Tesina di
Infrastrutture e Servizi per Reti Geografiche

Docenti: M. Baldi
F. Risso

EIGRP
Enhanced Interior Gateway Routing Protocol

Davide Boltri 93671
Matteo Onofrio Bovero 93152
Alessandro Zummo 96389

Typeset with LaTeX

Immagine in copertina tratta da “IGRP Network Design Solutions” edito da “Cisco Press”

Indice

1 Prerequisiti **1**

2 Introduzione teorica **1**
2.1 Il protocollo IGRP 1
2.2 Il protocollo EIGRP 2
2.3 I pacchetti EIGRP 4

3 Laboratorio **6**

4 Configurazione dei router **9**

5 Come EIGRP reagisce ai guasti **13**
5.1 Sequenza interfaccia down 13
5.2 Sequenza interfaccia up 17

Elenco delle tabelle

Elenco delle figure

1 Regola dello split-horizon 2
2 Struttura del laboratorio 7
3 Cattura dei pacchetti scatenati da un guasto nella rete 15
4 Cattura dei pacchetti scatenati dal ripristino di un router nella rete 18

1 Prerequisiti

Si presume che chi legga il presente materiale abbia una adeguata conoscenza dei protocolli di rete, una conoscenza di base riguardo alla configurazione dei router cisco (http://netgroup.polito.it/netlibrary/cisco/ConfigBase/) e manualità nell'uso di software di network analysing come Ethereal.

2 Introduzione teorica

2.1 Il protocollo IGRP

IGRP (Interior Gateway Routing Protocol) fu sviluppato nella metà degli anni '80 dalla Cisco come protocollo di routing all'interno degli Autonomous System (AS) per sostituire il precedente RIP (Routing Internal Protocol) che si era dimostrato poco efficiente per reti di grosse dimensioni.

IGRP appartiene alla famiglia dei protocolli di routing di tipo *distance vector*. Questi protocolli hanno la caratteristica di scegliere il percorso di instradamento dei pacchetti in base ad un criterio di convenienza che prende per l'appunto il nome di *distance*: tra le possibili alternative viene scelta quella che ha distance minore.

In IGRP tale criterio di scelta viene calcolato come il risultato della combinazione di alcuni parametri che sono:

- affidabilità: valutata su una scala da 1 a 255.
- carico: valutato su una scala da 1 a 255
- bandwidth: valutato su una scala da 1200 bps a 10 Gbps
- ritardi: valutati su una scala da 1 a 10^{24}

Per distribuire nella rete le informazioni necessarie al calcolo del distance vector e per aggiornare la rete su eventuali cambiamenti nella topologia (inserimento o eliminazione di una o più destinazioni) ogni router invia ai propri vicini, ad intervalli di t_U secondi (dove di default $t_U = 90$), dei messaggi di `update` nel quale viene trasmessa tutta o parte della propria routing table.

IGRP si accorge di eventuali situazioni di guasto, (rottura di un router o interruzione di un link) quando da un'interfaccia non sono più ricevuti pacchetti di update. In particolare se dopo un tempo pari a $3t_U$ un router non riceve messaggi di update da una porta, allora considera guasto il link che a quella porta era connesso e nel successivo messaggio di update verrà distribuita la routing table modificata.

Per migliorare l'efficienza e le prestazioni della rete, IGRP prevede dei meccanismi per incrementare la stabilità delle tabelle di routing:

holddown: Quando un router si accorge che uno dei suoi vicini si è guastato, modifica la propria routing table e la distribuisce con il prossimo messaggio di update. Può capitare che un router della rete non ancora informato del cambiamento della routing table spedisca un proprio messaggio di update, in cui il router guasto appare come ancora funzionante, ad

un altro router che invece era già stato raggiunto dal messaggio di update. Capita allora che la routing table di quest'ultimo router divenga instabile. Per evitare situazioni di questo tipo è previsto un tempo di holddown, che di default vale $3t_U$, che è il tempo che un router deve attendere prima di rendere effettiva la modifica alla propria routing table.

Split-horizion: Il meccanismo dello split-horizon prevede di non spedire messaggi di update contenenti informazioni di routing verso altri router che tali informazioni già le hanno. Per esempio, con riferimento alla figura 1 è inutile che nei messaggi di update spediti

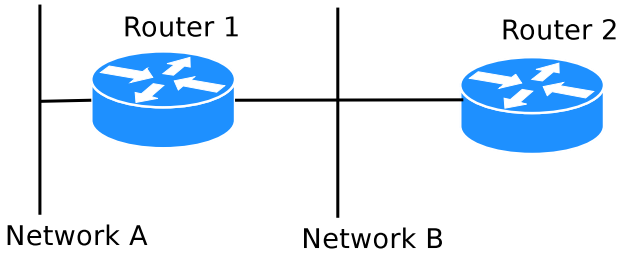

Figura 1: Regola dello split-horizon

dal router 2 verso il router 1 compaiono le informazioni relative al routing di R1 verso la rete A perchè il router 1 già le conosce. Il router 2 sa per certo che il router 1 conosce tale informazione perchè è da esso che l'ha ricevuta. Questo permette di diminuire il traffico generato dai messaggi di update e di evitare, in caso di quasto, la creazione di loop tra router adiacenti (ad esempio evita che, in caso di rottura dell'interfaccia di R1 verso la rete A, R1 indichi R2 come percorso alternativo per raggiungere la rete A, e R2, circolarmente, indichi R1 come percorso verso la rete A)

Poison reverse update: questo meccanismo serve per evitare la creazione di loop tra router non adiacenti. IGRP si accorge della creazione di loop quando i valori di distance aumentano di un fattore superiore a 1.1. La soluzione in tal caso è di inviare messaggi di poison reverse update che cancellano le tabelle di routing e mettono i router in holddown.

2.2 Il protocollo EIGRP

Per soddisfare le esigenze delle reti in continua espansione, agli inizi degli anni novanta Cisco progettò una versione migliorata di IGRP che prese il nome di EIGRP (Enhanced IGRP). Si tratta di un protocollo che presenta migliori prestazioni rispetto al semplice IGRP, ma con il quale mantiene la compatibilità delle tabelle di routing e delle configurazioni preesistenti.

