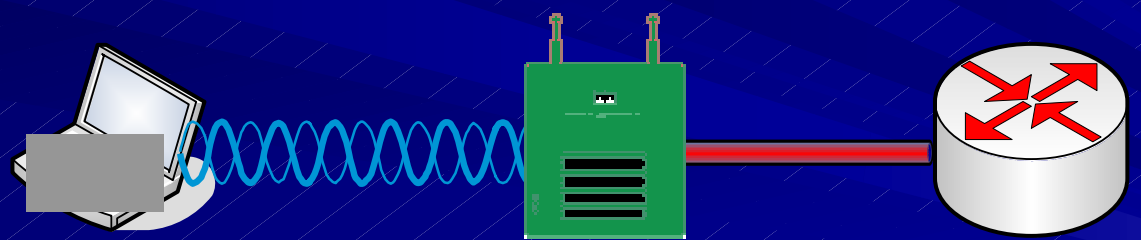
Università degli Studi di Udine

***C**entro **S**ervizi **I**nformatici e **T**elematici*

Claudio CASTELLANO

Nicola SUSAN

Wireless Local Area Network d'Ateneo



Wireless per gli studenti

Dal Settembre 2003 l'Università degli Studi di Udine offre, a tutti gli studenti e ai docenti , la possibilità di collegarsi ad Internet via Wireless

Wireless per gli studenti

É sufficiente che:

- gli utenti posseggano un notebook con scheda wireless con standard IEEE 802.11b/g integrata, PCMCIA o USB



- Il sistema operativo supporti lo standard IEEE 802.1x

  già presente nelle piattaforme con Windows XP (SP1 o 2) o Apple Mac OSX

Wireless per gli studenti

Con le stesse username e password utilizzate nei laboratori didattici è possibile effettuare un collegamento sicuro e riservato con Internet

Collocazione delle Wireless Zone all'interno del campus

Perché le reti Wireless LAN

- Estensione della LAN cablata preesistente;
  utenti non più vincolati ai soli laboratori.
- Istituzione di aree di lavoro temporaneo (conferenze – seminari…)
- Estrema scalabilità: connettività per pochi utenti fino a LAN complete.
- Mobilità nel campus grazie alla possibilità di Roaming

Perché le reti Wireless LAN

Velocità di trasferimento attualmente impiegate

- tecnologia IEEE 802.11b, che opera nella frequenza dei 2.4 GHz permette connessioni fino a 11 Mbps (condivisi).

- 802.11g con velocità di connessione fino a 54Mbps.

Sicurezza nelle reti Wireless LAN

Lo standard IEEE 802.1x

Sicurezza nelle reti Wireless LAN

L'adozione dello standard IEEE 802.1x permette di garantire all'utente sicurezza nella fase d'autenticazione (invio delle credenziali) e confidenzialità della connessione mediante l'impiego di chiavi di crittografia

