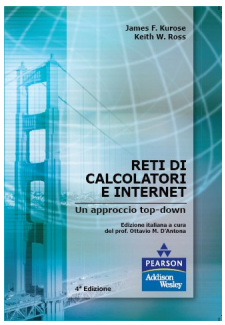
Laboratorio Wireshark: IP



In questo laboratorio studieremo il protocollo IP, focalizzandoci sulla struttura dei datagrammi IP. Lo faremo analizzando una traccia di datagrammi IP inviati e ricevuti dal programma `traceroute` (il programa `traceroute` in sé è stato analizzato in maggior dettaglio durante il laboratorio Wireshark ICMP). Studieremo i vari campi dell'intestazione IP e la frammentazione IP.

Prima di iniziare il laboratorio, vorrete probabilmente rivedere la sezione 1.4.3 nel libro di testo e la sezione 3.4 della RFC 2151 [ftp://ftp.rfc-editor.org/in-notes/rfc2151.txt] per aggiornarvi sulle operazioni del programma `traceroute`. Dovreste anche leggere la Sezione 4.4 nel libro di testo e probabilmente avere sottomano la RFC 791 [ftp://ftp.rfc-editor.org/in-notes/rfc791.txt] per una discussione del protocollo IP[1].

1. Catturare i pacchetti per una esecuzione di traceroute

In questo laboratorio faremo uso del programma `traceroute` per mandare datagrammi IP di differenti dimensioni verso la stessa destinazione, X. Ricordate che `traceroute` opera dapprima inviando uno o più datagrammi col campo time-to-live (TTL) nell'intestazione IP settato ad 1; successivamente invia una serie di ulteriori datagrammi verso la stessa destinazione con un TTL pari a 2; successivamente invia una serie di ulteriori datagrammi verso la stessa destinazione con un TTL pari a 3; e così via. Ricordate anche che un router deve decrementare il campo TTL di ogni datagramma ricevuto di 1 (in realtà, RFC 791 dice che il router deve decrementare il campo TTL di *almeno uno)*. Se il TTL raggiunge il valore 0, il router restituisce un messaggio ICMP (tipo 11 – TTL-exceeded) all'host mittente. Come risultato di qusto comportamento, un datagramma con un TTL di 1 (mandato dall'host che sta eseguendo `traceroute`) causerà l'invio di un pacchetto ICMP TTL-exceeded da parte del primo router incontrato; il datagramma mandato con TTL pari a 2 causerà l'invio del pacchetto ICMP da parte del secondo router; e così via. In questa maniera, il sistema terminale che esegue `traceroute` può imparare le identità dei router tra sé e la destinazione X guardando gli indirizzi IP sorgente nei datagrammi contenenti i messaggi ICMP TTL-exceeded.

Vogliamo eseguire `traceroute` e fargli mandare datagrammi di varia lunghezza.

- **Windows**. Il programma `tracert` (usato nel laboratorio Wireshark ICMP) fornito con Windows non consente di cambiare la dimensione del messaggio ICMP echo request (ping) inviato. Un scelta migliore per Windows è *pingplotter*, disponibile nelle versioni libere e shareware al sito http://www.pingplotter.com. Scaricate e installate *pingplotter*, e provatelo eseguendo un po' di traceroute verso i vostri siti preferiti. La dimensione del messaggio ICMP echo request può essere settata esplicitamente in *pingplotter* selezionando la voce di menù *Edit* → *Options* → *Packet Options* e riempiendo il campo *Packet Size*. La dimensioni di default è di 56 byte. Una volta che *pingplotter* ha mandato una serie di pacchetti con TTL

1 Tutti i riferimenti al testo riguardano il libro *Reti di calcolatori e Internet: Un approccio top-down*, 4a edizione italiana.

crescente, riparte il processo di spedizione di nuovo dal valore TTL di 1, dopo aver atteso un intervallo di tampo parti a *Trace Internal*. Il valore di *Trace Interval* e il numero di intervalli può essere impostato esplicitamente.

