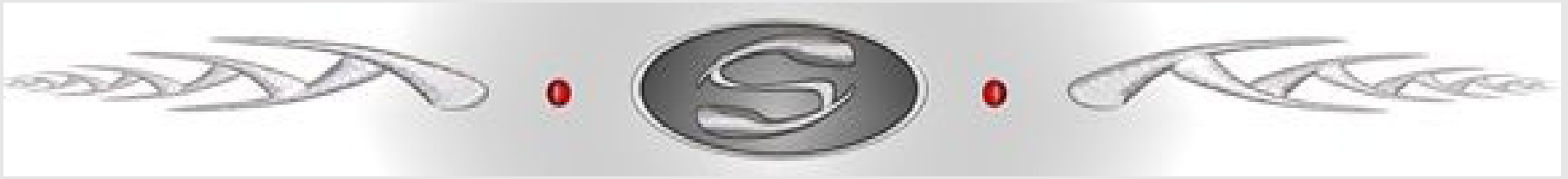


“Analisi di sicurezza dei protocolli di routing dinamico”

Marco 'embyte' Balduzzi
Michele 'mydecay' Marchetto
Valerio 'click' Genovese

<embyte/mydecay/click@spine-group.org>

Analisi di sicurezza dei protocolli di routing dinamico

- La routing table
- I protocolli di routing dinamico e le loro vulnerabilita'
  - RIP (e RIPv2)
  - OSPF
  - BGP4 (se rimane tempo)

La routing table

- *Processo di routing* : Gestione della routing table

- *Routing Table (RT)* : tabella utilizzata dal processo di forwarding per indirizzare i pacchetti verso l'interfaccia su cui e' raggiungibile *al minor costo* il destinatario

- Struttura di ciascuna *entry*:

```
Destinazione/rotta : next-hop : metrica
```

I protocolli di routing dinamico

- La RT (routing table) puo' essere popolata:
  - Con *rotte statiche* : configurate manualmente dall'amministratore e non variano nel tempo
  - Con *rotte dinamiche* : si autoadattano alla configurazione della rete (instradamento, caduta/aggiunta di un router)
- Protocolli di routing dinamico
  - Evitano l'errore umano di configurazione e di coordinamento tra network manager diversi
  - Permettono ai router di conoscere il *percorso migliore* verso una destinazione

La routing table: esempio

```
Router#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, * - candidate default
       U - per-user static route

Gateway of last resort is not set
C       192.168.2.0/24 is directly connected, 192.168.2.0
C       192.168.1.0/24 is directly connected, 192.168.1.0
R       192.168.4.0/24 [120/1] via 192.168.1.1, 00:06:26, Ethernet0
R       192.168.3.0/24 [120/1] via 192.168.2.1, 00:04:37, Ethernet1

Router#ping 192.168.3.0

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.3.0, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
```

Caratteristiche di un protocollo di routing dinamico

- Dinamicita': adattano velocemente e accuratamente la RT al comportamento della rete

- Scalabilita' : gestiscono routing table via via piu' complesse (le dimensioni della RT crescono linearmente rispetto al numero di reti da instradare direttamente)

- Coerenza : mantengono la coerenza tra tutte le routing table

- Rapidita': basso tempo di convergenza (tempo che trascorre dal cambiamento della tipologia della rete e alla ricostruzione della nuova tabella di routing)

Atonomous System

- Primi anni '80 :

  Internet come Single Network (SN)

- Autonomous System (AS) :

  Insieme di router sotto il controllo della stessa entita' amministrativa (provider, aziende, enti pubblici...)

Protocolli di routing dinamico: Classificazione

- *Classificazione*

  - Extra domain Gateway Protocols (EGP): permettono la comunicazione tra router di AS differenti (BGP4)

  - Inter-Domain Gateway Protocols (IGP): gestiscono la configurazione della RT di router appartenenti allo stesso AS (RIP, OSPF, EIGRP)

  - Link state: piccoli aggiornamenti a tutti (OSPF)

  - Distance Vector: aggiornamenti (anche tutta la RT) solo vicini (RIP)

  - Path vector: piccoli aggiornamenti ai peer (BGP4)

Protocolli di routing dinamico

- Ogni rotta della RT ha un tempo di scadenza

- *Refresh periodico* attraverso messaggi di update dei protocolli di routing

- *Metrica* : fattore che permette di scegliere la rotta migliore. Diversi criteri di scelta : lunghezza percorso (RIP) , costo del percorso (OSPF) etc...

Attacchi ai protocolli di routing dinamico

- Sono vulnerabili:
  - Protocolli di routing dinamico senza autenticazione (RIPV1 per esempio)
  - Protocolli che prevedono una autenticazione debole (trasmissione della password in plain-text in rete)
  - Altri!
- Fine dell'attacco:
  - *Sniffing* su rete switchata : dirottamento del traffico di rete attraverso l'attaccante (man in the middle)
  - *DoS*: dirottamento verso un host inesistente

RIP

- Protocolli di routing IP piu' vecchio ancora in uso
- Algoritmo distance vector sviluppato da Bellman, Ford e Fulkerson (1969)
- Ultima revisione: 1998 – RFC 1058
- *Metrica* : numero di link attraversati per raggiungere la destinazione (hop count). Numero compreso tra 0-15 (16 indica infinito)
- *Protocollo di trasporto* : UDP:520, broadcast

RIP

- Timers
  - Routing update timer (30s): tempo di update delle rotte
  - Route invalid timer (90s) : intervallo dopo il quale una route e' dichiarata irraggiungibile (distanza posta fino a == 16)
  - Route flash timer (270s): intervallo dopo il quale la rotta e' cancellata dalla routing table

RIP

- E' previsto un *comando di richiesta* per richiedere una parte o tutta la routing table

- Messaggi di update (*comando di risposta*) temporizzati ogni 30 secondi o in seguito a modifiche sulla routing table (ritardo casuale tra 1 e 5 secondi)

- All'arrivo di ogni messaggio di update il processo di routing verifica la validita' del messaggio (rotta non nulla, diversa da 127 e appartenente a una delle classi A, B o C)

Ripv1: l'algoritmo “distance vector”

- Se il messaggio è corretto la metrica viene incrementata di 1 ed è eseguito *l'algoritmo “distance vector”*:

a) voce non presente e metrica non infinita: la rotta viene aggiunta (next-hop inizializzato all'indirizzo del mittente)
b) rotta presente ma metrica più grande: vengono aggiornati i campi metrica e next-hop
c) rotta presente e il next-hop è il mittente del messaggio di risposta: la rotta viene sempre aggiornata
d) in tutti gli altri casi l'update viene ignorato

L'evoluzione: RIP Version 2

- Sviluppato da Gray Malkin – RFC 1388

- Supporto per le *sottoreti* (la netmask viene trasmessa nel campo “must be zero”)

- Trasmissione degli update in *multicast* (224.0.0.9) e *non* piu' broadcast

- Aggiunta *autenticazione* :

    - Segmento di autenticazione composto dai campi
        - AFI = 0xFFFF (0x2 per retrocompatibilita' v1)
        - Authentication Type (Plain text o MD5)
        - Chiave (16 bytes)

RIP Version 2

- Aggiunto il campo *next-hop* : un messaggio di update puo' indicare come next-hop un router diverso da se.

