Comandi di Rete

Principali Comandi di Rete.

Verificare , testare ed analizzare da Riga di Comando

PING: verifica la comunicazione tra due pc

- Il comando ping consente di verificare la connettività a livello IP. Durante la risoluzione dei problemi, è possibile utilizzare ping per inviare una richiesta echo ICMP a un nome host o a un'indirizzo IP di destinazione.
- ICMP: Internet Control Message Protocol
- Comunica messaggi di errore o altre situazioni che richiedono intervento.
- Utilizzare ping quando è necessario verificare che un computer host possa connettersi alla rete TCP/IP e alle risorse di rete. È anche possibile utilizzare ping per isolare problemi hardware della rete e configurazioni incompatibili.

PING Per diagnosticare problemi relativi alla connettività di rete, effettuare le operazioni seguenti:

- Eseguire il ping dell'indirizzo di loopback per verificare che TCP/IP sia configurato correttamente nel computer locale.

  ping 127.0.0.1

- Eseguire il ping dell'indirizzo IP del computer locale per verificare che sia stato aggiunto alla rete in modo corretto.

  ping *indirizzo_IP_host_locale*

- Eseguire il ping dell'indirizzo IP del gateway predefinito per verificare che il gateway predefinito sia in funzione e che sia possibile comunicare con un host locale nella rete locale.

  ping *indirizzo_IP_gateway_predefinito*

- Eseguire il ping dell'indirizzo IP di un host remoto per verificare che sia possibile comunicare attraverso un router.

  ping *indirizzo_IP_host_remoto*

PING UTILIZZO PRATICO -> " host raggiungibile "

:

- Di seguito vediamo come utilizzare il comando ping su un sistema Windows XP.

```
ping 192.168.0.1
```

- dove al posto di 192.168.0.1 va inserito l'indirizzo IP di cui si vuole verificare la raggiungibilità.
- Se l'host è raggiungibile, avremo una risposta di questo tipo:

```
Esecuzione di Ping 192.168.0.1 con 32 byte di dati:

Risposta da 192.168.0.1: byte=32 durata<1ms TTL=254
Risposta da 192.168.0.1: byte=32 durata<1ms TTL=254
Risposta da 192.168.0.1: byte=32 durata<1ms TTL=254
Risposta da 192.168.0.1: byte=32 durata<1ms TTL=254

Statistiche Ping per 192.168.0.1:
        Pacchetti: Trasmessi = 4, Ricevuti = 4, Persi = 0 (0% persi),
Tempo approssimativo percorsi andata/ritorno in millisecondi:
        Minimo = 0ms, Massimo =  0ms, Medio =  0ms
```

- Com'è possibile constatare, il sistema "mittente" tenta di mettersi in contatto con il sistema "destinatario" per 4 volte, e dopo aver effettuato i 4 tentativi, presenta le relative statistiche, indicando i pacchetti trasmessi, ricevuti ed eventualmente perduti, ed indicando il tempo minimo, il tempo massimo ed il tempo medio del percorso fatto dal pacchetto inviato.

PING UTILIZZO PRATICO -> "Richiesta scaduta"

```
Esecuzione di Ping 192.168.0.1 con 32 byte di dati:

Richiesta scaduta.
Richiesta scaduta.
Richiesta scaduta.
Richiesta scaduta.

Statistiche Ping per 192.168.0.1:
        Pacchetti: Trasmessi = 4, Ricevuti = 0, Persi = 4 (100% persi),
```

- La risposta "Richiesta scaduta" viene restituita quando l'host di destinazione è spento oppure quando è protetto da firewall. Infatti, se un sistema è protetto da firewall, non risponderà alle richieste provenienti dal comando **ping**.
- In questo caso bisogna fare attenzione, perchè il fatto che il sistema "destinatario" non risponda non significa che l'host sia spento, anzi, funziona perfettamente.
- E' possibile comunque mantenere la protezione del firewall ed abilitare il sistema a rispondere a richieste "**ping**" configurando in modo opportuno il proprio firewall, oppure, si può disabilitare la protezione firewall, che nel caso di una rete locale, non è così indispensabile.

