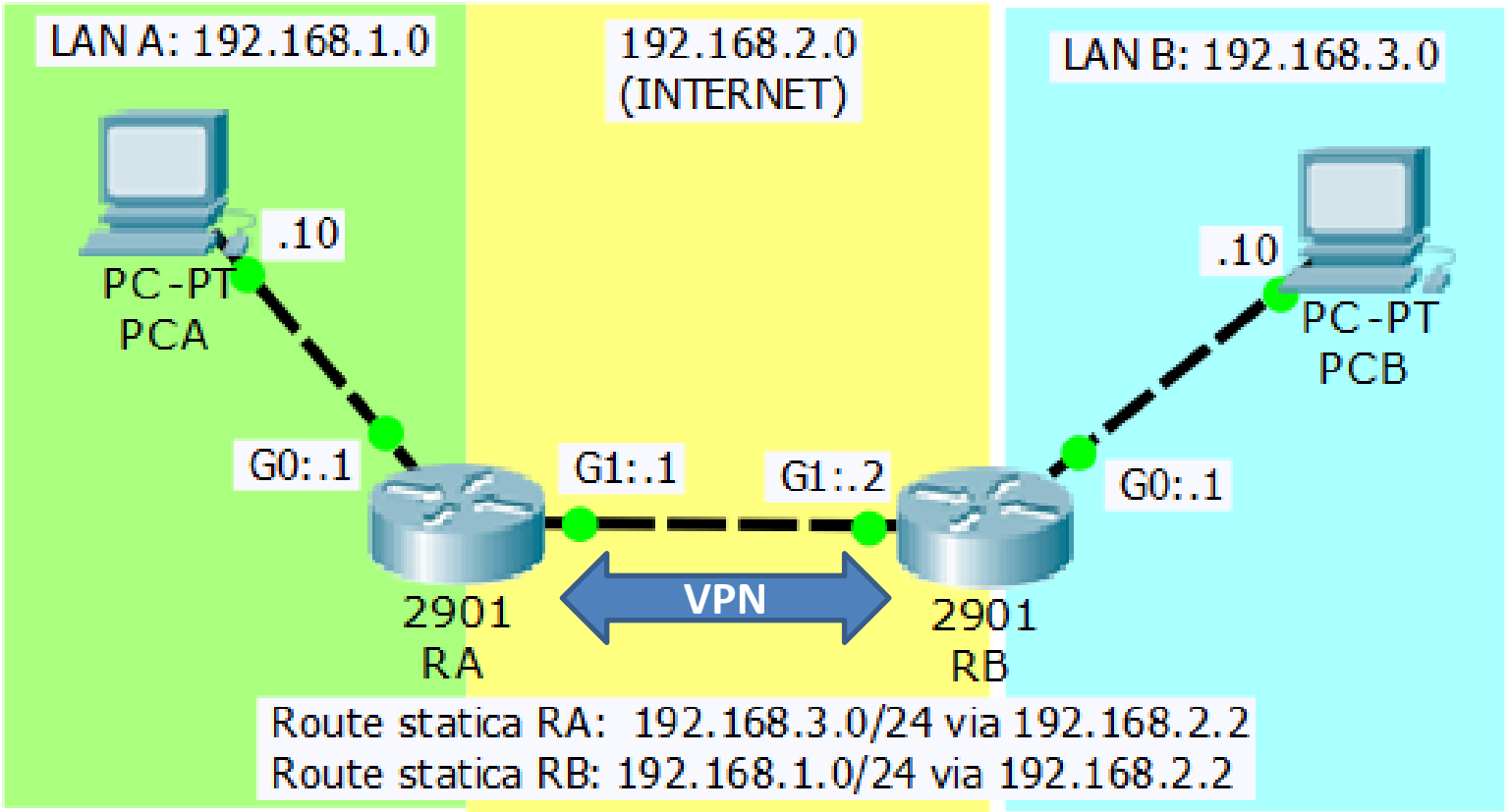
# Configurazione VPN Lan-to-Lan



# Fasi per la Configurazione VPN Lan-to-Lan

- Attivare il modulo Security (router 2901)
- Definire il Traffico Interessato alla VPN (access-list 110)
- Config. ISAKMP per lo scambio chiavi (ISAKMP policy 10)
- Definire la password condivisa per ISAKMP (password ABACUS)
- Config. IPSEC per criptare/autent. i pacchetti (transform-set MIOTS)
- Definire la “mappa” che fonde le varie impostazioni (MIAMAPPA)
- Applicare la Mappa all’interfaccia di uscita del Router

