ISACA®
Servire i professionisti dell'IT Governance
Rome Chapter

Wireless Security

Sicurezza, Privacy e Audit delle reti Wireless

Giancarlo Castorina – CISA, CISSP

Giancarlo.Castorina@acm.org

INDICE DELLA PRESENTAZIONE :

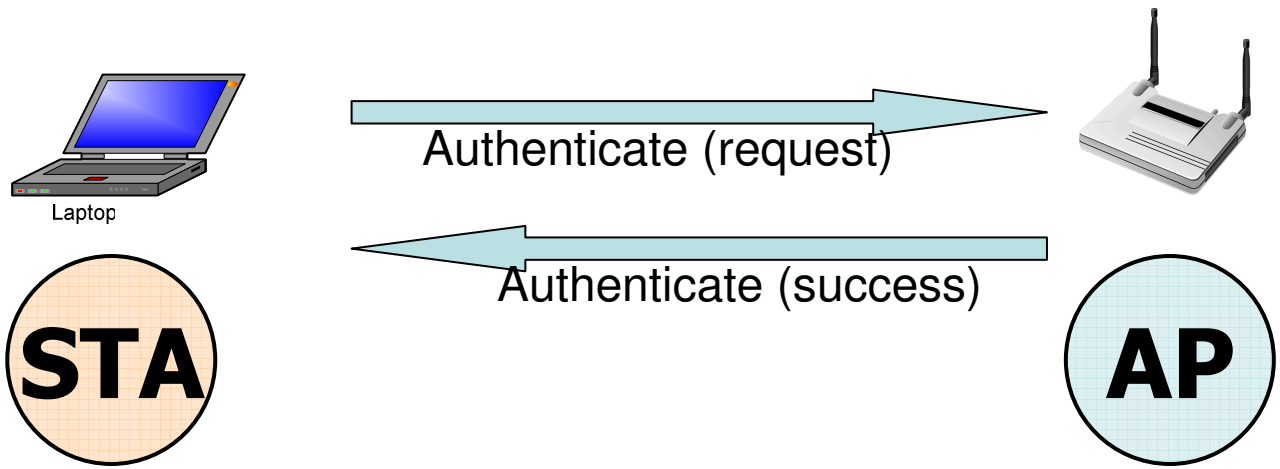
“Autenticazione e privacy” (1999)

ISACA®
Servire i professionisti dell'IT Governance
Rome Chapter

- La prima versione (1999) di IEEE 802.11 prevede due tipologie di autenticazione
  - *Open system*
  - *Shared Key*
- La confidenzialità è affidata al WEP (*Wired Equivalent Protocol*)

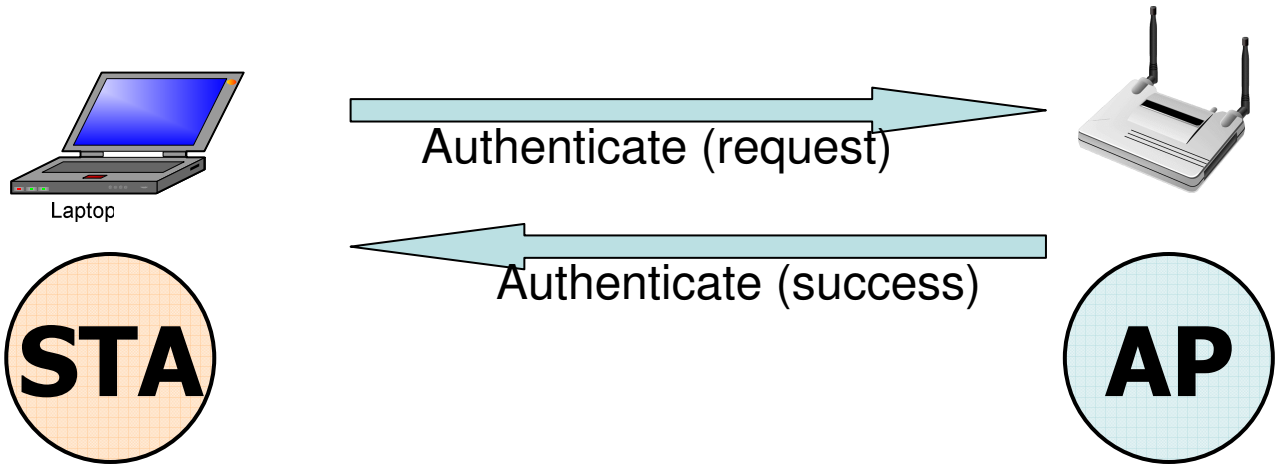
Open system authentication

- **Null** Authentication Algorythm
- **Default** Authentication Algorythm



Open system authentication

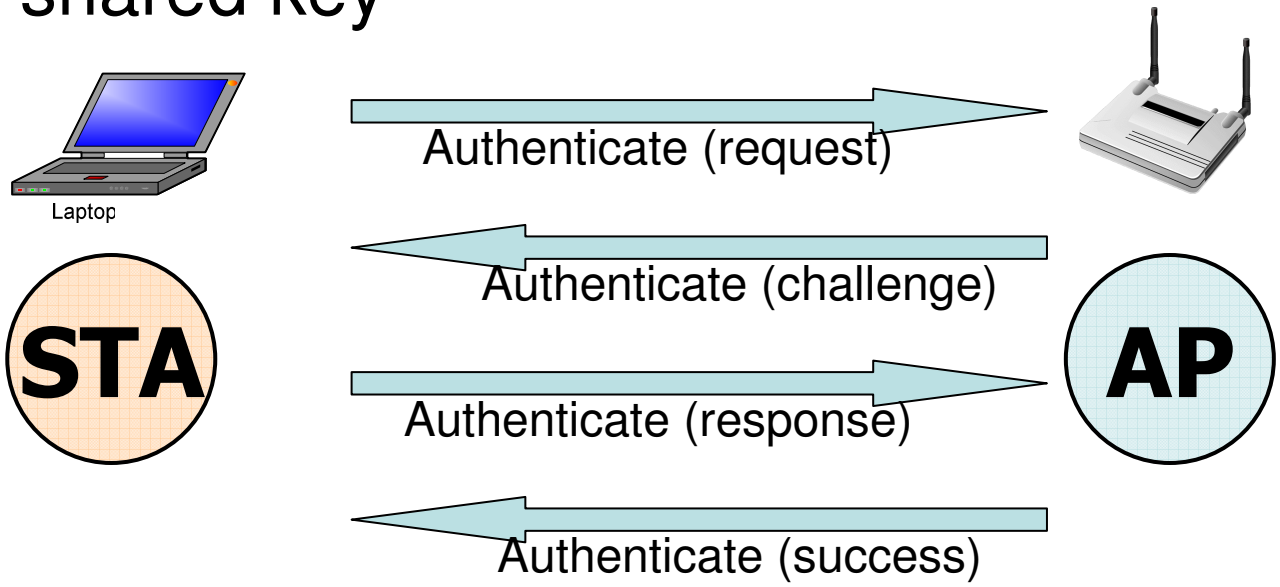
- Possibilità di filtrare in base al MAC Address
- *Nessuna prevenzione di camuffamenti*



Shared Key authentication

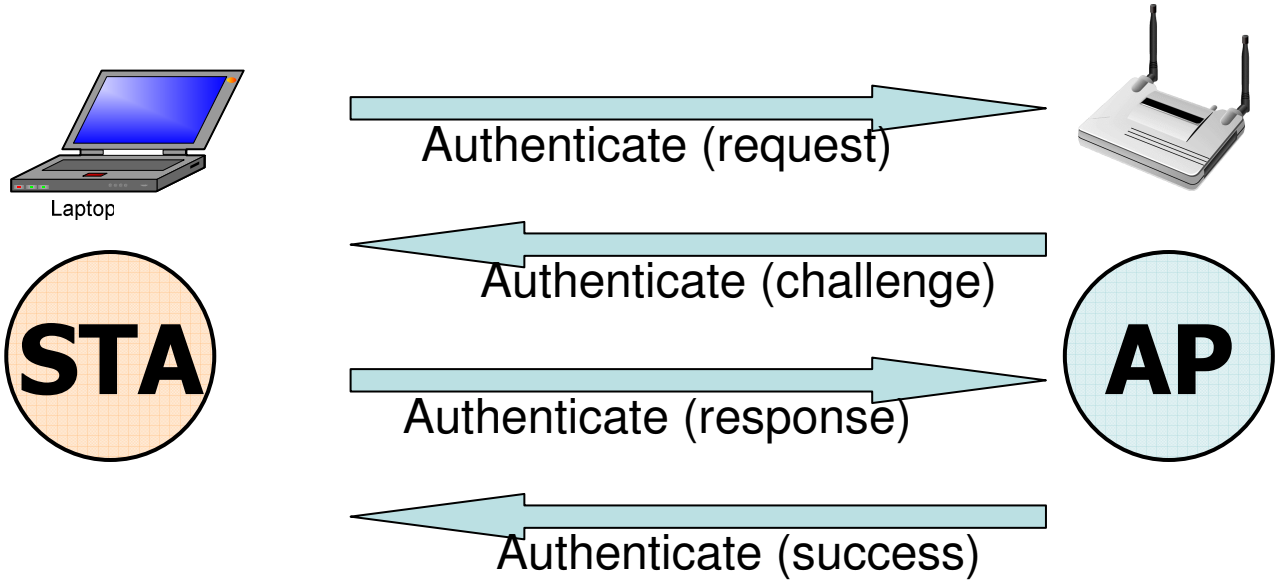
ISACA
Servire i professionisti dell'IT Governance
Rome Chapter

- Challenge: 128 bit random number
- Response: Challenge encrypted using the shared key



Shared Key authentication

- Problemi nella distribuzione della shared key
- Challenge e Response inviati in chiaro
  - Possibile analisi statistica



Autenticazione - Problematiche

ISACA
Servire i professionisti dell'IT Governance
Rome Chapter

- Opzionale
- Non esiste mutua autenticazione
- Mancano meccanismi di verifica dell'autenticità dei messaggi

Wired Equivalent Privacy

ISACA
Servire i professionisti dell'IT Governance
Rome Chapter

- *It is reasonably strong*
- *It is self synchronizing*
- *It is efficient*
- *It may be exportable*
- *It is optional*
  - Fonte: IEEE Std 802.11, 1999 Edition

Wired Equivalent Privacy

ISACA
Servire i professionisti dell'IT Governance
Rome Chapter

- *It is reasonably strong*
- *It is self synchronizing*
- *It is efficient*
- *It may be exportable*
- *It is optional*
  - Fonte: IEEE Std 802.11, 1999 Edition
- *It was broken*
  - Fonte: Real life

WEP – Uso di Chiavi

ISACA
Servire i professionisti dell'IT Governance
Rome Chapter

- Default Keys
  - Ogni dispositivo usa lo stesso set di chiavi (da 1 a 4)
  - *Spesso usata una sola chiave*
- Key Mapping Keys
  - Ogni dispositivo ha un set di chiavi univoco e una chiave “broadcast”
  - *In pratica non utilizzato (poco supportato)*

WEP – Uso di Chiavi - Problemi

ISACA
Servire i professionisti dell'IT Governance
Rome Chapter

- Gestione manuale e onerosa
  - Facilità di errori
  - Raramente le chiavi vengono cambiate
- Condivisione della chiave
- Stessa chiave utilizzata per autenticazione e crittografia