Le caratteristiche fondamentali di EIGRP sono le seguenti:

- fast convergence: un router con protocollo EIGRP memorizza al proprio interno le tabelle di routing dei router vicini così da poter rapidamente scoprire percorsi alternativi per l'instradamento dei pacchetti
- subnet mask di lunghezza variabile: rende possibile limitare il raggio d'azione di EIGRP a una sottorete limitata

- update parziali: EIGRP, a differenza di IGRP, non invia periodicamente dei messaggi di update, ma si limita a spedire dei messaggi di update parziali solo quando avvengono dei cambiamenti nei parametri di valutazione dei percorsi di routing. Tali messaggi di update possono inoltre essere spediti selettivamente solo alla sottorete interessata

Tutte queste caratteristiche fanno di EIGRP un protocollo molto più veloce e meno costoso in termini di banda rispetto al semplice IGRP.

I meccanismi di base che permettono ad EIGRP di essere estremamente efficiente sono:

Ricerca dei router vicini: Per capire quali sono i router vicini e se questi sono ancora attivi, EIGRP invia periodicamente dei piccoli pacchetti di *hello*. Se un router non vede arrivare pacchetti di hello da una porta assume che il link che a quella porta era connesso sia guasto.

Reliable Transport Protocol (RTP): Meccanismo che si occupa della spedizione in modo affidabile (richiesta di ACK) dei pacchetti EIGRP tra i router vicini. Per aumentare efficienza sono trasmessi in modo affidabile solo i pacchetti che veramente ne hanno bisogno. Per esempio i pacchetti di hello non richiedono l'invio di un ACK.

Procollo DUAL: Il Diffusing Update ALgorithm è l'algoritmo adottato da EIGRP per il calcolo delle tabelle di instradamento. Caratteristica del protocollo DUAL è che, nel momento in cui devono essere inviati dei pacchetti di update, ogni router si limita a trasmettere i distance vector relativi unicamente ai percorsi che gli sono direttamente connessi. Il calcolo delle informazioni di routing quindi avviene in modo distribuito, coinvolgendo tutti i router, ma pur sempre con un limitato utilizzo della banda.
Le informazioni necessarie all'algoritmo DUAL sono gestite in tre tabelle:

- La *Neighbor Table* in cui sono elencati i router adiacenti
- La *Topology Table* in cui sono elencati tutti i possibili percorsi di instradamento verso una certa destinazione
- La *Routing Table* in cui, per ogni destinazione, sono memorizzati il percorso migliore e senza loop per raggiungerla (*Successor*) e uno o più percorsi alternativi (fino ad un massimo di 6) da usare nel caso in cui il primo non sia più utilizzabile (*Feasible Successor*)

Con queste informazioni, qualora avvenga un guasto nella topologia della rete che impedisca di usare il Successor per l'instradamento dei pacchetti, EIGRP, senza fare calcoli o query, tenta con i Feasible Successor. Solamente nel caso in cui anche queste alternative dovessero fallire avviene il computo di un'altro percorso di routing.
Il ricomputo del routing avviene con l'invio di messaggi di query a tutti i router confinanti, i quali possono o rispondere immediatamente (messaggio di reply) se hanno un feasible successor per la destinazione, oppure iniziare a loro volta un ciclo di query. Solo dopo che si sono ricevuti messaggi di reply da tutti i router confinanti è possibile operare la scelta della nuova route.

Nel calcolo della distance, EIGRP usa gli stessi parametri di affidabilità (Reliability), carico (Load), bandwith (Bw) e ritardo (Delay) usati anche da IGRP. La formula per il calcolo della distance è la seguente

$$\text{metric} = 256 \cdot \left(K_1 \cdot \text{Bw} + \frac{K_2 \cdot \text{Bw}}{256 - \text{Load}} + K_3 \cdot \text{Delay} \cdot \frac{K_5}{\text{Reliability} + K_4} \right)$$

dove i K_i sono dei coefficienti che assegnano un peso diverso ai singoli parametri. Di fatto nella stragrande maggioranza dei casi sono ritenuti fondamentali i ritardi e la banda, per cui i coefficienti sono usati come segue:

$$K_1 = K_3 = 1; \qquad K_2 = K_4 = K_5 = 0$$

da cui segue che la formula di cui sopra si semplifica in:

$$\text{metric} = 256 \cdot (\text{Bw} + \text{Delay})$$

Un esempio di ambito in cui si usano configurazioni diverse dei K_i si ha per installazioni militari dove l'affidabilità è ritenuta requisito più importante della banda.

2.3 I pacchetti EIGRP

Il protocollo EIGRP utilizza cinque tipi di pacchetti:

- *Hello*: sono i pacchetti inviati sulla rete ogni 5 secondi per informare i router confinanti della propria presenza. Si tratta di messaggi multicast che non richiedono ACK.
- *Acknowledgement*: sono pacchetti unicast inviati dall'RTP per informare un mittente che la destinazione ha ricevuto correttamente un pacchetto.
- *Update*: pacchetti inviati per aggiornare i router vicini dei cambiamenti nella tabella di routing. In realtà i messaggi di update sono di due tipi:
  + pacchetti unicast verso uno specifico router vicino quando questo viene scoperto per la prima volta
  + pacchetti multicast inviati a tutti i router confinanti inviati solo quando si verificano dei cambiamenti nella topologia
- *Query*: pacchetti multicast inviati a tutti i router confinanti quando è avvenuto un cambiamento topologico nella rete, non esistono Feasible Successor validi e si rende necessario il ricomputo della route
- *Reply*: pacchetti unicast inviati in seguito ad un messaggio di query per informare il mittente che esiste un Feasible Successor da usare per il ricomputo della route.

