

POLITECNICO di TORINO
Dipartimento di Elettronica

Dispense parte di laboratorio corso
Introduzione alle reti
telematiche

Marco Mellia, Paolo Giaccone
E-mail: {mellia,giaccone}@tlc.polito.it

5 aprile 2006

Indice

1	Introduzione	3
1.1	Materiale richiesto	3
2	Configurazione software e hardware degli host: analisi a livello utente	4
2.1	Scopo	4
2.2	Documentazione disponibile	4
2.3	Descrizione dell'esercitazione	4
2.3.1	Configurazione di una rete	4
2.3.2	Verifica connettività a livello rete	5
2.3.3	Verifica modalità di funzionamento consegna diretta	5
2.3.4	Protocollo ARP	5
2.3.5	Configurazioni di indirizzamento atipiche e sbagliate	6
3	Configurazione software e hardware degli host: analisi a livello rete	7
3.1	Scopo	7
3.2	Documentazione disponibile	7
3.3	Descrizione dell'esercitazione	7
3.3.1	Analisi di base.	7
3.3.2	Consegna diretta e risoluzione di indirizzi: il protocollo ARP	9

1 Introduzione

Questa vuole essere una raccolta di esercitazioni da svolgere durante il corso di Introduzione alle reti telematiche. Verranno proposte diverse esercitazioni da svolgere in laboratorio. Il corso presenta contenuti fortemente sperimentali, e permette agli studenti di applicare le nozioni apprese nei corsi precedenti riguardanti il funzionamento delle reti locali (LAN) e dei protocolli della rete Internet.

Per lo svolgimento del corso, gli studenti hanno a disposizione un laboratorio attrezzato con diversi apparati di rete, quali hub, switch, cavi, etc. Sono inoltre a disposizione dei Personal Computer dotati di sistema operativo Linux, configurati come host.

Esiste tutta una documentazione online all'indirizzo <http://www.tlc-networks.polito.it/mellia/corsi/>. Essa raccoglie una serie di documenti che possono essere utili durante lo svolgimento del laboratorio. In parte, essa è stata prodotta appositamente; in parte invece è frutto di lavoro di altri, raccolto e messo a disposizione degli studenti.

1.1 Materiale richiesto

Per lo svolgimento del corso, ogni gruppo ha a disposizione:

- Personal Computer dotati di una o più interfacce Ethernet e dotato di Sistema Operativo Linux.
- cavi UTP, connettori RJ45
- 1 switch a 5 porte

2 Configurazione software e hardware degli host: analisi a livello utente

2.1 Scopo

Lo scopo di questa esperienza è capire i meccanismi di configurazione di host e router IP, provando a creare delle reti locali. Verranno connessi tramite hub/switch i PC a disposizione, e verrà controllato il corretto funzionamento delle reti create.

2.2 Documentazione disponibile

- Manuali dei comandi `ifconfig`, `ping`, `arp`, `route`

<http://www.telematica.polito.it/mellia/corsi/05-06/Laboratorio/doc/ifconfig.html>

<http://www.telematica.polito.it/mellia/corsi/05-06/Laboratorio/doc/ping.html>

<http://www.telematica.polito.it/mellia/corsi/05-06/Laboratorio/doc/route.html>

<http://www.telematica.polito.it/mellia/corsi/05-06/Laboratorio/doc/arp.html>

2.3 Descrizione dell'esercitazione

2.3.1 Configurazione di una rete

Ogni gruppo dispone di cavi UTP. In ogni isola, si connettano i terminali a disposizione tramite lo switch ethernet.

1. Si disabilitino le interfacce di rete con i comandi:

```
ifconfig eth0 down
ifconfig eth1 down (per gli host dotati di 2 schede di rete)
```

Si crei una rete con al massimo 128 hosts, utilizzando indirizzi privati IP di classe A (10.x.x.x). Per configurare l'indirizzo IP *IP_ADDRESS* (nel formato decimale X.X.X.X), la subnet mask *NET_MASK* e L'indirizzo di broadcast *BROADCAST* si utilizzi il comando

```
ifconfig eth0 IP_ADDRESS netmask NET_MASK broadcast BROADCAST
ifconfig eth0 up
```

2. Verificare la configurazione delle interfacce con il comando

```
ifconfig -a
```

Quante interfacce sono presenti? Come sono configurate? Gli indirizzi dell'host, di rete e di broadcast sono corretti?

