Generalita’ sulle reti

Reti di computer (1)

Una rete di computer e' l'insieme delle apparecchiature,e dei protocolli che consentono a degli host remotidi condividre e scambiare dati, informazioni e servizi

Le reti di computer si possono classificare in base a:

- Estensione
- Mezzo trasmissivo
- Protocollo

Reti di computer (2)

In base all'estensione, le reti di calcolatori si suddividono in:

- LAN (Local Area Network): sono reti private di piccola/media estensione, dislocate di norma in un solo piano, edificio o al massimo all'interno di una stessa struttura (campus universitari)
- MAN (Metropolitan Area Network): sono reti di medie dimensioni, spesso cittadine o municipali.
- WAN (Wide Area Network): sono reti di grandi dimensioni, che ricoprono una vasta area di territorio. Spesso si tratta di reti nazionali o internazionali, gestite da uno o piu' enti, pubblici o privati.

Reti di computer (3)

In base al mezzo trasmissivo utilizzato per il trasporto dei dati, le reti si suddividono in:

- Reti cablate: rame, fibra ottica
- Reti senza fili: onde radio, microonde

Reti di computer (4)

I piu’ diffusi stack protocollari esistenti sono:

TCP/IP (Transfer Control Protocol / Internet Protocol):

- Reti LAN/MAN/WAN
- E’ il protocollo di Internet

ATM (Asyncronous Transfer Mode)

- Reti MAN/WAN
- Alta velocita’ e affidabilita’
- E’ il protocollo delle "autostrade di Internet"

LAN

I principali tipi di reti LAN sono:

- Ethernet (rame - fibra ottica)
- WiFi (Wireless)
- Token bus (rame)
- DEC-net (rame)

Ethernet

Ethernet e’ una famiglia di standard IEEE per le reti LAN

Ne esistono diverse versioni:

- 10Base5 - Thick Ethernet (Thick Coax)
- 10Base2 - Thin Ethernet (Thin Coax)
- 10BaseT / 100BaseT (doppino intrecciato)
- 10BaseF/100BaseF/1000BaseF (fibra ottica)

La rete Internet

La Gande Rete

- Internet e’ la piu’ grande rete per la trasmissione di dati e informazioni mai costruita
- Fu inizialmente progettata dal DARPA per scopi militari (1967)
- Successivamente la rete venne estesa fino a coprire le maggiori Universita’ americane
- Oggi Internet e’ formata da centinaia di reti pubbliche e private connesse mediante il protocollo TCP/IP

Indirizzamento degli host

Per comunicare con un host appartenente ad una certa rete, e’ necessario indirizzarlo

In Internet esistono diversi livelli di indirizzamento:

- Interfaccia di rete (DLL - Indirizzo MAC)
- Host (Indirizzo IP)
- Servizio (Porta TCP)
- Nome di dominio

Indirizzamento DLL

Tutte le interfacce di rete possiedono un indirizzo

- Tale indirizzo si chiama "MAC Address" (Media Access Control Address)
- Ha una lunghezza di 48 bit
- Identifica univocamente una interfaccia di rete
- Esempio:

00:a4:bd:23:61:e2

Indirizzamento IP

Ogni host in Internet ha un indirizzo univoco (IP Address)

Nella attuale versione del protocollo IP (IPv4), tale indirizzo ha una lunghezza di 32 bit

Un indirizzo IP viene spesso scritto in notazione decimale puntata:

123.17.145.18

La parte alta dell’indirizzo indica la sottorete di cui l’host fa parte

La parte bassa viene utilizzata per indicare ciascun host

Classi di indirizzi

Lo spazio di indirizzamento IP e’ suddiviso in diverse classi:

- A: Indirizzi da 0.0.0.0 a 127.255.255.255
- B: Indirizzi da 128.0.0.0 a 191.255.255.255
- C: Indirizzi da 192.0.0.0 a 223.255.255.255
- D: Indirizzi da 224.0.0.0 a 247.255.255.255
- E: Indirizzi da 248.0.0.0 a 255.255.255.255

Indirizzamento TCP/UDP

Un indirizzo di porta (TCP/UDP) e’ un intero a 16 bit

Identifica in maniera univoca un servizio ospitato da un certo host

Le porte associate ai servizi piu’ noti sono:

- 80/TCP: HTTP (Hyper Text Transfer Protocol)
- 25/TCP: SMTP (Simple Mail Transfer Protocol)
- 21/TCP: FTP (File Transfer Protocol)
- 53/UDP: DNS (Domain Name System)
- 22/TCP: SSH (Secure SHell protocol)

Linux e le reti

Le interfacce di rete in Linux

In Linux le interfacce di rete non sono associate a file di dispositivo

Il loro nome varia a seconda del tipo di hardware:

- ethX : Interfacce Ethernet (e WiFi)
- pppX : Interfacce PPP (Point to Point Protocol)
- ....

ifconfig (1)

Il tool che si utilizza per configurare l’indirizzo IP di una interfaccia di rete e’ "ifconfig"

La sintassi e’ la seguente:

- ifconfig <interface> options | address ...