Ogni pacchetto EIGRP è formato dai seguenti campi

nome_campo	*bit*	*spiegazione*
`Version`	8	Versione del pacchetto
`Opcode`	8	Tipo del pacchetto: Update (1), Query (3), Reply (4), Hello (5). I pacchetti di ACK sono dei particolari pacchetti di Hello
`Checksum`	16	Controllo di errore
`Flags`	32	
`Sequence`	32	Numero di sequenza usato da RTP
`Ack`	32	Se > 0 il pacchetto è un ack
`AS`	32	Numero dell'autonomous System
`TLV`	variabile	Insieme di strutture dati che contengono informazioni su EIGRP e sulle route. Sono formati da una coppia di valori su 16 bit (tipo e lunghezza) che precedono le informazioni vere e proprie

Il contenuto della struttura TLV è diverso a seconda che il pacchetto sia destinato ad un'internal route oppure ad un'external route. Nel caso dei pacchetti internal route (gli unici che interessano perchè nel corso dell'esperienza di laboratorio tutti i pacchetti saranno scambiati all'interno dell'AS) i tipi contenuti nella struttura sono

- I parametri K_i del protocollo EIGRP
- Next Hop: Hop successivo
- Delay: Ritardo espresso in unità di 10μsec
- Bandwidth: banda disponibile
- MTU: Maximum Transmission Unit
- Hop Count: numero di Hop attraversati
- Reliability: tasso d'errore, dove $0xFF =$ affidabile
- Load: carico, dove $0xFF$ indica pieno carico
- Reserved: sempre impostato a $0x0000$
- Prefix Lenght: numero di bit usati per la netmask
- Destination: rete di destinazione

3 Laboratorio

Nel corso dell'esperienza di laboratorio si copriranno i seguenti punti:

- Configurazione dei protocolli IGRP/EIGRP su router Cisco.
- Simulazione di un guasto e analisi dei pacchetti con Ethereal per verificare in dettaglio il funzionamento del protocollo
- Ripristino della condizione di funzionamento e analisi dei pacchetti con Ethereal per verificare in dettaglio il comportamento del protocollo.

Il laboratorio è composto da 4 router Cisco più una macchina di gestione, così come schematizzato nella figura 2.
Descrizione:

- PC di gestione:
  - interfaccia 3COM: interfaccia di monitoring (passiva), riceve i pacchetti di tutte le LAN ethernet del laboratorio;
  - interfaccia SIS: interfaccia di scambio dati con i router (attiva), IP address 10.0.1.3/24
- R1: router Cisco 2610:
  - eth0/0: no ip address;
  - eth1/0: 10.0.1.1/24;
  - eth1/1: 10.0.2.1/24;
  - eth1/2: 10.0.3.1/24;
  - eth1/3: no ip address;
- R2: router Cisco 2503:
  - eth0: 10.0.1.2/24;
  - s0: 10.0.4.1/30;
- R3: router Cisco 2503:
  - s0: 10.0.4.2/30;
  - eth0: 10.0.2.2/24;
  - s1: 10.0.5.1/30;
- R4: router Cisco 2503:
  - eth0: 10.0.3.2/24;
  - s1: 10.0.5.2/30;

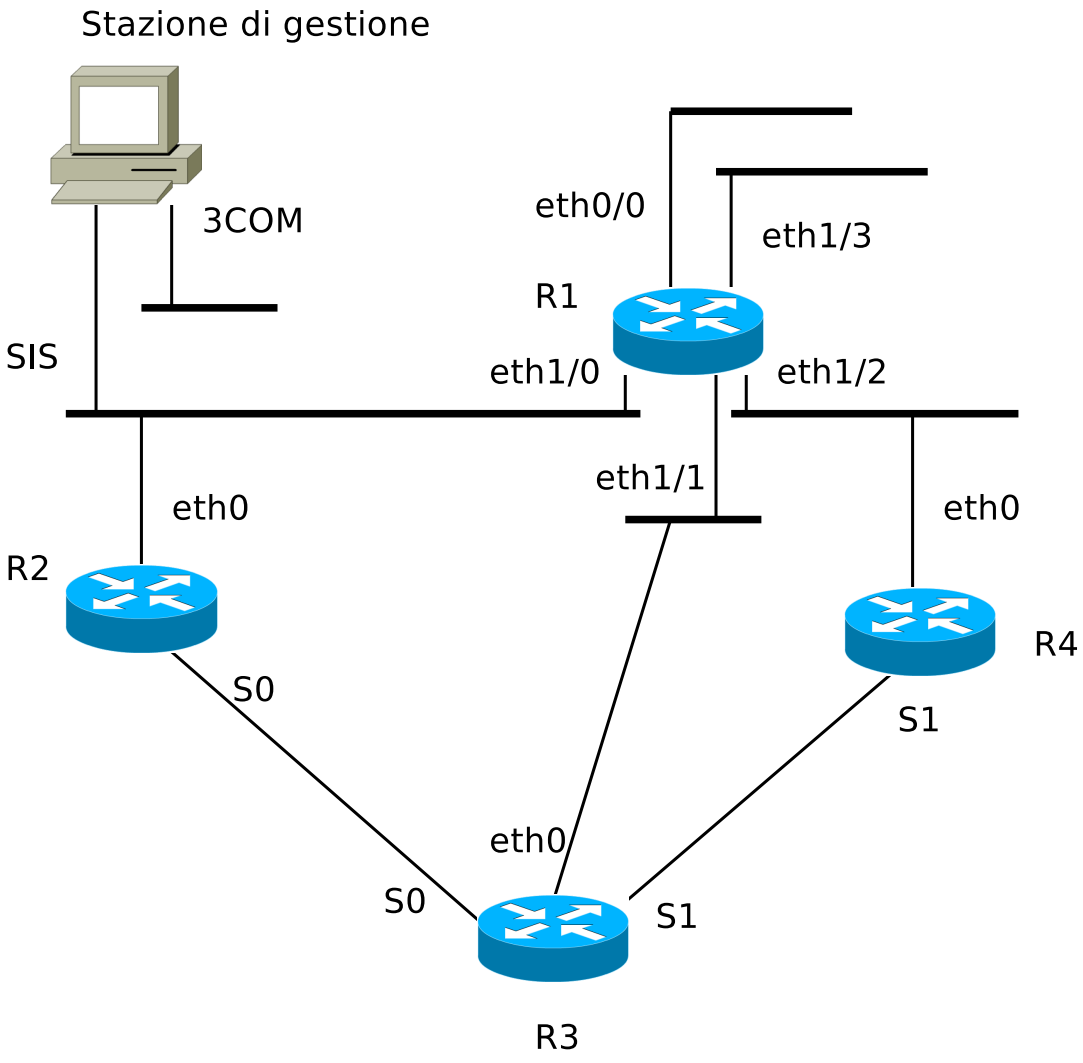

Figura 2: Struttura del laboratorio

Nella descrizione precedente le sigle `ethx` e `sx` corrispondono rispettivamente a ethernet `x` e serial `x`.