WEP2

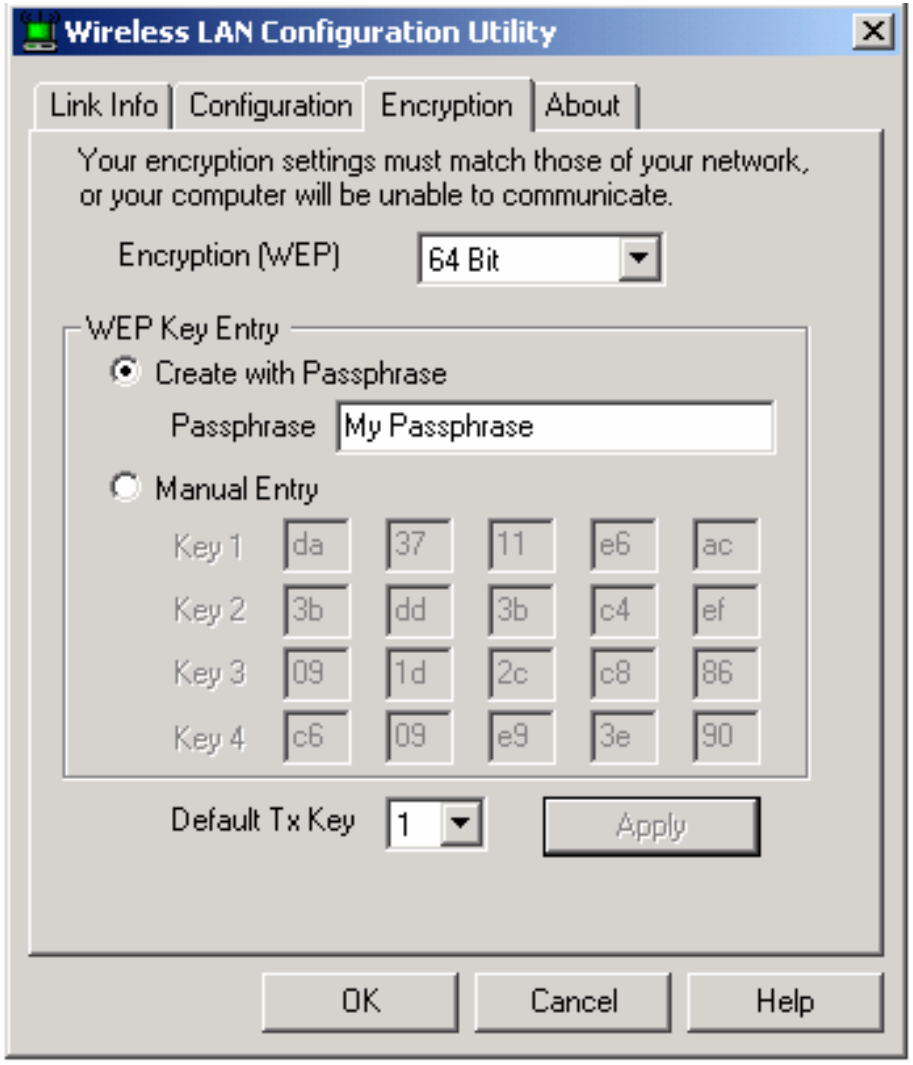
- WEP: Chiavi di 40 bits
- WEP2: Chiavi di 104 bits
- *Non risolve i problemi*

Generatori di chiavi WEP

ISACA®
Servire i professionisti dell'IT Governance
Rome Chapter

- Non standard ma utilizzati
- Derivano chiavi WEP da passphrases
- Riducono lo spazio delle chiavi a 21 bits
- *Favoriscono attacchi a forza bruta*

Key Entry Example



WEP Encryption

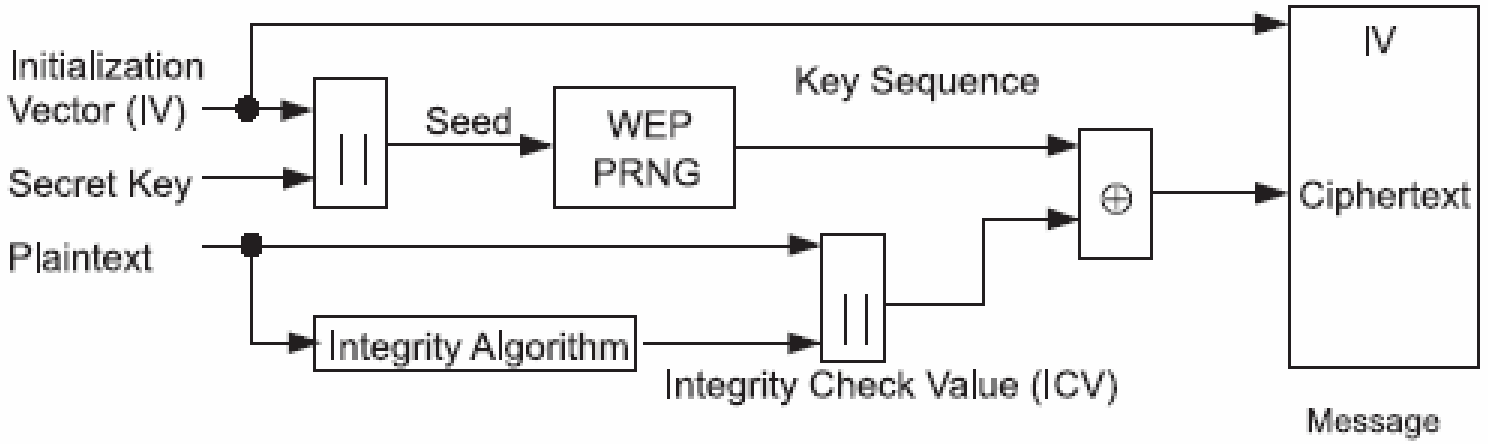


Figure 44—WEP encipherment block diagram

– Fonte: IEEE Std 802.11, 1999 Edition

WEP Decryption

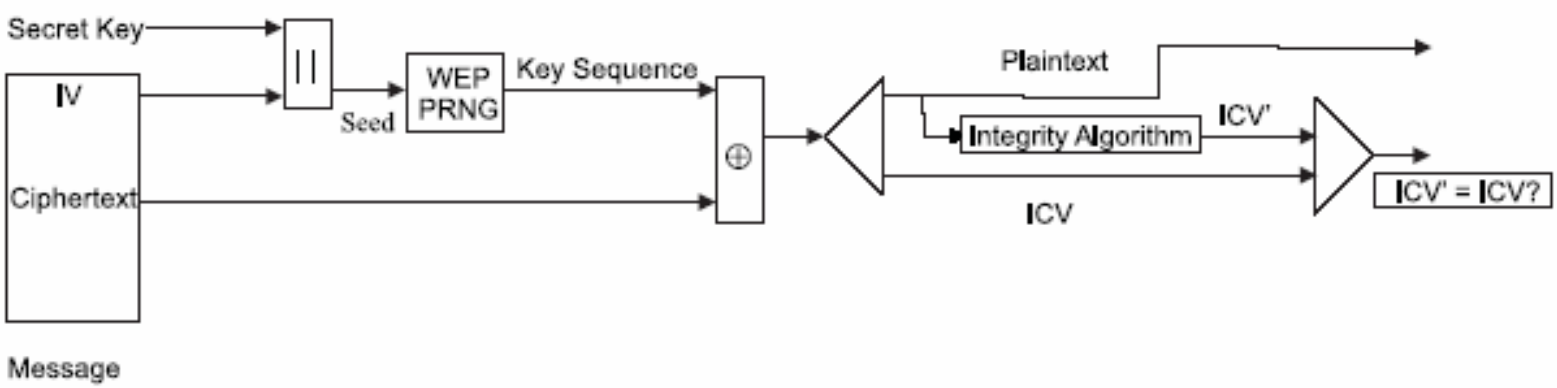


Figure 45—WEP decipherment block diagram

– Fonte: IEEE Std 802.11, 1999 Edition

2000-2001: Il crollo

ISACA
Servire i professionisti dell'IT Governance
Rome Chapter

- Walker, J. 2000. Unsafe at any key size; an analysis of the WEP encapsulation.
  - IEEE 802.11-00/362
- Arbaugh, W.A. May 2001. An inductive chosen plaintext attack against WEP/WEP2
  - www.cs.umd.edu/waa/wepwep2-attack.html
- Borisov, N.I. et al 2001. Intercepting mobile communications: the insecurity of 802.11
  - 7th ACM Conference on Mobile Computing and Networking
- Newsham, T. 2001. Cracking WEP Keys
  - http://lava.net/~newsham/wlan/WEP_password_cracker.pdf

Le debolezze WEP

ISACA
Servire i professionisti dell'IT Governance
Rome Chapter

- E' possibile autenticarsi senza conoscere la chiave
  - Si possono trarre informazioni utili per conoscere la chiave
  - *L'autenticazione è controproducente*
- Assenza di Access Control
  - Possibile (*ma aggirabile*) in base al MAC address

Le debolezze WEP

ISACA
Servire i professionisti dell'IT Governance
Rome Chapter

- Assenza di protezione dal replay di messaggi
- Meccanismi deboli di controllo dell'integrità dei messaggi
- Debolezze nell'uso di RC4
  - Short IV values (24 bits) – la frequenza di reutilizzazione rende IV quasi inutile
  - Alcuni IVs non si adattano a RC4
  - La concatenazione di IV e chiave rende possibile un attacco diretto alla chiave RC4

WEP: unsafe at any key size

ISACA
Servire i professionisti dell'IT Governance
Rome Chapter

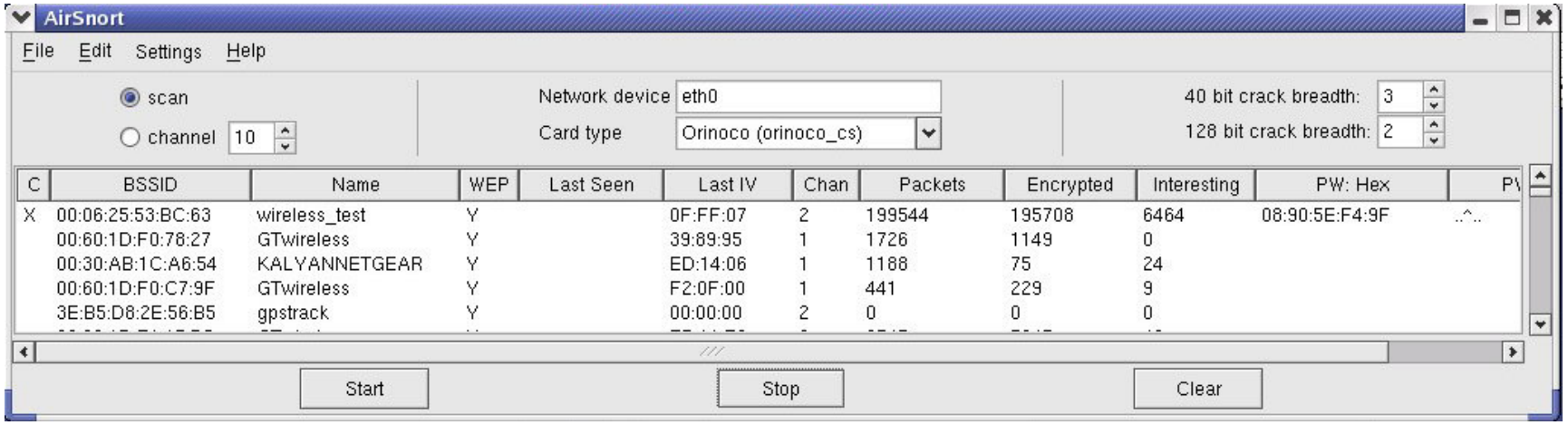
- "…WEP incapsulation remains insecure whether its key length is 1 bit or 1000 or any other size whatsoever, and the same remains true when any other stream cipher replaces RC4. The weakness stems from WEP's usage of its initialization vector. This vulnerability prevents the WEP encapsulation from providing a meaningful notion of privacy at any key size."
- *Jesse Walker (Intel) – IEEE P802.11-00/362*

