



Advanced
Network
Technologies
Laboratory



Infrastrutture e Protocolli per Internet Risposte alle domande dei Laboratori

Stefano Napoli

Alberto Pollastro

Politecnico di Milano



Laboratorio 2

Sniffing con Wireshark



Slide Lez 2, pag 11

- Cattura HTTP1:

- I client impiegati sono Wget 1.10.2 (programma di download di contenuti web, funziona da riga di comando) e Iceweasel 2.0.0.3 (si tratta della versione Debian di Mozilla Firefox).
- Utilizzando Wget si effettua il solo download del contenuto richiesto (ad esempio la pagina web, un'immagine...), per cui richiedendo una pagina che contiene immagini, si ottiene la sola pagina, ed è necessario effettuare il wget delle immagini separatamente. Di conseguenza, con la sola sessione catturata, con wget si è ottenuta solamente la pagina web, e non le immagini in essa contenute. Diversamente Iceweasel, essendo un web browser vero e proprio, dopo aver scaricato la pagina la analizza, rileva i contenuti ancora da scaricare, ed effettua i GET necessari, per cui è in grado di visualizzare correttamente la pagina.



Laboratorio 2



Sniffing con Wireshark (2)

Slide Lez 2, pag 11/12

- Cattura HTTP2:

- Come indicato nel pacchetto 21 della cattura, lo username è *pollastro* e la password *tipiacerebbesaperla*
- Il web server non trova lo script `externlink.js`, di conseguenza, per come è configurato, risponde con una pagina di errore (pacchetto 17)

- Cattura FTP

- Il client si connette sulla porta $(200+256+218=)$ **51418** del server per scaricare il file `server.png`

- Cattura POP 1

- Lo User Agent (client di posta) è visibile nell'header della mail: per visualizzarlo si segue lo stream TCP, e si trovi la stringa:

User-Agent: Icedove 1.5.0.10 (X11/20070307)



Laboratorio 2



Sniffing con Wireshark (3)

Slide Lez 2, pag 12

- Cattura POP2:

- Sempre seguendo il il flusso TCP si ottiene, osservando l'header, che l'encoding è di tipo *text/plain; charset=ISO-8859-1; format=flowed*
- Sempre negli header è indicata codifica: 7bit, il che indica che non è stata applicata alcuna codifica. In particolare 7bit indica che il contenuto può essere diviso in blocchi di 7 bit e interpretato come ASCII

- Catture SMTP

- La prima cattura SMTP è la cattura di una sessione in chiaro, mentre la seconda è la cattura di una sessione effettuata con TLS



Laboratorio 2

Attività 2



Slide Lez 2, pag 30

- Sulla rete transitano, oltre ai pacchetti CDP (Cisco Discovery Protocol, protocollo proprietario Cisco che non è rilevante ai fini del laboratorio), pacchetti ARP, necessari all'inoltro su rete locale dato che le tabelle di ARP partono vuote su tutti i dispositivi di rete.
- I pacchetti di ARP sono scambiati sui segmenti di rete per scoprire gli indirizzi fisici associati agli indirizzi IP.
- Si noti che dopo lo scambio di un ARP Request-ARP Response entrambi gli end della comunicazione hanno aggiunto una nuova entry nella tabella.



Laboratorio 2

Attività 3



Slide Lez 2, pag 32

- Rispetto all'esercizio precedente, si tratta di due reti IP collegate da un router.
- Siccome è stato impostato per tutti gli host il default gateway corretto, non ci sono problemi di routing
- Su ogni rete locale viene effettuato lo scambio di messaggi ARP: nel caso del ping da PC1 a Server1, è necessario uno scambio di messaggi ARP perchè PC1 conosca l'indirizzo MAC dell'interfaccia "sinistra" del router, e uno scambio di messaggi ARP perchè il router conosca l'indirizzo MAC dell'interfaccia di rete del Server1.
- Per il ritorno (Echo Reply) non saranno necessari ulteriori scambi, perchè le tabelle sono già state riempite.



