IT Administrator

Individuazione e risoluzione dei problemi relativi alla rete

Descrizione

- Quando un utente ha problemi
  - Dice sempre che 'non funziona nulla' ?
  - Riesce a descrivere cosa non riesce a fare ?
  - Come lo si può guidare a descrivere cosa non funziona ?
  - Cosa si può osservare ?
  - Di che strumenti si può disporre ?

Approccio sistematico

- Non si procede a caso
  - Non si ha garanzia della risoluzione del problema
  - Un approccio sistematico riduce tempi e costi della soluzione
  - Ogni catena di eventi può essere esaminata in una logica di ricerca binaria
  - Il guasto sta tra l'ultimo evento positivo ed il primo evento sbagliato

Uso della pila ISO/OSI

- Normalmente un utente segnala un malfunzionamento a livello applicativo
  - 'Non riesco a scaricare la posta'
  - 'Non riesco a navigare'
- Il guasto può essere in un qualunque livello, a partire da quello fisico
  - Connettore di rete 'strappato'
  - TCP/IP sconfigurato

Ottenere informazioni (1)

- Prima di far fare manovre parlare con l'utente
  - Fargli descrivere il problema a partire da ciò che vuole ottenere e non ottiene
  - Non accontentarsi di frasi imprecise come 'non va in rete'
  - Questo permette di stabilire qual'è il primo evento che non si verifica

Ottenere informazioni (2)

- Far compiere semplici osservazioni all'utente
  - Fargli osservare lo stato del connettore e del cavo di rete
  - Fargli riferire lo stato dei led presenti sulla scheda
  - Questo permette di stabilire qual'è l'ultimo evento che si verifica

Stringere il cerchio

- Ove possibile far eseguire dei controlli
  - La verifica della funzionalità di un altro servizio permette di escludere problemi nella parte più bassa della pila e concentrarsi sul servizio che non funziona
  - Un semplice ping spesso permette di verificare la corretta installazione dello stack TCP/IP e quindi ridurre le cose da osservare

Livelli

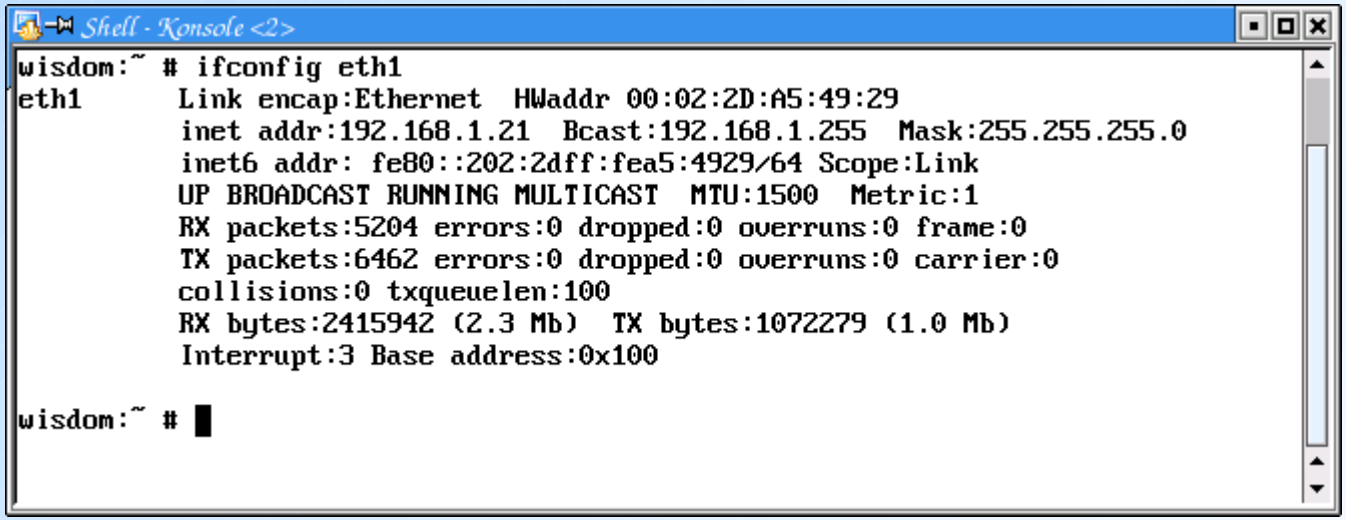
- Il comando ping può essere utile
  - Permette di capire se il problema riguarda il livello applicativo o di trasferimento oppure i livelli fisico, logico o di rete
  - Il non funzionamento del comando ping può essere imputato anche alla configurazione di router e firewall
  - Ping può essere usato anche per la verifica del funzionamento della risoluzione dei nomi