PING UTILIZZO PRATICO -> "Host di destinazione irraggiungibile"

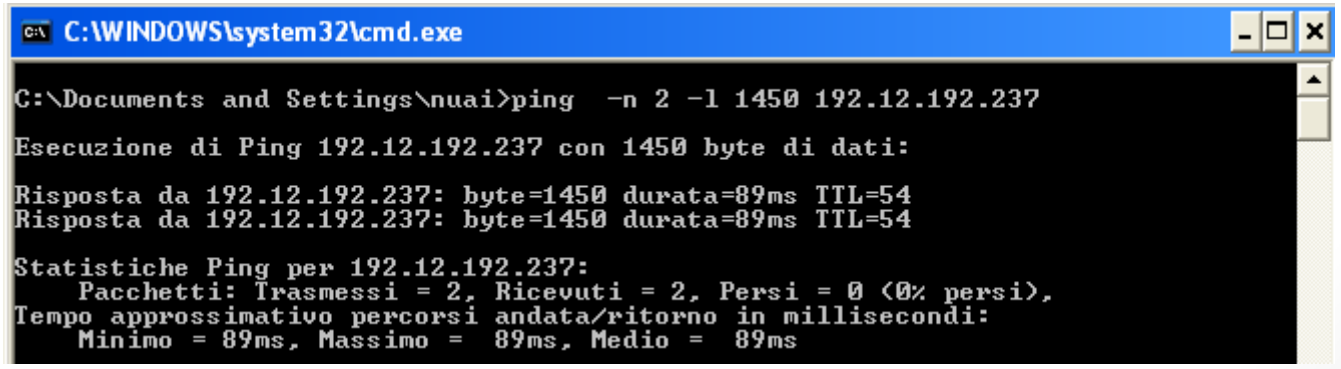
```
Esecuzione di Ping 192.168.0.1 con 32 byte di dati:

Host di destinazione irraggiungibile.
Host di destinazione irraggiungibile.
Host di destinazione irraggiungibile.
Host di destinazione irraggiungibile.

Statistiche Ping per 192.168.0.1:
        Pacchetti: Trasmessi = 4, Ricevuti = 0, Persi = 4 (100% persi),
```

- La risposta "Host di destinazione irraggiungibile" invece viene restituita quando è impossibile comunicare con l'host, anche se questo dovesse essere acceso e senza nessuna protezione.
- Ciò succede quando l'host di destinazione si trova in un'altra rete e non c'è nessun dispositivo in grado di connettere i due host (mittente e destinatario).
- Ad esempio, se **hostA** ha come indirizzo 192.168.1.1 e **hostB** 192.168.0.1, i due host non potranno comunicare tra loro (a meno che le due reti non siano connesse da un router), quindi la risposta al ping tra i due host sarà appunto "Host di destinazione irraggiungibile".

PING Nella tabella seguente sono elencate alcune opzioni utili del comando **ping**.

Opzione	Utilizzo
-n *Count*	Determina il numero di richieste echo da inviare. Il valore predefinito è 4 richieste.
-w *Timeout*	Consente di regolare il timeout in millisecondi. Il valore predefinito è 1.000 (timeout di un secondo).
-l *Size*	Consente di regolare la dimensione del pacchetto ping. La dimensione predefinita è 32 byte.
-f	Imposta il flag per la disattivazione della frammentazione nel pacchetto ping. Per impostazione predefinita il pacchetto ping consente la frammentazione.
/?	Visualizza informazioni della Guida sul comando.