# Configurazione Router RA per VPN Lan-to-Lan

```
... attivare il modulo security (necessario salvare e riavviare) ...
R(config)#  license boot module c2900 technology-package securityk9
... identificare il traffico ...
R(config)#  access-list 110 permit ip 192.168.1.0  0.0.0.255  192.168.3.0  0.0.0.255
... configurare ISAKMP (default: encryption 3DES, hash SHA-1, lifetime 86400 s)
R(config)#  crypto isakmp policy 10
R(config-isamkp)#  authentication pre-share
... imposta la chiave condivisa ...
R(config)#  crypto isakmp key ABACUS address 192.168.2.2
... configurare IPSEC ...
R(config)#  crypto ipsec transform-set  MIOTS esp-3des esp-md5-hmac
... configurare la mappa ...
R(config)#  crypto map MIAMAPPA 10 ipsec-isakmp
R(config-crypto-map)#  set transform-set MIOTS
R(config-crypto-map)#  set peer 192.168.2.2
R(config-crypto-map)#  match address 110
... applica la mappa all'interfaccia ...
R(config)#  interface GigabitEthernet 0/1
R(config-if)#  crypto map MIAMAPPA
```

# Configurazione della policy ISAKMP

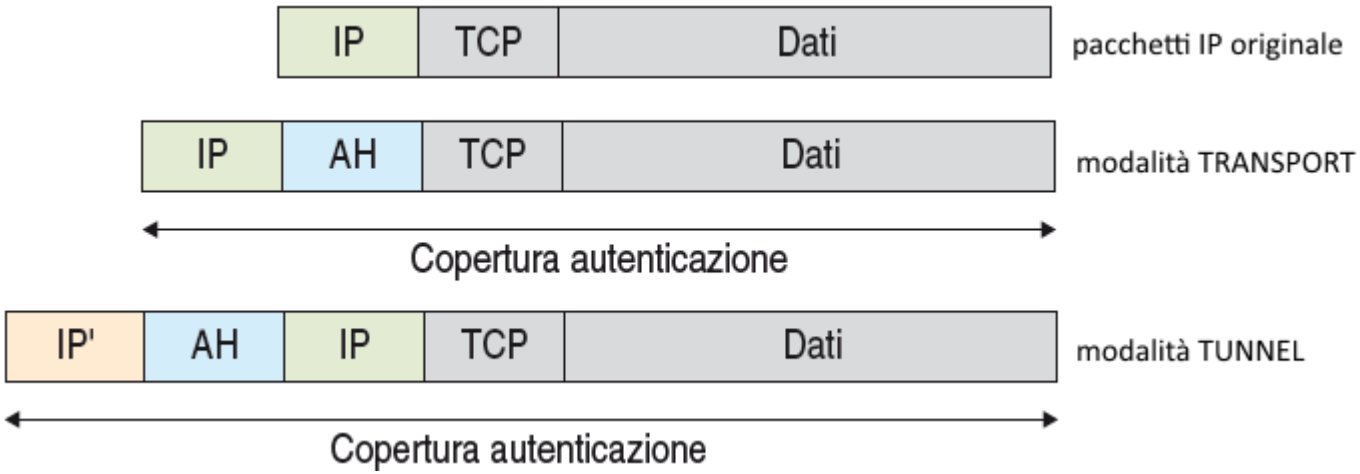
R(config)# **crypto isakmp policy 10**

- **authentication**: **RSA** (default) o **Chiave Condivisa** (pre-share)
- **encryption**: Algoritmo Crittografico (DES, **3DES** (default) o AES)
- **hash**: Algoritmo per l'Integrità (**SHA-1** (deafult), MD5, ecc.)
- **group**: Gruppo Diffie-Hellman (**Gruppo 1** (deafult), 2 o 5)
- **lifetime**: Tempo di Validità della S.A. (**86400 secondi = 1 giorno** (default))

R(config-isakmp)# **authentication** pre-share

*... nell'esempio, gli altri parametri non vengono configurati*
*e, quindi, restano impostati come da default (valori in verde) ...*