3. Verificare l'aggiornamento delle tabelle di routing tramite il comando

```
route -n
```

Che host risultano raggiungibili secondo le tabelle di routing? Provare a configurare una interfaccia aggiuntiva se disponibile. Come variano le tabelle di routing?

2.3.2 Verifica connettività a livello rete

Verificare la connettività da un host verso un'altro (e viceversa) con indirizzo IP *IP_ADDRESS* mediante il comando

```
ping IP_ADDRESS
```

Si indichi con una targhetta il nome della interfaccia eth0. Suggerimento: nel caso in cui non funzionasse il comando `ping`, provare a connettere la seconda interfaccia Ethernet e riprovare.

1. In che modo il Sistema Operativo associa i nomi logici alle interfacce?
2. Eseguendo il comando di ping, si riceve il seguente output:

```
PING 10.0.0.1 (10.0.0.1) from 10.0.0.2 : X bytes of data.  
Y bytes from 10.0.0.2: icmp_seq=0 ttl=253 time=3.3 ms
```

quale è il significato preciso dei valori *X* e *Y* ?

2.3.3 Verifica modalità di funzionamento consegna diretta

1. Si determini l'indirizzo MAC di TUTTE le schede di rete disponibili sull'host.
2. Si determini sperimentalmente il massimo range di indirizzi IP raggiungibili da un host, usando il comando `ping`.

Si ponga la netmask a 255.255.0.0 su tutti gli host. Supponendo di non conoscere la netmask (e quindi la dimensione della sottorete a cui si è connessi), come è possibile determinare il nuovo massimo range di indirizzi IP raggiungibile da un host.

3. Cosa succede se si mandano pacchetti ICMP verso l'indirizzo di rete?
4. Cosa succede se si mandano pacchetti ICMP verso l'indirizzo broadcast?
5. Spiegare brevemente tutte le opzioni di `ifconfig`, `ping`, `route` utilizzate finora.
6. Descrivere la configurazione corrente del proprio host, commentando tutti i campi di vostra conoscenza dell'output dei comandi `route`, `ifconfig`.

2.3.4 Protocollo ARP

Ricordando che tutti gli host appartengono alla stessa sottorete IP, i terminali scambiano tra loro delle PDU mediante il meccanismo di consegna diretta. Questo prevede che l'host sorgente crei una PDU di livello rete contenente come indirizzo di destinazione quello del terminare che si vuole contattare. Per poter trasmettere tale PDU, l'host sorgente deve creare una PDU Ethernet contenente come SDU la PDU IP. Come indirizzo MAC, l'host dovrà inserire quello del terminale remoto. Per poter conoscere tale indirizzo, l'host dovrà associare all'indirizzo IP (noto) della destinazione con l'indirizzo MAC (non noto) della stessa. Per fare questo si usa il protocollo *ARP* Address Resolution Protocol. Una volta effettuata l'associazione, il terminale mantiene tali informazioni in tabelle, dette *tabelle di ARP*. Per capire il funzionamento di tali meccanismi, si eseguano i seguenti punti.

1. Si configuri la rete come nel punto Sec. 2.3.1. Dopo aver eseguito in ping tra tutte le stazioni, si consultino le tabelle di ARP mediante il comando

`arp`

Spiegare il significato dell'output del comando.