Dalla teoria alla pratica …

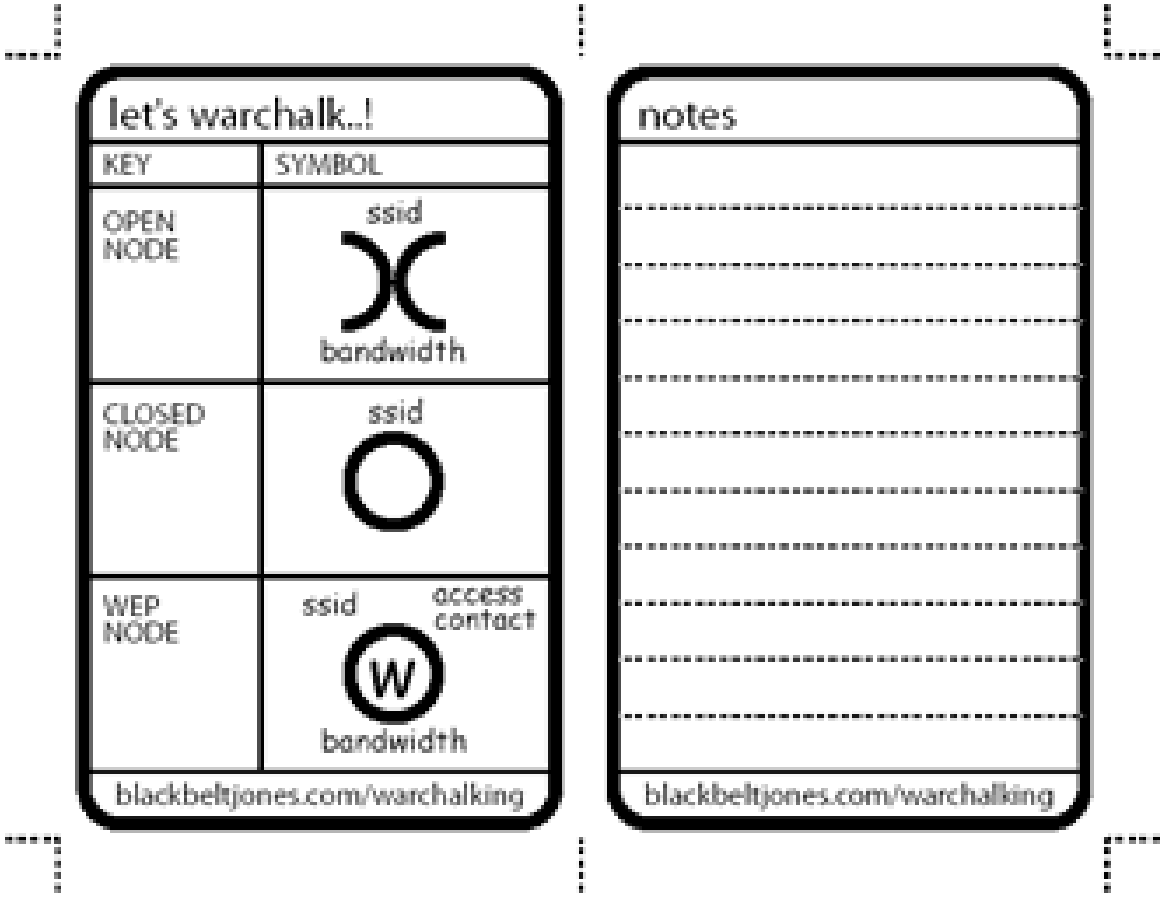
ISACA
Servire i professionisti dell'IT Governance
Rome Chapter

- Svariati WEP cracker sono stati sviluppati combinando strumenti di rilevazione della rete, di collezione del traffico e di analisi dei pacchetti 802.11
- *WAR driving*

Dalla teoria alla pratica …



Wardriving


let's warchalk..!
KEY
SYMBOL
OPEN NODE
ssid
bandwidth
CLOSED NODE
ssid
WEP NODE
ssid
access contact
W
bandwidth
blackbeltjones.com/warchalking
notes
blackbeltjones.com/warchalking

Contromisure

ISACA
Servire i professionisti dell'IT Governance
Rome Chapter

- Utilizzo combinato di altre tecnologie per proteggere autenticazione e confidenzialità
  - *IPSec*
  - *VPN*
- Sistemi non adatti ad un uso “pubblico” (Hot Spot)

IEEE 802.11i
Il Wireless “robusto”

ISACA®
Servire i professionisti dell'IT Governance
Rome Chapter

- Modifica dello standard IEEE 802.11 relativo a “Security Enhancements”
- Introduce “Robust Security Network” (RSN) con nuovi requisiti e funzionalità
- Prevede la possibilità di coesistenza con WEP (“Transitional Security Network” - TSN)

IEEE 802.11i
Nuove funzionalità

ISACA®
Servire i professionisti dell'IT Governance
Rome Chapter

- Autenticazione tramite 802.1X e EAP
- Nuovi protocolli crittografici (AES, TKIP)
- Nuova gestione delle chiavi
- Riguarda sia reti *infrastructure mode* che connessioni *ad-hoc mode*

WPA – Wi-Fi Protected Access

ISACA
Servire i professionisti dell'IT Governance
Rome Chapter

- Subset di IEEE 802.11i
- Certificazione di compatibilità rilasciata da Wi-Fi Alliance (Aprile 2003)
- Supporta TKIP (e non AES)
- Permette la transizione da WEP a RSN
- Non riguarda connessioni *ad-hoc mode*

WPA – Wi-Fi Protected Access

ISACA
Servire i professionisti dell'IT Governance
Rome Chapter

- *Due versioni, a seconda dei meccanismi di autenticazione:*
  - *WPA-Personal (pre-shared key - PSK)*
  - *WPA-Enterprise (authentication server - 802.1X)*

WEP vs WPA

ISACA
Servire i professionisti dell'IT Governance
Rome Chapter

WEP v. WPA

	WEP	WPA
Encryption	Flawed, cracked by scientists and hackers	Fixes all WEP flaws
	40-bit keys	128-bit keys
	Static – same key used by everyone on the network	Dynamic session keys. Per user, per session, per packet keys
	Manual distribution of keys – hand typed into each device	Automatic distribution of keys
Authentication	Flawed, used WEP key itself for authentication	Strong user authentication, utilizing 802.1X and EAP

WPA – Q&A

ISACA
Servire i professionisti dell'IT Governance
Rome Chapter

- *Q: Will products that support Wi-Fi Protected Access ship with it turned on or off as the default?*
- *A: Initially, the Wi-Fi Alliance will allow vendors the option to ship with Wi-Fi Protected Access turned on or off.*

WPA – Q&A

ISACA
Servire i professionisti dell'IT Governance
Rome Chapter

- ***Access Points will require a software upgrade. Clients will require a software upgrade*** *for the network interface card, and possibly a software update for the operating system.*
- *For enterprise networks, an authentication server, typically one that supports RADIUS and the selected EAP authentication protocol, will be added to the network.*

Wi Fi ALLIANCE

WPA2
Wi-Fi Protected Access 2

ISACA
Servire i professionisti dell'IT Governance
Rome Chapter

- Full set degli elementi obbligatori di IEEE 802.11i (supporta AES)
- Certificazione di compatibilità rilasciata da Wi-Fi Alliance (Settembre 2004)
- *Due versioni, a seconda dei meccanismi di autenticazione:*
  - *WPA2-Personal (pre-shared key - PSK)*
  - *WPA2-Enterprise (authentication server - 802.1X)*

WPA2 – Q&A

ISACA®
Servire i professionisti dell'IT Governance
Rome Chapter

- Some WPA products may be able to be upgraded to WPA2 by software. Others may require a hardware change due to the computationally intensive nature of WPA2's required AES encryption.

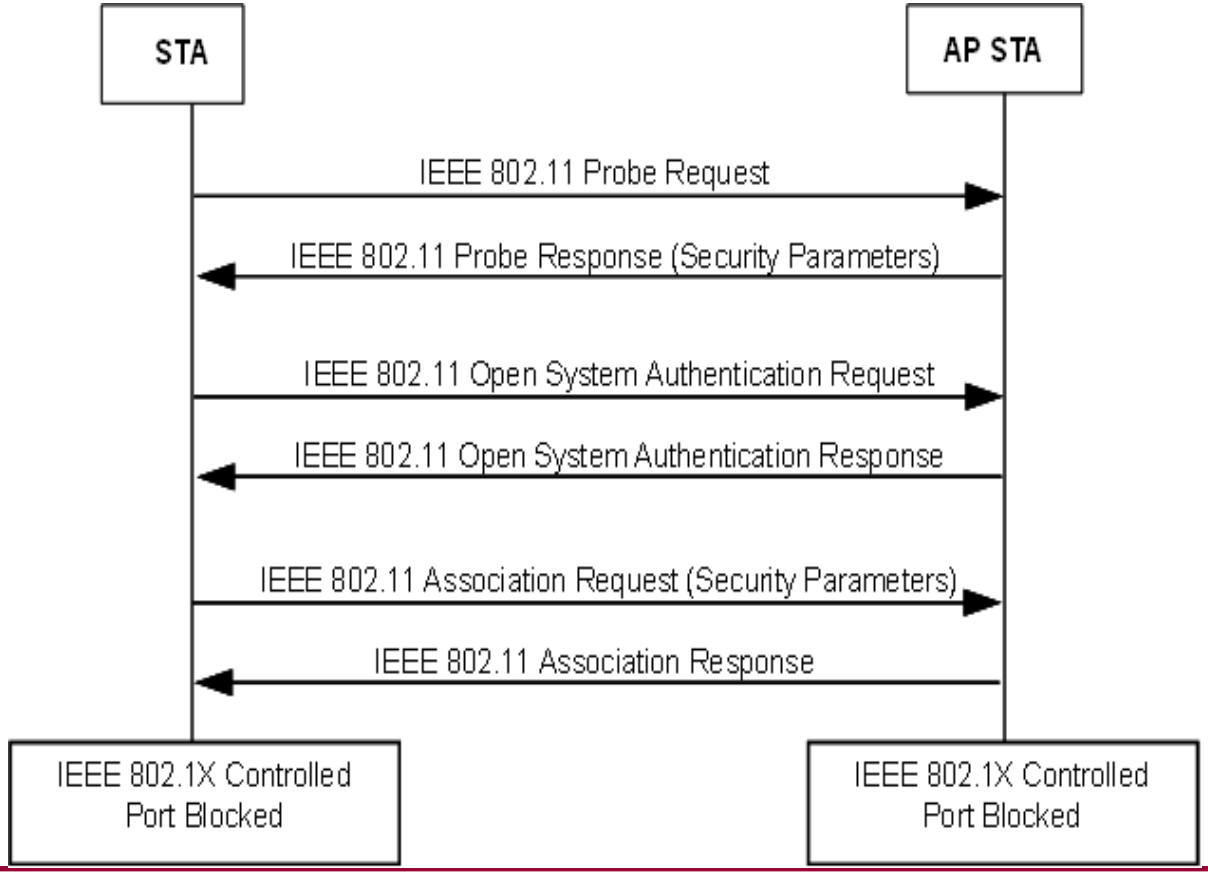
Modelli 802.11i

ISACA
Servire i professionisti dell'IT Governance
Rome Chapter

- Infrastructure mode – Authentication Server (WPA2-Enterprise)
- *Infrastructure mode – Pre-shared Key (WPA2-Personal)*

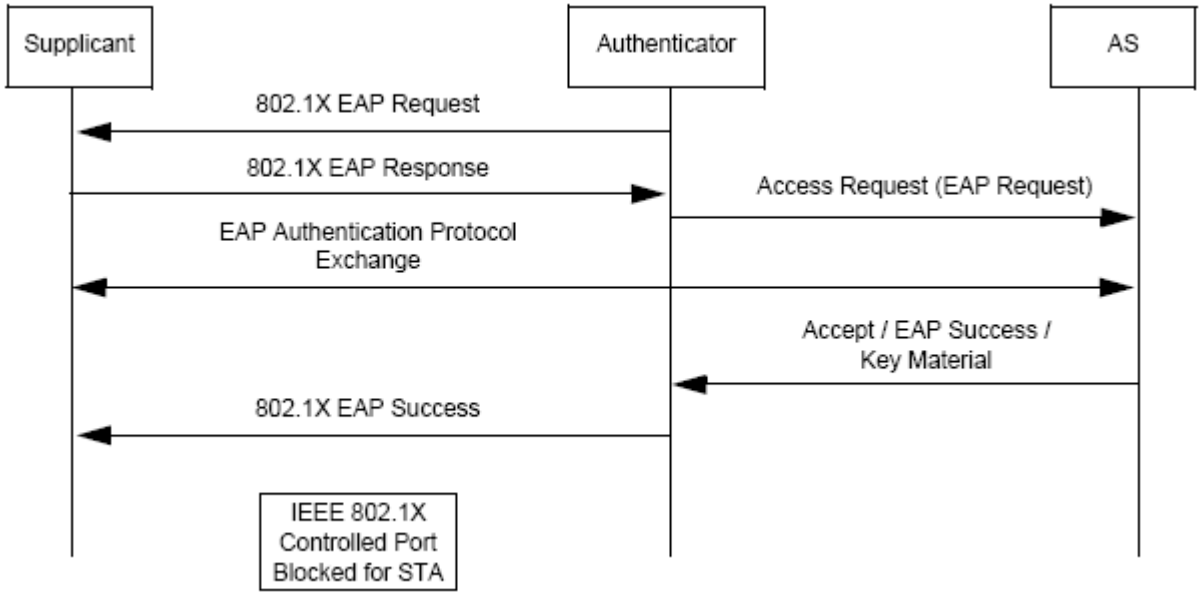
WPA/WPA2-Enterprise (1)

