



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

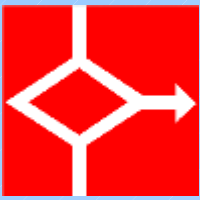


Ifconfig

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

```
Shell - Konsole <2>
wisdom:~ # ifconfig eth1
eth1      Link encap:Ethernet  HWaddr 00:02:2D:A5:49:29
          inet addr:192.168.1.21  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fe80::202:2dff:fea5:4929/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:5204 errors:0 dropped:0 overruns:0 frame:0
          TX packets:6462 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:100
          RX bytes:2415942 (2.3 Mb)  TX bytes:1072279 (1.0 Mb)
          Interrupt:3 Base address:0x100

wisdom:~ # █
```



Tcpdump

- Permette di vedere ed analizzare il traffico

```
Shell - Konsole <4>
wisdom:~ # tcpdump
tcpdump: listening on eth1
03:01:21.951824 host21.intranet.32772 > spider.cu.mi.it.domain: 64870+ A? nemo.mgeng.com. (32) (DF)
03:01:21.952757 host21.intranet.32773 > spider.cu.mi.it.domain: 61849+ PTR? 8.96.43.193.in-addr.arpa. (42) (DF)
03:01:22.010192 spider.cu.mi.it.domain > host21.intranet.32772: 64870 1/2/2 A 213.198.150.110 (128)
03:01:22.010697 host21.intranet > 213.198.150.110: icmp: echo request (DF)
03:01:22.013755 spider.cu.mi.it.domain > host21.intranet.32773: 61849* 1/3/3 PTR[ldomain]
03:01:22.014173 host21.intranet.32774 > spider.cu.mi.it.domain: 61850+ PTR? 21.1.168.192.in-addr.arpa. (43) (DF)
03:01:22.072441 spider.cu.mi.it.domain > host21.intranet.32774: 61850* 1/1/1 (117)
03:01:22.072806 host21.intranet.32774 > spider.cu.mi.it.domain: 61851+ PTR? 110.150.198.213.in-addr.arpa. (46) (DF)
03:01:22.074484 213.198.150.110 > host21.intranet: icmp: echo reply [tos 0x20]
03:01:22.074760 host21.intranet.32775 > spider.cu.mi.it.domain: 64871+ PTR? 110.150.198.213.in-addr.arpa. (46) (DF)
03:01:22.132482 spider.cu.mi.it.domain > host21.intranet.32774: 61851 NXDomain 0/1/0 (124)
03:01:22.136125 spider.cu.mi.it.domain > host21.intranet.32775: 64871 NXDomain 0/1/0 (124)
03:01:23.024090 host21.intranet > 213.198.150.110: icmp: echo request (DF)
03:01:23.092044 213.198.150.110 > host21.intranet: icmp: echo reply [tos 0x20]
03:01:23.092333 host21.intranet.32775 > spider.cu.mi.it.domain: 64872+ PTR? 110.150.198.213.in-addr.arpa. (46) (DF)
```

```
Shell - Konsole <5>
wisdom:~ # ping nemo.mgeng.com
PING nemo.mgeng.com (213.198.150.110) 56(84) bytes of data.
64 bytes from 213.198.150.110: icmp_seq=1 ttl=251 time=63.8 ms
64 bytes from 213.198.150.110: icmp_seq=2 ttl=251 time=67.9 ms

--- nemo.mgeng.com ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1013ms
rtt min/avg/max/mdev = 63.802/65.886/67.970/2.084 ms
wisdom:~ #
```