2. Si individui, sia nel caso di ARP-request che di ARP-reply, quali sono gli host che aggiornano le tabelle di ARP, spiegando la metodologia adottata.
3. Si provi a contattare un host inesistente appartenente alla propria sottorete e verificare il contenuto delle ARP tables.
4. Si provi a contattare un host inesistente non appartenente alla propria sottorete e verificare il contenuto delle ARP tables.
5. Verificare la durata delle entry nella tabella di ARP. Suggerimento: cancellare la tabella, e far creare due entry, una per un host raggiungibile, e una per un host non raggiungibile. Cronometrare usando il comando `date`.

2.3.5 Configurazioni di indirizzamento atipiche e sbagliate

1. Cosa succede se due host hanno lo stesso indirizzo IP? Verificare attentamente la connettività da un terzo host verso l'indirizzo comune consultando le tabelle ARP.
2. Si configurino due host in modo che un host veda l'altro come appartenente alla medesima sottorete ma non viceversa. Verificare la connettività tra i due host.

Si configuri l'host *A* con indirizzo *10.0.0.1/24* e l'host *B* con l'indirizzo *10.0.0.255/23*. Si verifichi la connettività reciproca tra i due host. Cosa succede? Che indirizzo usa *A* per *B*? Che indirizzo usa *B* per *A*?

3 Configurazione software e hardware degli host: analisi a livello rete

3.1 Scopo

Lo scopo di questa seconda esercitazione è ripetere alcune esperienze svolte durante l'esercitazione precedente, osservando le PDU che vengono generate a seguito dei comandi utente. Grazie all'uso di analizzatori di protocollo software, o *sniffer*, si potranno osservare le sequenze di PDU scambiate dagli host al seguito di comandi utente. Grazie alla possibilità delle schede Ethernet di attivare la modalità promiscua, E' possibile da una stazione osservare tutte le PDU che vengono ricevute dal livello fisico dal terminale, indipendentemente se destinate al terminale stesso o meno a livello collegamento. Questo permette quindi di osservare la sequenza di PDU che vengono trasmesse/ricevute sulla LAN.

Nota: per motivi di sicurezza, per poter attivare la cattura di pacchetti in modalità promiscua, è necessario avere i privilegi di amministratore di sistema (root in UNIX). E' necessario ricordare che l'abuso nell'uso di sniffer può violare il diritto alla riservatezza dei dati e pertanto è perseguibile legalmente. Pertanto si consiglia di non usare queste capacità in reti operative di cui non si hanno le autorizzazioni per l'uso di tali mezzi.

3.2 Documentazione disponibile

- Ethereal home page
<http://www.ethereal.com>
- RFC sourcebook
<http://www.networksorcery.com/enp/>
- Manuali dei comandi `route`, `nmap`
<http://www.telematica.polito.it/mellia/corsi/05-06/Laboratorio/doc/route.html>
<http://www.telematica.polito.it/mellia/corsi/05-06/Laboratorio/doc/nmap.html>

3.3 Descrizione dell'esercitazione

3.3.1 Analisi di base.

Lo scopo di questa prima parte della esercitazione è prendere confidenza con Ethereal, il programma di cattura PDU. Lo sniffer viene lanciato mediante il comando

```
ethereal &
```

(il carattere `&` permette di eseguire in comando che lo precede in background, ovvero restituendo immediatamente il controllo all'interprete dei comandi (shell), senza aspettare la fine dell'esecuzione del comando stesso.

Dal menu *Capture*, si avvia la cattura sull'interfaccia appropriata (eth0 o eth1). Da un host, si lancia il comando `ping` verso un altro host della propria sottorete. Dopo alcuni secondi, si clicca su STOP per fermare l'operazione di cattura. Sulla finestra principale del programma, comparirà la lista completa dei pacchetti catturati. Cliccando su ciascuno di essi, sarà possibile

verificare il contenuto a livello di frame Ethernet, pacchetto IP, ICMP, o qualunque altro tipo di protocollo riconosciuto dal programma di cattura.

Si faccia ora il ping da un host agli altri due dell'isola contemporaneamente, usando due finestre con interpreti dei comandi.

Per poter distinguere i pacchetti trasmessi da un terminale o dall'altro, è possibile usare dei *filtri*. Esistono due tipi di filtri in Ethereal:

- filtri di cattura
- filtri di visualizzazione.