- *Associazione IEEE 802.11*

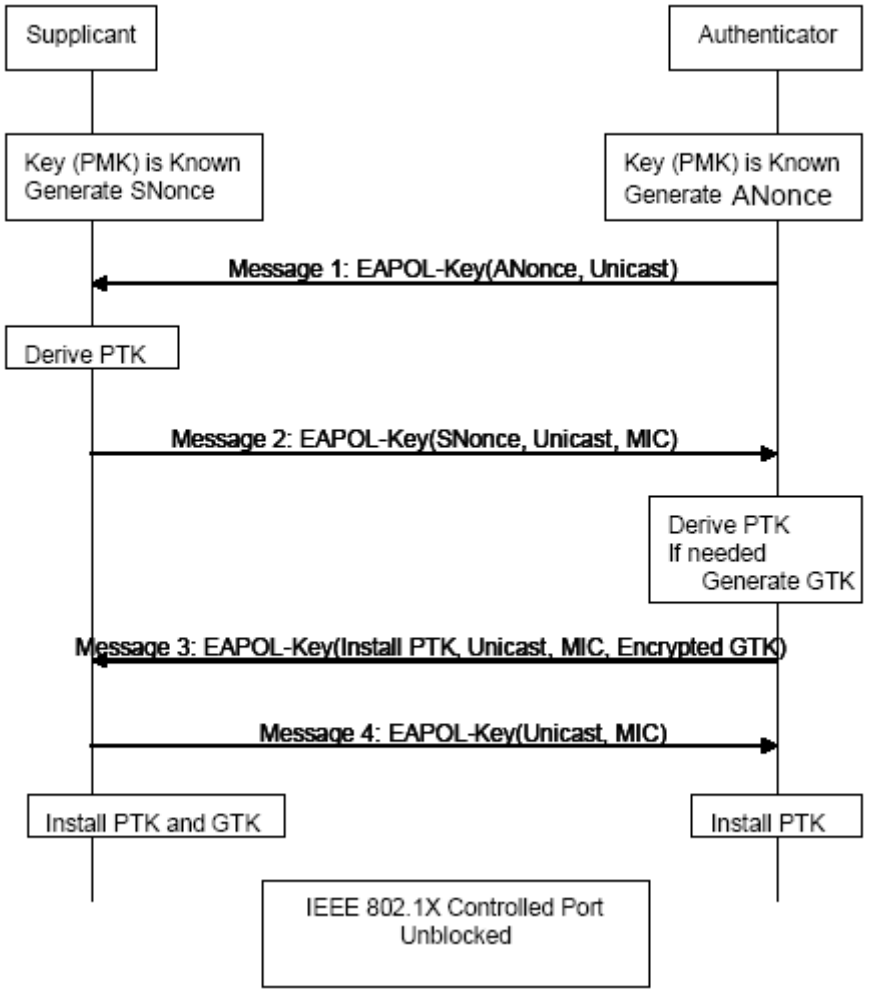


WPA/WPA2-Enterprise (2)

- *Autenticazione IEEE 802.1X EAP*
  - *(WPA/WPA2-Personal: n/a)*



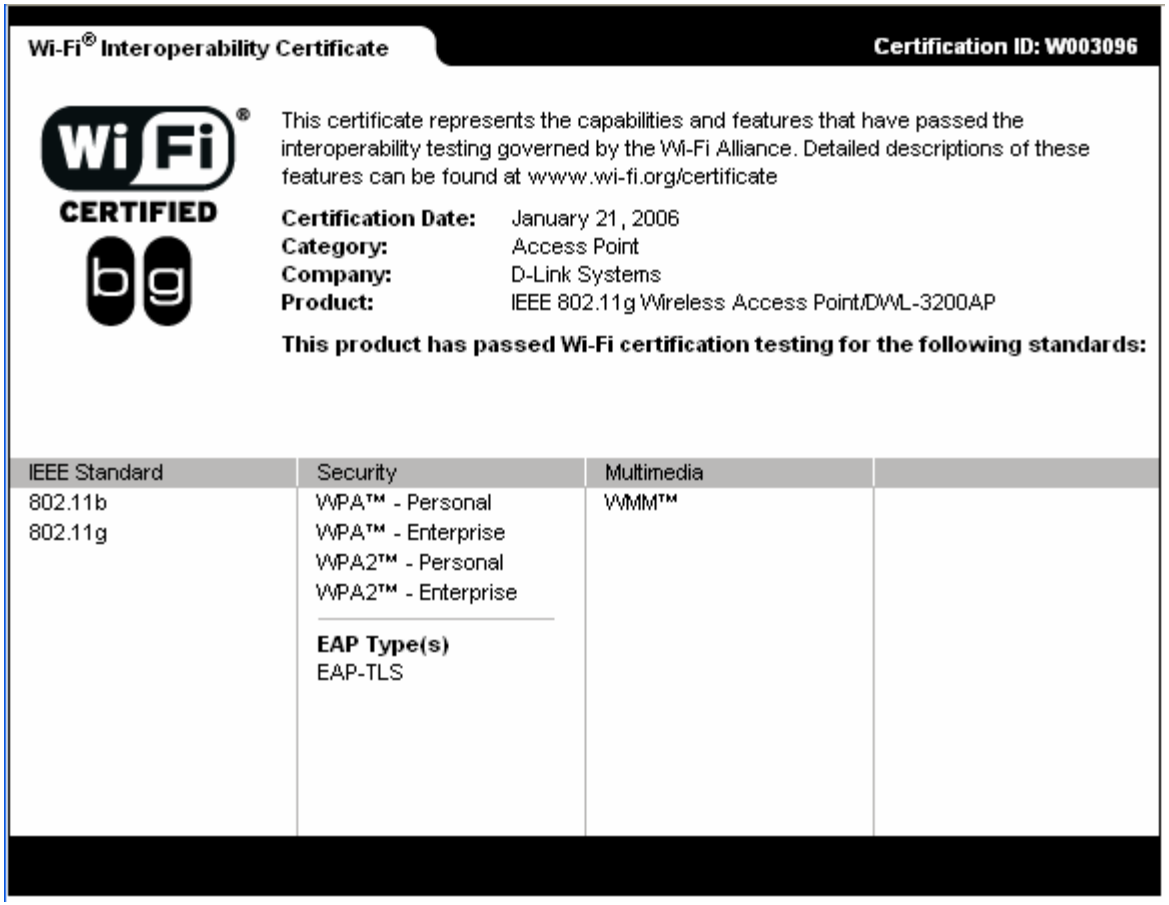
WPA/WPA2-Enterprise (3)



- *Scambio di chiavi*
  - *(WPA/WPA2-Personal: PMK=PSK)*

Certificazioni WPA/WPA2

ISACA
Servire i professionisti dell'IT Governance
Rome Chapter



Transizione a WPA

ISACA
Servire i professionisti dell'IT Governance
Rome Chapter

- *Infrastruttura 802.1X*
  - *Scelta dei protocolli EAP (client e server)*
  - *Scelta di un server (RADIUS)*
  - *Upgrade di AP certificati WPA*
  - *Upgrade di client (schede, driver o sistemi) certificati WPA*
- *Abbandonare al più presto connessioni WEP*
- *Soluzioni VPN possono coesistere*

Wi Fi ALLIANCE

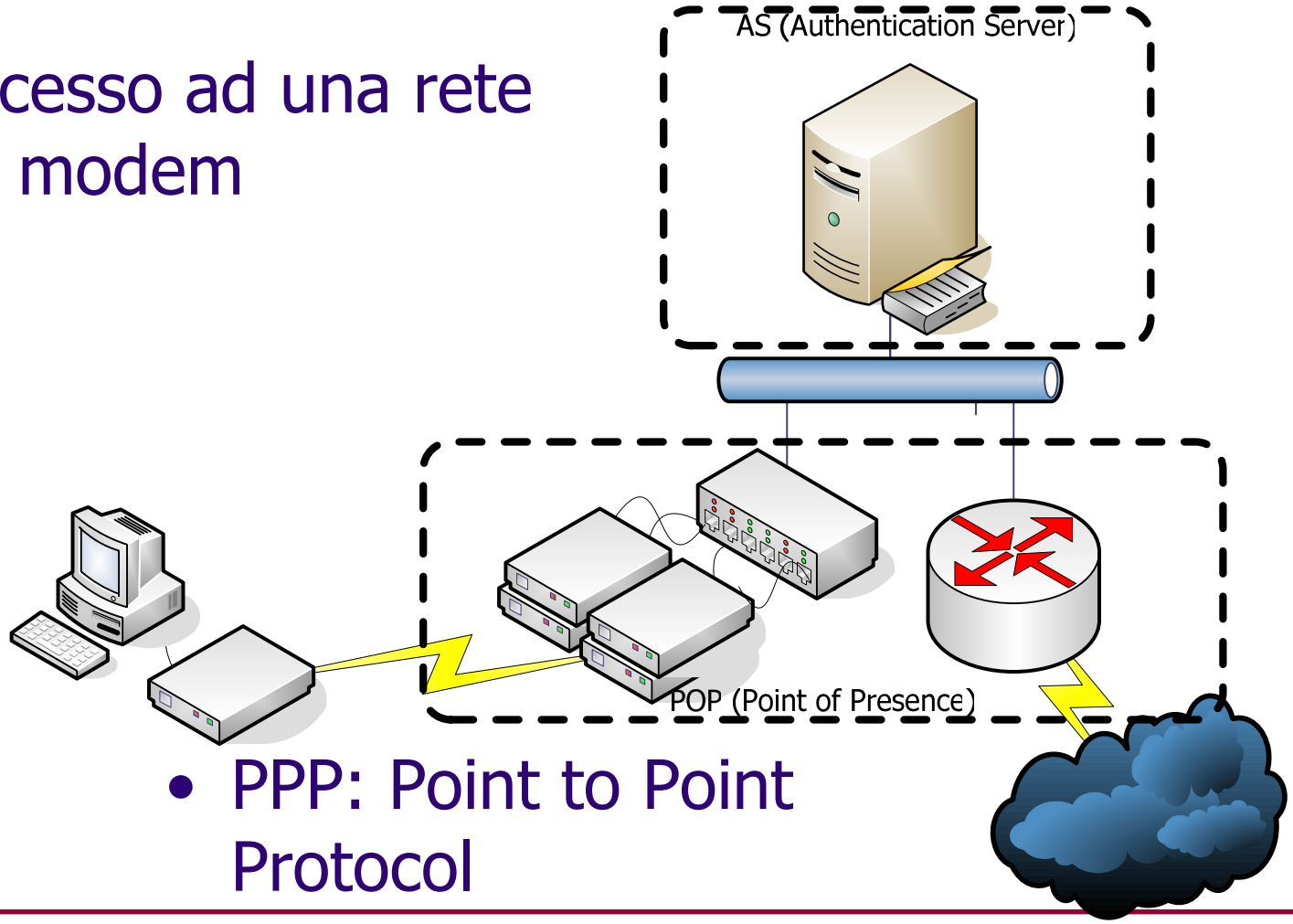
Problematiche di accesso a reti

ISACA
Servire i professionisti dell'IT Governance
Rome Chapter

- Identificazione ed autenticazione degli utenti
- Centralizzazione dell'autenticazione
- Facilità d'uso per gli utenti
- Facilità di gestione dell'infrastruttura
- Possibilità di integrare "guests"
- Flessibilità nei meccanismi di autenticazione