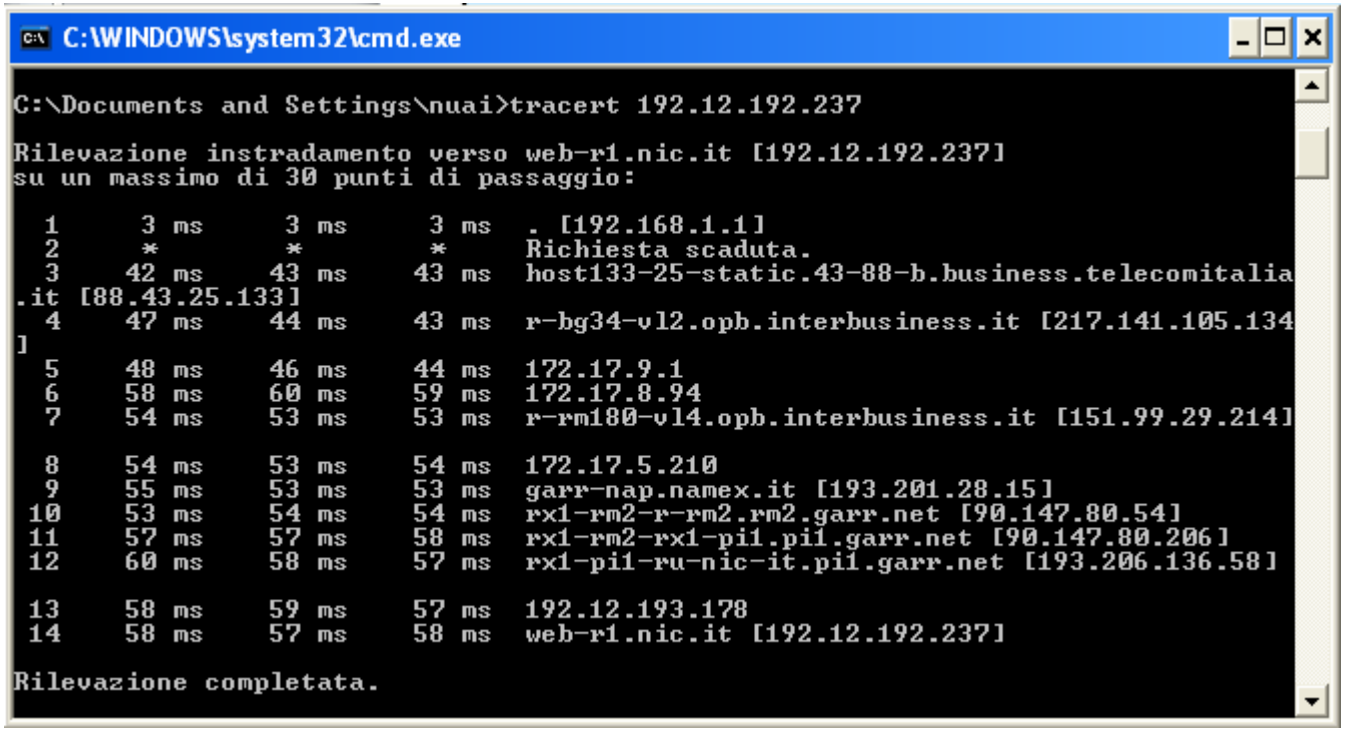
- Nell'esempio seguente viene illustrato come inviare due ping, ognuno della dimensione di 1.450 byte, all'indirizzo IP 192.12.192.237:



TRACERT: rintraccia tutti i passi che un pacchetto fa per arrivare a destinazione