- *Modifiche* dell'algoritmo visto in precedenza:

  a") voce non presente e metrica non infinita: la rotta viene aggiunta (next hop inizializzato al next-hop indicato dal pacchetto di update, può anche coincidere con il mittente)

  b") rotta presente e il mittente e' lo stesso che l'ha annunciata la prima volta : viene sempre aggiornato il campo next-hop e la metrica, anche se quella nella RT e' migliore (minore)

  e) rotte presente ma con netmask piu grande: viene aggiunta la nuova rotta

Esempio: RIP in IOS

```
Router#show ip protocols
Routing Protocol is "rip"
  Sending updates every 30 seconds, next due in 26 seconds
  Invalid after 180 seconds, hold down 180, flushed after 240
  Outgoing update filter list for all interfaces is
  Incoming update filter list for all interfaces is
  Redistributing:   rip
  Default version control: send version 1, receive any version
    Interface         Send  Recv   Key-chain
    Ethernet0         1     1 2
    Ethernet1         1     1 2
  Routing for Networks:
    192.168.1.0
    192.168.2.0
  Routing Information Sources:
    192.168.2.0           120      00:00:09
    192.168.1.0           120      00:00:09
  Distance: (default is 120)
```

Vulnerabilita'

- REQUEST e RESPONSE vengono mandate in multicast
- Le informazioni passano in chiaro
- In molte implementazioni, di default non esiste autenticazione
- RIP utilizza UDP quindi e' facile spooffare l'ip sorgente anche in LAN switchate
- Non esiste un modo per verificare che le informazioni ricevute siano consistenti

Cosa possiamo ottenere?

- Dirottamento del flusso delle connessioni
- Rendere irraggiungibile un host/un gruppo di hosts
- Influenzare il routing inter-AS
- Vedere il traffico di qualsiasi host

Modalita' di attacco

- Simulare di essere un router
  - Pubblicizzazione di rotte fasulle
    - Annunciare rotte inesistenti per variare il flusso inter-AS
    - Rendere irraggiungibili alcuni host/gruppi di host
  - Pubblicizzazione di metriche fasulle
    - Variare il flusso delle connessioni attraverso la pubblicizzazione di metriche migliori di quelle attuali
    - In alcuni casi rendere indisponibili alcuni gruppi di host
- Impersonare un router
  - Comodo perche' via UDP
  - Difficile da gestire in presenza di triggered updates (sempre :))
  - Piu' sicuro e piu' difficilmente scovabile

Alcuni trucchi

- Una netmask piu' precisa ha la precedenza su una netmask meno precisa
  - Possibilita' di aumentare le metriche per alcuni host
- Quando possibile impersonare un router invece di simularlo
  - Meno probabilita' di essere scoperti
- In alcuni casi e' possibile injectare rotte da remoto
  - Demoni di routing mal configurati

Autenticazioni

- Plain text
  - Utile solo per salvaguardare il routing da errori di configurazione
  - Totalmente insufficente contro un attaccante maligno
- MD5
  - Offre una buona sicurezza
  - Le chiavi non passano mai attraverso la rete (pre-shared)
  - MD5 e' stato dimostrato vulnerabile
- Tunnel criptati tra i router (VPN)
- Ipsec
  - Sicurezza massima
- Steganografia :)
- RIP-TP

MD5 - Pro e Contro

- PRO
  - Abbastanza sicuro per evitare l'injection di rotte
  - Sequence number per evitare reply attack
- CONTRO
  - Non impedisce di vedere il traffico di routing
  - Possible dictionari attack

RIP-TP (1)

- Controllo delle rotte ricevute attraverso un algoritmo a “triangolo”
- Tutte le rotte che arrivano vengono verificate sia attraverso l'algoritmo che con dei prob icmp
- E' possibile aggirarlo forgiando ad-hoc degli ICMP reply

RIP-TP (2)

- b annuncia ad a la sua metrica verso c
- a contolla:

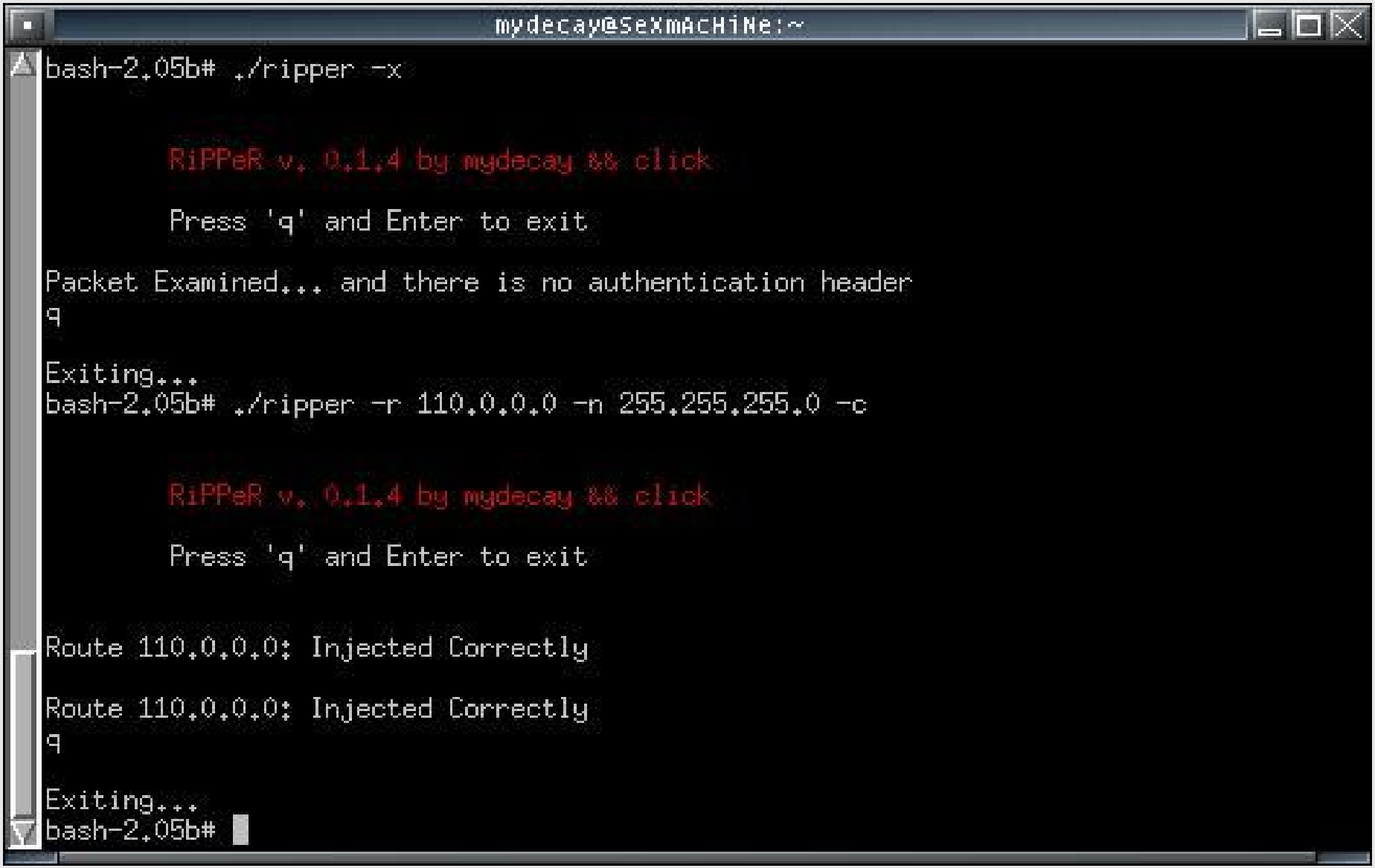
  Dist(a, c) <= Dist(a, b) + Dist(b, c)
- e con Z = nexthop(a, c):