Una volta avviato il terminale remoto verso i router, inserendo dal prompt la sequenza di comandi:

```
Router>enable
Router#show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2
i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
ia - IS-IS inter area, * - candidate default, U - per-user static route
o - ODR, P - periodic downloaded static route
```

si può ottenere l'elenco dei protocolli supportati dal router per l'instradamento dei pacchetti su reti IP. In particolare si può notare che i router R2, R3 e R4 supportano sia IGRP che EIGRP mentre il router R1 (a cui appartiene il listato precedente) supporta EIGRP ma non IGRP. In base a questa considerazione nel seguito si procederà a illustrare la configurazione del solo EIGRP sui router di laboratorio. A titolo informativo, la configurazione di IGRP procederebbe con comandi del tutto analoghi, ma ovviamente sarà diverso il tipo e la sequenza dei messaggi scambiati.

4 Configurazione dei router

Nel listato 1 vengono mostrati i parametri di configurazione del router 1.

Prima di tutto, si passa alla modalità di amministrazione (riga 1.1) e si visualizza la configurazione corrente (riga 1.2). Dalla riga 1.4 alla 1.36 si possono vedere tutti i parametri del router. Più in dettaglio, dalla riga 1.10 alla 1.25 ci sono le descrizioni delle interfaccie di rete, mentre dalla riga 1.28 alla 1.30 sono elencate le interfaccie di configurazione. Relativamente alle interfaccie di rete si noti come alcune di esse (per esempio Ethernet 0/0 e Serial 0/0) siano in stato *shutdown*, ovvero sono fisicamente collegate al router ma non disabilitate. Più avanti si procederà quindi ad attivarle per far sì che il router possa accedervi. Infine (riga 1.33) si passa alla modalità di configurazione terminale da dove si potrà procedere alla configurazione vera e propria di EIGRP.

Listato 1

```
1  Router>enable
2  Router#show run
3  Building configuration...
4  Current configuration : 899 bytes

5  version 12.3
6  service timestamps debug uptime
7  service timestamps log uptime
8  no service password-encryption

9  hostname Router

10 interface Ethernet0/0
11  no ip address
12  shutdown

13 interface Serial0/0
14  no ip address
15  shutdown

16 interface Ethernet1/0
17  ip address 10.0.1.1 255.255.255.0
18  shutdown

19 interface Ethernet1/1
20  ip address 10.0.2.1 255.255.255.0

21 interface Ethernet1/2
22  ip address 10.0.3.1 255.255.255.0

23 interface Ethernet1/3
24  no ip address
25  shutdown

26 no ip http server
```


```
27  ip classless

28  line con 0
29  line aux 0
30  line vty 0 4
31   login

32  end

33  Router#config
34  Configuring from terminal, memory, or network [terminal]?
35  Enter configuration commands, one per line.  End with CNTL/Z.
36  Router(config)#
```

Nel listato 2 sono elencati i comandi per la configurazione dell'EIGRP. Prima di tutto si definisce l'EIGRP come protocollo di routing (riga 2.1) specificando 109 come autonomous system, poi si inserisce l'elenco delle reti connesse (righe 2.2-4) (109 è stato scelto in modo arbitrario perchè tutti i router si trovano su una rete interna del laboratorio).

I comando alla riga 2.7 permette di visualizzare l'attuale configurazione dei protocolli di routing (righe 2.6-18). In questo caso si può notare che, alle righe che iniziano con C, sono mostrate le informazioni riguardanti reti direttamente connesse. L'internfaccia Ethernet 1/0 non compare perchè, come si ricorderà, è ancora disattivata.

Con il comando di riga 2.19 si visualizzano informazioni dettagliate per quanto riguarda il protocollo di routing abilitato (righe 2.21-36). Alla riga 2.25 si possono notare alcuni dei parametri di configurazione del protocollo EIGRP.

Listato 2

```
1   Router(config)#router eigrp 109
2   Router(config-router)#network 10.0.1.0
3   Router(config-router)#network 10.0.2.0
4   Router(config-router)#network 10.0.3.0
5   Router(config-router)#exit
6   Router(config)#exit
7   Router#show ip route
8   Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
9          D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
10         N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
11         E1 - OSPF external type 1, E2 - OSPF external type 2
12         i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
13         ia - IS-IS inter area, * - candidate default, U - per-user static route
14         o - ODR, P - periodic downloaded static route

15  Gateway of last resort is not set

16       10.0.0.0/24 is subnetted, 2 subnets
17  C       10.0.2.0 is directly connected, Ethernet1/1
18  C       10.0.3.0 is directly connected, Ethernet1/2
19  Router#show ip proto
```

```
20  Routing Protocol is "eigrp 109"
21    Outgoing update filter list for all interfaces is not set
22    Incoming update filter list for all interfaces is not set
23    Default networks flagged in outgoing updates
24    Default networks accepted from incoming updates
25    EIGRP metric weight K1=1, K2=0, K3=1, K4=0, K5=0
26    EIGRP maximum hopcount 100
27    EIGRP maximum metric variance 1
28    Redistributing: eigrp 109
29    EIGRP NSF-aware route hold timer is 240s
30    Automatic network summarization is in effect
31    Maximum path: 4
32    Routing for Networks:
33      10.0.0.0
34    Routing Information Sources:
35      Gateway         Distance      Last Update
36    Distance: internal 90 external 170
```

Questo tipo di configurazione va ripetuta in modo analogo sugli altri router del laboratorio.

Nel listato 3 l'interfaccia ethernet 1/0 che precedentemente era in shutdown viene abilitata (righe 3.1-6). Si fa notare come all'attivazione dell'interfaccia ethernet 1/0 (righe 3.4-8) l'algoritmo DUAL si accorge della presenza del router 2 e instaura una "adjacency", ovvero avviene uno scambio di pacchetti update unicast tra router 1 e router 2. Alle righe 3.9-14 si esegue un ping come ulteriore verifica che l'interfaccia sia realmente attiva. Successivamente si visualizzano nuovamente le informazioni sui protocolli di routing per verificare l'aggiunta delle nuove entry (righe 3.15-30). In questo caso si possono notare le righe 3.27-30 che iniziano con una D, ad indicare le interfacce non direttamente connesse per le quali il protocollo EIGRP ha trovato una route. Nelle righe 3.31-48 sono visualizzati alcuni test di connettività (invio di ping).