# Configurazione IPSEC (transform-set con AH)



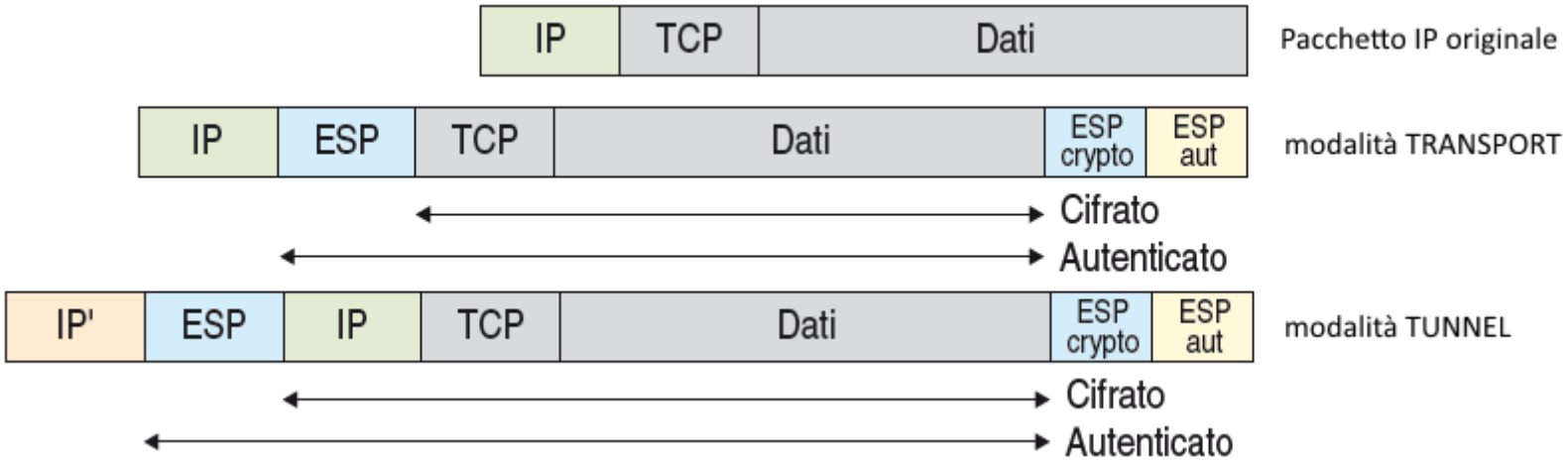

**Protocollo AH (Authentication Header): solo *AUTENTICAZIONE* dei pacchetti**

**Trasformazioni disponibili con AH: ah-md5-hmac ah-sha-hmac**

***R(config)#*** **crypto ipsec transform-set MIOTS ah-md5-hmac**

***… solo autenticazione tramite algoritomo MD5 e modalità TUNNEL …***

# Configurazione IPSEC (transform-set)

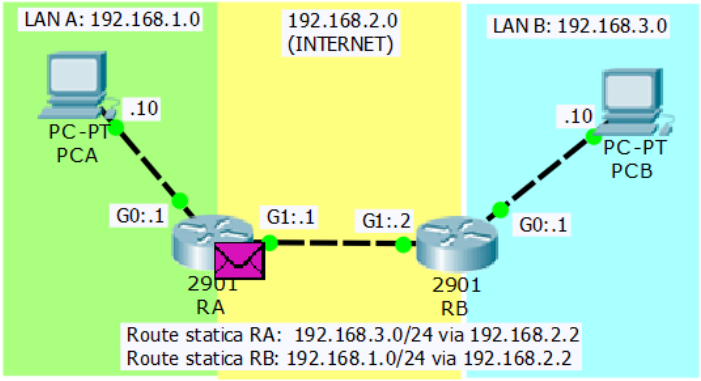



**Protocollo ESP (Encapsulating Security Payload)**
***AUTENTICAZIONE* e *CRITTOGRAFIA* dei pacchetti**

**Trasformazioni disponibili con ESP:**
**per la *crittorafia*: esp-des esp-3des esp-aes**
**per l'*autenticazione*: esp-md5-hmac esp-sha-hmac**

**R(config)# crypto ipsec transform-set MIOTS eps-3des eps-md5-hmac**
***… autenticazione con 3DES e autenticazione con MD5 in modalità TUNNEL …***