  Dist(Z, c) <= Dist(Z,b) + Dist(b, c)
  - Dist(Z, c) <= non e' nota ma deve essere <= 2 poiche' Z e b sono neighbor
- Vengono mandati degli ICMP di probing con TTL== Dist(b ,i) + 1
  - Se i prob falliscono, significa che il percorso e' piu' lungo di quello anninciato
  - La rotta viene scartata

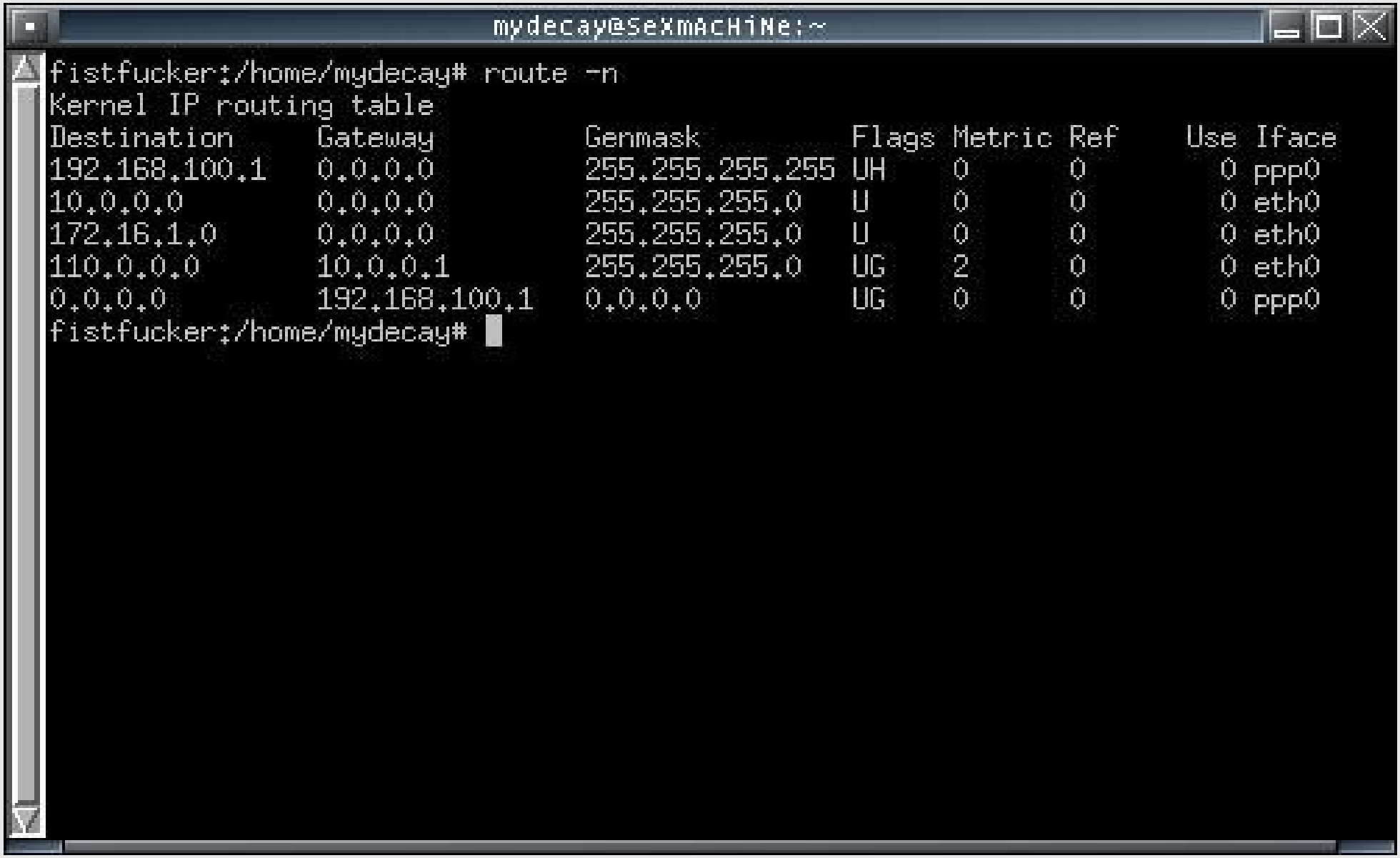
Ripper

- Injectare una o molteplici rotte fasulle complete di gw e netmask
- Sniffare password
- Scanner di routers RIPv2
- Possibilita' di mandare RESPONSE spooffate
- Possibilita' di mandare RESPONSE a peer remoti
- Capacita' di controllare se la rotta e' stata injectata correttamente
- Injecting con password

Un caso dimostrativo (1)



Un caso dimostrativo (2)



OSPF (Open Short Path First)

- Tecnologia “Link state”
- Database distribuito
- Protocollo di flooding
- Definizione di adjacency
- Routes esterne

- L'AS viene suddiviso in aree

“*OSPF allows collections of contiguous networks and hosts to be grouped together. Such group, together with routers having interfaces to any one of the included networks, is called an area*”

- Ogni area ha il suo link-state database e il grafico corrispondente (questo garantisce un basso utilizzo di CPU e memoria)
- I router interni ad un area non conoscono nulla della topologia dettagliata esterna all'area stessa

Reti broadcast

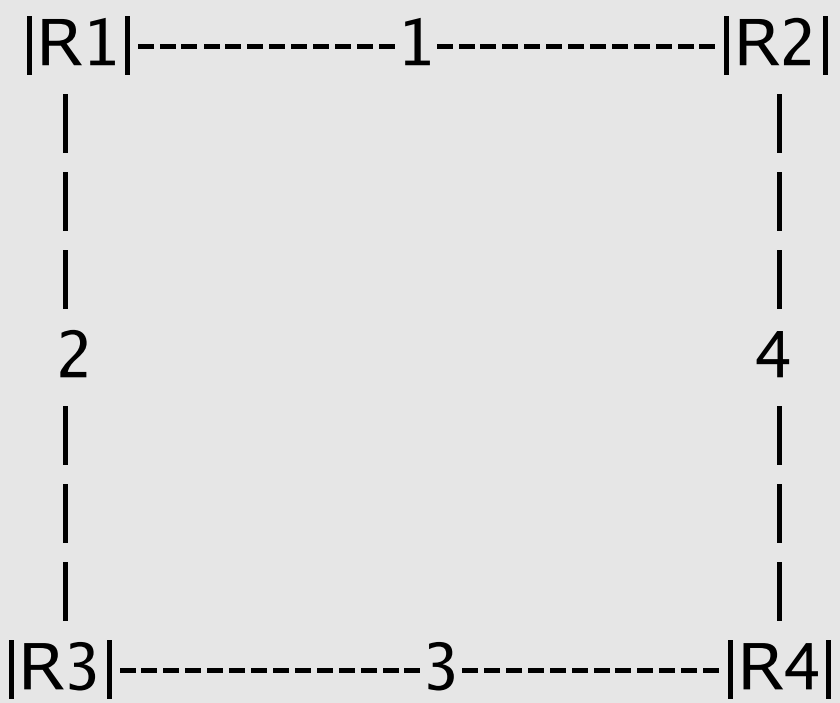
- Per questione di tempo tutti gli esempi e gli algoritmi trattati prenderanno in analisi solamente reti broadcast