Listato 3

```
1   Router(config)#int e 1/0
2   Router(config-if)#no shutdown
3   Router(config-if)#exit
4   2d04h: %LINK-3-UPDOWN: Interface Ethernet1/0, changed state to up
5   2d04h: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet1/0,
6    changed state to up
7   2d04h: %DUAL-5-NBRCHANGE: IP-EIGRP(0) 109: Neighbor 10.0.1.2 (Ethernet1/0) is
8    up: new adjacency
9   Router#ping 10.0.2.2

10  Type escape sequence to abort.
11  Sending 5, 100-byte ICMP Echos to 10.0.2.2, timeout is 2 seconds:
12  !!!!!
13  Success rate is 100 percent (5/5), round-trip min/avg/max = 4/4/4 ms
14  Router#show ip route
15  Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
16         D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
17         N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
```


```
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

     10.0.0.0/8 is variably subnetted, 6 subnets, 3 masks
C       10.0.2.0/24 is directly connected, Ethernet1/1
C       10.0.3.0/24 is directly connected, Ethernet1/2
C       10.0.1.0/24 is directly connected, Ethernet1/0
D       10.0.4.2/32 [90/2195456] via 10.0.1.2, 00:02:22, Ethernet1/0
D       10.0.4.0/30 [90/2195456] via 10.0.1.2, 00:00:56, Ethernet1/0
                    [90/2195456] via 10.0.2.2, 00:00:56, Ethernet1/1
D       10.0.5.0/30 [90/2195456] via 10.0.2.2, 00:00:56, Ethernet1/1
Router#ping 10.0.4.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.0.4.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/4/8 ms
Router#tracer 10.0.4.2
Type escape sequence to abort.
Tracing the route to 10.0.4.2

  1 10.0.1.2 4 msec 4 msec 4 msec
  2 10.0.4.2 4 msec *  4 msec


2d04h: %DUAL-5-NBRCHANGE: IP-EIGRP(0) 109: Neighbor 10.0.1.2 (Ethernet1/0) is
 down: holding time expired

Router#tracer 10.0.4.2

Type escape sequence to abort.
Tracing the route to 10.0.4.2

  1 10.0.2.2 4 msec *  0 msec
  2 10.0.4.2 8 msec *  4 msec
Router#
```

5 Come EIGRP reagisce ai guasti

Al fine di mostrare la risposta del protocollo EIGRP ad eventuali cambiamenti nella topologia della rete, si simulerà l'interruzione del link fra il router 1 e il router 2 abbattendo l'interfaccia ethernet 0 del router 2.

Per meglio comprendere il meccanismo di recupero guasti dell'EIGRP, si rivela utile effettuare una cattura e successiva analisi dei pacchetti mediante il tool Ethereal (open source, liberamente scaricabile al sito www.ethereal.com).

5.1 Sequenza interfaccia down

Nel listato 4 si è visualizzata la topologia della rete prima di abbattere l'interfaccia. Si nota alle righe (4.11-12) che il router 1 conosce come unico modo di accedere alla rete 10.0.4.2 passando per il router 2 tramite l'interfaccia eth0.

Listato 4

```
1  Router#show ip eigrp topology
2  IP-EIGRP Topology Table for AS(109)/ID(10.0.7.1)

3  Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply,
4         r - reply Status, s - sia Status

5  P 10.0.2.0/24, 1 successors, FD is 281600
6          via Connected, Ethernet1/1
7  P 10.0.3.0/24, 1 successors, FD is 281600
8          via Connected, Ethernet1/2
9  P 10.0.1.0/24, 1 successors, FD is 281600
10         via Connected, Ethernet1/0
11 P 10.0.4.2/32, 1 successors, FD is 2195456
12         via 10.0.1.2 (2195456/2169856), Ethernet1/0
13 P 10.0.6.0/24, 1 successors, FD is 281600
14         via Connected, Ethernet0/0
15 P 10.0.7.0/24, 1 successors, FD is 281600
16         via Connected, Ethernet1/3
17 P 10.0.5.1/32, 1 successors, FD is 2195456
18         via 10.0.3.2 (2195456/2169856), Ethernet1/2
19 P 10.0.4.0/30, 2 successors, FD is 2195456
20         via 10.0.2.2 (2195456/2169856), Ethernet1/1
21         via 10.0.1.2 (2195456/2169856), Ethernet1/0
22 P 10.0.5.0/30, 2 successors, FD is 2195456

23 Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply,
24        r - reply Status, s - sia Status

25         via 10.0.3.2 (2195456/2169856), Ethernet1/2
26         via 10.0.2.2 (2195456/2169856), Ethernet1/1


27 Router#show ip eigrp neighbors
```

```
IP-EIGRP neighbors for process 109
H   Address                 Interface       Hold Uptime   SRTT   RTO  Q  Seq
                                            (sec)         (ms)       Cnt Num
2   10.0.3.2                Et1/2             13 00:02:35   24   200  0  4
1   10.0.2.2                Et1/1             10 00:04:47   27   200  0  4
0   10.0.1.2                Et1/0             10 00:05:18   14   200  0  9
```

Per mettere in shutdown l'interfaccia eth0, dal router 2 si dà la sequenza di comandi:

```
Router#config
Router(config)#int e 0
Router(config-if)#no shutdown
Router(config-if)#exit
```

In risposta all'abbattimento dell'interfaccia ethernet 0 (IP address 10.0.1.2) del router 2 i router iniziano l'interscambio degli opportuni pacchetti EIGRP al fine di bypassare il link guasto. Nella figura 3 è mostrata la schermata di Ehtereal con l'elenco dei pacchetti catturati. Nel listato 5 sono riportati i dettagli sui pacchetti più interessanti.

