Layer 2 Security

Reti e Sicurezza Informatica - 2010

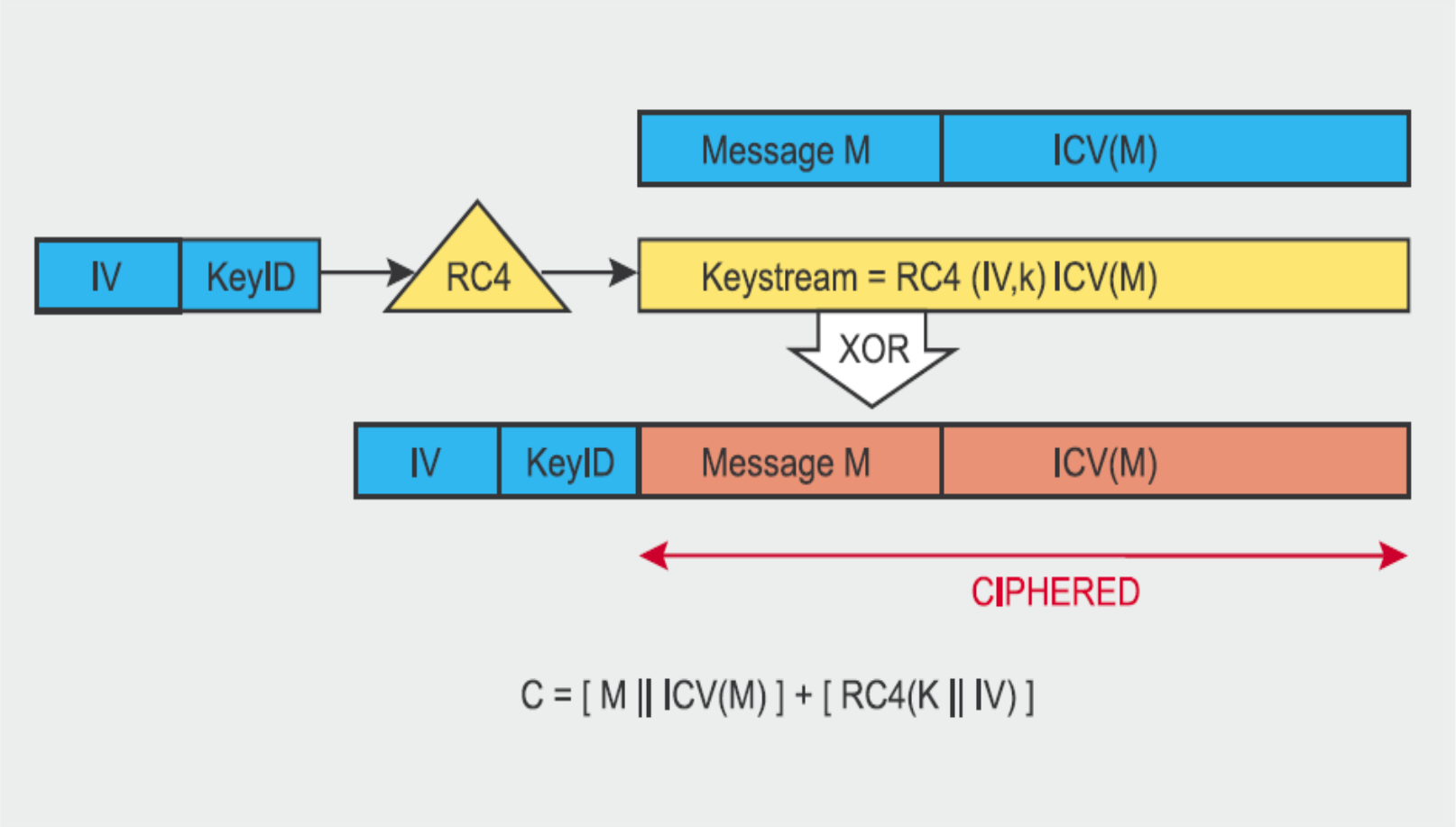
WLAN open

- Equivalente a una rete wired con hub
- Possibile sniffing, ESSID e BSSID spoofing
- De-authentication attack

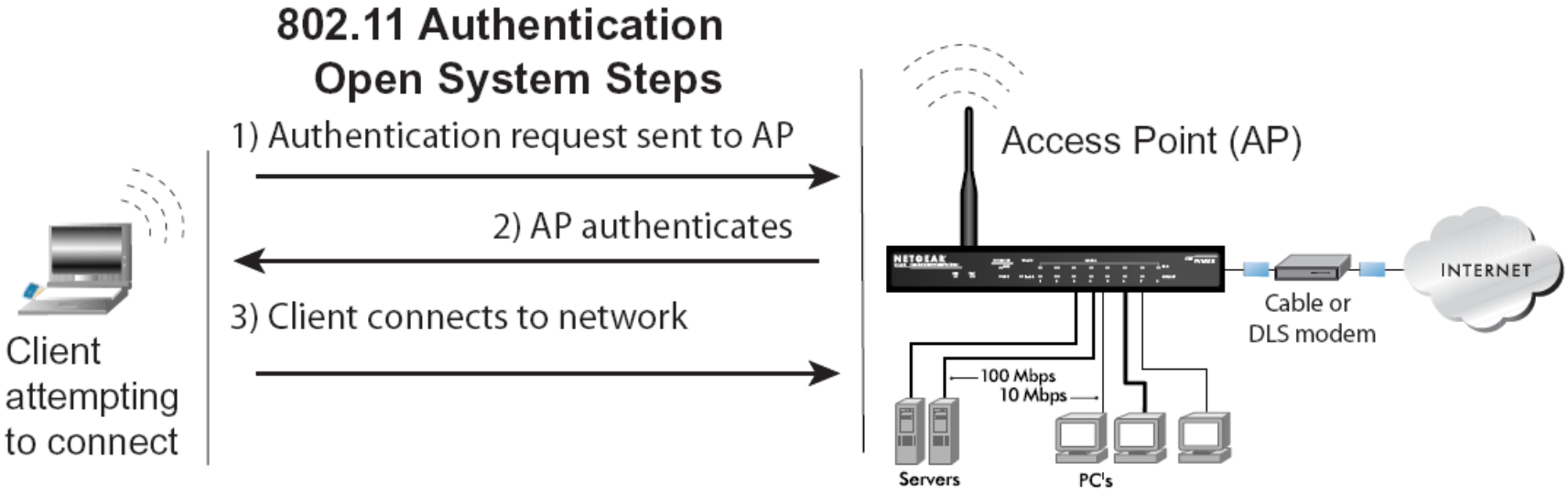
WLAN WEP

- Modalità molto semplice di crittografia a chiave pre-condivisa
- Ogni pacchetto viene crittografato in base a
  RC4(Chiave || IV)
- IV viene trasmetto in chiaro, per ogni frame
- La conoscenza della chiave consente Hub equivalent sniffing
- Senza conoscere la chiave è possibile comunque la contraffazione dei frame (manipolando ICV)