- Reti ethernet o token ring offrono principalmente 2 tipi di servizi :

 - Piena connettivita' : Ogni stazione puo' inviare un pacchetto a qualsiasi altra stazione

- Capacita' broadcast : Una stazione puo' inviare un pacchetto a tutte le altre stazioni (broadcast) o a tutte le altre stazioni facenti parte di un gruppo (multicast)

Il Protocollo di flooding (1)



*Supponiamo cada il link 1 tra R1 e R2

*R1 invia a R3 un messaggio dicendo che tra R1 e R2, attraverso il link 1 la distanza e' infinita.

*R3 a R4

Il Protocollo di flooding (2)

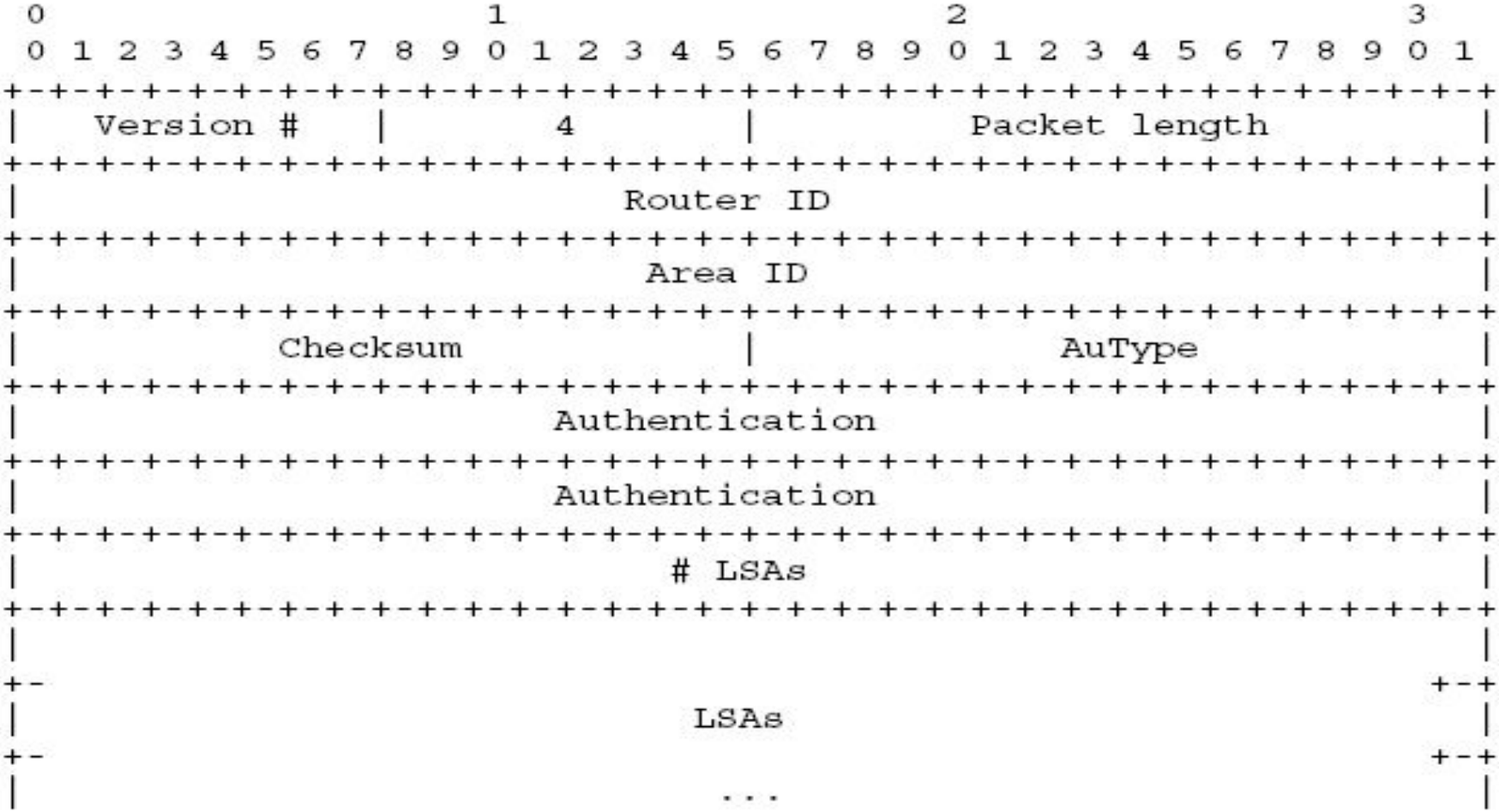
che vecchi messaggi tornino indietro e compromettano il database

- Ogni messaggio conterra' un quantificatore (ora oppure numero incrementato nel tempo) che permette di verificare l'eta' e quindi l'affidabilita' del pacchetto