- Il comando tracert, assieme al comando ping viene usato dagli amministratori di rete per analizzare host remoti e verificare la presenza di eventuali problemi.
- Quando desideriamo verificare la raggiungibilità di un server remoto o un computer in rete usiamo il comando ping, questo tramite una serie di messaggi di richiesta e risposta ne verifica la connettività, **purtroppo però essendo le reti di calcolatori dei sistemi distribuiti, quasi sempre (a meno di non trovarsi in una piccola rete domestica) tra un computer e l'altro vi sono diversi elementi di rete, quali i router, responsabili degli instradamenti dei pacchetti,**
- il problema pertanto della connettività limitata o assente **potrebbe risiedere in uno di questi elementi intermedi**. In tal caso il comando ping non è in grado di fornirci informazione alcuna su di essi, invece il comando **tracert consente di ottenere inforamazioni anche su detti elementi intermedi.**

TRACERT: rintraccia tutti i passi che un pacchetto fa per arrivare a destinazione

- 

- come si nota l'uso e del tutto analogo a quello del comando ping, solo che questa volta il comando tracert ci riporta tutti gli IP ed il nome di ogni host per cui passano le richieste ed il tempo impiegato per ogni salto; se l'host a cui facciamo la richiesta non viene raggiunto riceveremo un messaggio di "Destinazioni non raggiungibile", diversamente una volta concluso il suo lavoro, tracert ci mostreà il messaggio finale di "Traccia completata", potete vederne un esempio nella figura dalla quale si nota che il primo nodo di rete incontrato è proprio il gateway (il router) della mia rete locale che poi mi connette ad internet.

- Con il comando tracert è pertanto possibile diagnosticare con relativa facilità eventuali problemi di rete presenti in un router intermedio tra sorgente e destinazione, infatti se un pacchetto impiega troppo tempo per effettuare un salto da un nodo ad un altro della rete, è plausibile che l'errore stia proprio lì.

TRACERT: opzioni principali

- Tracert può essere usato con delle opzioni aggiuntive che ne modificano il comportamento predefinito:
- **-d**: se usato, il nome dell'host (router) per il quale passa il pacchetto non viene riportato tra la lista delle informazioni;
- **-h** valore intero: esprimendo un valore, indichiamo il numero massimo di salti che la richiesta deve effettuare per raggiungere la destinazione;
- **-d** valore intero: consente di settare il tempo massimo (espresso in millisecondi) di attesa della risposta (Echo Reply) di una richiesta (Echo Request).
- Non c'è molto altro d'aggiungere, se non che il comando tracert amplia la possibilità di diagnosi ed analisi di una rete offerta dal comando ping.