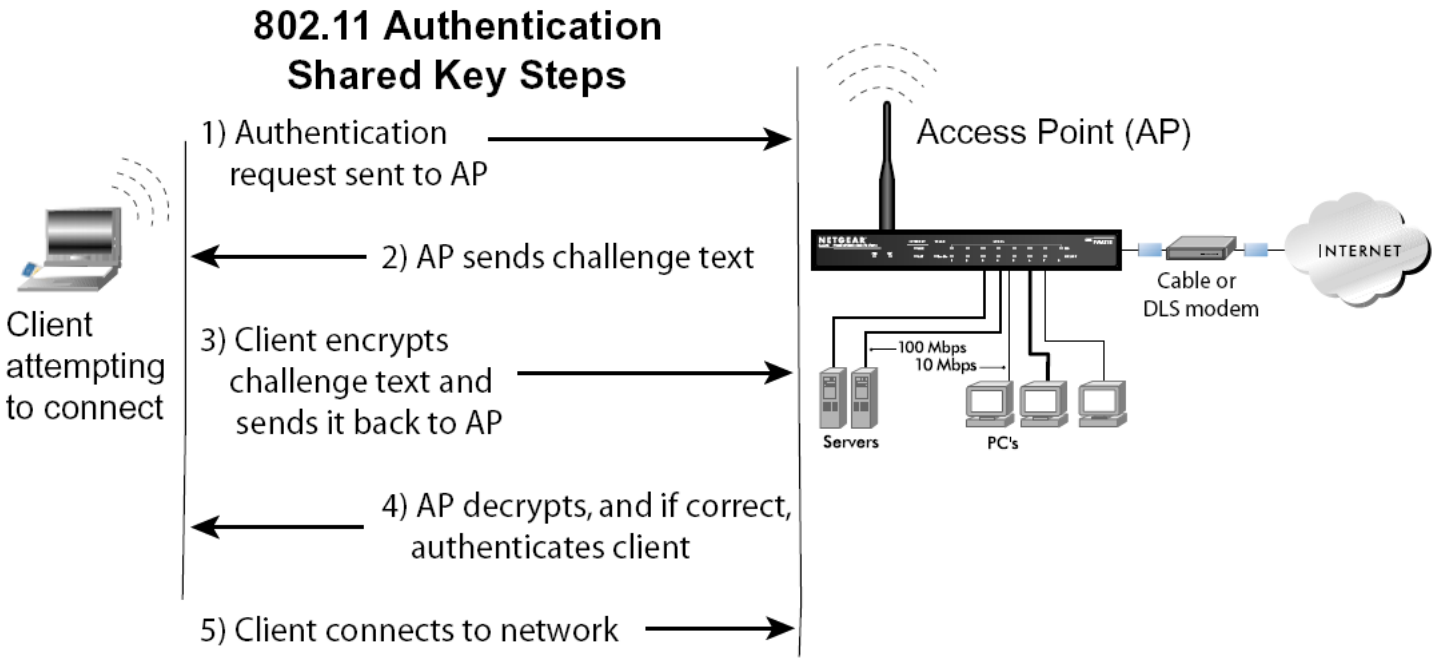
Wep Frame Format



WEP Authentication (open)



