

Network Troubleshooting

Introduzione e concetti base

di Giovanni Perteghella [Digital Lab]



Webb.it 2004 - Padova

Copyright

Questo insieme di trasparenze è protetto dalle leggi sul copyright e dalle disposizioni dei trattati internazionali. Il titolo ed i copyright relative alle trasparenze (ivi inclusi, ma non limitatamente a, ogni immagine, fotografia, animazione, video e testo) sono di proprietà degli autori indicati.

Le trasparenze possono essere riprodotte ed utilizzate liberamente dagli istituti di ricerca, scolastici ed universitari afferenti al Ministero della Pubblica Istruzione per scopi istituzionali, non a fine di lucro. Ogni altra utilizzazione o riproduzione (ivi incluse, ma non limitatamente a, le riproduzioni a mezzo stampa, su supporti magnetici o su reti di calcolatori) in toto o in parte è vietata, se non esplicitamente autorizzata per iscritto, a priori, da parte dell'autore.

L'informazione contenuta in queste trasparenze è ritenuta essere accurata alla data della pubblicazione. Essa è fornita per scopi meramente didattici e non per essere utilizzata in progetti di impianti, prodotti, ecc.

L'informazione contenuta in queste trasparenze è soggetta a cambiamenti senza preavviso. Gli autori non si assumono alcuna responsabilità per il contenuto di queste trasparenze (ivi incluse, ma non limitatamente a, la correttezza, completezza, applicabilità ed aggiornamento dell'informazione).

In ogni caso non può essere dichiarata conformità all'informazione contenuta in queste trasparenze.

In ogni caso questa nota di copyright non deve mai essere rimossa e deve essere riportata anche in utilizzi parziali.

Sommario

- Di cosa parliamo
- Modello ISO/OSI
- Hardware
- Software

Di cosa parliamo

Le reti di comunicazione sono oggetti complessi , composti da un'insieme interconnesso di apparati hardware e software tramite i quali vengono forniti servizi agli utenti.

Diventa quindi estremamente importante identificare DOVE e COME si verifica il problema.

Cosa è il troubleshooting

Identificazione del problema

Raccolta delle informazioni

Progettazione della soluzione

Implementazione della soluzione

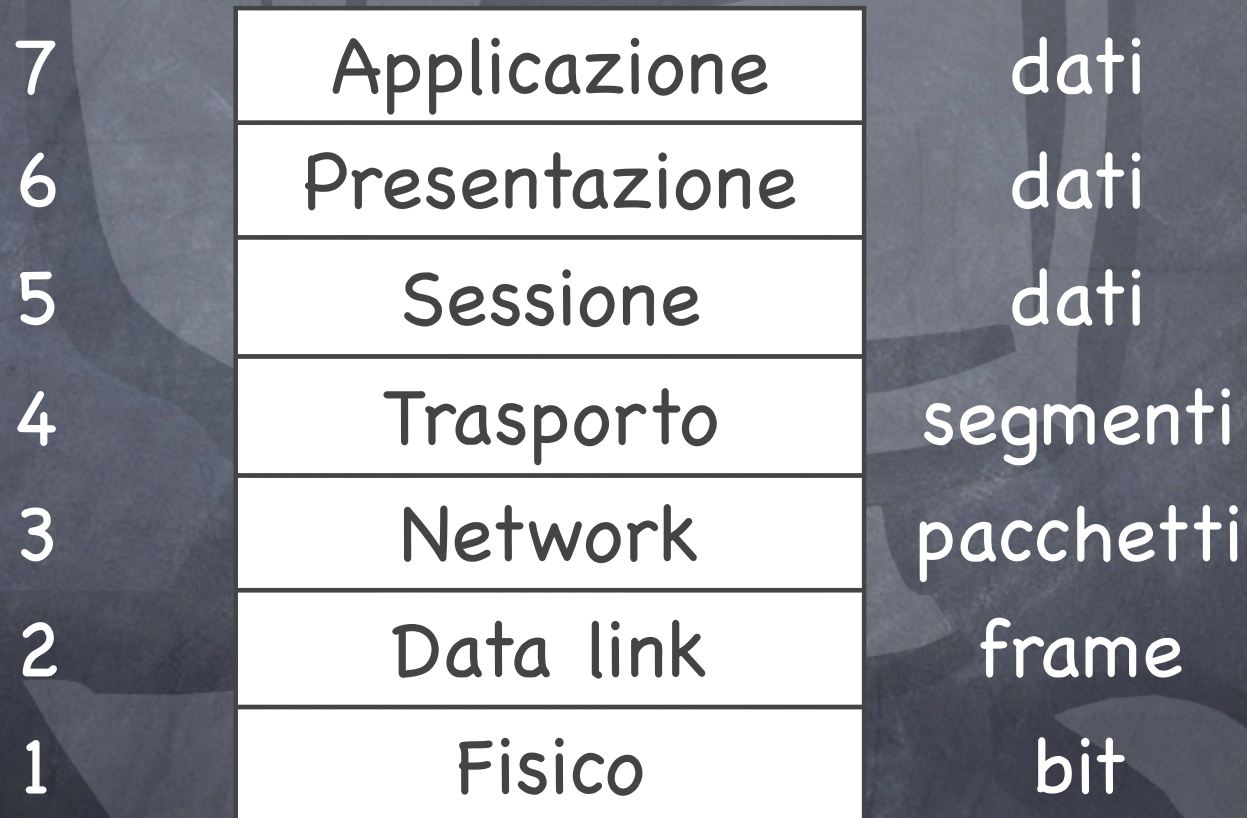
Il problema è risolto ?