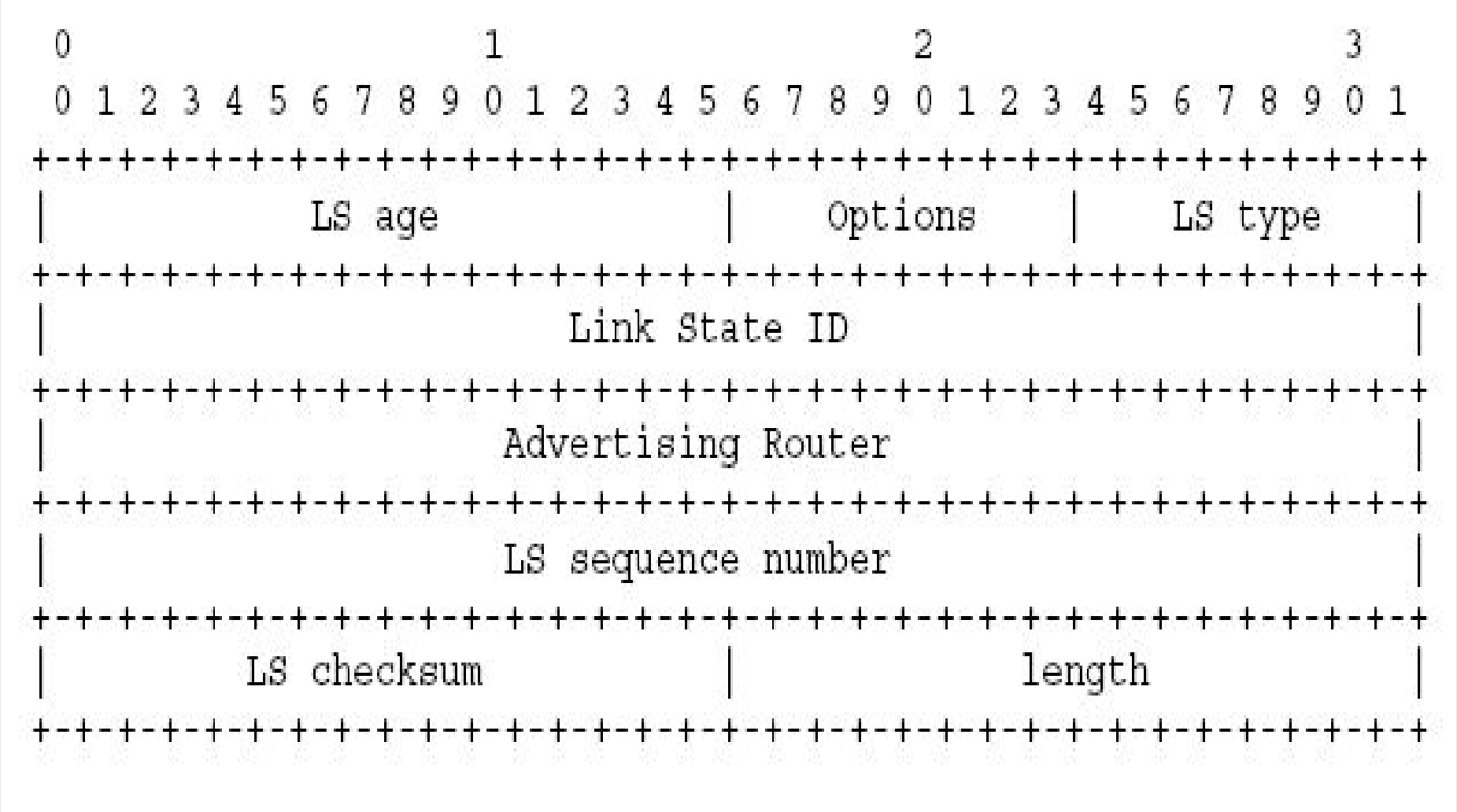
- Il protocollo di fooding si occupa quindi di gestire la procedura di aggiornamento dei database nel modo piu' veloce e performante possibile

Link State Update

- OPSF gestisce gli aggiornamenti dei vari link attraverso i pacchetti Link State Update



Link State Acknowledgement



Le adiacenze....queste sconosciute

- Definizioe di adiacenza

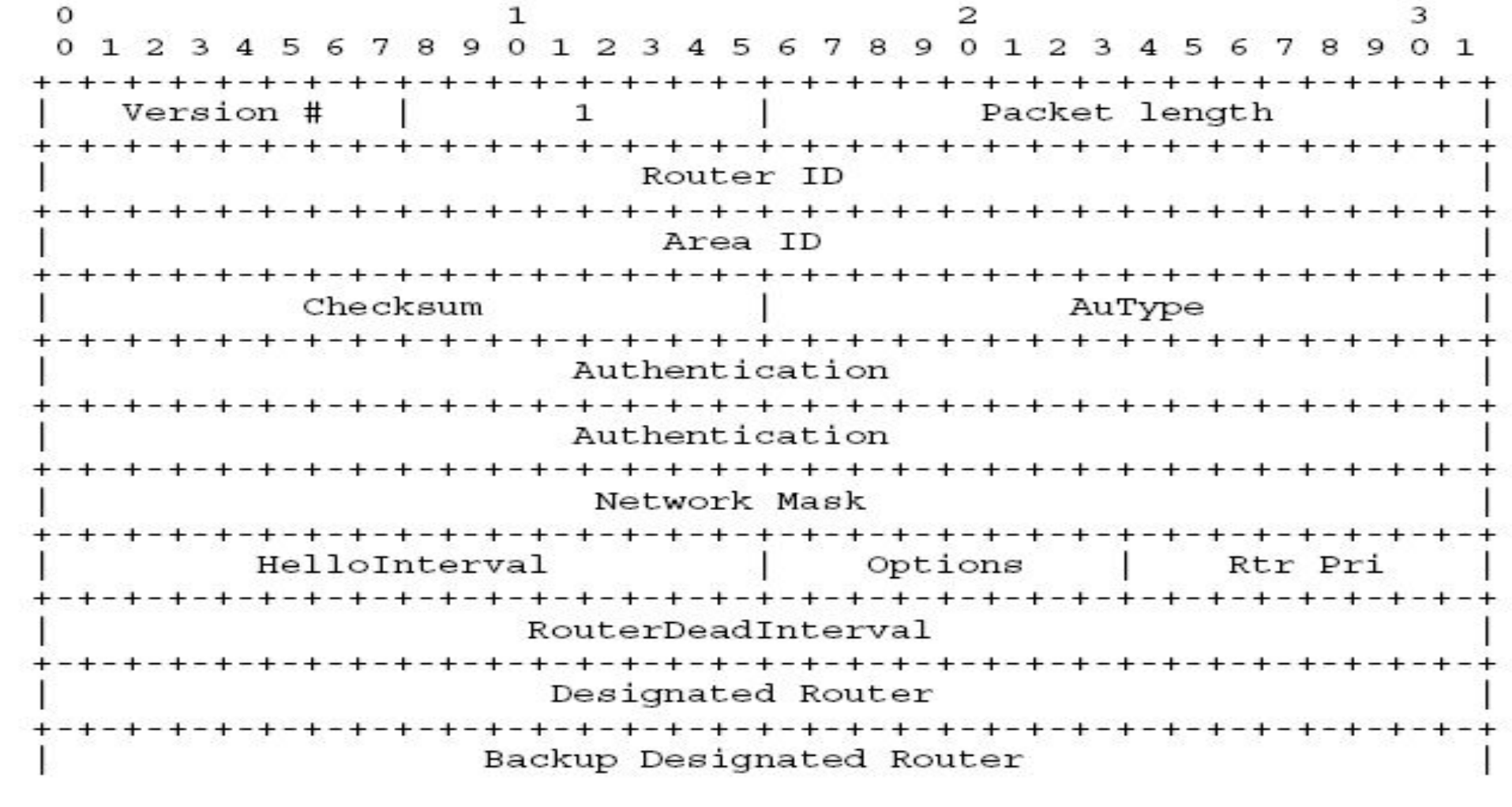
“A relationship formed between selected neighboring router for the purpose of exchanging routing information”

- Il Designated Router
  - Elenca i routers attaccati nel network
  - Diventa adiacente a tutti gli altri routers della rete. Fino a quando i link state databases sono sincronizzati attraverso le adiacenze, i il DR gioca un ruolo centrale nel processo di sincronizzazione.