Livelli 1 e 2

- Osservazioni possibili
  - Link di stato sulle apparecchiature
- Misure possibili
  - Verifiche sui cavi con tester appositi
  - In Linux è possibile usare il comando ifconfig per avere delle statistiche minimali
  - In Linux il comando tcpdump permette di vedere il traffico di rete

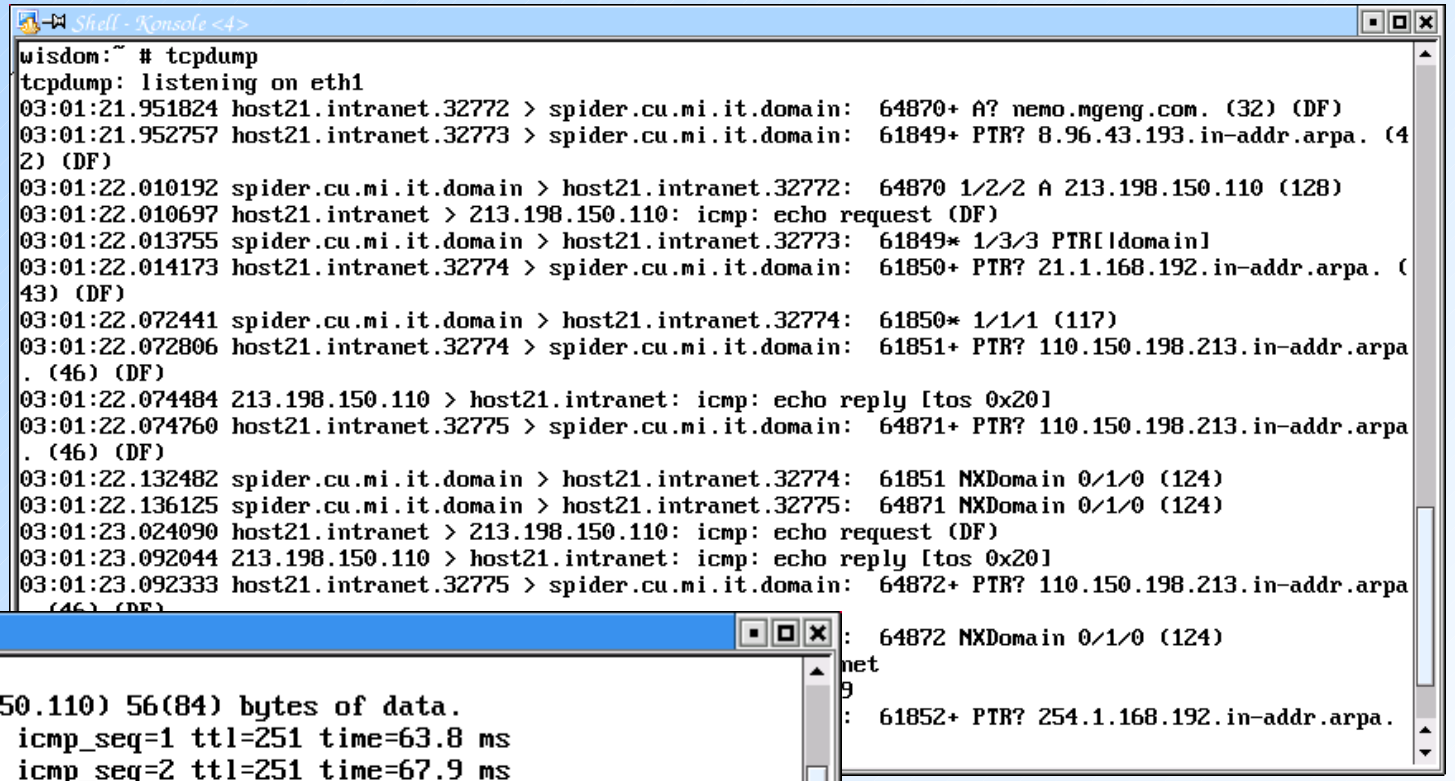
Ifconfig

- Consente di vedere la configurazione dell' interfaccia così come alcuni dati statistici