WEP Shared key



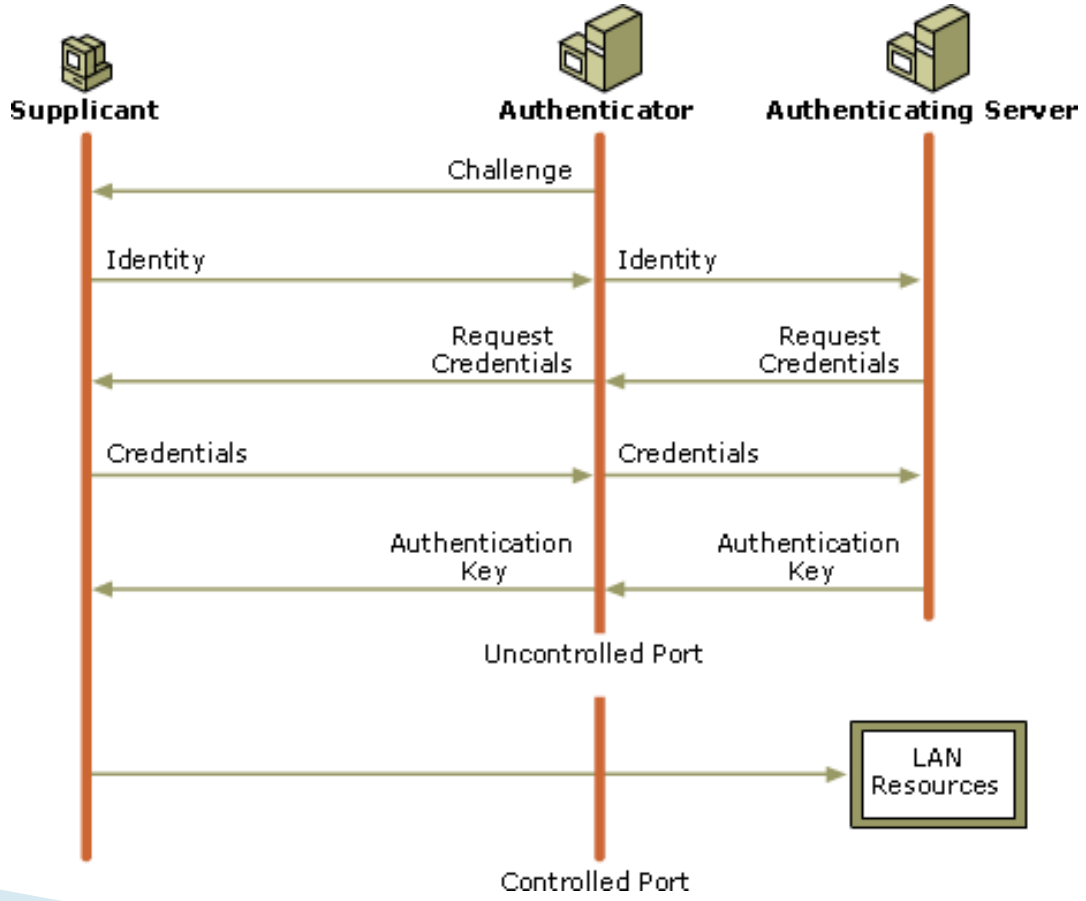
WPA Personal

- A chiave condivisa

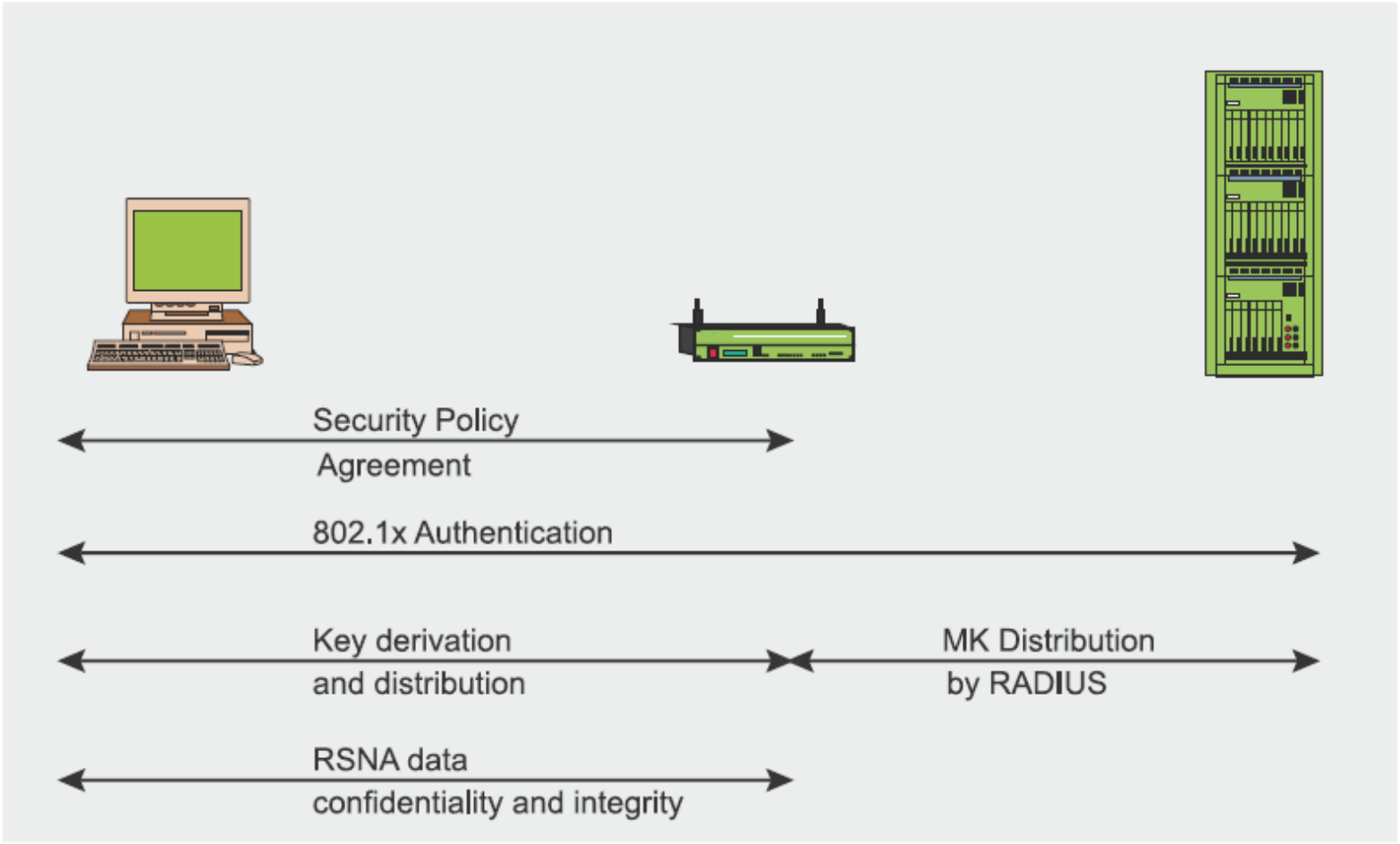
  TKIP: sempre RC4 ma IV più lunghi. Inoltre è stato aggiunto il MIC (Message integrity check)
- WPA2 -> AES e Cipher suite
- Fase di autenticazione (EAPOL based) in cui vengono scambiate PTK e GTK
- La conoscenza della chiave non implica la possibilità di osservare il traffico altrui
- Possibilità di Re-keying periodico