- Con la presenza di un DR abbiamo anche un BDR *(Backup Designated Router)*

L'HELLO protocol

- Il DR e il BDR vengono eletti attraverso l'hello protocol



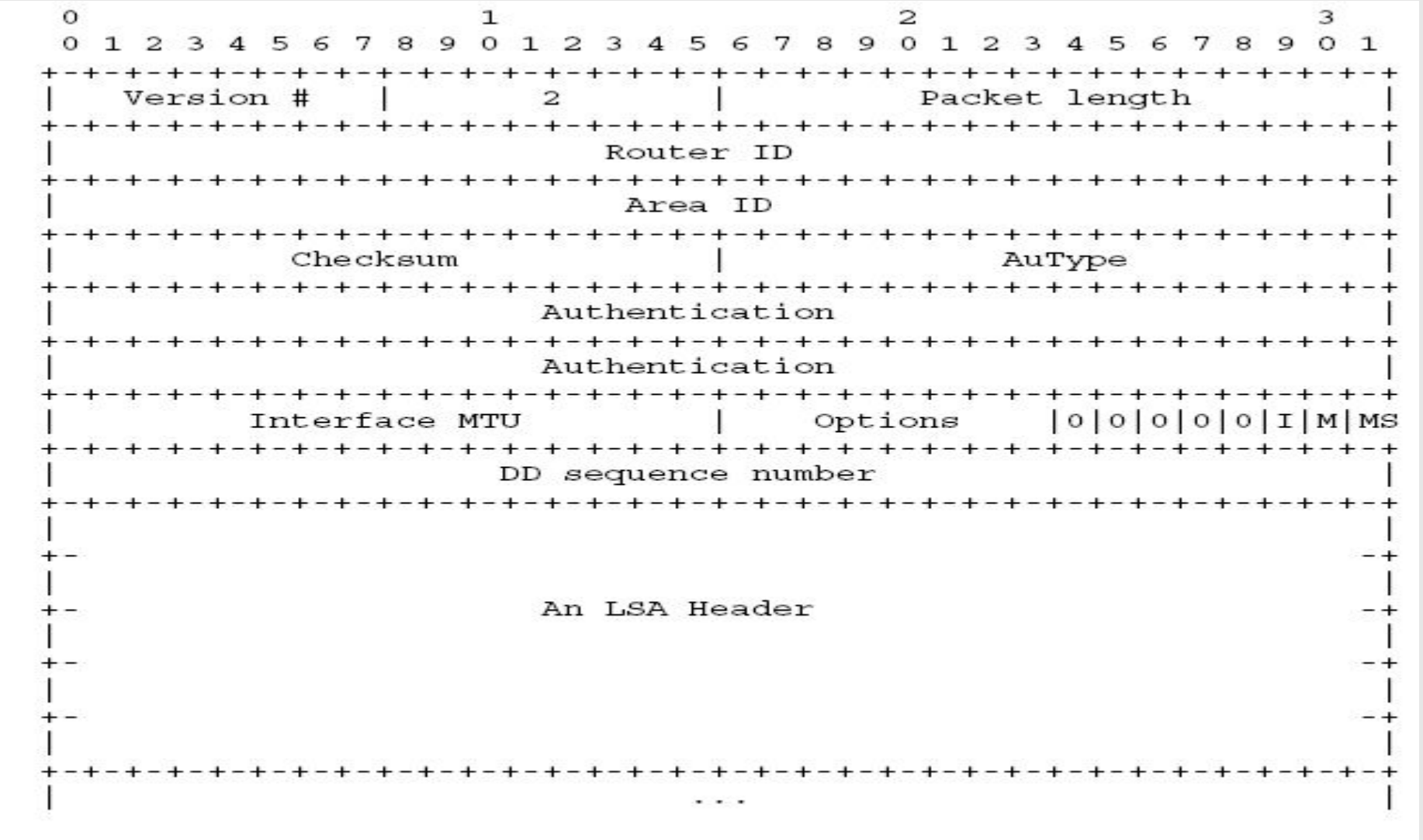
La procedura di exchange

- La sincronizzazione dei Database con il DR e il BDR avviene attraverso una procedura di exchange, poi sara' il protocollo di flooding ad occuparsi di mantenera aggiornati i database.

- Protocollo asimmetrico (master/slave)

- Per lo scambio dei Databases si utilizza il Database Description Packet

Database Description Packet



La procedura di exchange

- Il master emette un pacchetto vuoto con settati I,M e MS piu' un numero di sequenza.

- Lo slave risponde con un pacchetto di acknowledgement con lo stesso numero di seq e i bit I e M settati a 1 , quello MS a 0

- Il primo router emette pacchetti DD con I settato a 0, M e MS settati a 1 (eccetto M per l'ultimo pacchetto). I pacchetti saranno numerati in sequenza e inviati uno alla volta

- Lo slave risponde ad ogni DD con un DD acknowledgement che riporta la sua descrizione del database, con lo stesso seq ma con MS settato a 0

La procedura di exchange

- Se il master non riceve l'ack entro un tot di tempo ri-invia il pacchetto originale DD

- Durante lo scambio sia il master che lo slave controllano di avere l'LSA inviato della controparte, e questo non deve essere piu' vecchio di quello ricevuto.Altrimenti al termine della procedura avverra' una richiesta di LSA tramite i pacchetti Link State Request [LST LSID AR]

- Questi pacchetti, identificati nel campo type dell'header comune, vengono inviati alla fine del DD se sono stati rilevati LSA da sincronizzare

- Gli LSA richiesti sono inviati attraverso il protocollo di flooding

OSPF (in)security

- Protocollo di flooding

“Come detto in precedenza il protocollo di flooding e' reliable, cio' assicura che tutti i router nella stessa area abbiano lo stesso Database.”

- Router “buoni” che correggono quelli “cattivi”

- Attacchi del genere facilmente individuabili dagli IDS, almeno in teoria

- “Routing gerarchico” che prevede la suddivisione di parti indipendenti connesse ad un area centrale definita backbone.

OSPF (in)securities

Il routing gerarchico oltre ad essere un'ottima soluzione per la gestione del carico di calcolo dei router si rivele essere valido anche dal punto di vista della sicurezza.

- Compromissione di un router interno:

Un router interno non conosce la topologia esterna alla sua area, il danno che potra' fare sara' quindi limitato alla sua area

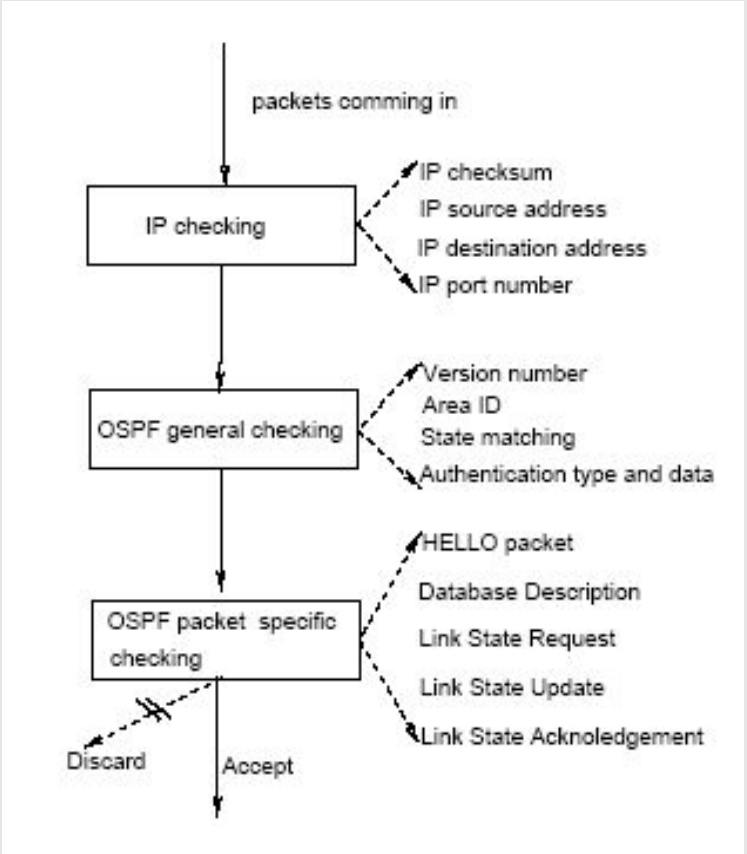
- ABR (Area Bounder Router) e' compromesso:

Se nella rete vi e' un solo ABR o l'ABR compromesso e' l'unico attaccato al backbone, allora i danni che si possono apportare sono gravi. Se invece ci sono altri ABRs, per ridondanza si dovrebbe poter identificare un eventuale conflitto.