Dial-Up networks

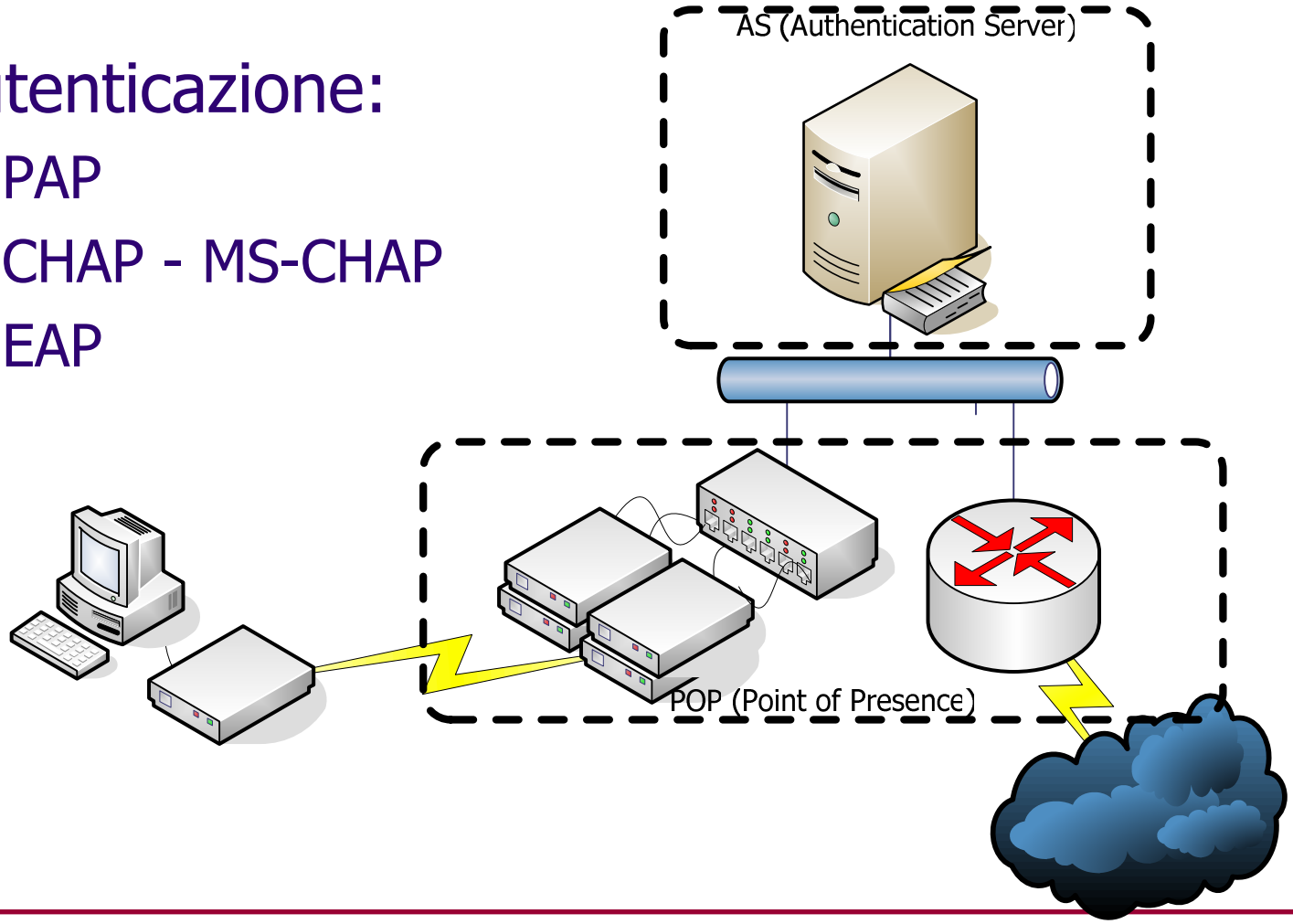
- Accesso ad una rete via modem



- PPP: Point to Point Protocol

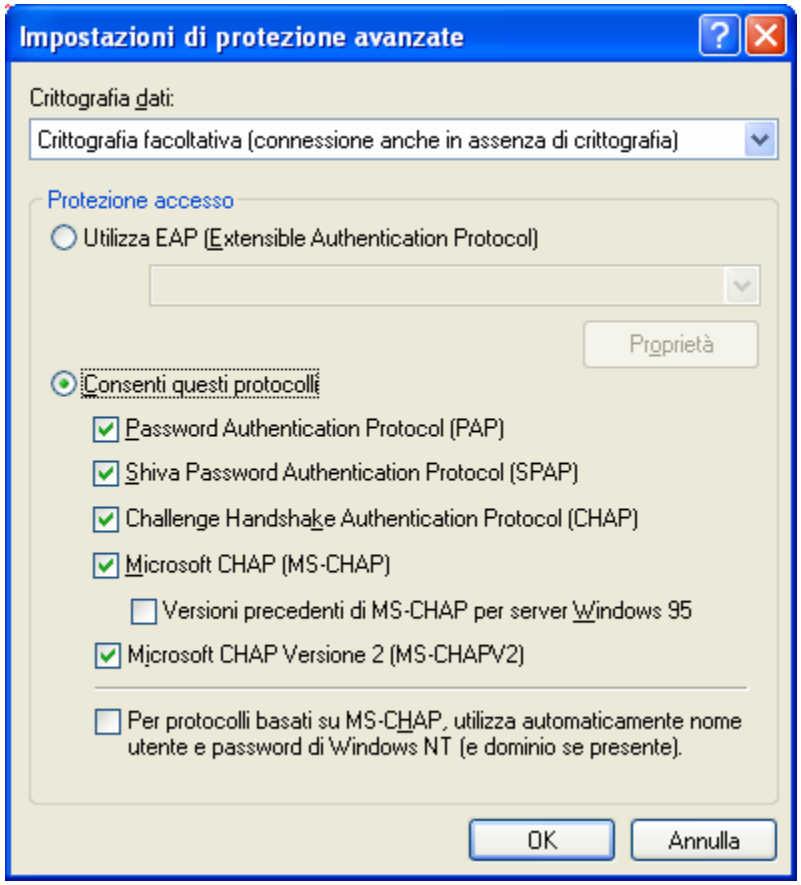
Dial-Up networks

- Autenticazione:
  - PAP
  - CHAP - MS-CHAP
  - EAP



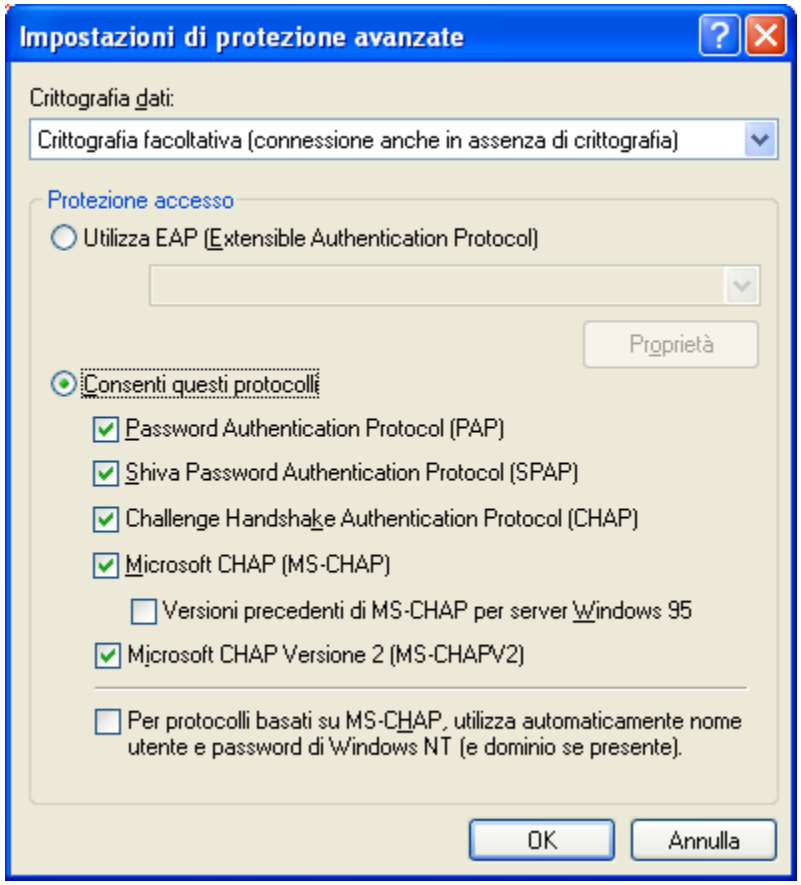
Autenticazione PPP (1)

- **PAP** (rfc1334)
  - user/password in chiaro
- **CHAP** (rfc1994)
  - Challenge <> MD5 Hashed challenge
  - La password è conservata in chiaro



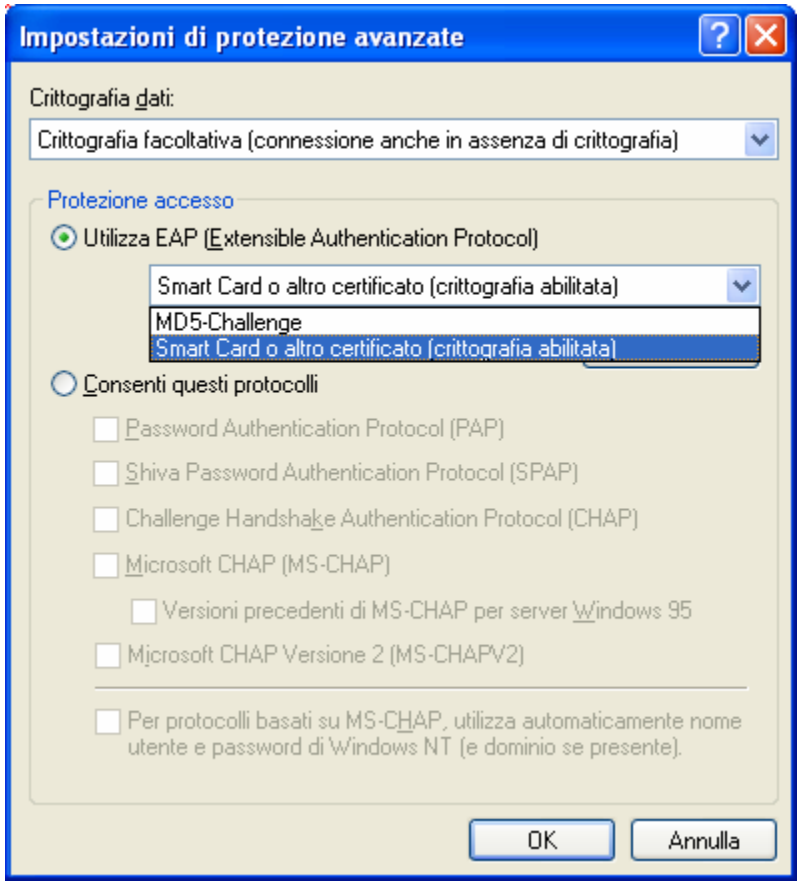
Autenticazione PPP (2)

- **MS-CHAP** (rfc2433)
  - Integrazione con Windows NT
  - Cambio password
  - La password viene conservata hashed
- **MS-CHAPv2** (rfc2759)
  - Mutua autenticazione



Autenticazione PPP (3)

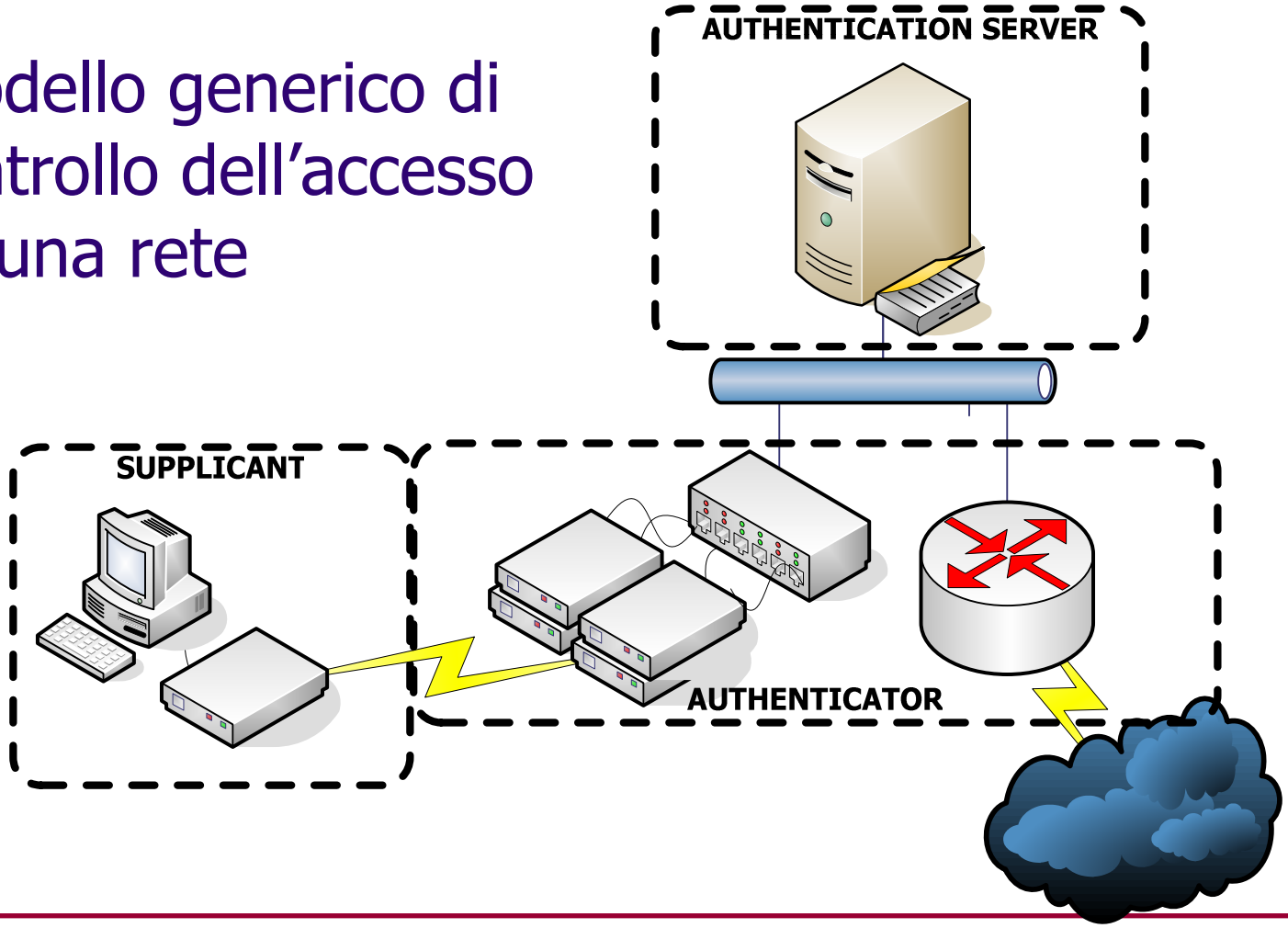
- **EAP** (rfc2284)
  - Protocollo di autenticazione flessibile
  - Utilizzo di un server di autenticazione
  - “strong authentication”
    - one-time password
    - smart-card
    - certificati digitali