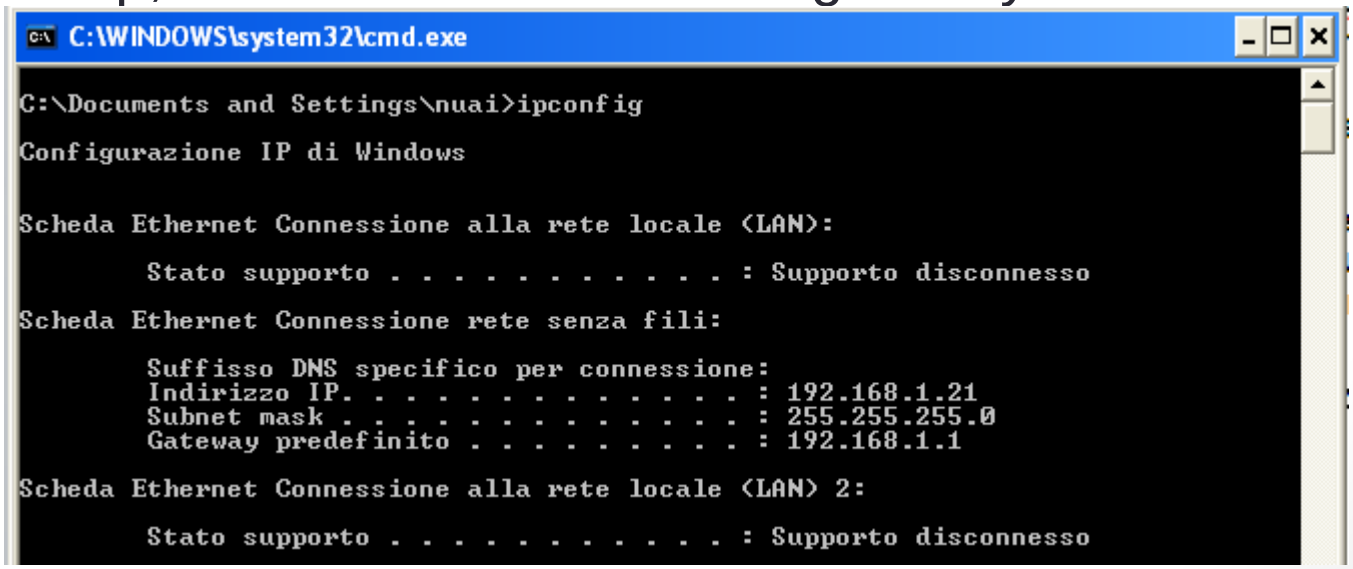
PING & TRACERT: sicurezza

- Da quanto indicato precedentemente si può intuire che il PING oltre ad essere un utile strumento potrebbe essere sfruttato da malintenzionati per ottenere degli attacchi di tipo DoS(Denial of Service).
- Ciò avviene inviando continue richieste ad un server da numerosi calcolatori in maniera da saturare la banda o la capacità di calcolo, oppure si potrebbero inviare PING di grosse dimensioni per ottenere gli stessi risulati indicati precedentemente;
- per queste ragioni spesso in internet il PING viene disabilitato e lo stesso vale per il TRACEROUTE. .

- https://www.google.it/#hl=it&q=How+to+DoS+Attack

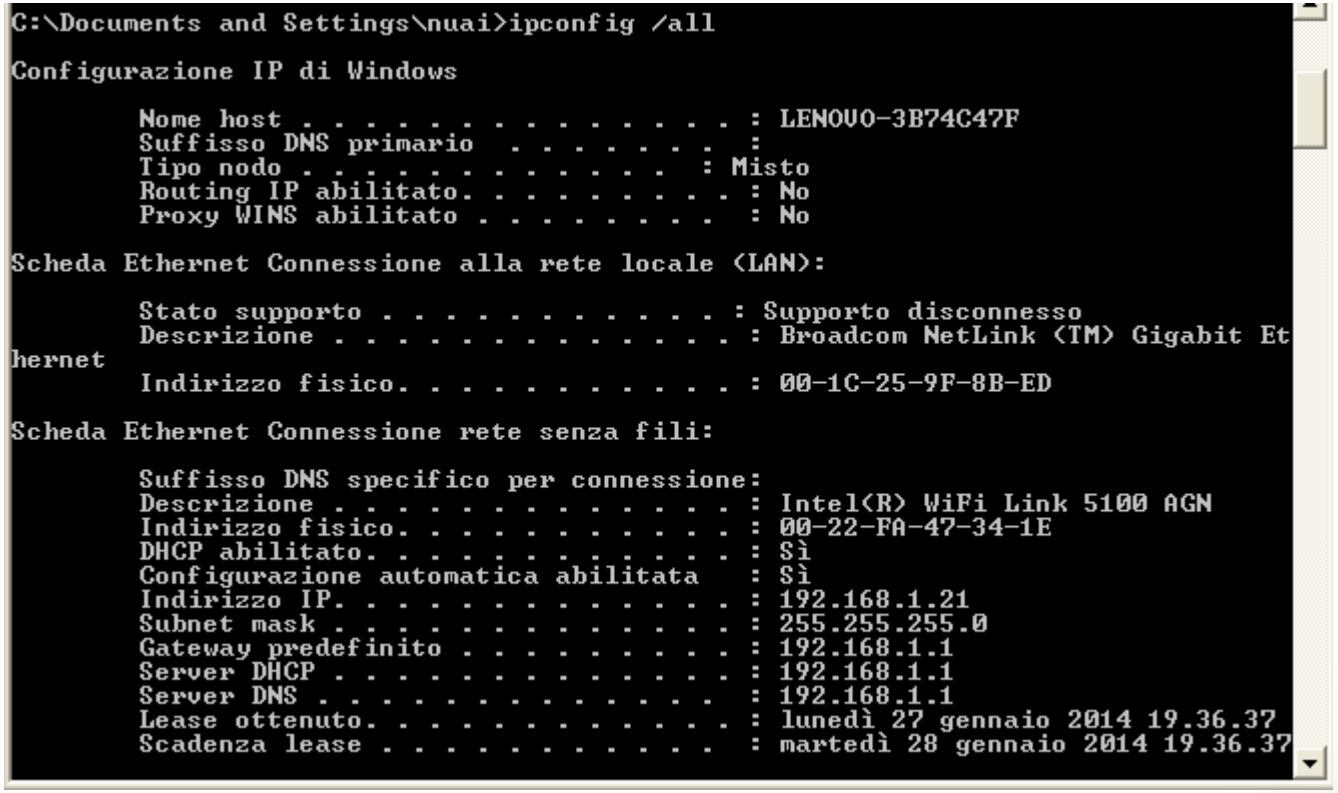
IPCONFIG fornisce informazioni dettagliate sul vostro IP