OSPF (in)securities

- ASBR (Autonomous System Border Router) compromesso:
OSPF utilizza ASBR per importare routing information esterne. Non vi e' possibilita di controllo su cioe' che l'ASBR dice (almeno stando all'RFC), cio' rappresenta sicuramente una seria “insicurezza” del protocllo.

- OSPF packet procedure checking:

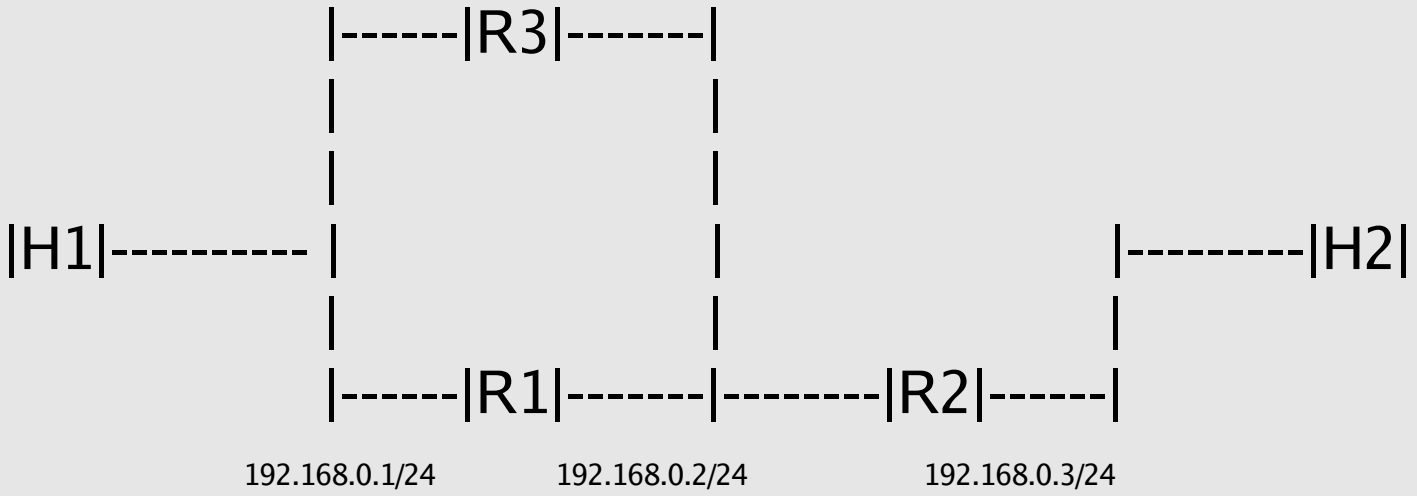


OSPF (in)securities

- I campi piu' “caldi” che potrebbero essere soggetti ad attacchi sono : metriche, sequence number e age. Le prime due possono essere risolte con l'MD5 auth, ma non la terza

- Man In The Middle attacks

- ICMP redirect attack



OSPF (in)securities

1) ICMP redirect attack su H1 : in questo modo devio il traffico di H1 su R3, il router malizioso

2) R3 lancia processi OSPF maliziosi: R3 deve utilizzare l'HELLO protocol per portare avanti le adiacenze con i vicini (in questo caso R1 e R2), e mantanere questa relazione inviando periodicamente HELLO packets

3) Il flusso di dati e' stato cambiato

OSPF (in)securities

- La questione sui DR e BDR

- Attacco facilmente rilevabile dagli IDS (almeno a liv teorico)

- Attacchi di tipo DoS

BGP (1)

- Exterior Gateway Protocol (EGP) a vettore di percorso (Path Vector)

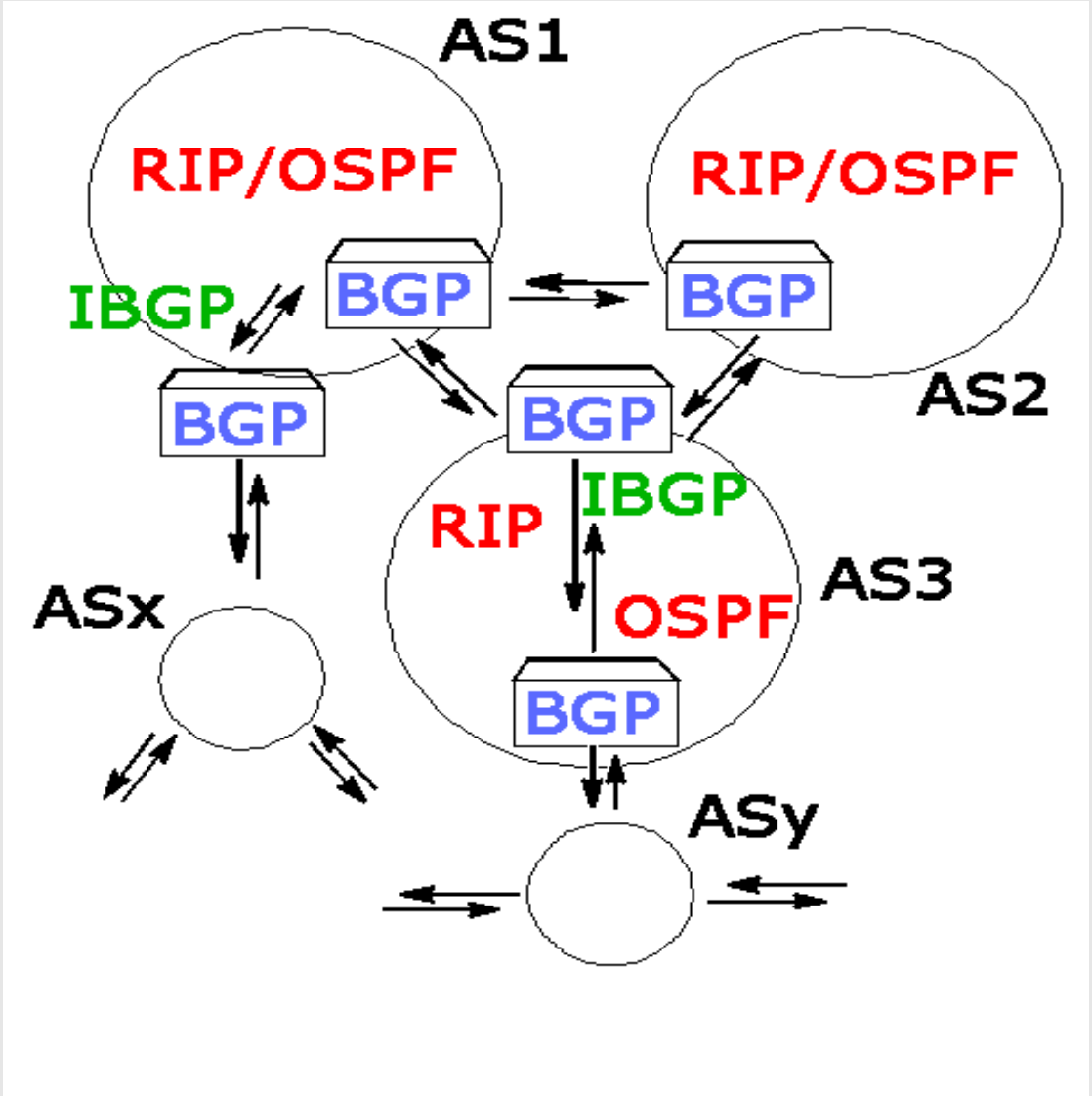
- Permette ad AS differenti di comunicarsi gli aggiornamenti di routing