Dopo circa 15 secondi (pari a 3 vole il tempo di Hello), il router 1 si accorge che l'interfaccia eth0 è caduta e, non avendo altri Successor per quella route invia una pacchetto di Query multicast (righe 5.1-11) in cui informa i router vicini che l'interfaccia 10.0.4.2 non è raggiungibile e manda un pacchetto di update (righe 5.12-22) per informare i router vicini del cambiamento avvenuto nella topologia. Il router 3, che ha ovviamente un successore verso la rete 10.0.4.0 risponde al router con un pacchetto Reply (righe 5.23-33). Si noti che lo scambio dei messaggi Query, Update e Reply è sempre accompagnato da messaggi di Acknowledge perchè necessitano di una trasmissione affidabile con RTP

Listato 5

```
No.     Time        Source                Destination           Protocol Info
116     61.066271   10.0.2.1              224.0.0.10            EIGRP    Query

Cisco EIGRP
    Version      = 2
    Opcode       = 3 (Query)
    Checksum     = 0xb331
    Flags        = 0x00000000
    Sequence     = 11
    Acknowledge  = 0
    Autonomous System  : 109
    IP internal route  =   10.0.4.2/32 - Destination unreachable

No.     Time        Source                Destination           Protocol Info
118     61.078196   10.0.2.1              224.0.0.10            EIGRP    Update

Cisco EIGRP
    Version      = 2
    Opcode       = 1 (Update)
```

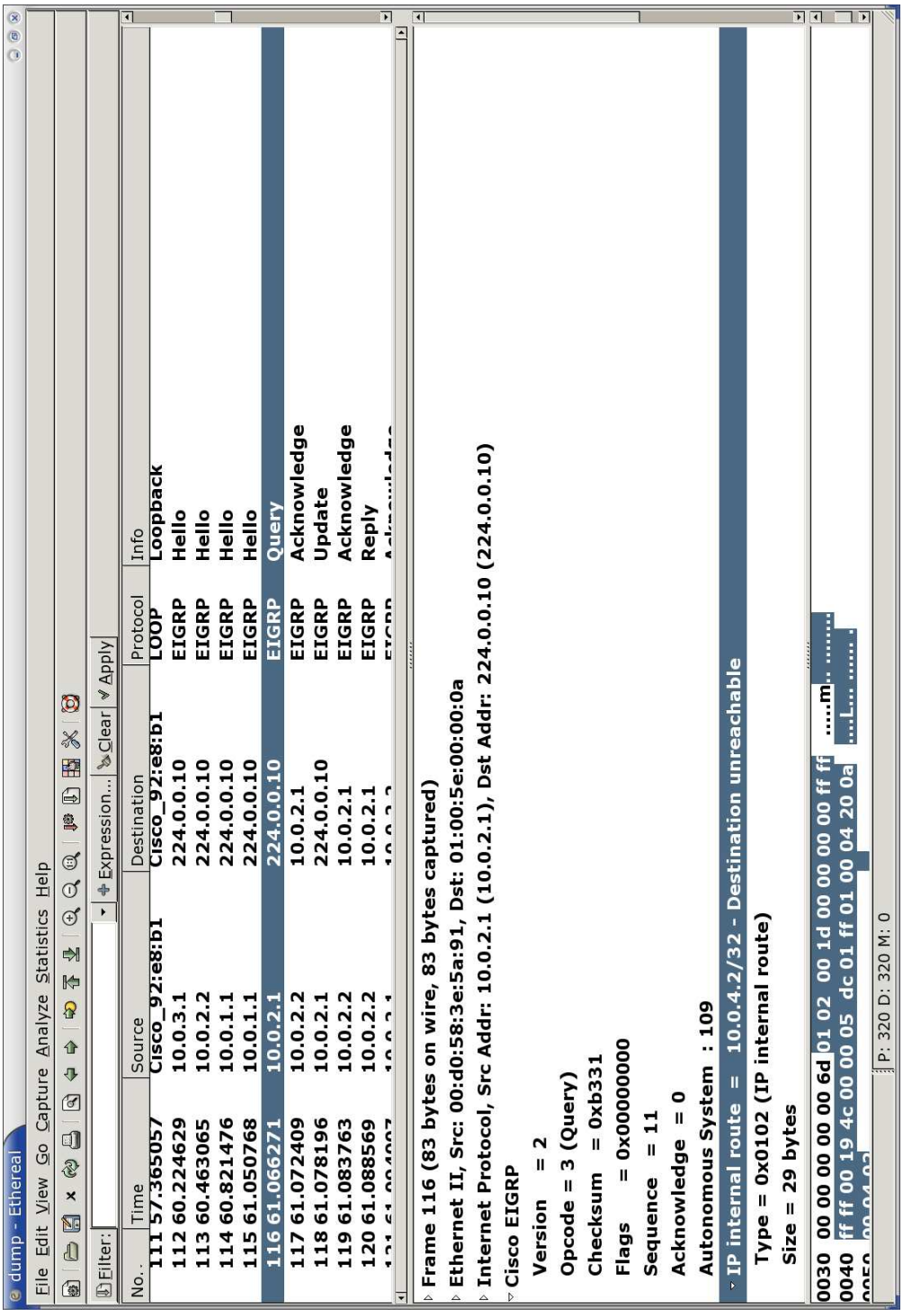

Figura 3: Cattura dei pacchetti scatenati da un guasto nella rete

```
17      Checksum     = 0xb736
18      Flags        = 0x00000000
19      Sequence     = 12
20      Acknowledge  = 0
21      Autonomous System  : 109
22      IP internal route  =   10.0.4.0/30 - Destination unreachable

23  No.     Time        Source                Destination           Protocol Info
24  120     61.088569   10.0.2.2              10.0.2.1              EIGRP    Reply

25  Cisco EIGRP
26      Version      = 2
27      Opcode       = 4 (Reply)
28      Checksum     = 0xda48
29      Flags        = 0x00000000
30      Sequence     = 9
31      Acknowledge  = 12
32      Autonomous System  : 109
33      IP internal route  =   10.0.4.2/32 - Destination unreachable
```

Rivisualizzando la tabella di routing del router 1 si osserva alle righe 6.17-18 che ora il router 1 accede alla rete 10.0.4.0 passando per il router 3. La rete ha quindi reagito correttamente al guasto e ha trovato una route alternativa!