WPA Enterprise

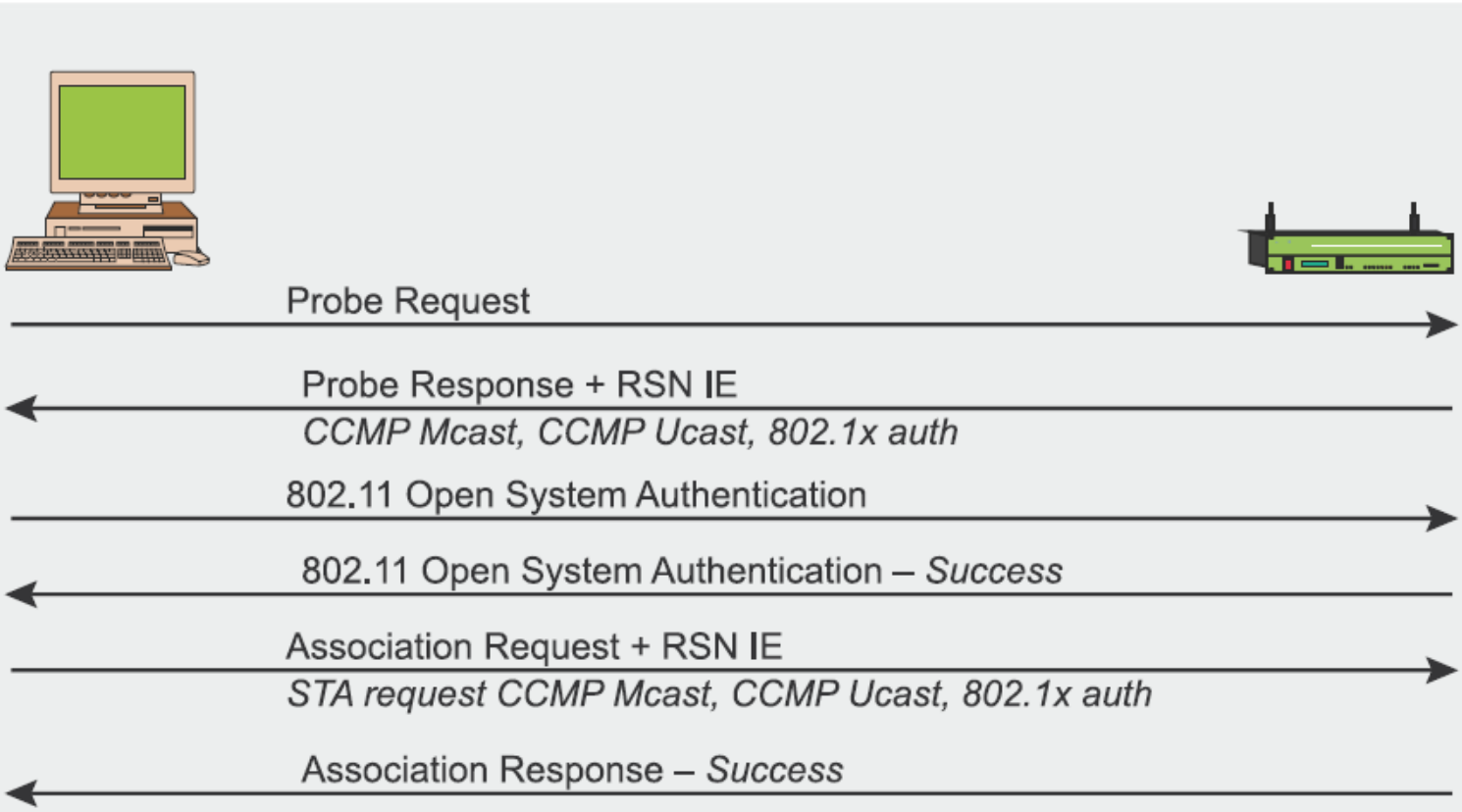
- Autenticazione via server



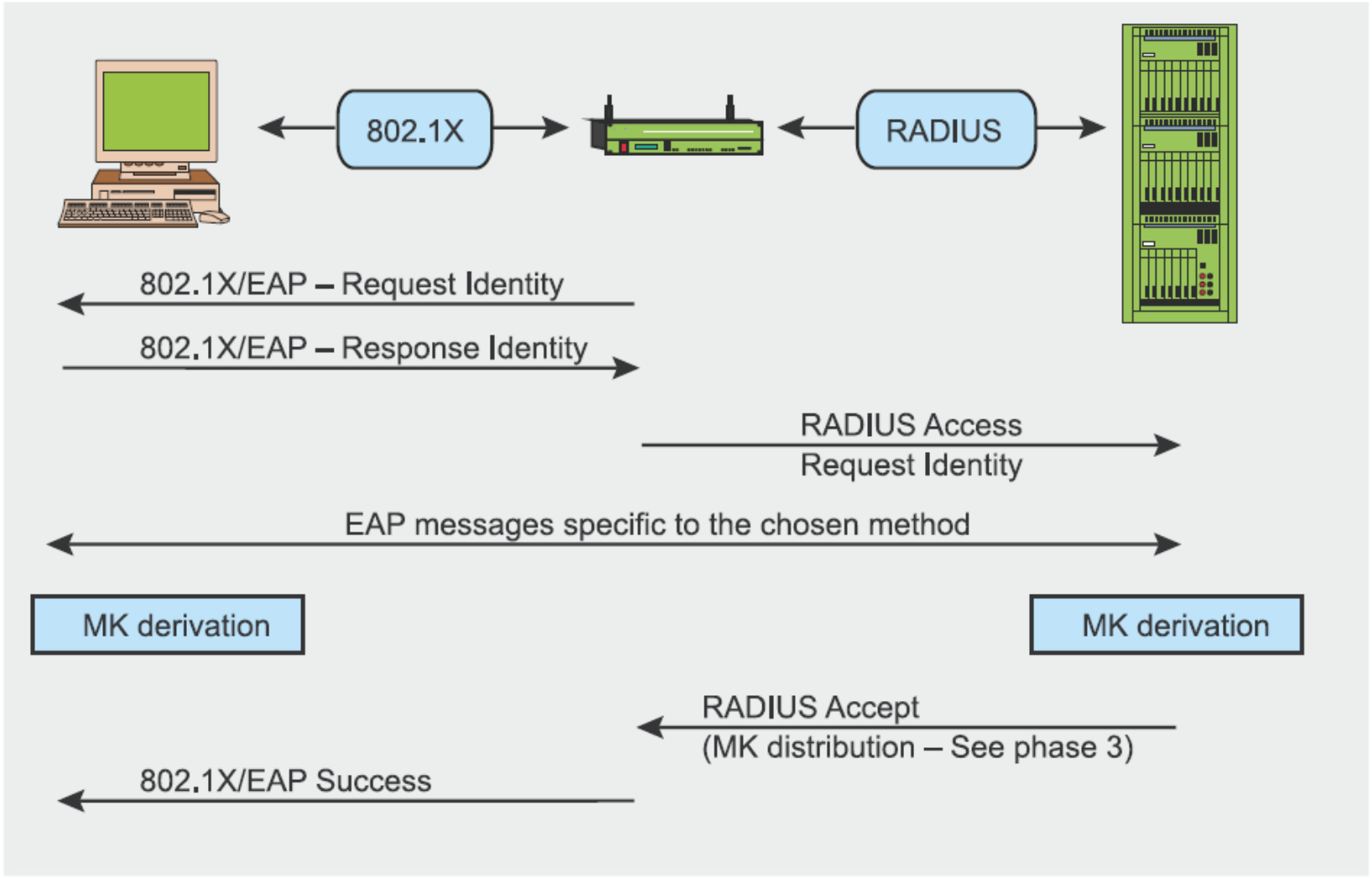
802.1x Authentication steps



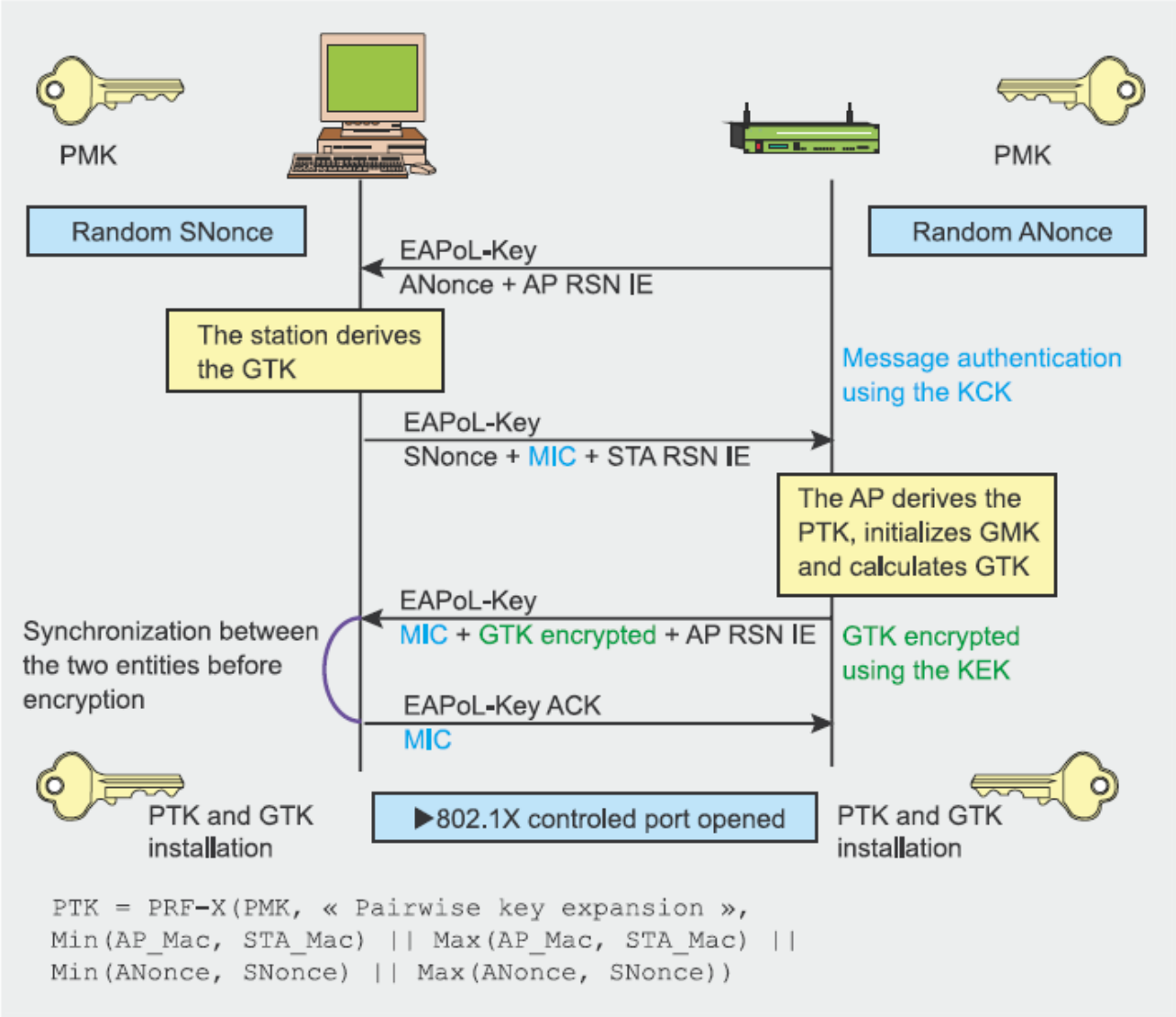