Il framework IEEE 802.1X

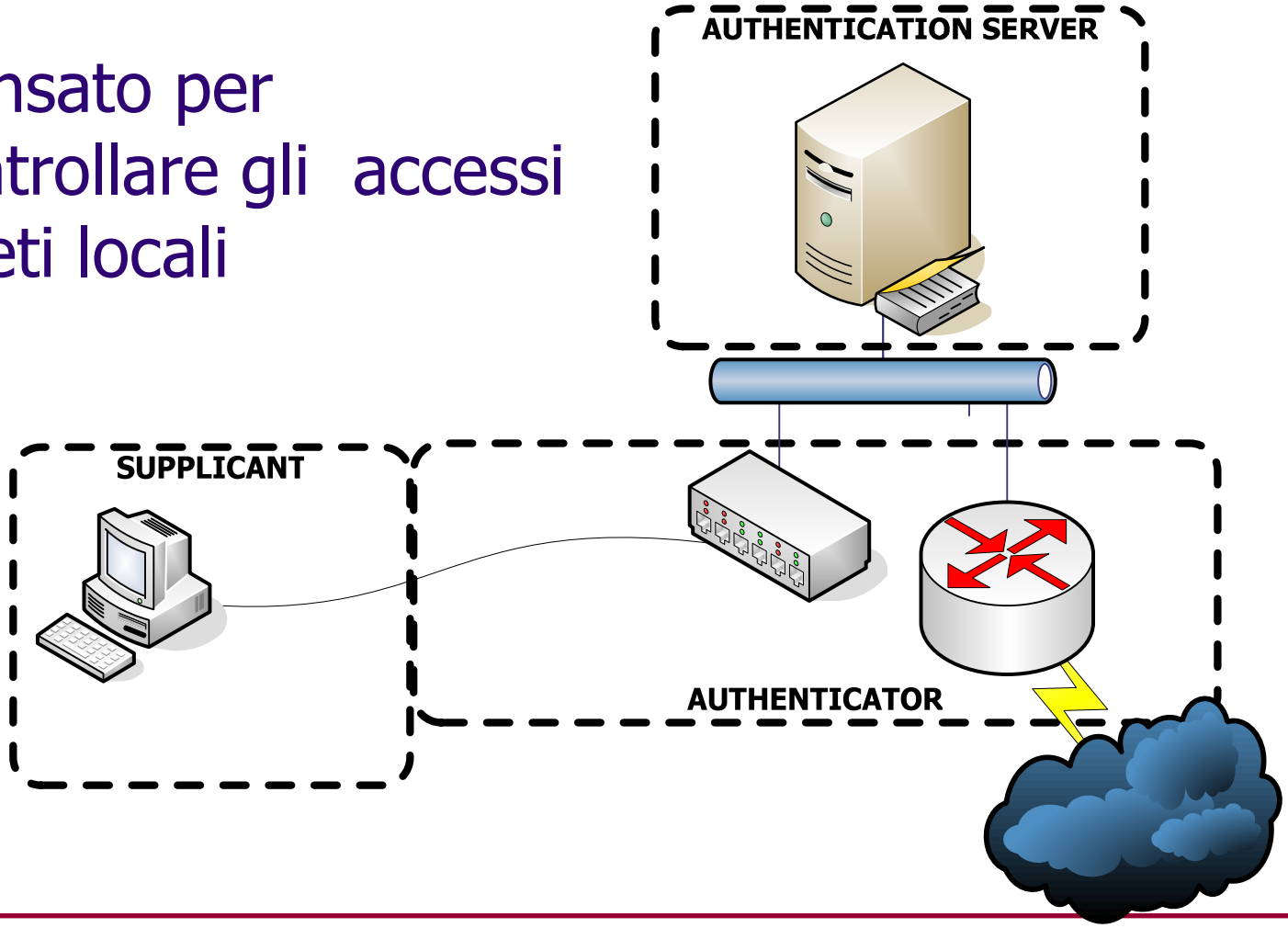
ISACA
Servire i professionisti dell'IT Governance
Rome Chapter

- Modello generico di controllo dell'accesso ad una rete



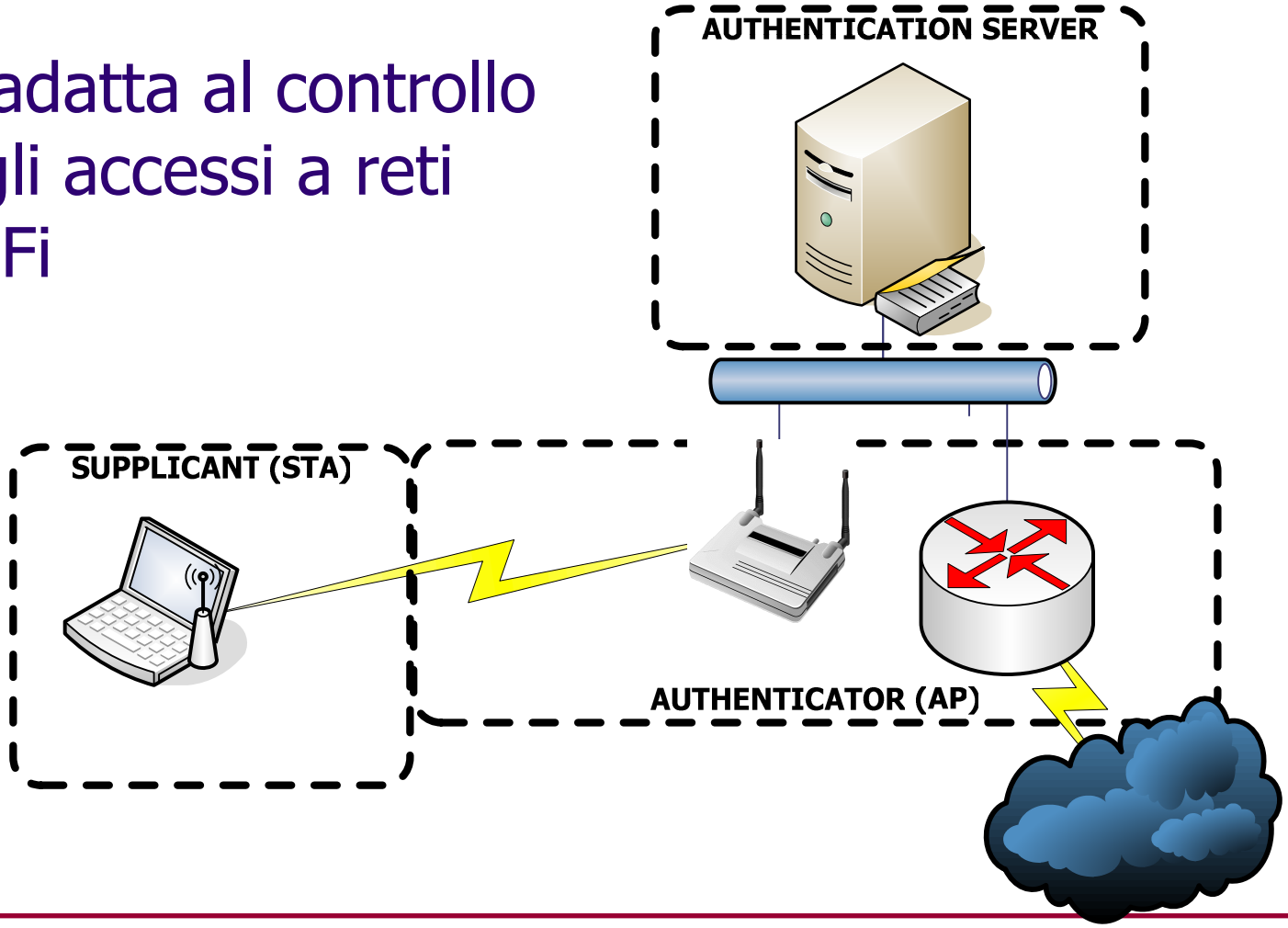
Il framework IEEE 802.1X

- Pensato per controllare gli accessi a reti locali



Il framework IEEE 802.1X

- Si adatta al controllo degli accessi a reti Wi-Fi



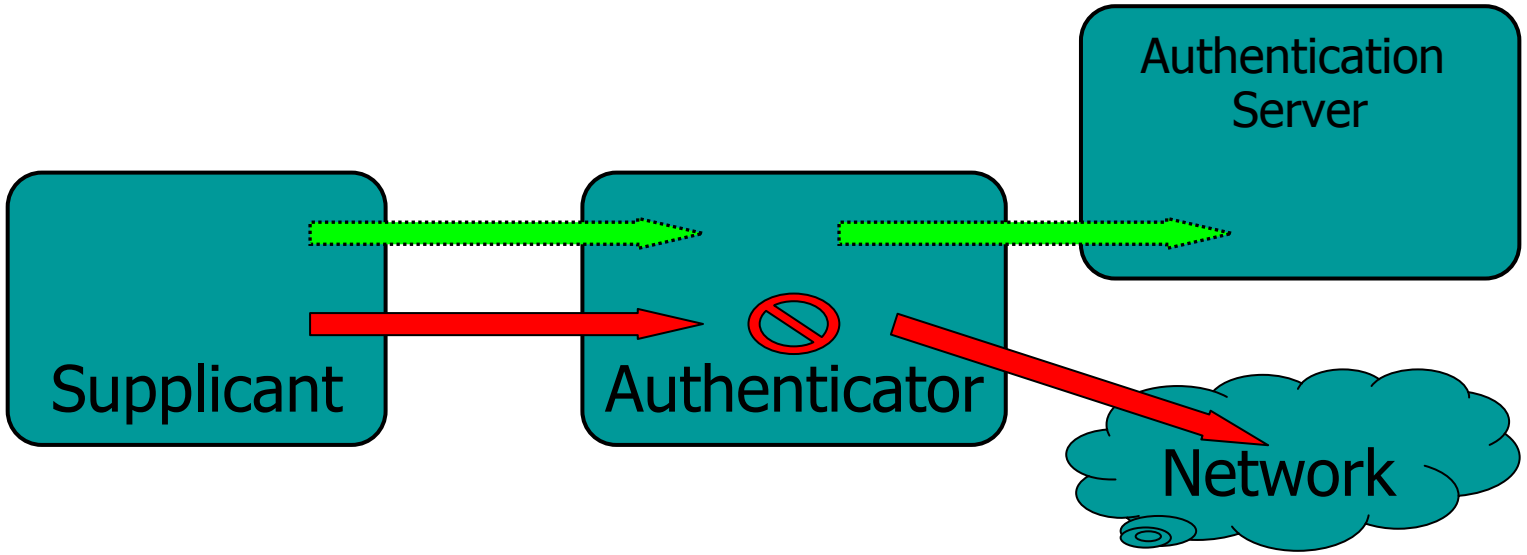
IEEE 802.1X: Principi

ISACA
Servire i professionisti dell'IT Governance
Rome Chapter

- Il collegamento di rete si attua attraverso due porte logiche
  - Porta controllata (bloccata fino ad autenticazione avvenuta)
  - Porta non controllata (permette solo scambio di messaggi per l'autenticazione)