Tcpdump

- Permette di vedere ed analizzare il traffico



Tcpdump

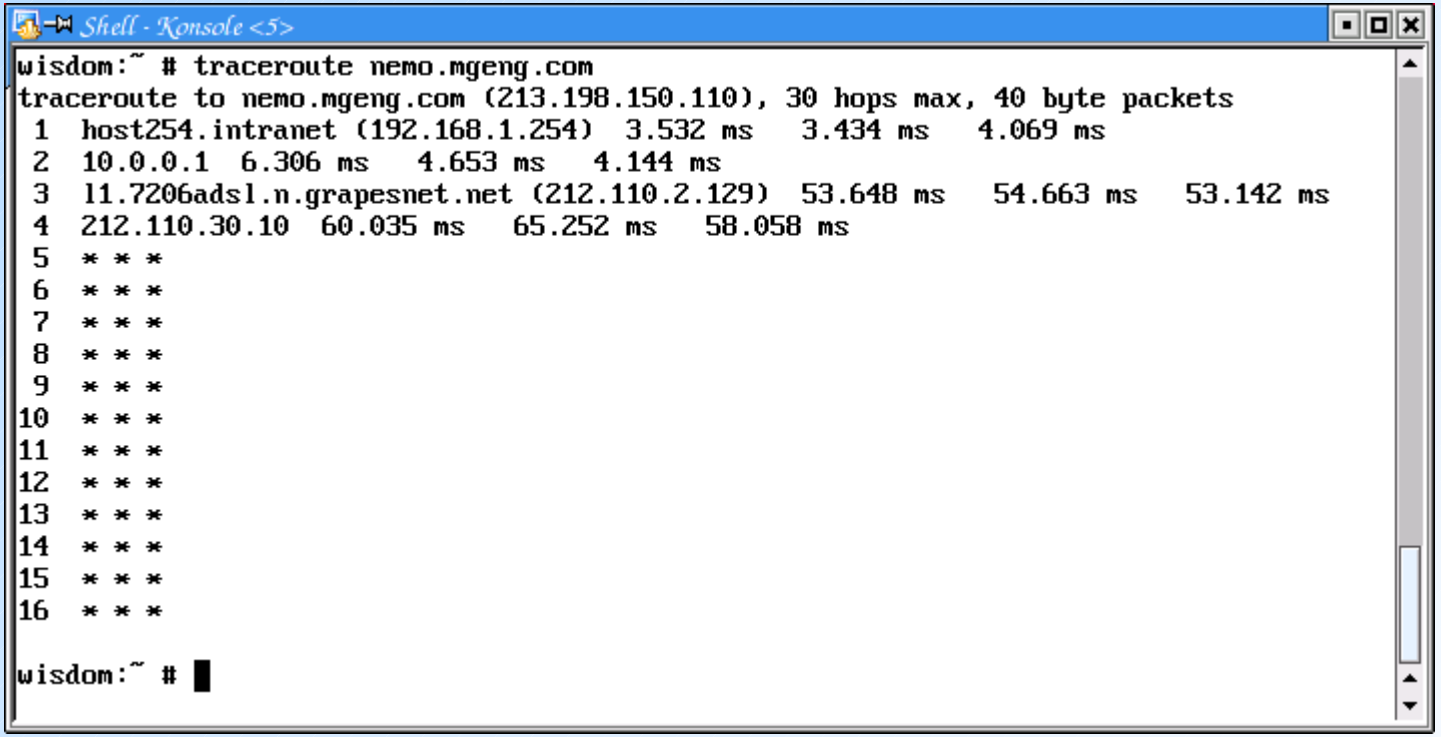
- Per funzionare deve poter mettere la scheda di rete in modalità promisqua
- Può vedere traffico che non coinvolge il PC su cui si opera se non si utilizzano switch ma hub
- Ettercap riesce comunque a farlo perchè usa arp poisoning e/o port stealing