Step 1: pre-auth



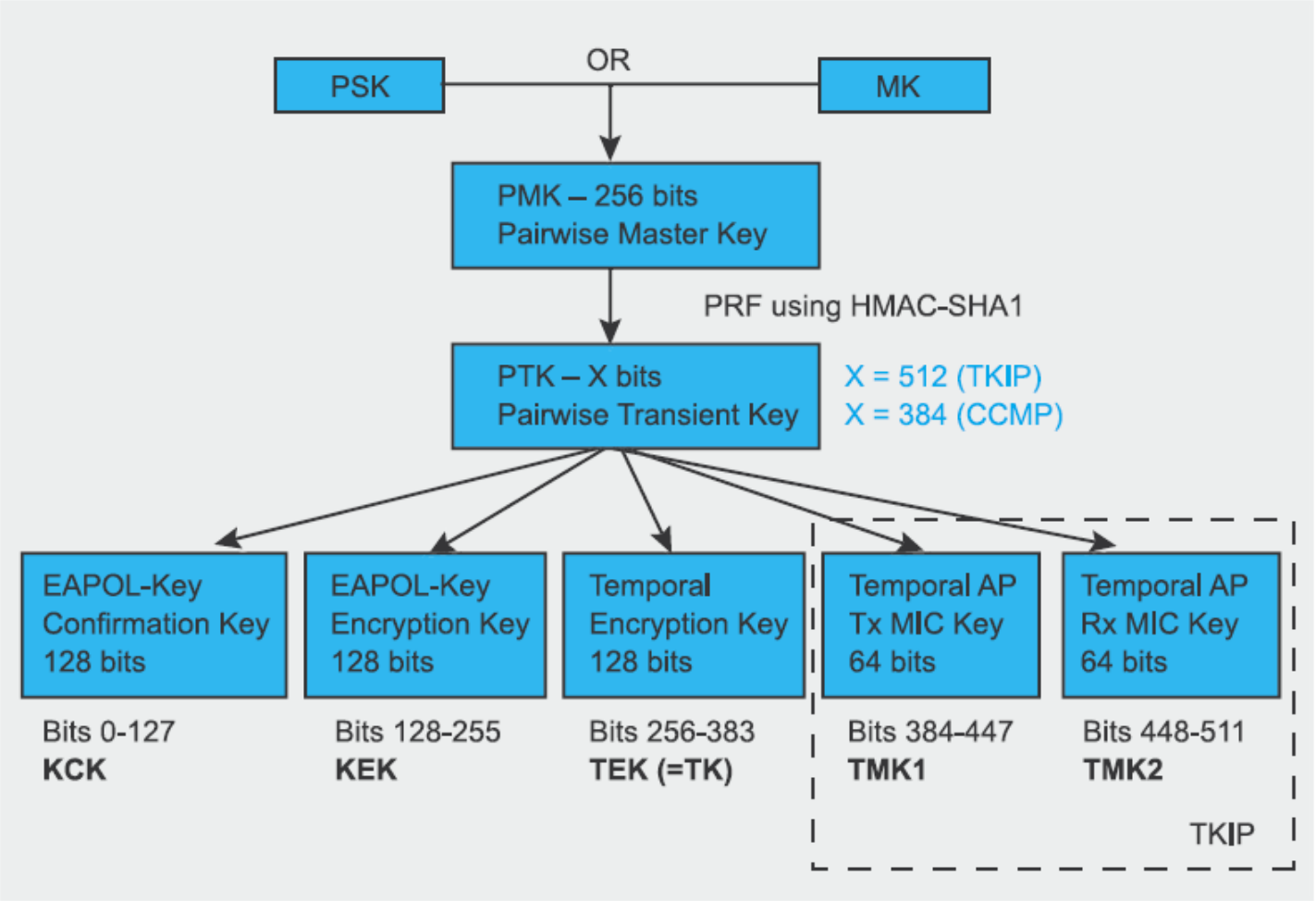
Step 2: Authentication



Step 3: WPA Authorization process



Key hierarchy

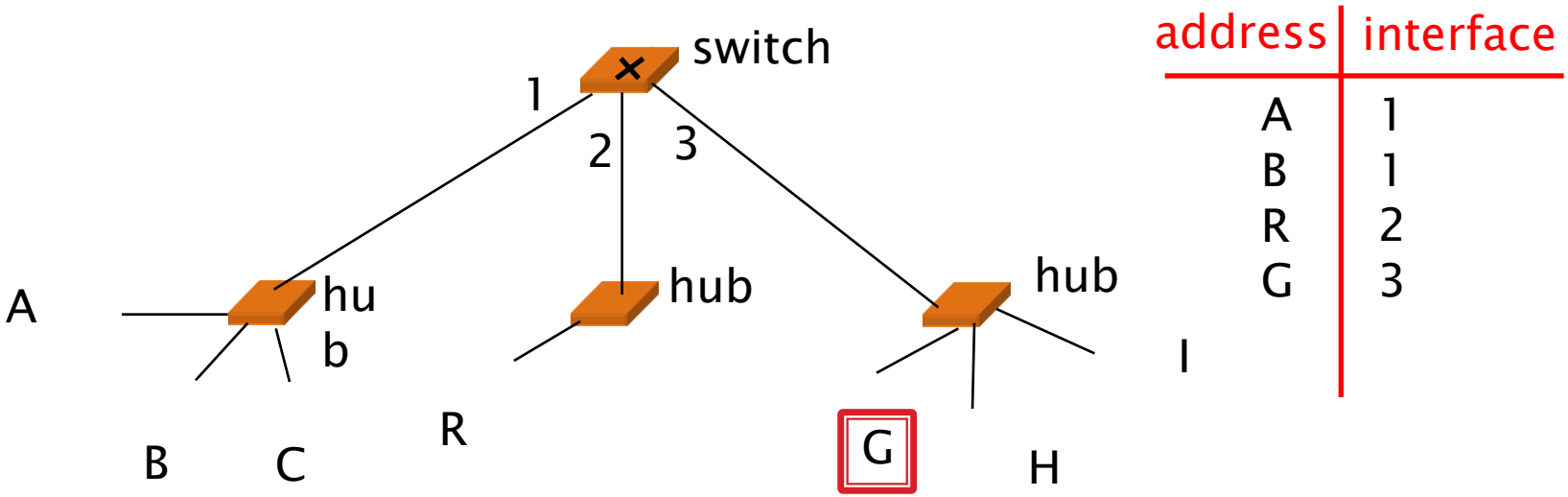


Wired & Wireless

- Wired
  - MAC Spoofing
  - ARP ←→ IP Spoofing
  - DHCP Spoofing
  - Broadcast attacks
- Wireless
  - Open WLANs
  - WEP WLANs
  - WPA & WPA2 WLANs