I *filtri di cattura* vengono attivati direttamente durante la cattura delle PDU. Se la PDU appena ricevuta non passa il filtro di cattura, questa verrà scartata e non verrà mostrata. La sintassi dei filtri di cattura è specificata dalla libreria `libpcap`. Essa è di fatto uno standard per programmi di cattura, che pertanto permettono tutti di specificare dei filtri di cattura secondo la stessa sintassi. Per una descrizione dei filtri di cattura possibili, fare riferimento al manuale di `tcpdump`.

I *filtri di visualizzazione* permettono di mostrare solo le PDU già catturate che soddisfano il filtro impostato. La sintassi dei filtri di visualizzazione è diversa da quella dei filtri di cattura, in quanto propria di Ethereal. Una descrizione dei filtri di visualizzazione è disponibile sul manuale di Ethereal. Inoltre risulta molto utile usare i filtri di visualizzazione per evidenziare PDU particolari, per esempio usando colori diversi.

1. Si descrivano i filtri in cattura per selezionare solo i pacchetti che coinvolgono due host.
2. Si descrivano i filtri in visualizzazione per selezionare solo i pacchetti che coinvolgono due host.
3. Si descrivano i filtri per colorare di colore differente i pacchetti *ICMP Echo request* e *ICMP Echo reply*.
4. Mediante i risultati riportati dallo sniffer, si disegni l'incapsulamento a livello collegamento (Ethernet), rete (IP) e controllo (ICMP), specificando le dimensioni dell'header e payload di ciascuno.
5. Eseguendo il comando di ping, si riceve il seguente output:

```
PING 10.0.0.1 (10.0.0.1) from 10.0.0.2 : X bytes of data.  
Y bytes from 10.0.0.2: icmp_seq=0 ttl=253 time=3.3 ms
```

quale è il significato preciso dei valori X e Y? Rispetto a quanto identificato senza l'uso dell'analizzatore di protocolli, cosa è stato possibile identificare in aggiunta?

6. Verificare il tipo di protocollo di livello collegamento (IEEE 802.3 o Ethernet II) viene usato per comunicare tra i diversi host.

3.3.2 Consegna diretta e risoluzione di indirizzi: il protocollo ARP

Verificare che le tabelle di ARP siano vuote mediante il comando

```
arp
```

Eseguire un ping, mentre si è attivata la cattura su un altro terminale.

1. Descrivere lo scambio di messaggi che avvengono mediante un diagramma spazio-tempo. Eseguire la prova per almeno 70 secondi.

Per i pacchetti ARP-request e ARP-reply, quali sono gli indirizzi MAC di destinazione?

2. Si utilizzi una dimensione dei pacchetti di ICMP pari a 1,10,100,5000 bytes. Si disegni l'incapsulamento a livello Ethernet, IP e ICMP, visualizzando tutte le informazioni relative all'incapsulamento.

Si osservino tutti i campi che variano nelle PDU Ethernet, IP e ICMP, al variare dei seguenti fattori: messaggi ICMP ECHO REQUEST/REPLY, numero di tentativo di ping, dimensione del pacchetto di ping (1,10,100,5000)

3. Si descriva come avviene la frammentazione a livello IP nel caso in cui si dia il comando:

```
ping -s 5000
```

4. Se si perde connettività tra due host a causa dell'interruzione del cavo, durante un ping, cosa succede?
5. Se si perde connettività a causa di un guasto tra due host a causa del cambiamento temporaneo di indirizzo dell'interfaccia, durante un ping, cosa succede? Se il guasto dura meno di 5 secondi? Più di 5 secondi? Oltre 60 secondi?
6. Come viene calcolato il Round Trip Time (RTT) mediante il comando ping? Mostrare un caso in cui il RTT del primo pacchetto ICMP del ping sia chiaramente superiore a quello calcolato tramite i successivi pacchetti e spiegarne il motivo.