- **Linux/Unix**. Col comando `traceroute` di Unix, la dimensione del datagramma UDP mandato verso la destinazione può essere impostato esplicitamente indicando il numero di byte nel datagramma; il valore viene immesso nella riga di comando di `traceroute` immediatamente dopo il nome o l'indirizzo della destinazione. Per esempio, per inviare datagrammi `traceroute` di 2000 byte verso gaia.cs.umass.edu, il comando sarebbe:

```
traceroute gaia.cs.umass.edu 2000
```

Fate quanto segue:

- Fate partire Wireshark e iniziate la cattura dei pacchetti.
- Se state usando una piattaforma Windows, fate partire *pingplotter* e immettete il nome di un sistema terminale destinazione nella finestra "Address to Trace". Immettete 3 nel campo "# of times to Trace", così che non raccogliate troppi data. Selezionate la voce di menù *Edit* → *Advanced Options* → *Packet Options* e immettete il valore 56 in campo *Packet Size*, poi premete OK. A questo punto premete il pulsante Trace. Dovreste vedete la finestra di *pingplotter* che assomiglia a questa:
  Successivamente, inviate altri datagrammi con una dimensione maggiore, selezionando *Edit* → *Advanced Options* → *Packet Options*, immettendo il valore 2000 nel campo *Packet Size* e premendo OK. Quindi premere il tasto Resume.

  Infine, mandare altri datagrammi con una dimensione ancora maggiore, selezionando *Edit* → *Advanced Options* → *Packet Options*, immettendo il valore 3500 nel campo *Packet Size* e premendo OK. Quindi premere il tasto Resume.
- Se state usando una piattaforma Unix/Linux, immettete tre comandi `traceroute`, uno con una dimensione di 56 byte, uno con una dimensione di 2000 byte e uno con una dimensione di 3500 byte, verso un host a vostra scelta. In aula informatica, inserire goemon come host destinazione.

  Interrompete la cattura dei pacchetti.

Se non siete in grado di eseguire Wireshark su una connessione di rete dal vivo, potete scaricare un file con la traccia di pacchetti catturata, eseguendo le istruzioni di cui sopra, da uno dei computer Windows degli autori[2]. Potreste trovare utile scaricare questa traccia anche se avete catturato la vostra, e usarla assieme quando risponderete alle domande che seguiranno.

2. Uno sguardo alla traccia catturata

Nella vostra traccia dovreste essere in grado di vedere la serie di pacchetti ICMP Echo Request (nel caso di macchine Windows) o segmenti UDP (nel caso di Unix) inviati dal vostro computer, e i messaggi ICMP TTL-exceeded restituiti al vostro computer dai router intermedi. Nelle domande che seguiranno, assumeremo che stiate usando una macchina Unix; le corrispondenti domande per il caso di macchine Windows dovrebbero essere chiare. Quando possibile, nel rispondere ad una domanda, dovreste consegnare una stampa dei pacchetti all'interno della traccia che avete usato per rispondere. Annotate la stampa per spiegare la costra risposta. Per stampare un pacchetto usate *File* → *Print*, scegliere *Selected packet only*, scegliete *Packet Summary Line* e selezionate il minimo

2 Scaricare il file http://gaia.cs.umass.edu/wireshark-labs/wireshark-traces.zip ed estraete il file *ip-ethereal-trace-1*. Le tracce in questo file zip sono state raccolte da Wireshark in esecuzione su uno dei computer degli autori, eseguendo i passi indicati qui sopra. Una volta scaricata la traccia, la potete caricare ed esaminare in Wireshark usando il menù a discesa *File*, scegliendo *Open*, e selezionando il file ip-ethereal-trace-1.

ammontare di dettagli che è necessario per rispondere alla domanda.

1. Selezionate il primo pacchetto UDP inviato dal vostro computer, ed espandete la sezione relativa a Internet Protocol nella finestra dei dettagli sui pacchetti. Qual è l'indirizzo IP del vostro computer?
2. All'interno della intestazione IP, qual è il valore del protocollo di livello superiore?
3. Quanti byte ci sono nell'intestazione IP? Quanti byte ci sono nel payload del datagramma IP. Spiegate come avete determinato il numero di byte del payload.
4. Questo datagramma IP è stato frammentato? Spiegate come avete determinato se il datagramma IP è stato frammentato o meno.