Livello di rete

- Verifica configurazioni con il comando route
  - route -n in Linux
  - route print in Windows
  - Si può usare il comando traceroute per tracciare il percorso fatto da un pacchetto
    - Traceroute lavora manipolando TTL
    - Traceroute si basa su ICMP e quindi ha gli stessi limiti del comando ping
    - In ambiente windows esiste il comando tracert

Traceroute

- Percorso del pacchetto
  - Spesso bloccato dai firewall

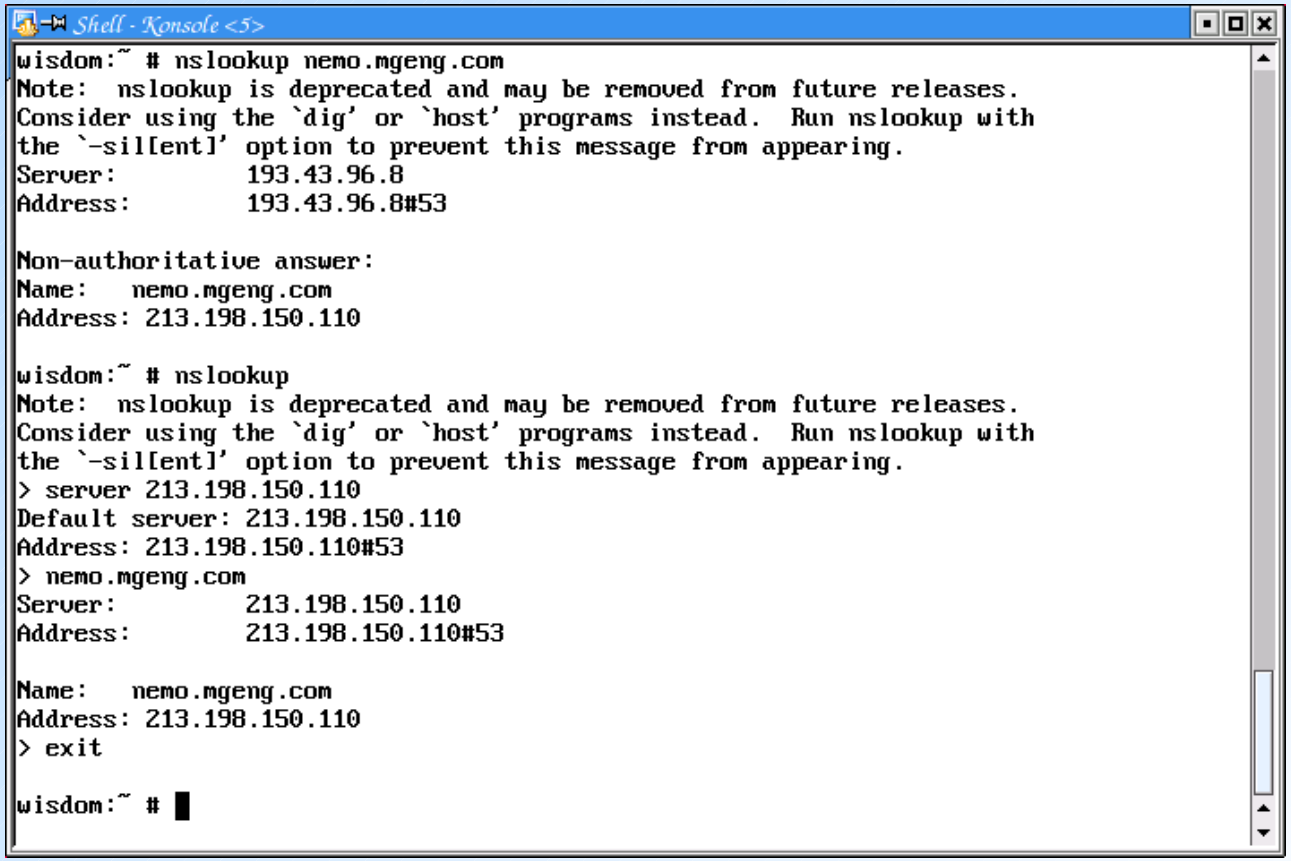


Livello applicativo

- Risoluzione dei nomi
  - In linux nslookup o dig
  - Si può usare un comando ping per forzare una risoluzione dei nomi
  - In supporto alla spedizione di mail è importante la query di tipo MX per verificare a quale mailserver viene inviata la posta per un certo dominio