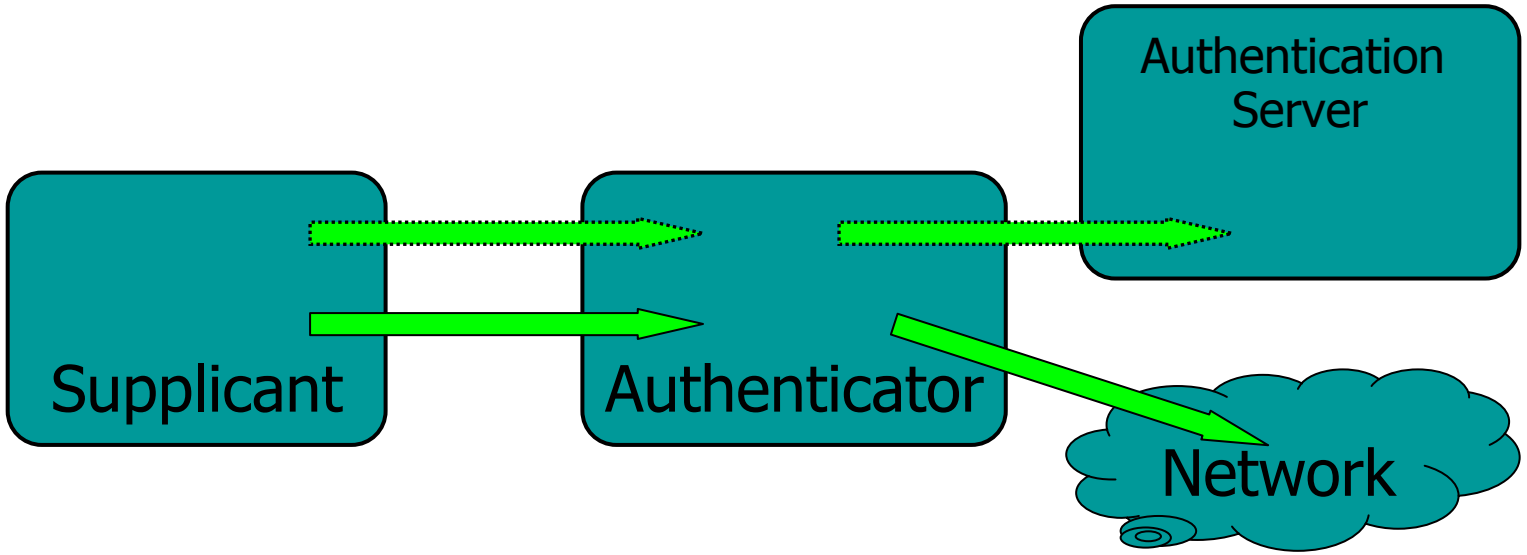
IEEE 802.1X: Principi

- Sulla porta non controllata vengono scambiati messaggi EAPoL (EAP over LAN)

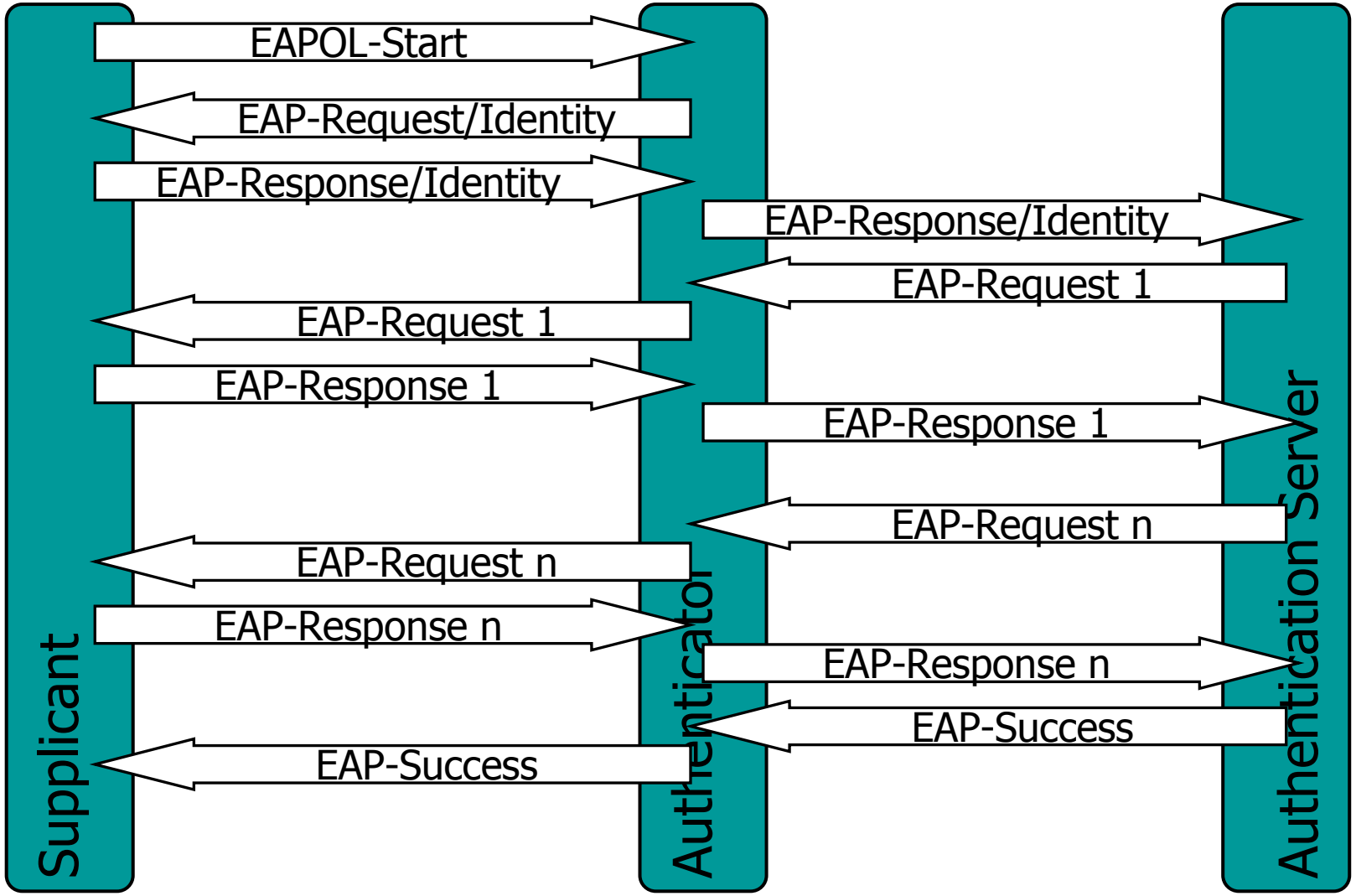


IEEE 802.1X: Principi

- La porta controllata viene aperta a seguito dell'autenticazione



IEEE 802.1X: Messaggi



Meccanismi di autenticazione EAP (1)

ISACA
Servire i professionisti dell'IT Governance
Rome Chapter

- **EAP-MD5 (CHAP)**
  - *Non abilita la cifratura della connessione*
  - *Userid/Password*
  - *Assenza di mutua autenticazione*
- **EAP-OTP, EAP-GTC**
  - *Userid/One-time Password o Userid/TokenCard*

Meccanismi di autenticazione EAP (2)

ISACA
Servire i professionisti dell'IT Governance
Rome Chapter

- **EAP-TLS**
  - *Abilita la cifratura della connessione*
    - *La connessione non é cifrata da TLS, ma viene usata la chiave di sessione TLS*
  - *Certificati digitali (client e server)*
  - *Mutua autenticazione*
- **EAP-TTLS (Tunneled TLS)**
- **PEAP (Protected EAP)**
  - *L'autenticazione avviene in un tunnel TLS*
  - *Certificati digitali (solo server)*
  - *Mutua autenticazione*

Meccanismi di autenticazione EAP (3)

ISACA
Servire i professionisti dell'IT Governance
Rome Chapter

- **PEAP (Protected EAP)**
  - *L'autenticazione avviene in un tunnel TLS*
  - *Certificati digitali (solo server)*
  - *Mutua autenticazione*

Meccanismi di autenticazione EAP (4)

ISACA
Servire i professionisti dell'IT Governance
Rome Chapter

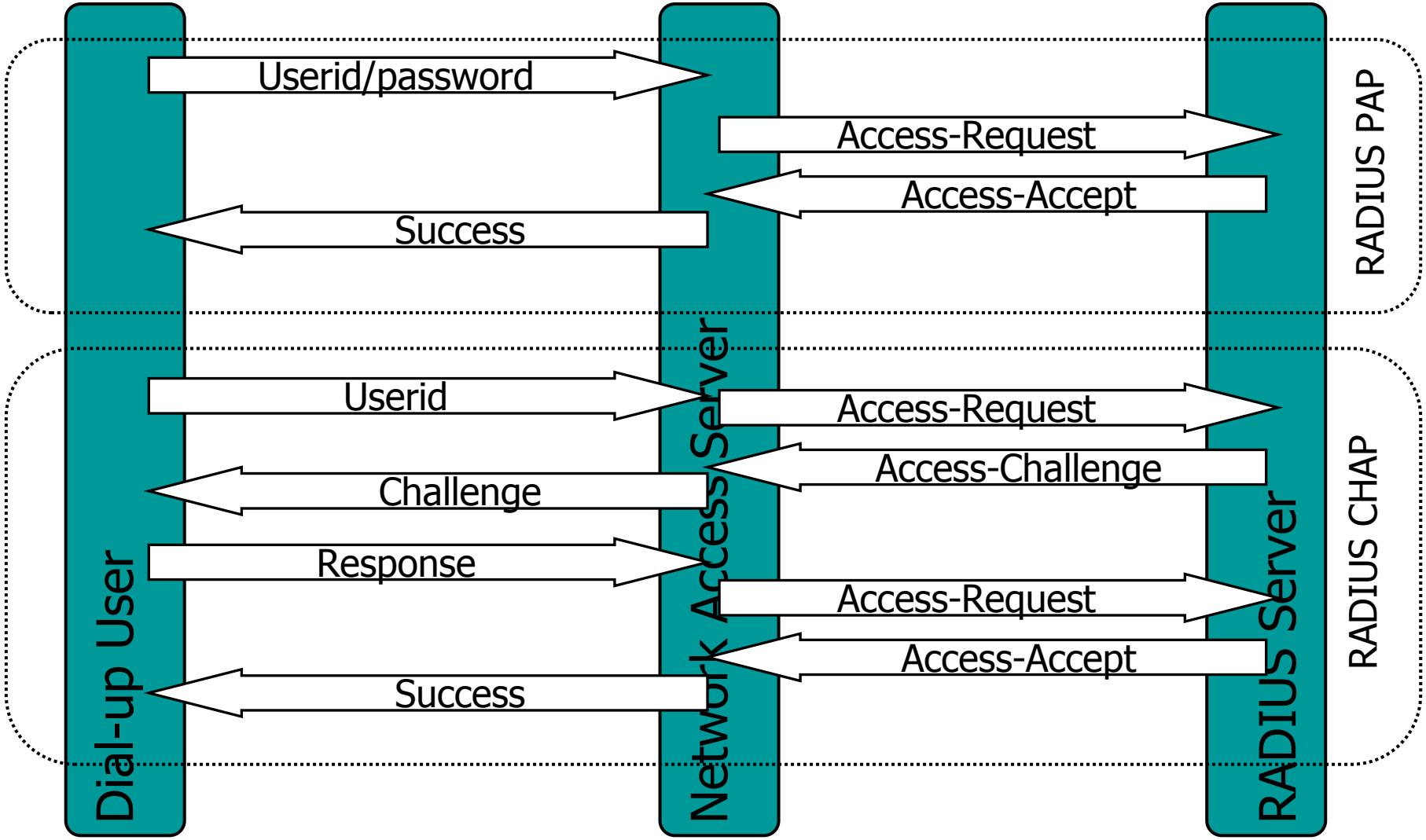
- **LEAP (CISCO Wireless)**
  - *Protocollo proprietario, prima implementazione di IEEE 802.1X*
  - *Autenticazione con shared key (MS-CHAP)*
  - *Mutua autenticazione (doppio challenge)*
  - *Gestione centralizzata*
  - *Chiavi di crittografia temporanee*
  - *Authentication server RADIUS*

RADIUS

ISACA
Servire i professionisti dell'IT Governance
Rome Chapter

- **Remote Access Dial-In User Service**
  - Protocollo di autenticazione
  - *RADIUS Server*: Server di autenticazione centralizzato
  - Diffusione iniziale a supporto degli ISP
  - IETF rfc2865
  - Supporto di EAP over RADIUS (rfc2869)