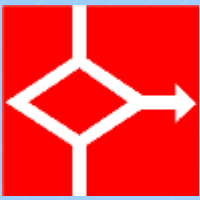
Tcpdump

- Per funzionare deve poter mettere la scheda di rete in modalità promiscua
- 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

```
Shell - Konsole <5>
wisdom:~ # traceroute nemo.mgeng.com
traceroute to nemo.mgeng.com (213.198.150.110), 30 hops max, 40 byte packets
 1  host254.intranet (192.168.1.254)  3.532 ms   3.434 ms   4.069 ms
 2  10.0.0.1  6.306 ms   4.653 ms   4.144 ms
 3  11.7206adsl.n.grapesnet.net (212.110.2.129)  53.648 ms   54.663 ms   53.142 ms
 4  212.110.30.10  60.035 ms   65.252 ms   58.058 ms
 5  * * *
 6  * * *
 7  * * *
 8  * * *
 9  * * *
10  * * *
11  * * *
12  * * *
13  * * *
14  * * *
15  * * *
16  * * *

wisdom:~ # █
```



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

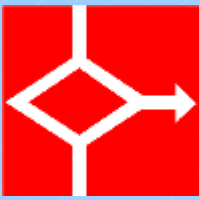
```
Shell - Konsole <5>
wisdom:~ # nslookup nemo.mgeng.com
Note: nslookup is deprecated and may be removed from future releases.
Consider using the `dig` or `host` programs instead. Run nslookup with
the `-slientl` option to prevent this message from appearing.
Server:          193.43.96.8
Address:         193.43.96.8#53

Non-authoritative answer:
Name:   nemo.mgeng.com
Address: 213.198.150.110

wisdom:~ # nslookup
Note: nslookup is deprecated and may be removed from future releases.
Consider using the `dig` or `host` programs instead. Run nslookup with
the `-slientl` option to prevent this message from appearing.
> server 213.198.150.110
Default server: 213.198.150.110
Address: 213.198.150.110#53
> nemo.mgeng.com
Server:          213.198.150.110
Address:         213.198.150.110#53

Name:   nemo.mgeng.com
Address: 213.198.150.110
> exit

wisdom:~ # █
```

Nslookup

- Query MX

```
Shell - Konsole <5>
> wisdom:~ # nslookup
Note: nslookup is deprecated and may be removed from future releases.
Consider using the 'dig' or 'host' programs instead. Run nslookup with
the '-silent]' option to prevent this message from appearing.
> set type=MX
> openfor.com
Server:          193.43.96.8
Address:         193.43.96.8#53

Non-authoritative answer:
openfor.com      mail exchanger = 10 pleiades.openfor.net.
openfor.com      mail exchanger = 20 cassiopea.openfor.net.

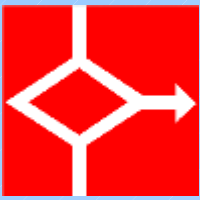
Authoritative answers can be found from:
openfor.com      nameserver = pleiades.openfor.net.
openfor.com      nameserver = cassiopea.openfor.net.
pleiades.openfor.net  internet address = 212.110.26.38
cassiopea.openfor.net  internet address = 213.198.143.245
> exit

wisdom:~ # █
```



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

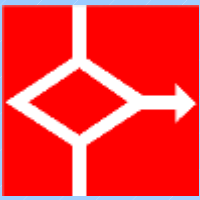
- Esempio di verifica che porta ad un errore di Relaying non permesso

```
Shell - Konsole <5>
wisdom:~ # telnet smtp.unimi.it 25
Trying 159.149.10.3...
Connected to smtp.unimi.it.
Escape character is '^I'.
220 smtp.unimi.it -- Server ESMTTP (iPlanet Messaging Server 5.1 (built May 7 2001))
HELO mgeng.com
250 smtp.unimi.it OK, [212.110.7.44].
MAIL FROM: gwb@whitehouse.com
250 2.5.0 Address Ok.
RCPT TO: gfranza@mgeng.com
550 5.7.1 Relaying not allowed: gfranza@mgeng.com
```



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

```
Shell - Konsole <5>
wisdom:~ # telnet localhost pop3
Trying ::1...
Connected to localhost.
Escape character is '^I'.
+OK ready <29265.1080524345@mercurio.mgeng.com>
user giovanni
+OK Password required for giovanni.
pass zxcvbnm
-ERR [AUTH] Password supplied for "giovanni" is incorrect.
user +OK Pop server at mercurio.mgeng.com signing off.
Connection closed by foreign host.
wisdom:~ # █
```