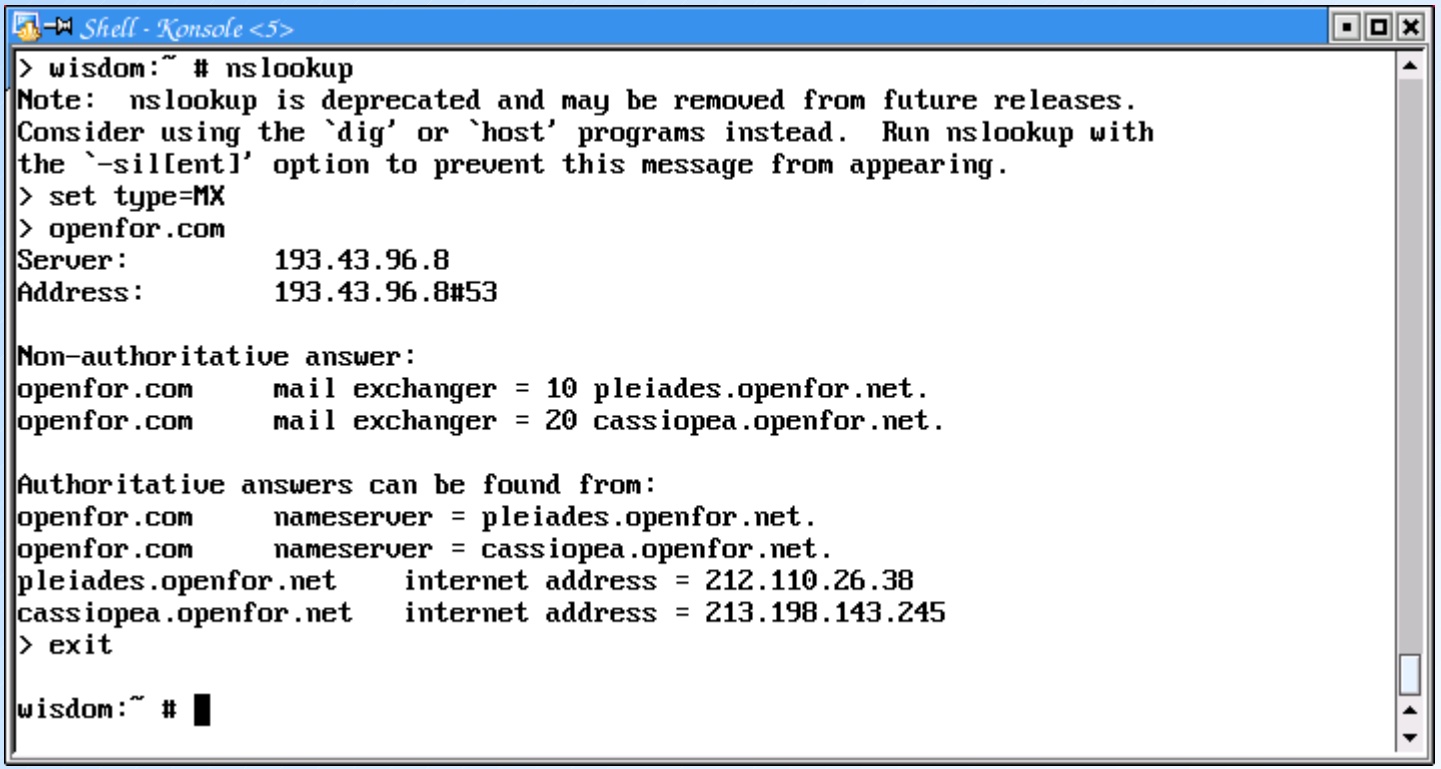
Nslookup

- Uso normale e settaggio del server



Nslookup

- Query MX

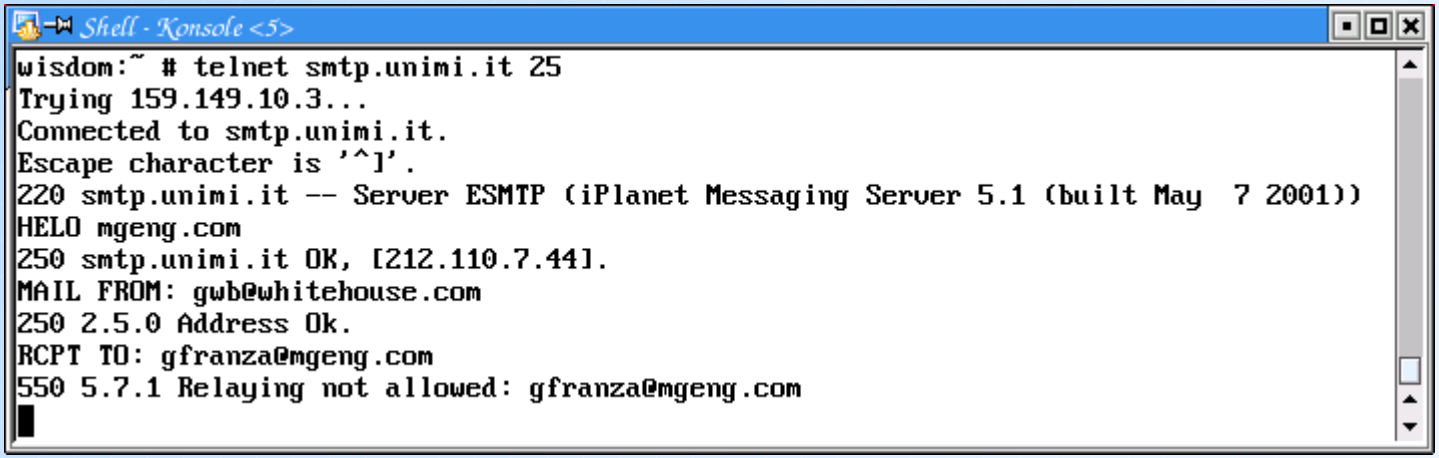


Livello applicativo

- Invio di posta
  - Si inizia con una query MX per scoprire a quale server inviarle
  - Si può continuare cercando di inviare la posta 'a mano'
    - Telnet sulla porta 25 del server
    - Si forniscono i comandi HELO/MAIL FROM/RCPT TO/DATA
    - Può essere utile in caso di risposte 'strane' magari dovute ad indirizzi malformati

SMTP

- Esempio di verifica che porta ad un errore di Relaying non permesso



Livello applicativo

- Ricezione di posta
  - Possibile utilizzare una connessione sulla porta pop3 o imap del server in modo da verificare il protocollo
    - La verifica principale è sull'attivazione del servizio e sulla validità della password

POP3

- Esempio di sessione manuale
  - La connessione avviene
  - La password è errata e quindi non si può proseguire