Documentare il problema e la soluzione

Strumenti necessari

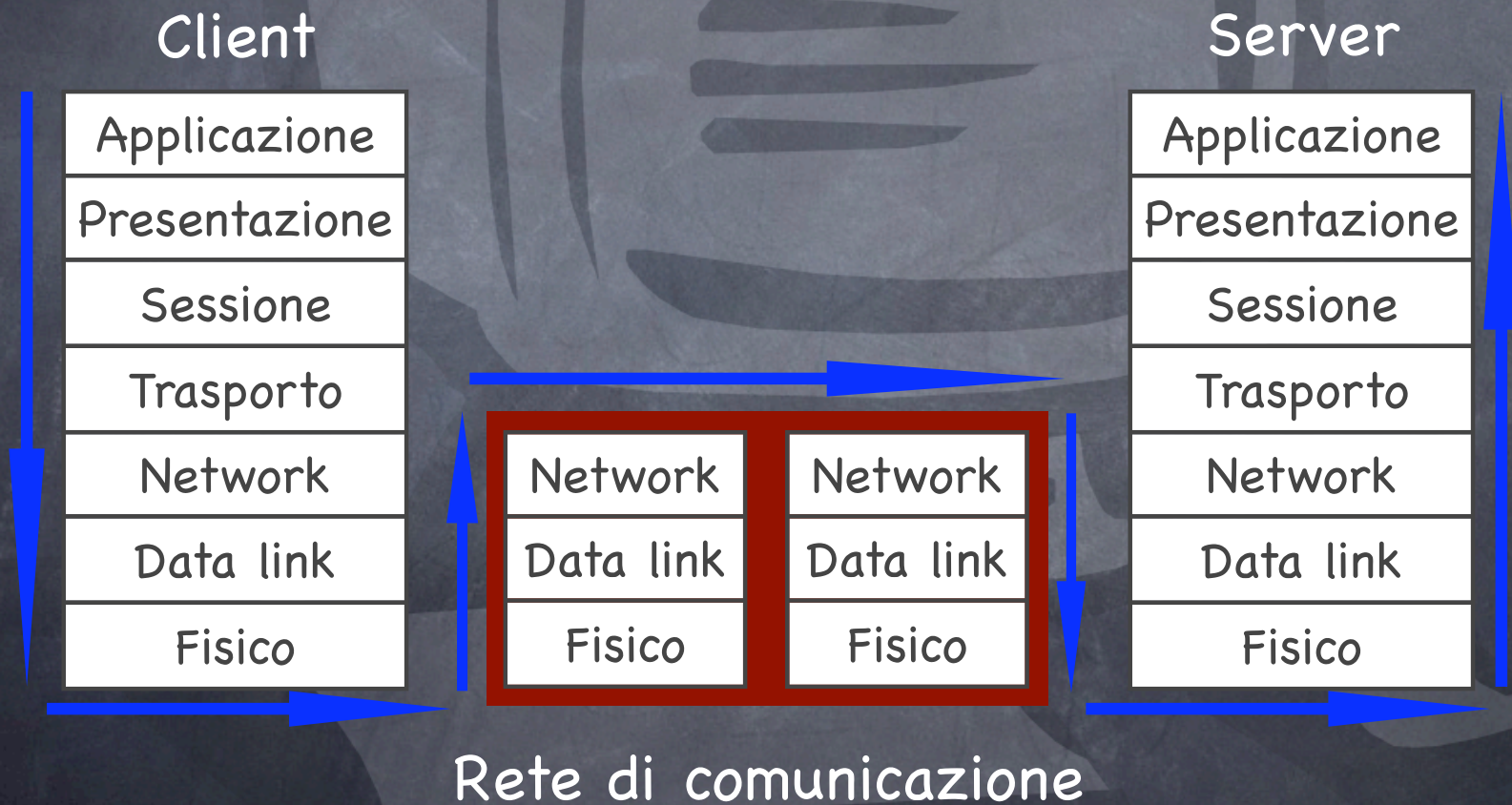
- Competenze sulle tecnologie e i protocolli utilizzati
- Esperienza
- Apparecchiature di misura
- Strumenti software di test