Sicurezza nelle reti Wireless LAN

Principali caratteristiche del protocollo 802.1x

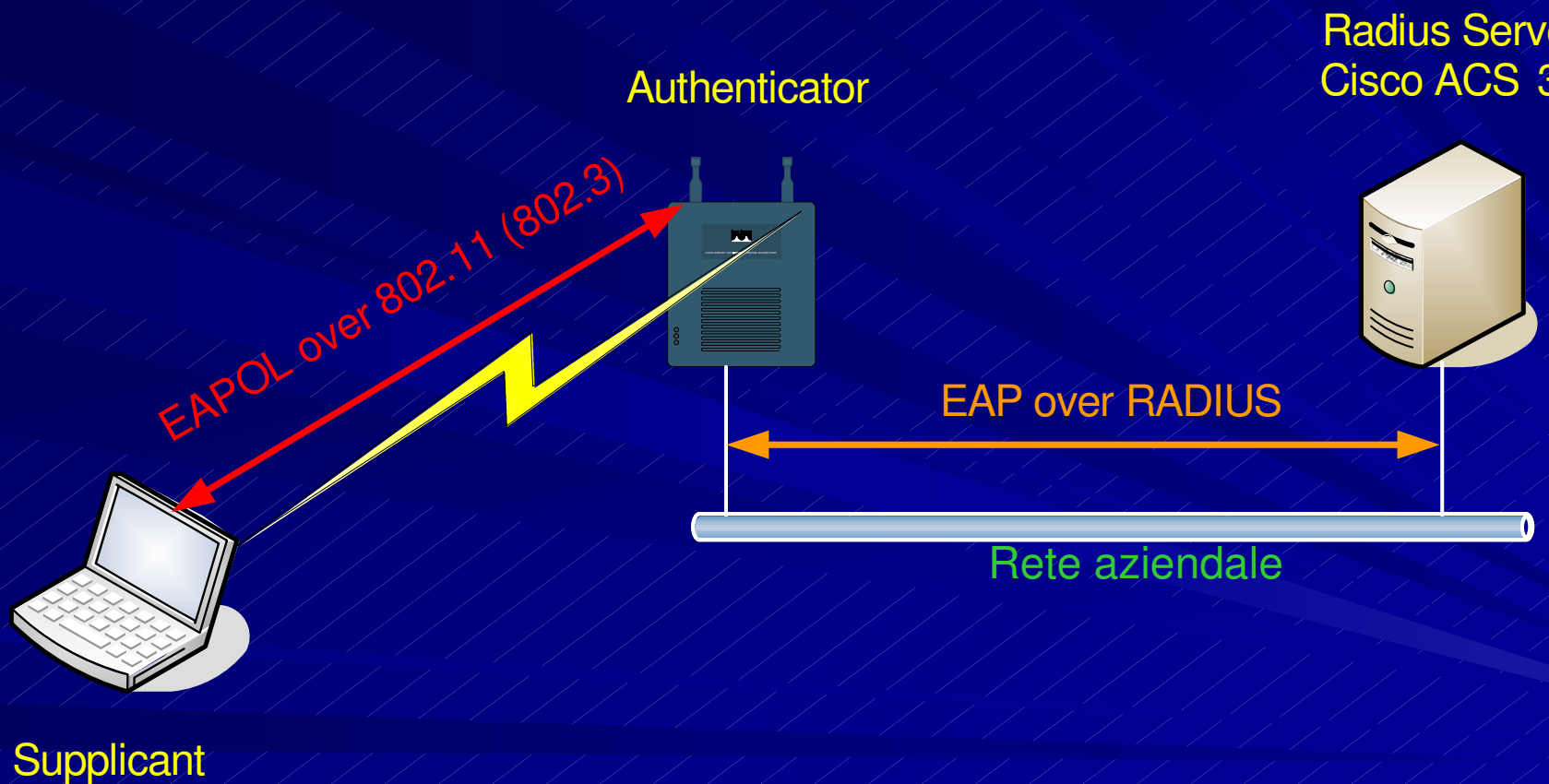
- L'obiettivo è fornire un *servizio* (connettività) SOLO ad utenti autenticati e autorizzati
- Fornisce un *architectural framework* che permette l'impiego di diversi metodi d'autenticazione (smartcard, certificati, OTP, usr e pwd…)
- Impiegabile per diverse tecnologie: IEEE802.3, Token Ring, FDDI e 802.11
- Si basa su protocolli e standard preesistenti e già impiegati:
  - Extensible Authentication Protocol (EAP)
  - Remote Authentication Dial-In User Service (RADIUS)

