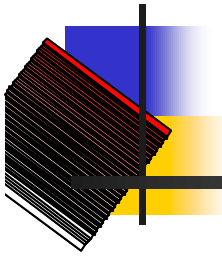
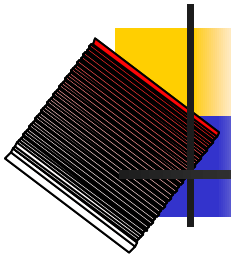


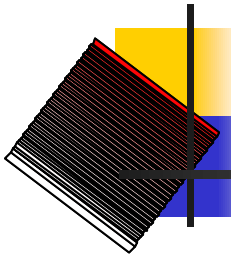
Esercitazione sui tools di rete

Corso di Amministrazione di Reti
A.A.2002/2003



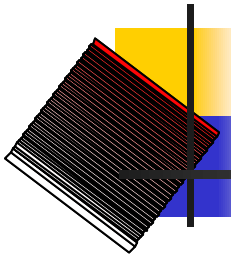
Argomenti

- Ping
- Netstat
- Traceroute
- Comandi per la lettura/scrittura di un MIB



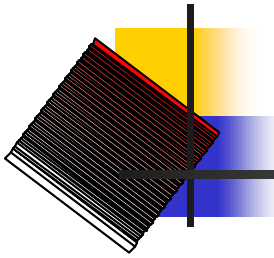
Ping: verifico la connettività

- ping 127.0.0.1 = verifico se lo stack protocollare è correttamente installato
- /sbin/ifconfig: determino il mio IP
- ping Mio_IP = verifico se lo stack protocollare è in binding con la NIC
- /sbin/route –n : determinare l'IP_GW del default gateway
- ping IP_GW = se risponde allora dovrei poter comunicare con gli tutti gli altri host sullo stesso segmento di rete… se non ci riesco, provo a pingare un qualunque altro host. Se ancora non riesco, cosa può essere ? Può dipendere dalla netmask ?



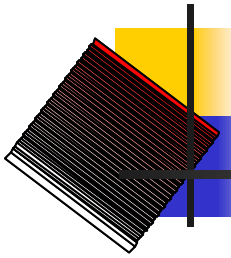
Ping: verifico la connettività

- Ping IP_Remoto : se non risponde, quali possono essere i problemi ? Può dipendere anche dalla netmask ?



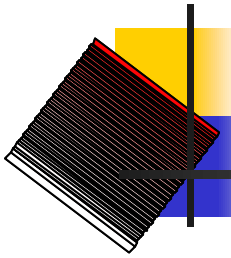
PING : altri usi

- Posso utilizzare il comando ping per misurare le prestazioni della mia rete ?
- Provate a misurare il throughput dal vostro PC verso il PC adiacente. I tempi che misurate possono essere utilizzati per calcolare anche la bit-rate ?



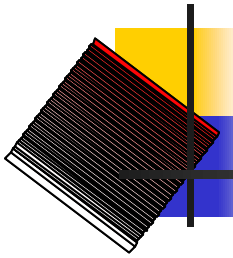
Netstat

- Eseguite il comando “netstat –a”. Cosa viene visualizzato ?
- Leggete il manuale ed aggiungete le opzioni necessarie affinché “netstat –a” fornisca ora indirizzi e porte in formato numerico. Salvate il risultato in un file netstat.txt
- Si può utilizzare netstat al posto del comando route per visualizzare le tabelle di routing?
- Adesso connettetevi ad un sito web con un browser ed eseguite di nuovo netstat. A quale porta/e si è connessi ? Quale porta/e si sta(nno) utilizzando sul sistema host ?



Traceroute

- Eseguite il comando traceroute www.google.com . Cosa viene visualizzato ? Cosa è scritto sulla prima riga di output ?
- Dopo aver LETTO il manuale… Se un firewall vi blocca tutte le porte UDP, potete pensare di continuare ad utilizzare questo comando ? Quale opzione vi può aiutare ? Trovata la risposta, scrivete il tracciato ottenuto nel file trace.txt e giustificatela brevemente.

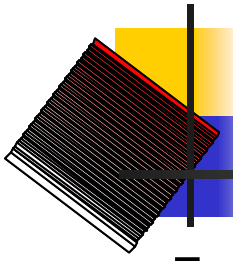


SNMP

- Leggete il man dei comandi snmpget e snmpwalk… utilizzando uno o entrambi questi comandi salvate sul file group.txt il contenuto di tutto il system group (OID radice = 1.3.6.1.2.1.1). Usate a questo scopo la sintassi:

snmpXXX –v 1 –c "public" IP_Agent OID

Cosa rappresentano –v 1 e –c "public" ? Il comando snmpset riuscirebbe a scrivere nel MIB ?



SNMP

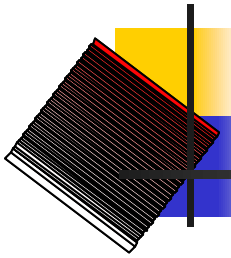
- Eseguite ora:

snmpwalk -v 1 -c public 192.168.69.6 1.3.6.1.2.1.2.2.1.6

- In quale parte (gruppo) del MIB siete finiti ? Cosa viene visualizzato ?
- Risalite ora all'interno del MIB (OID 1.3.6.1.2.1.2.2.1). Usando il comando grep "down", potete vedere quali porte dello switch sono inutilizzate ?
- Risalite ancora nel MIB all'OID 1.3.6.1.2.1 ed aiutandovi con il comando grep cercate l'oggetto chiamato "ifNumber". Cosa rappresenta ?
- Se usate il comando

  snmpwalk -v 1 -c public 192.168.69.6 1.3.6.1.2.1.interfaces.1

  ottenete lo stesso risultato ?
- Usando ora l'opzione –O n , scrivete nel file OID.txt:
  - OID dell'oggetto ifNumber
  - Valore dell'oggetto
  - Sintassi ASN.1 dell'oggetto



Compitini

- Scrivere uno script bash che faccia il polling del traffico in ingresso allo switch ogni 10 secondi ed estragga la porta con maggiore traffico, appendendo il valore ottenuto nel file max_traffic.txt. Si consiglia di utilizzare l'OID 1.3.6.1.2.1.2.2.1.10.
- Cercare nel MIB il MAC address del vostro PC. A quale porta siete collegati ?