Il seguente comando:

- ifconfig eth0 192.168.10.21

assegna all’interfaccia eth0 l’indirizzo 192.168.10.21

ifconfig (2)

E’ possibile anche visualizzare l’attuale configurazione di una interfaccia:

```
/sbin/ifconfig eth0
eth0      Link encap:Ethernet  HWaddr 00:E0:18:06:A3:8F
          inet addr:192.168.0.7  Bcast:192.168.0.255  Mask:255.255.255.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:5322 errors:0 dropped:0 overruns:0 frame:0
          TX packets:5626 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:4292125 (4.0 MiB)  TX bytes:869302 (848.9 KiB)
          Interrupt:11 Base address:0xc000
```

ifconfig (3)

Alcuni esempi di utilizzo di ifconfig:

- ifconfig eth0 down (disabilita eth0)
- ifconfig eth0 hw ether 00:12:23:23:34:ed (cambia il MAC)
- ifconfig eth0:0 10.0.0.1 (Crea un alias)

Routing

- Per poter contattare host al di fuori della propria rete e’ necessario servirsi di un "router"
- I router si occupano di instradare i pacchetti dalla rete dell’host sorgente a quella hell’host destinazione
- E’ necessario quindi impostare sempre un "default router"
- Per la configurazione del routing si utilizza il comando "route"

route (1)

- Per visualizzare l’attuale tabella di routing:
  - route
- Per configurare il router di default 10.0.0.1:
  - route add default gw 10.0.0.1
- Per configurare un routing statico verso la rete 192.168.10.0:
  - route add -net 192.168.10.0/24 dev eth1

DNS

- Il DNS (Domain Name System) consente di tradurre un nome di dominio (latolaz.homeunix.net) in un indirizzo IP.
- Per effettuare tale conversione, e’ necessario connettersi ad un server DNS
- La lista dei server DNS accessibili dall’host e’ riportata in etc/resolv.conf

Esempio: IP, routing, DNS

Accesso ad Internet

- Per accedere ad Internet e’ necessario appartenere ad una delle reti che ne fanno parte....
- Vi sono diverse possibili modalita’ di accesso:
  - Connessione permanente (linea dedicata)
  - Connessione on-demand (modem, adsl, GPRS...)

Connessione permanente (1)

Tipici esempi di connessioni permanenti sono:

- Le connessioni dirette mediante reti nazionali o internazionali (GARR)
- Le connessioni dedicate, mediante reti private (TELECOM)

Ad una connessione permanente e’ associato staticamente almeno un indirizzo IP

Connessione permanente (2)

Per accedere ad Internet da una LAN che dispone di una connessione permanente e’ necessario:

- Configurare gli indirizzi IP (privati) degli host della LAN
- Configurare il default router
- Compilare la lista dei DNS accessibili

Connessione on-demand

- Nel caso di connessione on-demand, e’ necessario collegarsi ad un "Internet Service Provider" (ISP)
- L’ISP concede l’accesso ad Internet ai clienti abilitati
- La connessione ad Internet e’ solitamente limitata nel tempo
- L’host abilitato ottiene in concessione temporanea dall’ISP un indirizzo IP
- L’host risulta raggiungibile da Internet per tutto il tempo della connessione

Connessione tramite modem

- Si utilizza una normale linea telefonica
- E’ necessario un MODEM (MOdulatore/DEModulatore)
- Utilizza il protocollo PPP / CSLIP
- Banda fino a 56 KBit/sec

Configurazione di una connessione tramite modem (KPPP)

Connessione ADSL

- Asymmetric Digital Subscriber Line
- Il canale tra l'host e l'ISP utilizza ATM
- E' necessario un router multiprotocollo ATM
- Banda fino a 12 Mbit/sec Down - 3.5 Mbit/sec Up

Sicurezza di rete

Sicurezza in rete

- Un host connesso a Internet "vede" tutti gli altri host della rete...
- ... ma a sua volta puo’ essere "visto" da tutti gli altri host....
- ... e Internet non e’ proprio il paese delle meraviglie.
- Proprio per questo e’ necessario preoccuparsi della sicurezza di un host

Attacchi e compromissioni

- "In teoria", connettendosi ad un computer da remoto, si potrebbe accedere soltanto ai servizi messi a disposizione dall'host...
- ...ma "in pratica" si potrebbe anche:
  - Accedere a dati personali degli utenti
  - Compromettere il funzionamento del sistema
  - Utilizzare il sistema compromesso come base per ulteriori attacchi
- Tutto cio' sfruttando errori di programmazione e/o di configurazione

Alcuni attacchi

- Esistono diverse centinaia di attacchi informatici
- I piu’ comuni sono:
  - Denial Of Service (DOS)
  - Distributed Denial Of Service (DDOS)
  - Site defacement
  - IP Spoofing
  - TCP Hijacking (Man-in-the-Middle)
  - Remote Exploit

Arginare gli attacchi

- Per arginare attacchi alla propria rete si utilizzano diverse tecniche:
  - Vulnerability scanning
  - Network monitoring
  - Intrusion Detection Systems
  - File Integrity Check
  - Firewall

Vulnerability Scanning

- Tecnica preventiva
- Ha l’obiettivo di rilevare per tempo eventuali buchi di sicurezza
- Si basa sul controllo dei servizi offerti dagli host della rete
- Alcuni esempi:
  - netstat (network status)
  - nmap (port scanner)
  - nessus (security auditor)

Network monitoring

- Ha come obiettivo la rilevazione di attivita’ anomale
- Si basa sul controllo del livello e del tipo di traffico
- Spesso utilizza dei sistemi di intercettazione dei pacchetti (Sniffer):
  - tcpdump
  - sniffit
  - Ethereal

Intrusion Detection

- Insieme di tecniche che consentono di rilevare i tentativi di attacco
- Si basano su:
  - Rilevazione automatica del traffico
  - Ricostruzione del protocollo
  - Monitoring delle porte TCP/UDP
  - Analisi del traffico
- Esempi: snort, acidlab

File Integrity Check

- Tecnica che consente di rilevare un attacco andato a buon fine
- Si basa sul monitoraggio dei file di sistema
- Consente di scoprire modifiche effettuate da utenti non autorizzati
- Esempi:
  - tripwire
  - fcheck

Esempio: nmap, tcpdump, sniffit, fcheck, ethereal....