Protocollo IEEE 802.1X

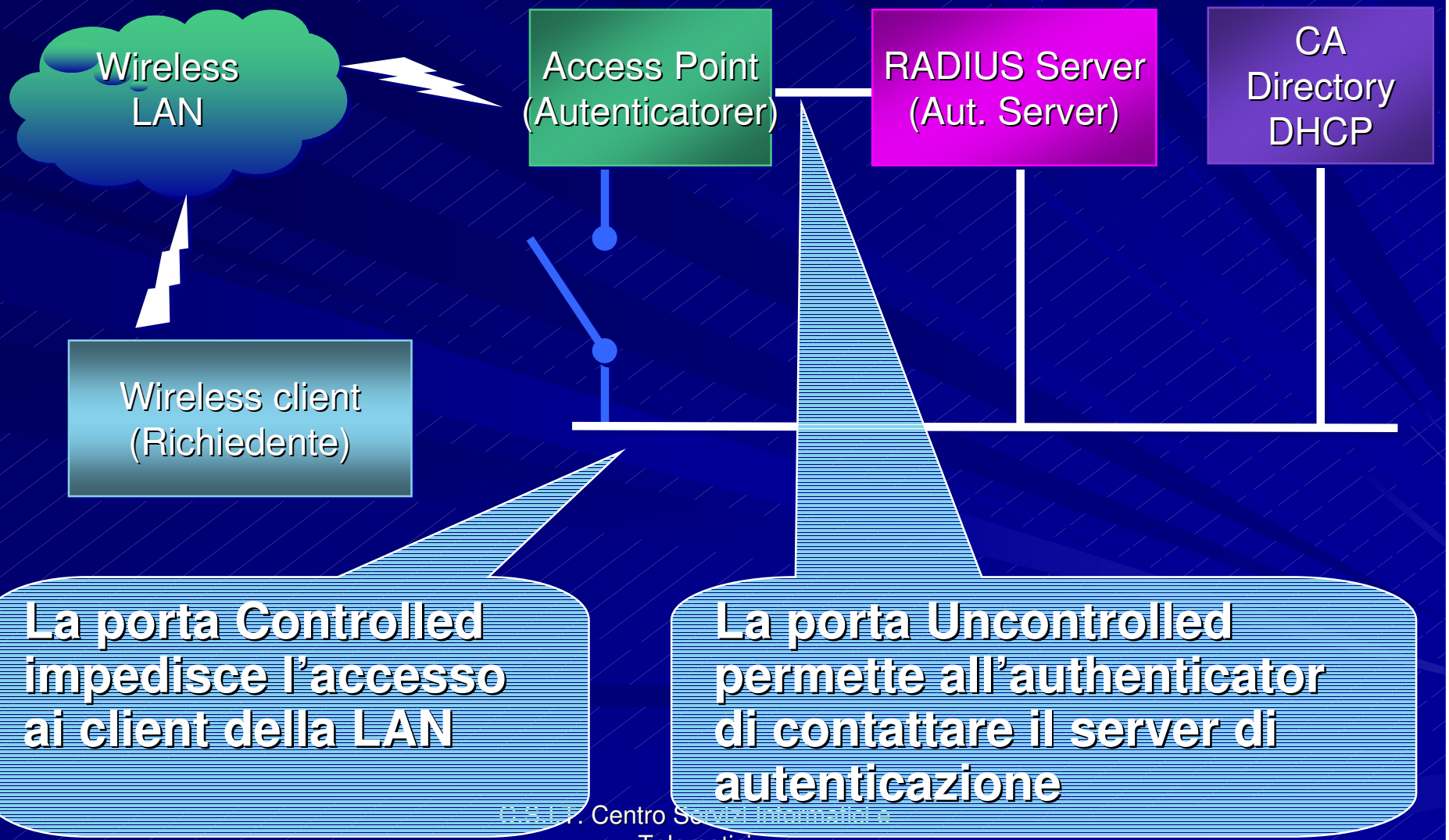
Identifica 3 entità:

- *Supplicant* (wireless PC card, Ethernet NIC,…)
- *Authenticator* (AP, switch,…)
- *Authentication Server* (Radius,…)