# Incapsulamento in Simulazione




Simulation Panel

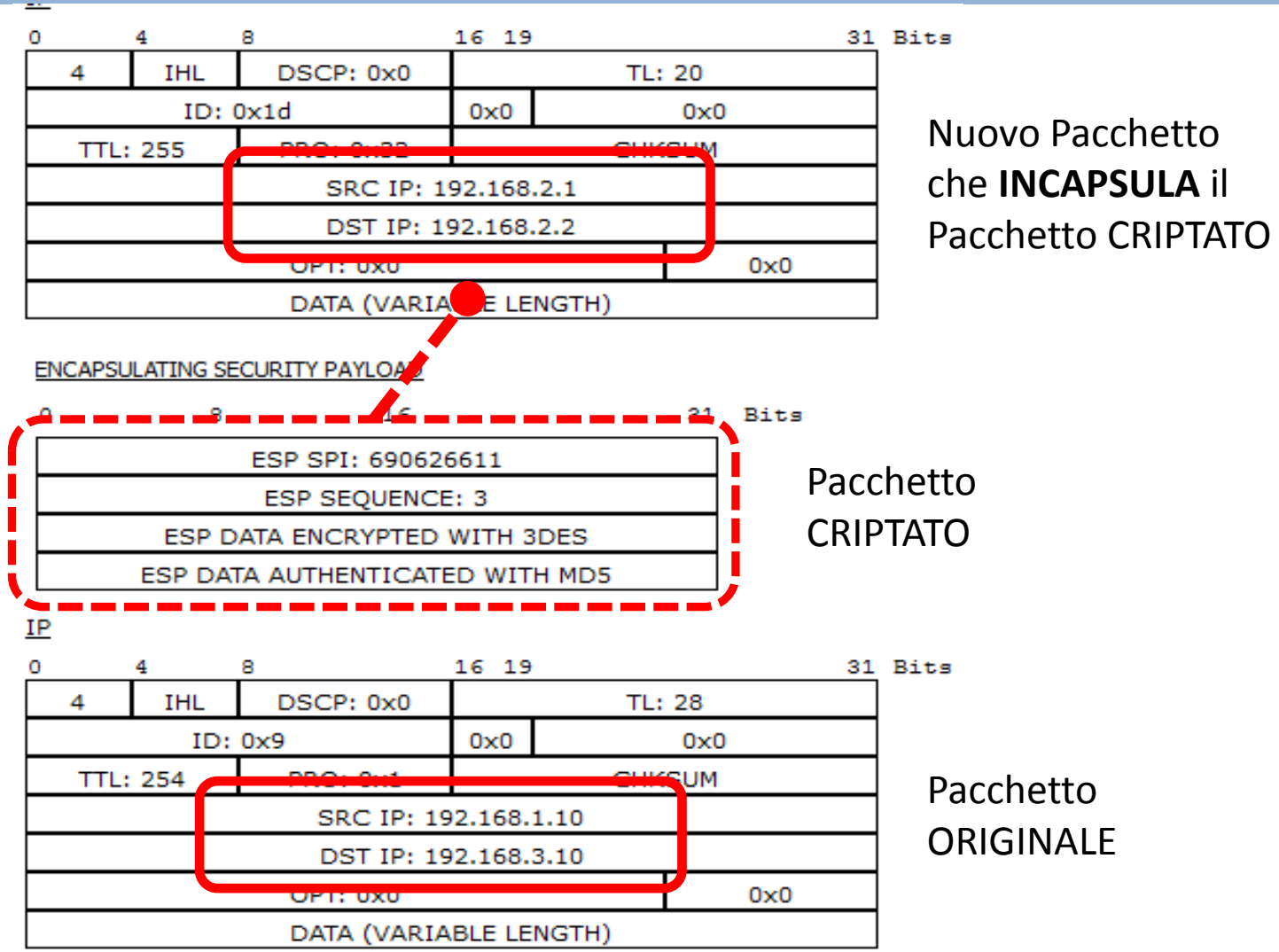
Event List

| Vis. | Time(sec) | Last Device | At Device | Type | Info |
|---|---|---|---|---|---|
| | 0.000 | -- | PCA | ICMP | |
| | 0.001 | PCA | RA | ICMP | |
| | 0.002 | RA | RB | ICMP | |
| | 0.003 | RB | PCB | ICMP | |
| | 0.004 | PCB | RB | ICMP | |
| | 0.005 | RB | RA | ICMP | |
| | 0.006 | RA | PCA | ICMP | |

| In Layers | Out Layers |
|---|---|
| Layer7 | Layer7 |
| Layer6 | Layer6 |
| Layer5 | Layer5 |
| Layer4 | Layer4 |
| Layer 3: IP Header Src. IP: 192.168.1.10, Dest. IP: 192.168.3.10 ICMP Message Type: 8 | Layer 3: IP Header Src. IP: 192.168.2.1, Dest. IP: 192.168.2.2 ICMP Message Type: 8 |
| Layer 2: Ethernet II Header 00D0.5837.723E >> 00D0.FF97.0001 | Layer 2: Ethernet II Header 00D0.FF97.0002 >> 000C.8545.BADC |
| Layer 1: Port GigabitEthernet0/0 | Layer 1: Port(s): GigabitEthernet0/1 |

1. The CEF table has an entry for the destination IP address.
2. The device decrements the TTL on the packet.
3. The traffic is interesting traffic and needs to be encrypted and encapsulated in IPSec PDUs.
4. The packet is getting encrypted and encapsulated in IPSec PDUs.
5. ESP encrypts the received packet.
6. The device encapsulates the data into an IP packet.
7. The device looks up the destination IP address in the CEF table.
8. The CEF table has an entry for the destination IP address.
9. An IPSEC (ESP/AH) message is sending out of GigabitEthernet0/1.

# Incapsulamento in Simulazione




Nuovo Pacchetto che **INCAPSULA** il Pacchetto CRIPTATO

Pacchetto CRIPTATO

Pacchetto ORIGINALE