Listato 6

```
1   Router#show ip eigrp topology
2   IP-EIGRP Topology Table for AS(109)/ID(10.0.7.1)

3   Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply,
4          r - reply Status, s - sia Status

5   P 10.0.2.0/24, 1 successors, FD is 281600
6           via Connected, Ethernet1/1
7   P 10.0.3.0/24, 1 successors, FD is 281600
8           via Connected, Ethernet1/2
9   P 10.0.1.0/24, 1 successors, FD is 281600
10          via Connected, Ethernet1/0
11  P 10.0.6.0/24, 1 successors, FD is 281600
12          via Connected, Ethernet0/0
13  P 10.0.7.0/24, 1 successors, FD is 281600
14          via Connected, Ethernet1/3
15  P 10.0.5.1/32, 1 successors, FD is 2195456
16          via 10.0.3.2 (2195456/2169856), Ethernet1/2
17  P 10.0.4.0/30, 1 successors, FD is 2195456
18          via 10.0.2.2 (2195456/2169856), Ethernet1/1
19  P 10.0.5.0/30, 2 successors, FD is 2195456
20          via 10.0.3.2 (2195456/2169856), Ethernet1/2
21          via 10.0.2.2 (2195456/2169856), Ethernet1/1
```

```
Router#show ip eigrp neighbors
IP-EIGRP neighbors for process 109
H   Address                 Interface       Hold Uptime   SRTT   RTO  Q  Seq
                                            (sec)         (ms)       Cnt Num
2   10.0.3.2                Et1/2             12 00:05:05   14   200  0  8
1   10.0.2.2                Et1/1             10 00:07:17   18   200  0  7
```

5.2 Sequenza interfaccia up

In questa ultima parte dell'esperienza di laboratorio viene riportata in funzione l'interfaccia 10.0.1.2 del router 2. Nella figura 4 è mostrata la schermata di Ethereal che mostra la cattura dei pacchetti mentre nel listato 7 sono riportati i pacchetti più interessanti.

Dopo che l'interfaccia è stata ripristinata, l'arrivo dei pacchetti di Hello del router 2 al router 1 e viceversa lungo la rete 10.0.1.0 informano i due router della reciproca esistenza nella rete. Da questo momento in avanti avviene lo scambio di alcuni pacchetti di update con i quali i due router si informano per l'aggiornamento delle tabelle di routing.

Il router 2 manda al router 1 un pacchetto di update (numero 267 nella sequenza) unicast (righe 7.1-15) per informarlo delle route da lui conosciute, elencate nelle righe iniziate dalla frase "IP internal route". Il router 1 risponde al router 2 con un pacchetto di update unicast (numero 269, righe 7.18-29) con cui informa a sua volta il router 2 delle route conosciute. I router leggono dai pacchetti, oltre agli indirizzi delle reti raggiungibili, anche i parametri che consentono di calcolare la metrica per il distance vector. In base a questo il router 2 evince che le reti 10.0.2.0, 10.0.3.0 e 10.0.5.0 si possono raggiungere più convenientemente dal router 1, e avverte quindi tutti i router connessi sull'interfaccia 10.0.1.2 di non inviargli pacchetti a tali destinazioni contrassegnandole, per la regola dello split-horizon, come unreacheble (pacchetto 271 righe 7.31-42).

A questo punto si nota nella sequenza catturata un fenomeno inatteso: i pacchetti numerati nella sequenza come 274 e 280 sono un duplicato dei pacchetti 269 e 271. La spiegazione dell'invio di questi pacchetti la si evince dall'analisi con Ethereal: il pacchetto 269 non ha ricevuto un ACK in tempo utile e quindi il pacchetto 274 ne è un suo duplicato mandato dal router 1 nella convinzione che il router 2 non avesse ricevuto il pacchetto precedente. In realtà il pacchetto era stato correttamente ricevuto, quindi 271 e 280 sono dei duplicati, causati da un errore di trasmissione, che non hanno parte attiva nel protocollo.

Continuando l'analisi della sequenza "corretta", con il pacchetto 278 (righe 7.58-68) il router 2 avverte il router 1 di essere il percorso più conveniente per la rete 10.0.4.0 e il router 1 avverte a sua volta con un update multicast (pacchetto 282, righe 7.83-93) tutti i router connessi all'interfaccia 10.0.1.1 che egli non si occupa più dell'instradamento dei pacchetti verso la rete 10.0.4.0 dichiarata unracheable per lo split-horizon. Da questo punto in avanti si è ripristinata la situazione di partenza.

Listato 7

```
No.     Time        Source                Destination           Protocol Info
267     151.759543  10.0.1.2              10.0.1.1              EIGRP    Update
```