- Questo comando assieme a ping è tra i comandi di rete dos il più noto ed utilizzato,
- ci permette di ottenere tutte le informazioni su un qualsiasi adattatore di rete (scheda ethernet, scheda wi-fi, gateway, router, modem, …) del nostro sistema;
- usato normalmente fornisce delle informazioni di base quale ip, maschera di sottorete e gateway



IPCONFIG opzioni

- usato invece assieme all'opzione /all elenca tutte le informazioni della scheda di rete tra cui anche: indirizzo MAC, DNS, indirizzo IPv6 ed altro ancora.



IPCONFIG opzioni…

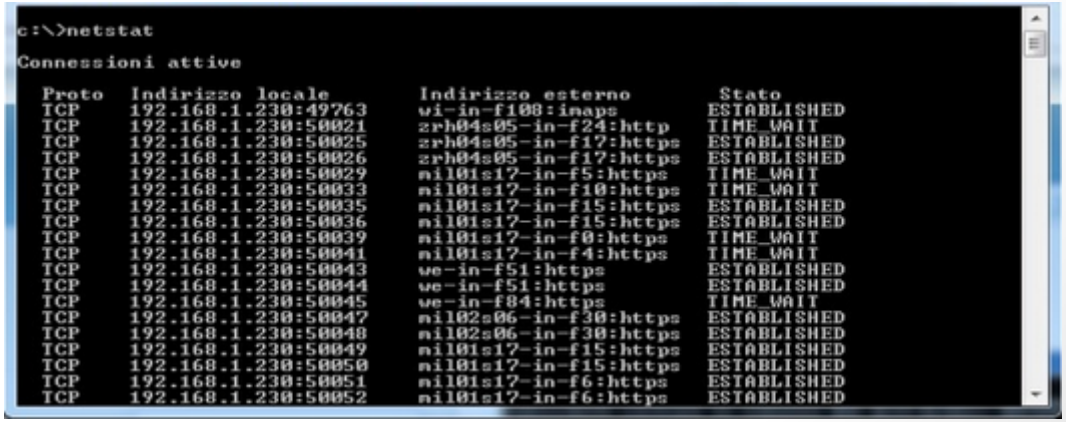
- Elenco delle varie opzioni utilizzabili per ottenere informazioni più dettagliate sulla propria configurazione TCP/IP:

- **/all**: elenca le informazioni dettagliate di tutte le schede di rete presenti nella propria configurazione;

- Per ulteriori opzioni:
- **ipconfig /?**

Comando netstat

- Il comando netstat è utile per avere informazioni sulle connessioni di rete attive del proprio computer, esso infatti elenca tutte le connessioni in entrata ed in uscita, fornendo per ognuna di esse: il protocollo utilizzato (ad es. TCP), l'indirizzo ip locale e la relativa porta utilizzata (socket: ip + porta), l'indirizzo esterno al quale si collega ed infine lo stato della connessione che può essere stabilia (established) o in attesa (time_wait) o ancora in ascolto (listening).