RADIUS: Messaggi



RADIUS: Attributi

ISACA
Servire i professionisti dell'IT Governance
Rome Chapter

- I messaggi RADIUS sono composti da una serie di attributi
- Facilità di estensione
  - MS-CHAPv2
  - EAP over RADIUS
- Distribuzione di chiavi
  - MS-MPPE-Recv-Key Attribute (usato da WPA)
- IEEE 802.11i non ha come requisito RADIUS, al contrario di WPA

RADIUS: Debolezze

ISACA
Servire i professionisti dell'IT Governance
Rome Chapter

Hill, 2001 segnala una serie di vulnerabilità

- *The User-Password protection technique is flawed in many ways. It should not use a stream cipher, and it should not use MD5 as a cipher primitive.*
- *The Response Authenticator is a good idea, but it is poorly implemented.*
- *The Access-Request packet is not authenticated at all.*
- *Many client implementations do not create Request Authenticators that are sufficiently random.*
- *Many administrators choose RADIUS shared secrets with insufficient information entropy. Many client and host implementations artificially limit the shared secret key space.*

RADIUS-EAP Servers

ISACA
Servire i professionisti dell'IT Governance
Rome Chapter

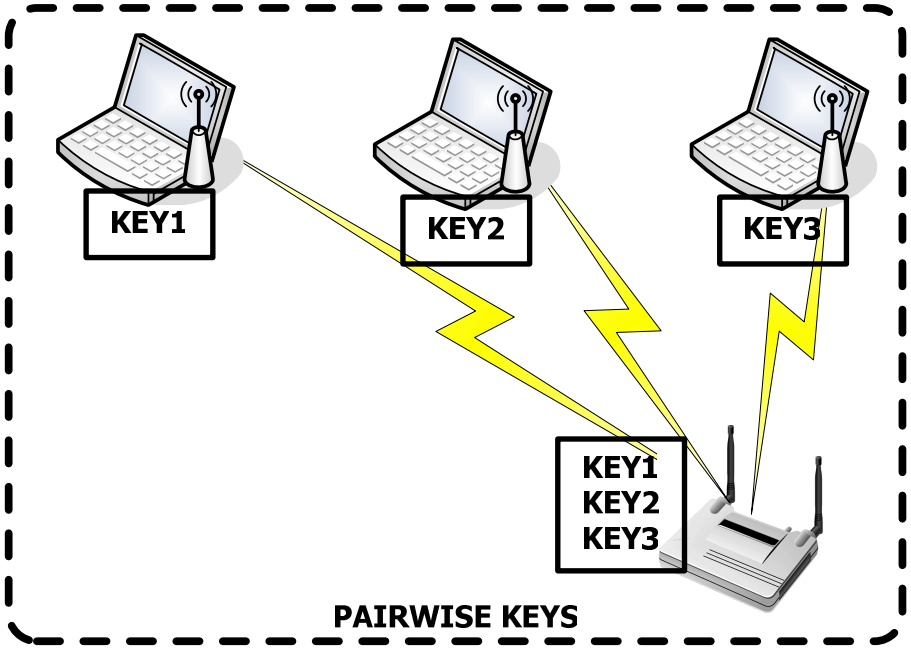
- RADIUS Servers EAP-ready
  - FreeRADIUS
    - www.freeradius.org
  - Microsoft IAS
    - www.microsoft.com/ias
  - Steel Belted RADIUS
    - www.funk.com
  - Radiator
    - www.open.com.au/radiator

IEEE 802.11i: Gestione delle chiavi

- Due set di chiavi

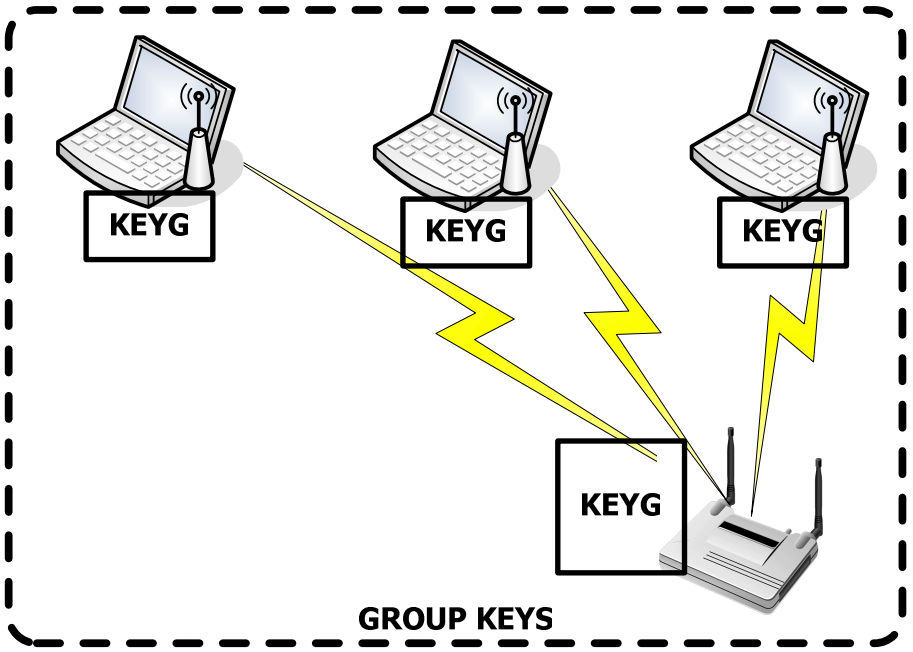
  Pairwise keys

  – Protezione messaggi *unicast*



IEEE 802.11i: Gestione delle chiavi

- Due set di chiavi
  Group keys
  – Protezione messaggi *multicast* e *broadcast*



Pairwise key hierarchy

ISACA
Servire i professionisti dell'IT Governance
Rome Chapter

- *Pairwise Master Key (PMK)*
  - Generata durante l'autenticazione 802.1X
  - Pre-shared Key (WPA-PSK)
- *Pairwise Transient Key (PTK)*
  - Derivata da PMK e "nonces"
  - Univoca per sessione
  - Composta da più chiavi, utilizzate per cifrare e assicurare integrità (sia durante l'autenticazione che successivamente)

Group key hierarchy

ISACA
Servire i professionisti dell'IT Governance
Rome Chapter

- *Group Master Key (GMK)*
  - Generata dall'Access Point
- *Group Transient Key (GTK)*
  - Derivata da GMK allo stabilirsi di ogni sessione
  - Distribuita ai client (STA)
  - Composta da più chiavi, utilizzate per cifrare e assicurare integrità

IEEE 802.11i
Uso delle chiavi

ISACA
Servire i professionisti dell'IT Governance
Rome Chapter

1. AS (server RADIUS) fornisce PMK ad AP
   - La comunicazione tra AS e AP deve essere sicura
2. 4-Way Handshake tra STA e AP per derivare e verificare PTK
   - PTK non viene trasmessa
   - Mutua autenticazione
   - Possibile DoS (He, 2004)
3. AP deriva GTK e la invia a STA
   - Protezione ed integrità del messaggio tramite PTK

IEEE 802.11i
Protezione dei dati

ISACA
Servire i professionisti dell'IT Governance
Rome Chapter

- TKIP (Temporal Key Integrity Protocol)
  - Basato su RC4
  - WPA – Soluzione temporanea
- CCMP (Counter Mode-CBC MAC Protocol)
  - Basato su AES
  - WPA2 – Soluzione a lungo termine

TKIP

ISACA®
Servire i professionisti dell'IT Governance
Rome Chapter

- Permette l'upgrade di dispositivi WEP
- Necessario per proteggere gli investimenti
- Corregge le debolezze WEP
- WEP wrapper, non è una sostituzione

TKIP – Message Integrity

ISACA
Servire i professionisti dell'IT Governance
Rome Chapter

- Proteggere dalle contraffazioni
- Nuovo algoritmo “leggero”: **Michael**
- Opera su frame (MSDU) e non su frammenti (MPDU) - Minore appesantimento
- Usa chiavi di 64 bits
- Adotta contromisure se si accorge di attacchi
  - Rigenerazione di chiavi
  - Blackout di 60 secondi
- Ha dei difetti: è il punto debole di WPA

TKIP – Message Replay

ISACA
Servire i professionisti dell'IT Governance
Rome Chapter

- Evitare replay dei messaggi
- **TSC**, TKIP Sequence Counter
- Incremento ad ogni pacchetto
- Eliminazione dei pacchetti fuori sequenza
  - Entro una finestra di 16

TKIP
Una Chiave per pacchetto

ISACA
Servire i professionisti dell'IT Governance
Rome Chapter

- Evitare le chiavi deboli RC4
- Evitare il riuso di IV (portato a 48 bits)
- Cambiare chiave ad ogni pacchetto per evitare criptanalisi: **Per-Packet Key Mixing**
- **Fase 1.** Una chiave intermedia é calcolata in base a: Session Key, MAC Address (per generare univocità tra le STA), 32 bits di IV
- **Fase 2.** La chiave per pacchetto è calcolata in base alla chiave intermedia ed a 16 bits di IV

TKIP – Debolezze

ISACA
Servire i professionisti dell'IT Governance
Rome Chapter

- E' stata rilevata una debolezza nel calcolo delle chiavi intermedie (Moen, 2004)
- A parità di IV, sono sufficienti pochi chiavi RC4 per calcolare la chiave intermedia (TK) e la chiave MIC
- Per il momento è una debolezza più teorica che pratica
  - Grazie allo spazio dei 32 bits di IV usati
- Lezione: AES "é" più affidabile (oggi)

CCMP

ISACA®
Servire i professionisti dell'IT Governance
Rome Chapter

- Basato su AES-CCM (Counter Mode con CBC-MAC)
- Richiede nuovo hardware (AES)
- Protocollo del tutto nuovo (senza WEP)
- Si applica ad ogni singolo frammento (MPDU)

AES Counter Mode

ISACA®
Servire i professionisti dell'IT Governance
Rome Chapter

- Ogni singolo blocco é combinato (XOR) con la cifratura AES di un Contatore
- *Blocchi uguali danno risultati diversi*
- Il contatore è inizializzato
- *Messaggi uguali danno risultati diversi*

CCM

- Viene calcolato un MIC in base ad header, lunghezza dei dati e dati con CBC-MAC (cipher block chaining).
- I dati vengono cifrati con AES-CTR
- MIC viene cifrato con AES-CTR
- CCM fornisce autenticità e cifratura

Flusso operativo CCMP

ISACA
Servire i professionisti dell'IT Governance
Rome Chapter

1. Ogni MSDU viene divisa in MPDU
2. Tra il MAC Header e i dati viene inserito un CCMP Header
3. Viene calcolato il MIC di MAChdr+CCMPhdr+Dati ed appeso in fondo
4. Viene cifrato Dati+MIC
5. L'MPDU é ricomposta da MAChdr+CCMPhdr+ciphertext

WEP vs TKIP vs CCMP

ISACA
Servire i professionisti dell'IT Governance
Rome Chapter

	WEP	**TKIP**	**CCMP**
Cipher	RC4	RC4	AES
Key Size	40/104 bits	128 bits (enc) 64 bits (mic)	128 bits
IV	24 bits	48 bits	48 bits
Packet key	Concat	Mixing Key	n/a
Data Integrity	CRC-32	Michael	CCM
Header Integrity	None	Michael	CCM
Replay	None	Use IV	Use IV
Key Mgmt	None	EAP-based	EAP-based

Tutto risolto ?

ISACA
Servire i professionisti dell'IT Governance
Rome Chapter

- Discovery delle reti (mitigato)
  - Non considerato da 802.11i, ma il rafforzamento delle reti rende meno probabili attacchi
- Denial of Service (non risolto)
  - Non considerato da 802.11i, Management and Control frames continuano a non essere autenticate
  - 4-way Handshake soggetto a DoS
  - Impensabile difesa da interferenze radio
- Shared key authentication attacks (risolto)
- Camuffamento MAC Address (risolto)

Tutto risolto ?

ISACA
Servire i professionisti dell'IT Governance
Rome Chapter

- Message modification and replay (risolto)
  - Però CCM è meglio di Michael
- Dictionary-based WEP key recovery (risolto)
  - Ma attenzione a chiavi generate da una passphrase
  - Debolezze in WPA-PSK
- RC4 weak keys (risolto)
- Falsi AP (risolto)
  - Ma attenzione ai certificati del server
- Debolezze RADIUS

A che prezzo ?

ISACA
Servire i professionisti dell'IT Governance
Rome Chapter

- Hardware upgrade
  - AES-based chipsets
- Security infrastructure
  - RADIUS Server
  - PKI (Digital certificates)
  - Scelta dei meccanismi EAP
- Lan design
  - Disegno di LAN e VLAN