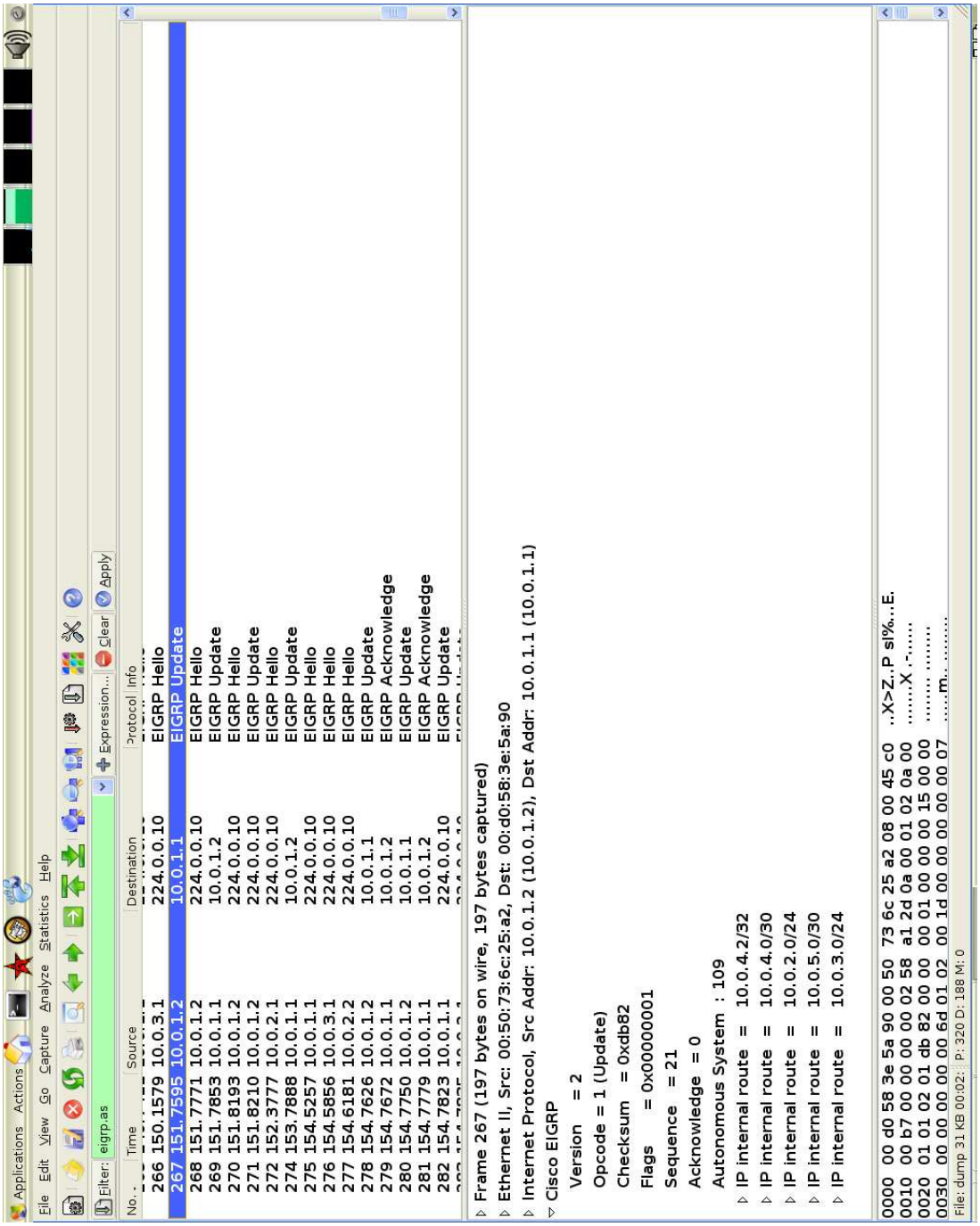

Figura 4: Cattura dei pacchetti scatenati dal ripristino di un router nella rete


```
Cisco EIGRP
    Version      = 2
    Opcode       = 1 (Update)
    Checksum     = 0xdb82
    Flags        = 0x00000001
    Sequence     = 21
    Acknowledge  = 0
    Autonomous System  : 109
    IP internal route  =   10.0.4.2/32
    IP internal route  =   10.0.4.0/30
    IP internal route  =   10.0.2.0/24
    IP internal route  =   10.0.5.0/30
    IP internal route  =   10.0.3.0/24

No.     Time        Source                Destination           Protocol Info
269     151.785312  10.0.1.1              10.0.1.2              EIGRP    Update

Cisco EIGRP
    Version     = 2
    Opcode      = 1 (Update)
    Checksum    = 0xab3b
    Flags       = 0x00000009
    Sequence    = 13
    Acknowledge = 0
    Autonomous System  : 109
    IP internal route  =   10.0.2.0/24
    IP internal route  =   10.0.3.0/24
    IP internal route  =   10.0.5.0/30
    IP internal route  =   10.0.4.0/30

No.     Time        Source                Destination           Protocol Info
271     151.821014  10.0.1.2              224.0.0.10            EIGRP    Update

Cisco EIGRP
    Version      = 2
    Opcode       = 1 (Update)
    Checksum     = 0xfeb9
    Flags        = 0x00000002
    Sequence     = 22
    Acknowledge  = 0
    Autonomous System  : 109
    IP internal route  =   10.0.2.0/24 - Destination unreachable
    IP internal route  =   10.0.3.0/24 - Destination unreachable
    IP internal route  =   10.0.5.0/30 - Destination unreachable

No.     Time        Source                Destination           Protocol Info
274     153.788831  10.0.1.1              10.0.1.2              EIGRP    Update

Cisco EIGRP
```


```
    Version     = 2
    Opcode       = 1 (Update)
    Checksum     = 0xab3b
    Flags        = 0x00000009
    Sequence     = 13
    Acknowledge  = 0
    Autonomous System  : 109
    IP internal route  =   10.0.2.0/24
    IP internal route  =   10.0.3.0/24
    IP internal route  =   10.0.5.0/30
    IP internal route  =   10.0.4.0/30

No.     Time        Source                Destination           Protocol Info
278     154.762625  10.0.1.2              10.0.1.1              EIGRP    Update

Cisco EIGRP
    Version      = 2
    Opcode       = 1 (Update)
    Checksum     = 0x8d02
    Flags        = 0x00000001
    Sequence     = 21
    Acknowledge  = 13
    Autonomous System  : 109
    IP internal route  =   10.0.4.2/32
    IP internal route  =   10.0.4.0/30

No.     Time        Source                Destination           Protocol Info
280     154.775066  10.0.1.2              10.0.1.1              EIGRP    Update

Cisco EIGRP
    Version      = 2
    Opcode       = 1 (Update)
    Checksum     = 0xfeae
    Flags        = 0x00000000
    Sequence     = 22
    Acknowledge  = 13
    Autonomous System  : 109
    IP internal route  =   10.0.2.0/24 - Destination unreachable
    IP internal route  =   10.0.3.0/24 - Destination unreachable
    IP internal route  =   10.0.5.0/30 - Destination unreachable

No.     Time        Source                Destination           Protocol Info
282     154.782347  10.0.1.1              224.0.0.10            EIGRP    Update

Cisco EIGRP
    Version      = 2
    Opcode       = 1 (Update)
    Checksum     = 0x63ee
    Flags        = 0x00000000
```


```
89      Sequence     = 14
90      Acknowledge  = 0
91      Autonomous System  : 109
92      IP internal route  =   10.0.4.2/32 - Destination unreachable
93      IP internal route  =   10.0.4.0/30 - Destination unreachable
```

Una considerazione conclusiva: il protocollo EIGRP manifesta la sua efficienza nella rapidità con cui ha reso possibile il recupero dai guasti e per il fatto che quasi tutti i pacchetti utilizzati per il ripristino sono stati scambiati tra i soli router interessati. Paga tuttavia questa efficienza con una maggiore complessità rispetto al protocollo IGRP il quale è più invasivo nell'occupazione di banda all'atto dello scambio delle informazioni di routing ma d'altra parte è molto più semplice (basti pensare che IGRP utilizza unicamente pacchetti di Update anzichè i cinque tipi diversi di pacchetti di EIGRP).

Riferimenti bibliografici