Comando netstat opzioni

- E' possibile combinare svariate opzioni al comando netstat di modo da avere informazioni più precise sulle connessioni di rete, di seguito ne riporto un breve elenco:

- -a: elenca tutte le connessioni aperte e le porte corrispondenti;
- -e: elenca un insieme di dati sui byte ed i pacchetti ricevuti e trasmessi dalla scheda di rete;
- -n: elenca nel formato numerico gli indirizzi ip locali e quelli esterni con le relative porte utilizzate;
- -p nome_protocollo: elenca le sole connessioni (ip + porta) del protocollo specificato dopo l'opzione -p;
- -r: elenca le tabelle di routing (responsabili dell'instradamento dei pacchetti);
- -s: elenca un insieme d'informazioni riassuntive sui protocolli di rete utilizzati dal sistema (ad es. TCP, UDP, IP, ICMP etc. etc.), combinandolo con l'opzione -p è possibile ottenere le sole informazioni di un dato protocollo;
- Questo non è l'elenco completo delle opzioni utilizzabili con il comando netstat ed ovviamente alcuni di essi possono essere combinati in modo da avere informazioni più specifiche o mirate.
- Per avere l'elenco completo basta riferirsi all'help in linea, basta digitare al prompt dei comandi del dos la seguente istruzione:

- netstat /?

Comando netsh

- Per mezzo del comando netsh è possibile configurare ed ottenere svariate informazioni sulla propria rete, a differenza dei comandi diretti come ping, netsh è un vero e proprio programma lanciato sotto dos, pertanto digitando netsh al prompt richiamiamo il programma dopodichè bisogna dare l'istruzione che si vuole eseguire.
- Una volta lanciato il prompt del dos, è possibile usare netsh in due modi, digitando ogni volta netsh seguito da una istruzione, oppure entrando in modalità netsh (che diventa il prompt) e via via digitare i comandi senza bisogno di ripetere "netsh".
- Un comando di netsh molto comodo per ottenere diverse informazioni sugli elementi di rete è diag, và usato in questo modo:
- netsh diag show all
- così facendo abbiamo tutte le informazioni degli elementi di rete del nostro sistema come: l'account di posta di outlook, il server proxy (se impostato) d'internet explorer, il modem, le schede di rete ed altro ancora.
- Se invece volessimo pingare il nostro server dhcp basterà scrivere
- netsh diag ping dhcp

Comando netsh opzioni

- Bene, come vedete tramite l'utility netsh è possibile ottenere tantissime informazioni con l'istruzione diag, eccone una lista dei comandi con cui è possibile combinarli:
- diag ping adapter: si connette con l'adattatore di rete specificato
- diag ping dhcp: si connette col server dhcp
- diag show adapter: mostra i nomi di tutte le schede di rete presenti sul pc
- diag show all: mostra una lista riportante tutte le informazioni degli elementi di rete presenti sul computer;
- diag show dhcp: mostra informazioni sul dhcp
- diag show dns: mostra le informazioni (gli IP) dei server dns, sia primario che secondario;
- diag show gateway: mostra le informazioni (nome ed indirizzo ip) dei gateway della rete;
- diag show connect ieproxy: si connette con il server proxy d'internet explorer;
- diag show connect mail: si connette con il server di posta di outlook.

- Il comando nestsh è usato sotto Windows XP, per altri sistemi operativi di casa Microsoft le istruzioni e le opzioni potrebbero essere leggermente diverse.