Il modello ISO/OSI

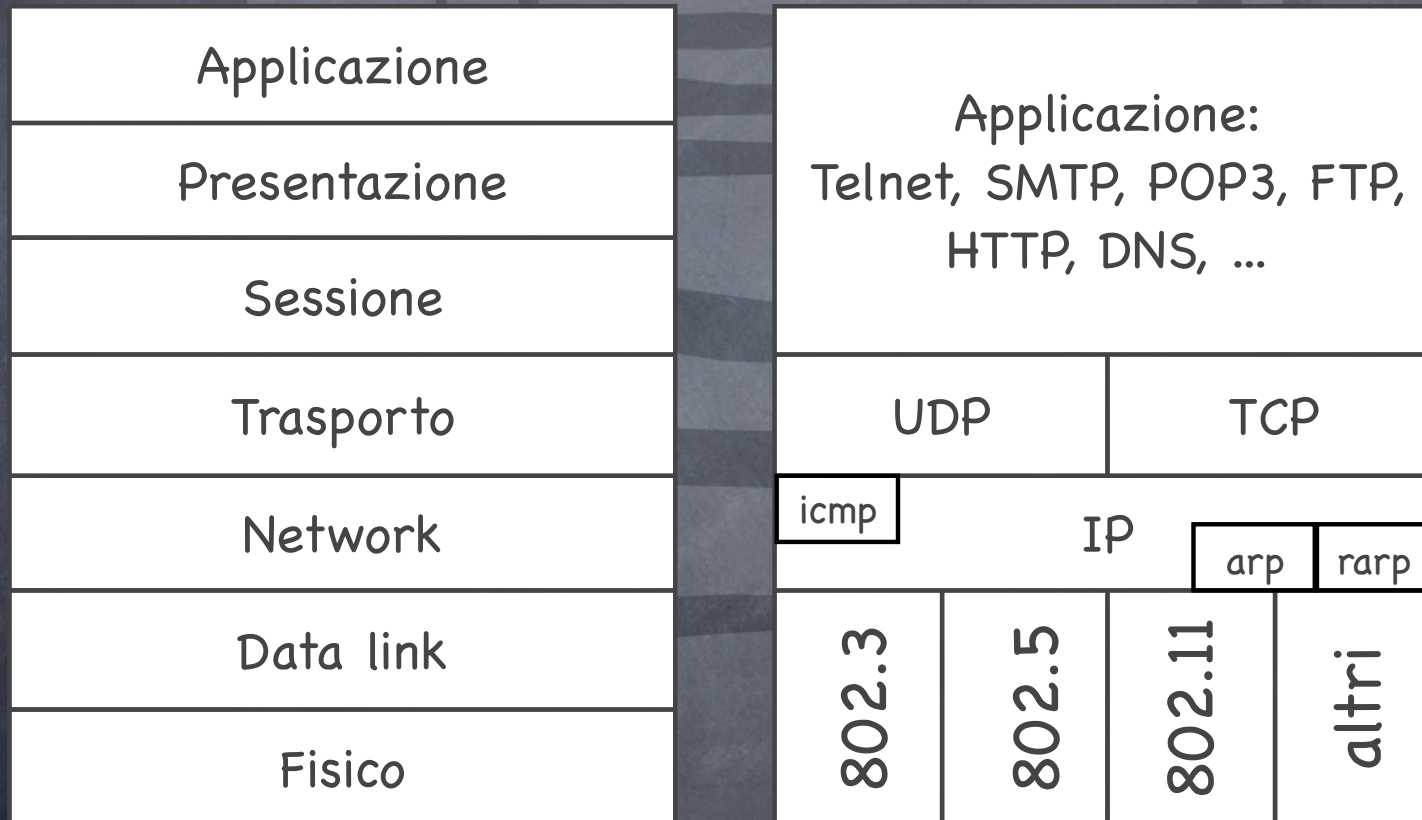


ISO International Standard Organization
OSI Open Systems Interconnection

Comunicazione client-server



ISO/OSI e TCP-IP



Livello 1: fisico

- Si occupa di trasmettere sequenze di bit sul canale di comunicazione definendo degli standard per :
 - le codifiche binarie per il mezzo trasmissivo
 - le caratteristiche dei mezzi trasmissivi e dei connettori

Problemi livello 1

- Interconnessioni elettriche e meccaniche non affidabili
- Cablaggio strutturato non certificato
- Interferenze EMI e RFI
- Problemi di messa a terra
- Parametri ambientali ostili

E' necessario utilizzare strumentazione dedicata per misurare questi fenomeni fisici.