Port Stealing: Esempio

C manda un frame a R



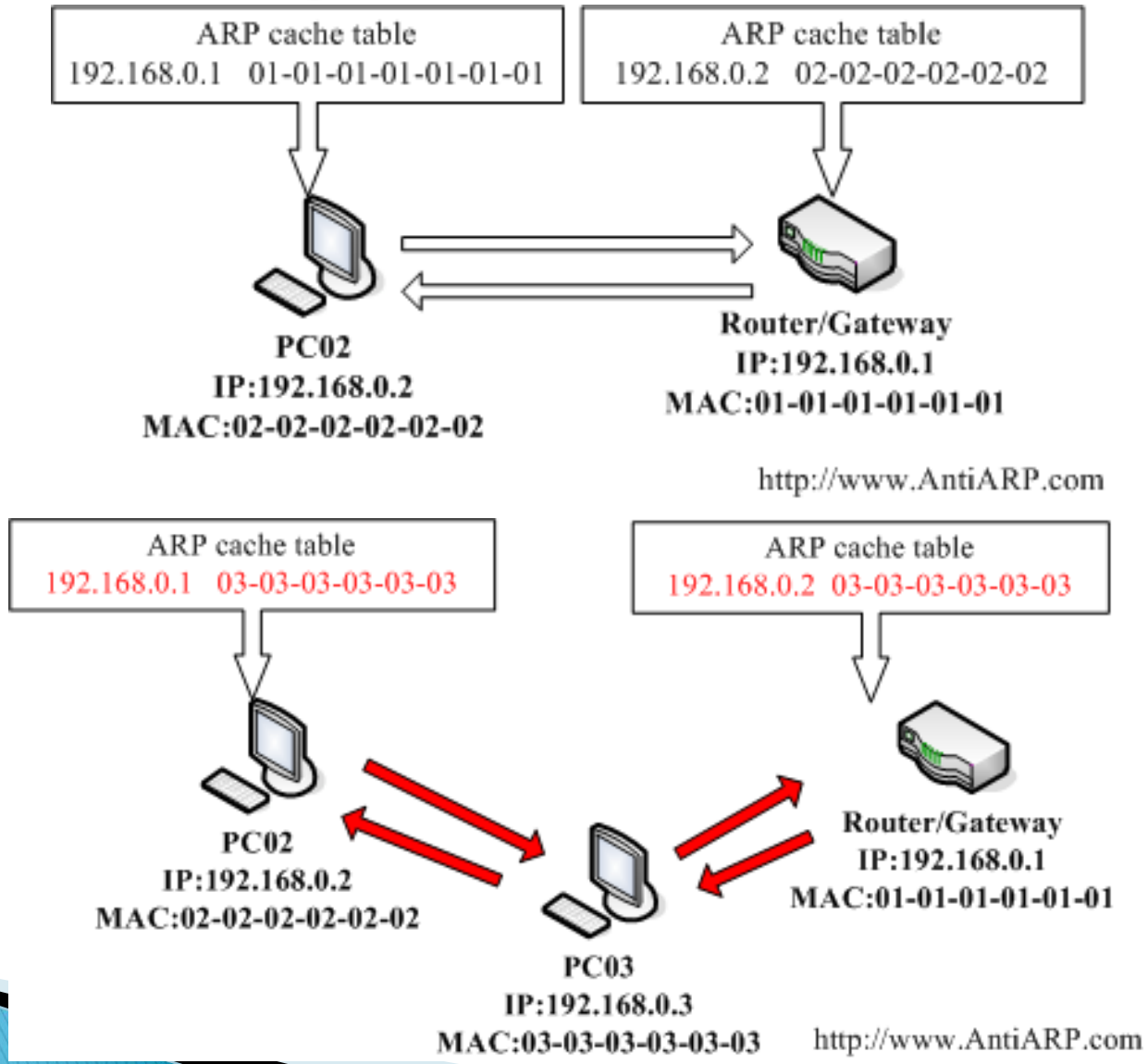
address	interface
A	1
B	1
R	2
G	3

- Un qualsiasi frame originato da G con MAC di R forza un aggiornamento nella switch table
- G cattura i pacchetti destinati a R, li esamina, li filtra, forza R a riaggiornare la tabella e ritrasmette i frame catturati

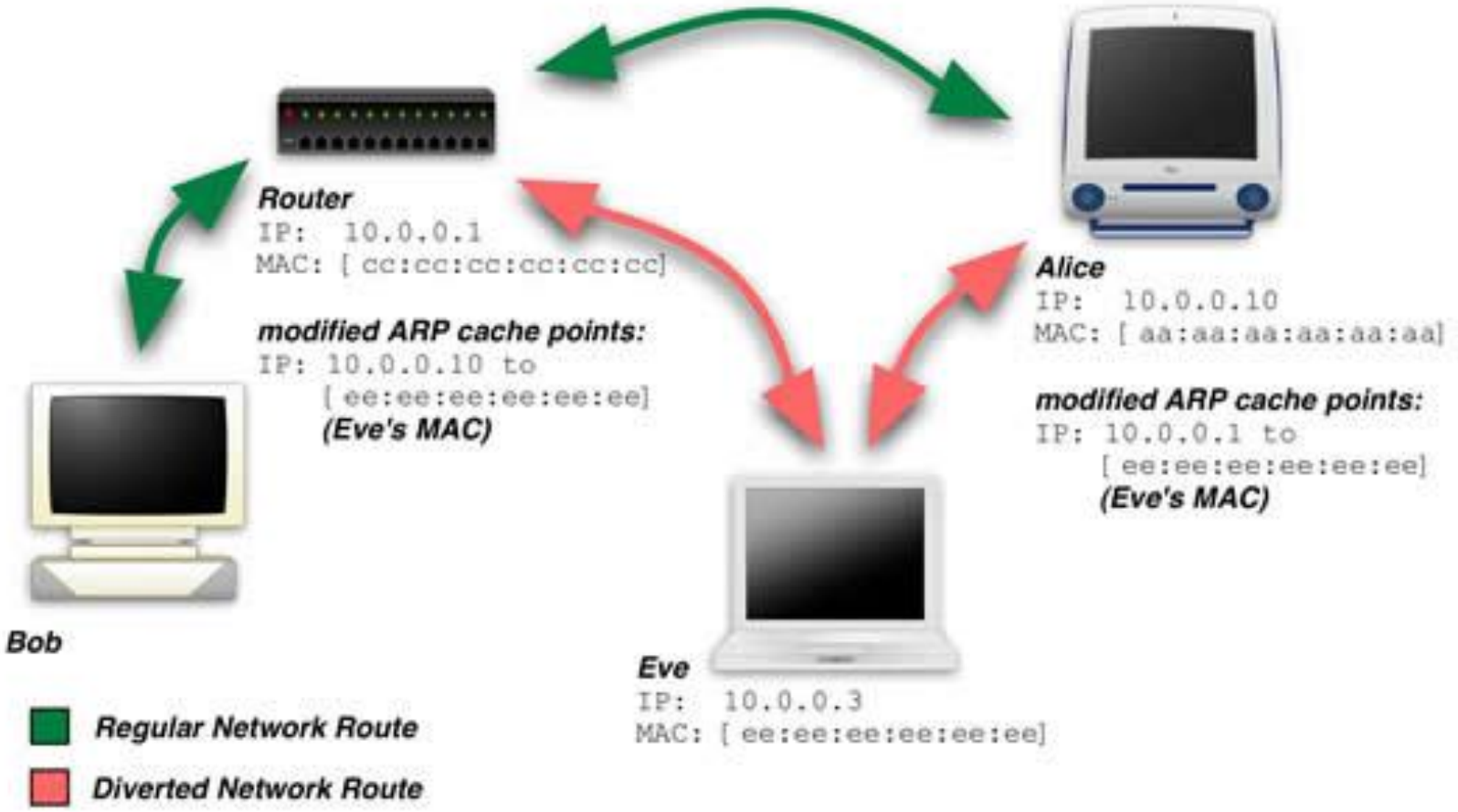
MAC Spoofing / Flooding

- Flooding: inondare lo switch di MAC casuali, fino a saturazione della sua switch table.
- Contromisure: port locking.
- Domande. Cosa succede in una rete con hub? E in una rete WLAN open? WEP? WPA?