- BGP e' in grado di costruire un albero di AS in base alle informazioni scambiate attraverso il quale puo' instradare pacchetti verso qualsiasi destinazione

- Presuppone che il routing intra-AS sia effettuato attraverso un IGP

- I peer BGP di uno stesso AS possono dialogare attraverso connessioni IBGP

BGP (2)


AS1
RIP/OSPF
RIP/OSPF
IBGP
BGP
BGP
BGP
BGP
AS2
RIP
IBGP
OSPF
AS3
ASx
BGP
ASy

Il protocollo (1)

- OPEN, UPDATE, KEEPALIVE, NOTIFICATION
- OPEN: Apre una connessione tra due peer *BGP
- UPDATE: Aggiorna le informazioni nella routing table dei router
- KEEPALIVE: Mantiene up una connessione
- NOTIFICATION: Notifica errori di vario genere
- Si appoggia al TCP al quale delega tutto il lavoro di mantenere lo stato della connessione , il controllo degli errori...

Il protocollo (2)

- Tra due parti BGP viene istituita una connessione TCP
  - L'autenticita' di due parti viene stabilita in base a delle ACL presenti nel router ed eventualmente attraverso una signature MD5 (analizzata dopo)

- I due pari si scambiano le nuove rotte, le rotte non piu' raggiungibili e quelle che hanno cambiato attributi

- La connessione viene tenuta viva dai messaggi di KEEPALIVE e rimane in questo stato fino al verificarsi di un errore

Possibili attacchi

- Attacchi al TCP
  - DDoS , Resource Saturation, hijacking, spoofing
- Attacchi a BGP
  - Pacchetti malformati, packet injection, ...
- Attacchi alle configurazioni
  - ACL troppo permissive, ...
- Attacchi a MD5
  - Dictionary attack, brute force
- Attacchi agli IGP
  - Injectare rotte negli IGP per influenzare BGP

Attacchi al TCP

- Dipendenti dalle implementazioni dei router e indipendenti di BGP
  - DDoS , Syn-flood ...
- Spoofing cieco
  - Sfruttare ACL che agiscono a layer > 4
  - Saturare la coda di connessioni possibili
- Spoofing vedente (BGP e' stateless)
  - Hijacking
  - Packet injection
  - Connection reset

Attacchi a BGP

- Connection breacking
  - Pacchetti malformati
- Router Injection
  - Possiamo variare il routing per porzioni di Internet
  - Date le premesse precedenti (TCP) e' estremamente facile injectare rotte

Attacchi alle configurazioni

- ACL inesistenti
- ACL che permettono accesso a range di ip
- ACL che permettono accesso per AS
- Controllo dell'accesso a layer > 4

Attacchi a MD5

- Dictionary attack
  - Passwd, data, source port, dest port (facile)

- Brute force su password particolarmente deboli
  - Passwd, data, source port, dest port (facile)

- Attacchi molto difficili da attuare data la quantita' di cose da indovinare, anche avendo la possibilita' di vedere il traffico

Attacchi agli IGP

- La forza di una catena e' data dalla forza del suo anello piu' debole

- Modificando il routing interno all'AS e' possibile, in certi casi, modificare le route trasmesse ad altri AS

- Agire sugli IGP interni all'AS e piu' agile
  - Traffico multicast (PIMV2 Sparse mode)
  - Compromissione di router

Contromisure: BGP-MD5(1)

- PRO
  - Previene numerosi attacchi
  - Agile da configurare
- CONTRO
  - Le implementazioni di free (Quagga, Zebra) non prevedono
  - L'algoritmo MD5 e' dimostrato vulnerabile
    ftp://ftp.rsasecurity.com/pub/cryptobytes/crypto2n2.pdf

BGP-MD5(2)

- I pari BGP creano una signature che inseriranno nel pacchetto nel seguente modo:

- MD5 tra
  - TCP pseudo-header (souce add, dest addr, protocol number, length)
  - TCP header senza opzioni e checksum = = 0
  - TCP data
  - Una password scelta dal sysadmin e MAI trasmessa on the wire

S-BGP (1)

- S-BGP rappresenta una serie di policy che rendono il protocollo (abbastanza) sicuro:
  - PKI (Public Key Infrastructure)
  - attestations
  - Ipsec (ESP)
- PKI utilizza tre tipi di certificati x.509 v3:
  1) Assegna una chiave pubblica ad un range di IP
  2) Assegna una chiave pubblica ad una organizzazione e ad un set di AS
  3) Assegna una chiave pubblica ad un AS e ai router ID

Queste chiavi sono utlizzate per verificare che un dato IP appartenga effettivamente all'AS

S-BGP (2)

- Le attestazioni sono firmate usando chiavi PKI

- AA (Adress Attestation)
  - Sono utilizzati per confermare che i prefissi nel messaggio di UPDATE sono autorizzati dall'ISP
  - Deve esserci un AA per ogni organizzazione di cui e' presente un prefisso IP nel messaggio di UPDATE

- RA (Route Attestation)
  1) Assegna una chiave pubblica ad un range di IP
  2) Assegna una chiave pubblica ad una organizzazione e ad un set di AS
  3) Assegna una chiave pubblica ad un AS e ai router ID

Queste chiavi sono utlizzate per verificare che un dato IP appartenga effettivamente all'AS

S-BGP (3)

- IPsec (ESP)
- Garantita l'integrita' del playload grazie a ESP
- Immune ai reply attack
- Sicurezza massima ottenibile
- Immune a sniffing del traffico

References

Tutto il materiale presentato in questa esposizione sara' disponibile sull'homepage dello S.P.I.N.E. Group: www.spine-group.org

Sito dell'evento SecurityDate: http://www.securitydate.it

Approfondimenti sui singoli protocolli sono disponibili su www.networkingitalia.it

Si consiglia inoltre la lettura del testo reperibile all'indirizzo: www.cs.ucsb.edu/~rsg/Routing/references/wang98vulnerability.pdf