Livello 2: data link

- Comunicazione sufficientemente affidabile ed efficiente tra nodi adiacenti.
- Nelle reti locali gestione della condivisione del mezzo trasmissivo.
- Servizi forniti al livello di rete
 - Impacchettamento
 - Controllo degli errori
 - Controllo di flusso
- Protocolli: HDLC, PPP, Ethernet

Problemi livello 2

- Problemi sugli indirizzi MAC
- Funzionamento degli switch come hub
- Protocollo di incapsulamento errato o malconfigurato
- Autenticazione fallita

Strumenti: arp, sniffer di rete

Livello 3: network

- Gestione dell'instradamento dei messaggi e determinazione se e quali sistemi intermedi devono essere attraversati dal pacchetto per raggiungere la destinazione.
- Determinazione del percorso migliore e gestione delle tabelle di instradamento e percorsi alternativi in caso di guasti (fault tolerance).

Protocollo TCP/IP: indirizzi e maschere di rete

Problemi livello 3

- Problemi sugli indirizzi IP
- Problemi sulle maschere di rete/sottorete
- Problemi con il Default Gateway
- Protocolli di routing non configurati sui router
- Problemi con il DHCP

Strumenti: arp, ifconfig, ping, traceroute, netstat -r

Livello 4: trasporto

- Servizi per il trasferimento dei dati end-to-end
- Aprire e chiudere le connessioni
- Frammentare e riassemblare i messaggi
- Rilevare e correggere gli errori
- Controllare il flusso e le congestioni
- Gestire connessioni multiple

Protocollo TCP/IP: porte dei servizi

Problemi livello 4

- Problemi sulle porte dei servizi
- Problemi di DNS
- Configurate errate nelle liste di controllo accessi dei router (ACL)
- Configurate errate nei Firewall

Strumenti: telnet, netstat, dig

Livelli 5-6-7

- Organizzazione del dialogo (mono o bidirezionale) e della sincronizzazione tra due programmi applicativi e del conseguente scambio di dati
- Gestione dei formati e compressione dei dati
- Presentazione dei dati all'utente

Applicativi client e server

Problemi livello 5-6-7

- Applicativi lato server configurati in maniera errata
- Applicativi client configurati in maniera errata
- Configurate errate nei Proxy

Strumenti: telnet

Strumenti software

- ifconfig (ipconfig)
- ping e traceroute
- arp
- telnet
- netstat
- nslookup e dig
- ethereal

ifconfig

Mostra le configurazione dell'interfaccia di rete

```
[Titanium:~] giovanni% ifconfig
en1: flags=8863<UP,BROADCAST,SMART,RUNNING,SIMPLEX,MULTICAST> mtu 1500
    ether 00:30:65:aa:bb:cc
    media: autoselect (<unknown type>) status: inactive
    supported media: autoselect
ppp0: flags=8051<UP,POINTOPOINT,RUNNING,MULTICAST> mtu 1500
    inet 85.211.80.17 --> 212.11.128.86 netmask 0xff000000
```

ping

Determina se il sistema remoto è raggiungibile

```
[Titanium:~] giovanni% ping www.webb.it  
PING webb.it (217.12.181.190): 56 data bytes  
64 bytes from 217.12.181.190: icmp_seq=0 ttl=51 time=225.169 ms  
64 bytes from 217.12.181.190: icmp_seq=1 ttl=51 time=209.397 ms  
64 bytes from 217.12.181.190: icmp_seq=2 ttl=51 time=192.884 ms
```

ping 2

```
ping [-Rdfnqrv] [-c count] [-i wait] [-l preload] [-p  
pattern]  
      [-s packetsize] host
```

