100% ma possono dare un certo grado di protezione soprattutto se combinate fra loro.

- Cifratura WEP:

Wired Equivalent Privacy 64 o 128 bit, praticamente ormai inutile in quanto facilmente craccabile in pochi minuti, può servire solo a tenere

fuori dalla vostra rete utenti casuali

- Cifratura WPA - WPS2 PSK:

Wi-Fi Protected Access. Più robusta della WEP, offre buona protezione se le chiavi sono protette bene.

- Cifratura LEAP:

sistema proprietario di cifratura, non offre buona protezione ma è meglio di WEP

- Controllo del MAC:

In aggiunta all'autenticazione del client mediante chiave crittografata si può impostare l'access point in modo che riconosca solo le schede abilitate tramite il loro indirizzo MAC. Purtroppo il MAC è¨ spoofabile...

- Separazione della rete wireless:

in una rete locale è meglio tenere l'access point in una sottorete separata da quella utilizzata per il lavoro. Una eventuale compromissione non renderà immediatamente disponibile l'accesso alla rete ed ai servizi principali.

- NO al DHCP:

non rendete facili le cose ad un attaccante fornendogli una comoda configurazione automatica

- SSID nascosto:

configurare l'access point per non divulgare il proprio SSID (identificativo)

- Spento se non usato:

Se non servono, l'access point e/o la scheda di rete è meglio tenerli spenti

fonte principale Paolo Giardini pgiar@solution.it http://blog.solution.it

augscaATyahoo.it