Laboratorio 2



Attività 4

Slide Lez 2, pag 35

- Lo schema della rete è analogo a quello dell'esercizio precedente, tuttavia sussiste un problema di routing che fa sì che il ping funzioni normalmente tra PC2 e Router3 e non tra PC2 e Router4
- PC2, dall'attività precedente, ha un default gateway impostato, mentre Router 4 non ce l'ha
- Di conseguenza l'Echo Request viene regolarmente inviato da PC2 a Router3, e da Router 3 a Router4 (tutti sanno come raggiungere la destinazione), ma quando Router4 deve inviare la risposta, non ha una rotta per PC2 o per la sua rete, dunque scarta il pacchetto.
- Il problema si risolve impostando una rotta statica su Router2 per la rete di PC2



Laboratorio 3

Attività 1/2



Slide Lez 3, pag 10

- Nella rete proposta uno dei due link è di tipo seriale, mentre l'altro è di tipo FastEthernet su fibra ottica
- Il meccanismo ARP è proprio di Ethernet, dunque lo scambio avviene solo sul link in fibra
- Sul link seriale, tale scambio non avviene
- La restante parte della comunicazione è identica

Slide Lez 1, pag 21

- Le informazioni richieste nell'esercizio sono reperibili tramite i comandi show indicati in precedenza
- Prestare attenzione al prompt da cui sono disponibili i diversi show e alle informazioni che essi forniscono



Laboratorio 3

Attività 5



Slide Lez 3, pag 38

- Impostando il timeout dell'ARP cache a 7 secondi, si ottiene che dopo 7s le entry della tabella scadano, per cui è necessario rifare la procedura ARP Request-ARP Reply
- Nella fattispecie, siccome il ping dura più di 7 secondi, trascorso tale tempo scade l'arp entry sul router; il messaggio Echo Request viene inviato regolarmente dal PC, però il router non ha più l'indirizzo MAC del PC a cui deve rispondere e scarta il pacchetto causando lo scadere del timeout del mittente.
- Il router effettua dunque una ARP Request, e il PC risponde, per cui la entry viene ricreata nella cache del router.
- La comunicazione può ora riprendere, e i rimanenti scambi di Echo request e Echo Reply potranno transitare regolarmente



Laboratorio 3

Attività 5 (2)



Slide Lez 3, pag 38

- Il PC sta però ancora aspettando una risposta alla Echo Request da lui inviata
- Prima di inviare una nuova Echo Request, attenderà tanto tempo quanto indicato nel suo timeout di trasmissione per il ping
- Osservando quindi la distanza temporale tra l'Echo Request che non ha ricevuto risposta e l'Echo Request successivo, si ottiene il timeout di trasmissione del PC (*che non ha niente a che vedere col timeout di scadenza dell'ARP Cache!*)
- È possibile osservare tali timeout in modalità simulazione



Laboratorio 4



Attività 1

Slide Lez 4, pag 6

- Il programma traceroute utilizza messaggi Echo Request ed Echo Reply per stabilire quali sono i router che si trovano sulla “strada” verso un determinato host
- In particolare, vengono generati Echo request verso tale host con TTL crescente, a partire da 1
- Il primo echo request verrà scartato dal primo router, che notificherà la cosa (TTL Exceeded) al dispositivo da cui si sta tracciando la “strada”; il secondo echo request sarà scartato dal secondo router, e così via
- Si compila così l'elenco dei router che si attraversano
- Questo meccanismo funziona se i messaggi Echo sono gestiti opportunamente dai router attraversati



Laboratorio 4

Attività 2/3/4



Slide Lez 4, pag 13

- I messaggi RIP nella versione 1 sono broadcast
- Viene utilizzata la tecnica dello Split Horizon

Slide Lez 4, pag 15

- Le principali differenze tra i messaggi RIPv1 e RIPv2 sono:
 - I messaggi sono multicast invece che broadcast
 - Si annunciano anche le netmask -> routing classless