- c invia "count" pacchetti poi termina
- f invia alla massima velocità i pacchetti sull'interfaccia
- i tempo di attesa fra un pacchetto e l'altro
- n non risolve gli indirizzi in nomi host
- s invia pacchetti di dimensione diversa da 56 (dati) + 8 (ICMP)
- v mostra tutti i pacchetti ICMP ricevuti

traceroute

Determina il percorso per raggiungere il sistema remoto

```
[Titanium:~] giovanni% traceroute www.webb.it
traceroute to webb.it (217.12.181.190), 30 hops max, 40 byte packets
 1  padz-as550-001.swip.net (212.11.128.86)  124.076 ms  112.852 ms  151.978 ms
 2  padz-ro7304-001.gigabiteth0-0.swip.net (212.151.132.65)  108.241 ms  119.963 ms  116.07 ms
 3  milz-ro7304-001.pos2-0.swip.net (212.151.130.25)  109.696 ms  109.57 ms  101.301 ms
 4  mill-core.gigabiteth0-0.swip.net (130.244.194.33)  117.323 ms  110.502 ms  101.334 ms
 5  * zurl-core.pos2-0.swip.net (130.244.194.97)  115.463 ms  106.569 ms
 6  fe0-0-sinister-sam.zur.router.colt.net (194.42.48.4)  108.241 ms  123.432 ms  110.274 ms
 7  fa2-0-0-caesar.mil.router.it.colt.net (212.31.224.102)  362.338 ms  201.798 ms  201.748 m
 8  212.31.233.2 (212.31.233.2)  189.788 ms  191.991 ms  189.24 ms
 9  217.12.178.211 (217.12.178.211)  197.364 ms  181.686 ms *
10  webbit.160-191.webbitpro.com (217.12.181.190)  234.561 ms  201.895 ms  188.964 ms
```

arp

Visualizza la tabella di associazione fra indirizzi MAC (L2) e indirizzi IP (L3)

```
arp [opzioni] [hostname]
```

- a - visualizza il contenuto della cache locale
- s - aggiunge una voce statica alla tabella
- d - cancella una voce della tabella

netstat

Mostra le statistiche e lo stato delle connessioni TCP/IP attive

```
NETSTAT [-a] [-e] [-n] [-s] [-p proto] [-r]  
[intervallo]
```

-a Visualizza tutte le connessioni e le porte di ascolto.

-n Visualizza gli indirizzi e i numeri di porta in forma numerica.

-p proto Visualizza connessioni del protocollo specificato da 'proto' che può essere TCP o UDP. Se usato con l'opzione -s per le statistiche, 'proto' può essere TCP, UDP, o IP.

netstat

-r Visualizza la tabella di routing
-s Visualizza le statistiche per protocollo. Per impostazione predefinita, le statistiche sono visualizzate per TCP, UDP e IP; l'opzione -p può essere utilizzata per specificare un sottoinsieme dell'impostazione predefinita.
Intervallo rivisualizza le statistiche selezionate, interrompendo per un numero di secondi pari a "intervallo" tra ogni visualizzazione. Premere CTRL+C per fermare la visualizzazione delle statistiche.

telnet

- Permette di verificare e interagire con applicativi di livello 7 tramite un'emulazione di terminale.
- E' necessario conoscere la sintassi del protocollo utilizzato (es. HTTP, POP3, SMTP, ...)

telnet 2

```
[Titanium:~] giovanni% telnet mail.tin.it 25
Trying 62.211.72.20...
Connected to mail.tin.it.
Escape character is '^]'.
220 vsmt2.tin.it ESMTP Service (7.0.027) ready
helo
250 vsmt2.tin.it Missing required domain name in
HELO, defaulted to your IP address [81.211.10.17]
quit
221 vsmt2.tin.it QUIT
Connection closed by foreign host.
```

dig

- Interroga il servizio DNS, senza il quale internet sarebbe praticamente inutilizzabile.
- `dig @193.205.245.66 www.webb.it any`

Sniffer di rete

- Per problemi complessi è necessario catturare e decodificare il flusso dei dati in transito tramite degli sniffer di rete che si “mettono in ascolto passivo” sul mezzo trasmissivo.
- TcpDump e Ethereal sono alcuni dei software più noti.



Domande ?

Contatti e riferimenti

- email: giovanni@sirio.com
- slides disponibili su:
<http://webb.it/event/eventview/3275/>
<http://sirio.com/dl/>



<http://www.macitynet.it>

pòc

<http://www.poc.it>



<http://www.sirio.com>



<http://www.ifoait>

Bibliografia

Internet e Reti di calcolatori

James F.Kurose, Keith W.Ross

McGraw-Hill

ISBN 88-386-6011-5

CCNA INTRO

Wendell Odom

Cisco Press

ISBN 1-57870-094-5

CCNA ICND

Wendell Odom

Cisco Press

ISBN 1-57720-083-x