Adesso ordinate i pacchetti sulla base dell'indirizzo IP sorgente, cliccando sulla intestazione della colonna *Source*; una piccola freccia verso il basso dovrebbe comparire accanto alla parola *Source*. Se la freccia punta verso l'alto, cliccate di nuovo sull'intestazione della colonna. Selezionare il primo pacchetto UDP inviato dal vostro computer, ed espandete la sezione relativa a *Internet Protocol* nella finestra di "dettaglio dei pacchetti". Nella finestra di "elenco dei pacchetti catturati" dovreste vedere, sotto il primo messaggio UDP, tutti i successivi messaggi UDP (possibilmente con pacchetti in più inframezzati, inviati da altre applicazioni in esecuzione sul vostro computer). Usate i tasti freccia sulla tastiera per muoversi attraverso questi messaggi UDP.

5. Quali campi nei datagrammi IP cambiano *sempre* da un datagramma al successivo all'interno di questa serie di messaggi UDP inviati dal vostro computer?
6. Quali campi sono costanti? Quali dei campi devono *essere* costanti? Quali campi devono cambiare? Perché?
7. Descrivere lo schema che vedete nel valore del campo Identification del datagramma IP.

Successivamente (con i pacchetti ancora ordinati in base all'indirizzo sorgente) trovare la serie di risposte ICMP TTL-exceeded inviati al vostro computer dal router di primo hop.

8. Quali sono i valori del campo Identification e del campo TTL?
9. Questi valori rimangono invariati per tutti i pacchetti ICMP TTL-exceeded inviati al vostro computer dal router di primo salto? Perché?
10. Come si fa a collegare un pacchetto ICMP TTL-exceeded con il pacchetto ICMP echo-request o UDP che lo ha causato?

3. Frammentazione

Ordinate i pacchetti di nuovo in base al tempo cliccando sulla colonna *Time*.

11. Trovate il primo segmento UDP con dimensione di 2000 byte che è stato inviato dal vostro computer. Questo segmento è stato frammentato in più di un datagramma IP? [Nota: se trovate che il pacchetto non è stato frammentato dovete scaricare il file zip http://gaia.cs.umass.edu/wireshark-labs/wireshark-traces.zip ed estrarre la traccia *ip-ethereal-trace-1*. Se il vostro computer ha una interfaccia Ethernet, un dimensione di pacchetto di 2000 byte *deve* causare frammentazione.[3]]

3 I pacchetti in *ip-ethereal-trace-1* nel file http://gaia.cs.umass.edu/wireshark-labs/wireshark-traces.zip sono tutti più piccoli di 1500 byte. Questo accade perché il computer sul quale questa traccia è stata catturata ha una interfaccia Ethernet, che limita la lunghezza dei pacchetti IP a 1500 byte. Se la vostra traccia indica la presenza di un datagramma di dimensione superiore a 1500 byte, e il vostro computer sta usando una connessione Ethernet, allora Wireshark sta restituendo una dimensione errata; probabilmente mostrerà anche un unico grosso datagramma IP invece che molti piccoli datagrammi IP. Questa inconsistenza è dovuta all'interazione tra i driver della scheda Ethernet e il software Wireshark. Nel caso si verifichi questa inconsistenza, raccomandiamo che portiate avanti il laboratorio usando il file di traccia *ip-ethereal-trace-1* fornito dagli autori del libro.

12. Stampate il primo frammento del datagramma IP frammentato. Quale informazione nell'intestazione IP indica che il datagramma è stato frammentato. Quale informazione nell'intestazione IP indica che questo è il primo frammento, piuttosto che un frammento successivo. Quanto è lungo questo datagramma IP?
13. Stampate il secondo frammento del datagramma IP frammentato. Che informazione nell'intestazione IP indica che questo non è il primo frammento? Ci sono altri frammenti? Come fate a dirlo?
14. Che campi cambiano nella intestazione IP tra il primo e il secondo frammento?

Ora trovate il primo messaggio UDP di dimensione 3500 byte che è stato inviato dal vostro computer.

15. Quanti frammenti sono stati creati dal datagramma originale?
16. Quali campi cambiano nella intestazione IP tra i vari frammenti?