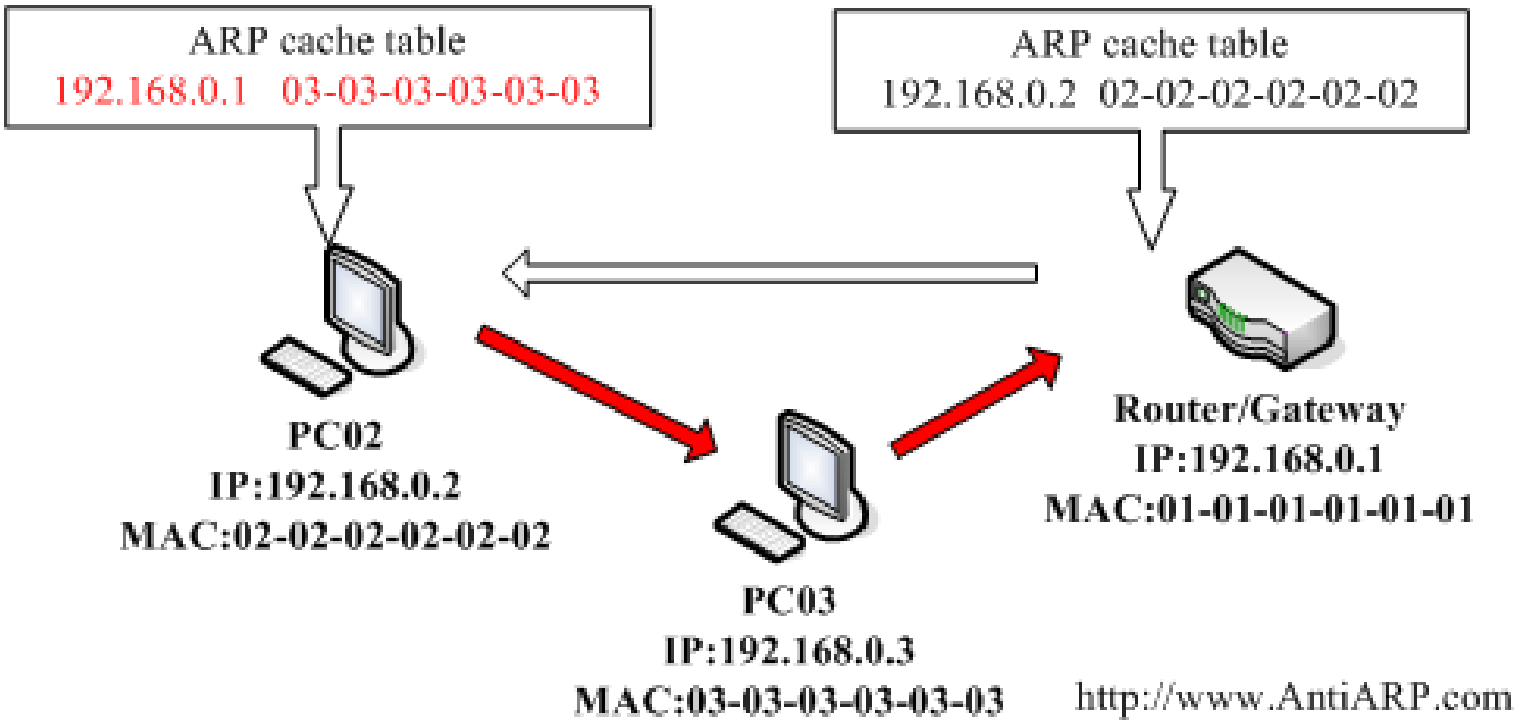
IP Spoofing in LAN



IP Spoofing in LAN



Half mitm


ARP cache table
192.168.0.1 03-03-03-03-03-03
ARP cache table
192.168.0.2 02-02-02-02-02-02
PC02
IP:192.168.0.2
MAC:02-02-02-02-02-02
PC03
IP:192.168.0.3
MAC:03-03-03-03-03-03
Router/Gateway
IP:192.168.0.1
MAC:01-01-01-01-01-01
http://www.AntiARP.com

Contromisure

- ARP Watching
- Tabelle ARP statiche
- ARP Jamming
- IP Sec, Tunnels, VPN, SSH

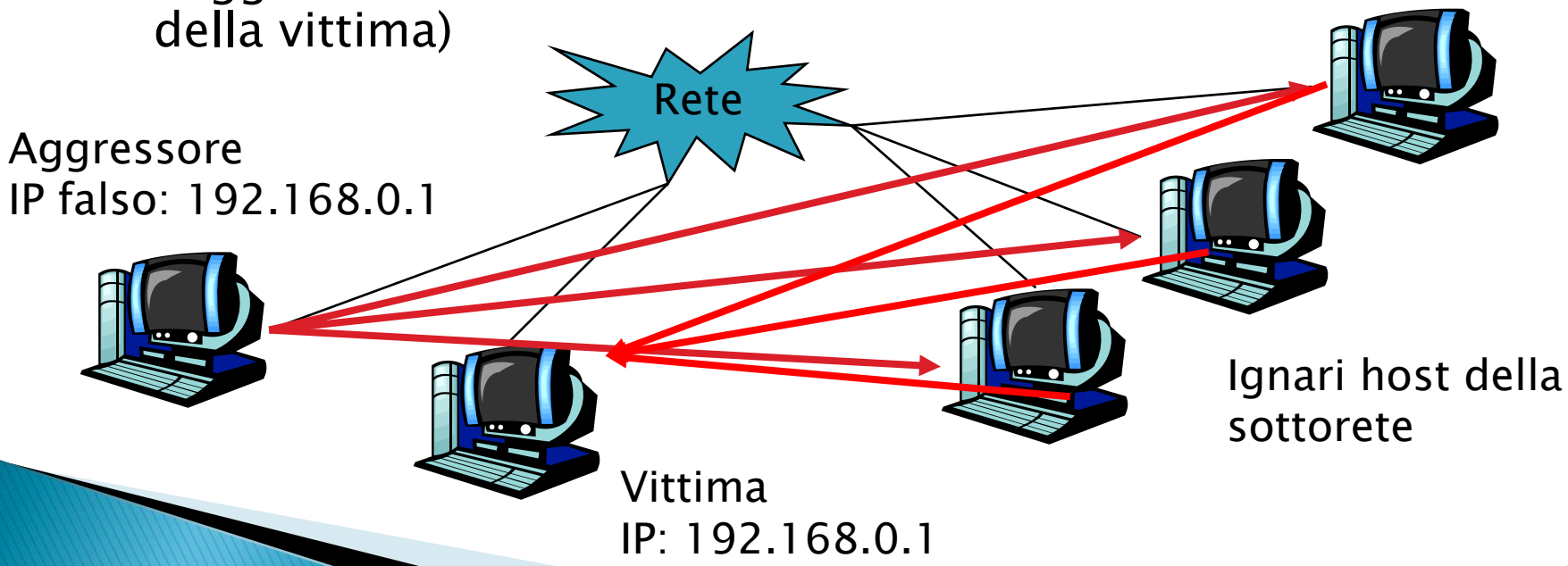
DHCP Spoofing

- Consente Half – MITM
- Bisogna essere presenti all'accensione e cercare di assegnare un indirizzo IP predeterminato, un gateway e un DNS

- Contromisure:
  - Rilevamento di DHCP reply multiple

Attacchi broadcast

- Attacchi broadcast:
  - Fingere di avere l'IP della vittima (IP spoof)
  - Mandare dei ping broadcast a suo nome
  - Le risposte raggiungono la vittima e non l'aggressore
  - Necessità delle condizioni adatte (di solito l'aggressore sta fisicamente nella stessa sottorete della vittima)



Contromisure

- Limitazione ICMP e altri protocolli broadcast su router e host
- Configurazione opportuna firewall

- Limiti dell'IP spoofing fuori LAN