Slide Lez 4, pag 17

- Attivando la modalità passiva, non vengono più inviati messaggi RIP sulle reti tra Router0 e PC0 e tra Router1 e PC1
- Router 0 e Router2 continuano ad annunciare le reti a loro attaccate come in precedenza



Laboratorio 4



Attività 5

Slide Lez 4, pag 18

- Quando viene spenta l'interfaccia Fa0/1 del Router0 non vengono generati Triggered Updates perché non ci sono reti da annunciare sulla Fa0/0 che venivano raggiunte attraverso tale interfaccia (la rete che non è più raggiungibile perché è stata spenta l'interfaccia Fa0/1 non viene più annunciata nel DV)
- Il router centrale si accorge del cambiamento di topologia dopo che è scaduto il suo timeout per quella rotta, quindi dopo un tempo compreso tra 180 secondi e $(180-30=)$ 150 secondi
- Il Router2 si accorge del cambiamento dopo che Router1 se n'è accorto, perché riceve da Router1 un messaggio RIP che annuncia la rete come irraggiungibile (hop-count=16)



Laboratorio 4

Attività 5/6/7



Slide Lez 4, pag 18

- Quando viene accesa l'interfaccia Fa0/1, viene inviato un Triggered Update sull'interfaccia Fa0/0
- Gli altri router si accorgono subito del cambio di topologia
- Router1 e Router2 se ne accorgono sostanzialmente in contemporanea: appena Router1 riceve il Triggered Update da Router0, crea a sua volta un Triggered Update, che invia a Router2

Slide Lez 4, pag 20

- Analoghe considerazioni valgono per l'attività 6

Slide Lez 4, pag 23

- La sostanziale differenza tra RIP ed EIGRP è la metrica impiegata ed annunciata nei messaggi



Laboratorio 5



Attività 1/2

Slide Lez 5, pag 5

- Il Ping tra PC1 e Totti non funziona
- Totti non ha una rotta per raggiungere la rete 192.168.0.0/24
- Il messaggio Echo Request raggiunge quindi Totti, ma non torna indietro la Echo Reply

Slide Lez 5, pag 9

- Ora il ping funziona perché Totti vede come indirizzo sorgente l'ip dell'interfaccia FastEthernet 0/0 di DelPiero (ossia quella "overloadata").
- In questo modo tutti i pacchetti inviati sullo spezzone di rete tra Totti e DelPiero hanno indirizzi di livello 3 appartenenti alla rete 88.1.0.0/16.



Laboratorio 5

Attività 3/4



Slide Lez 5, pag 10

- E' possibile pingare Inzaghi dal PC1
- Non è possibile pingare PC1 da Totti
- Come prima, il router Totti non conosce l'esistenza della rete 192.168.0.0/24 poiché è una rete privata “nattata”, quindi non può aprire comunicazioni verso indirizzi che appartengono a quella rete

Slide Lez 5, pag 12

- Possono essere impostate in modalità passiva per EIGRP le interfacce Fa0/0 e Fa0/1 del router Totti nell'attività successiva l'interfaccia Fa0/1 del router Buffon.
- Non è necessario disabilitare l'auto-summary, poiché nessun router ha la necessità di annunciare delle sottoreti (il router Totti può annunciare direttamente l'intera rete 88.0.0.0/8 e non le tre singole sottoreti).



Laboratorio 5

Attività 5



Slide Lez 5, pag 15

- Non è necessario modificare la configurazione di EIGRP poiché la rete appena creata è una rete privata che verrà poi “nattata”, quindi gli altri router non avranno bisogno di sapere come raggiungerla.
- Lo spazio di indirizzamenti della rete privata avrebbe potuto essere lo stesso della prima rete locale; infatti tali indirizzi sono riservati alle reti privati e non vengono mai visti dagli altri router sulla backbone, quindi non ci sarebbe ambiguità nell'indirizzamento.

I file di configurazione e gli scenari delle varie attività configurati correttamente sono disponibili per il download sul sito web del corso