Protocollo IEEE 802.1X

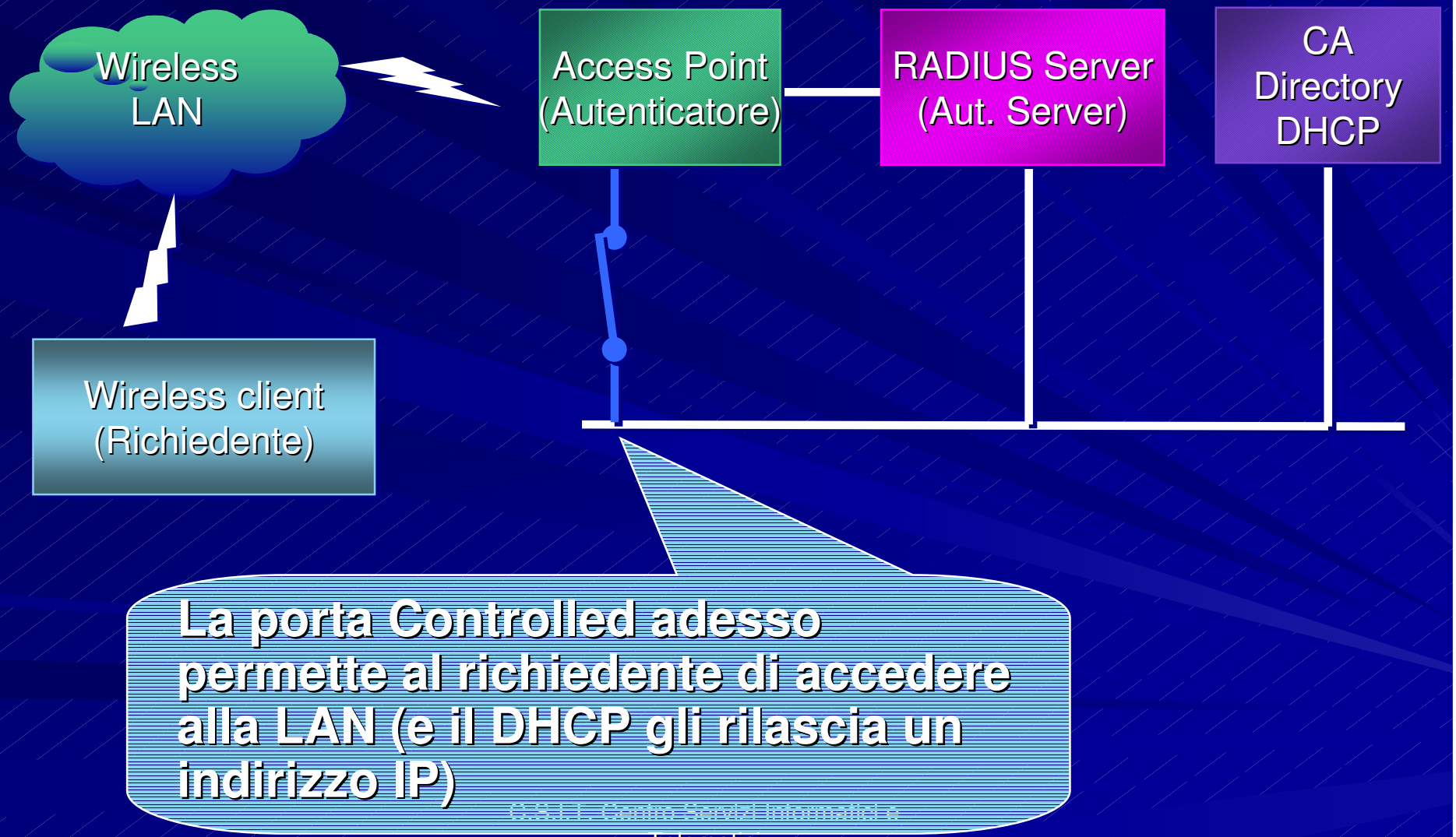


802.1x : Fase di “Association”



Fonte:www.microsoft.it

802.1x: “Association” avvenuta



Fonte:www.microsoft.it

Protocollo IEEE 802.1X

All'uso delle chiavi statiche, siano WEP o WPA, 802.1x fornisce:

- Accesso al servizio previa autenticazione ed autorizzazione
- Creazione chiavi di sessione dinamiche per ogni utente
- Rotazione delle chiavi di sessione
- Autenticazione, integrità e confidenzialità a livello di singolo pacchetto

Protocollo IEEE 802.1X

Vulnerabilità del protocollo EAP:

- Debolezza nella protezione delle credenziali dell'utente nella fase di autenticazione
- Mancanza di standardizzazione nello scambio delle chiavi
- Debolezza nel supporto di fast-reconnect
- Assenza di un metodo per la gestione di fragmentation e reassembly dei pacchetti

L’introduzione di TLS permette di far fronte alle vulnerabilità di EAP sopra indicate

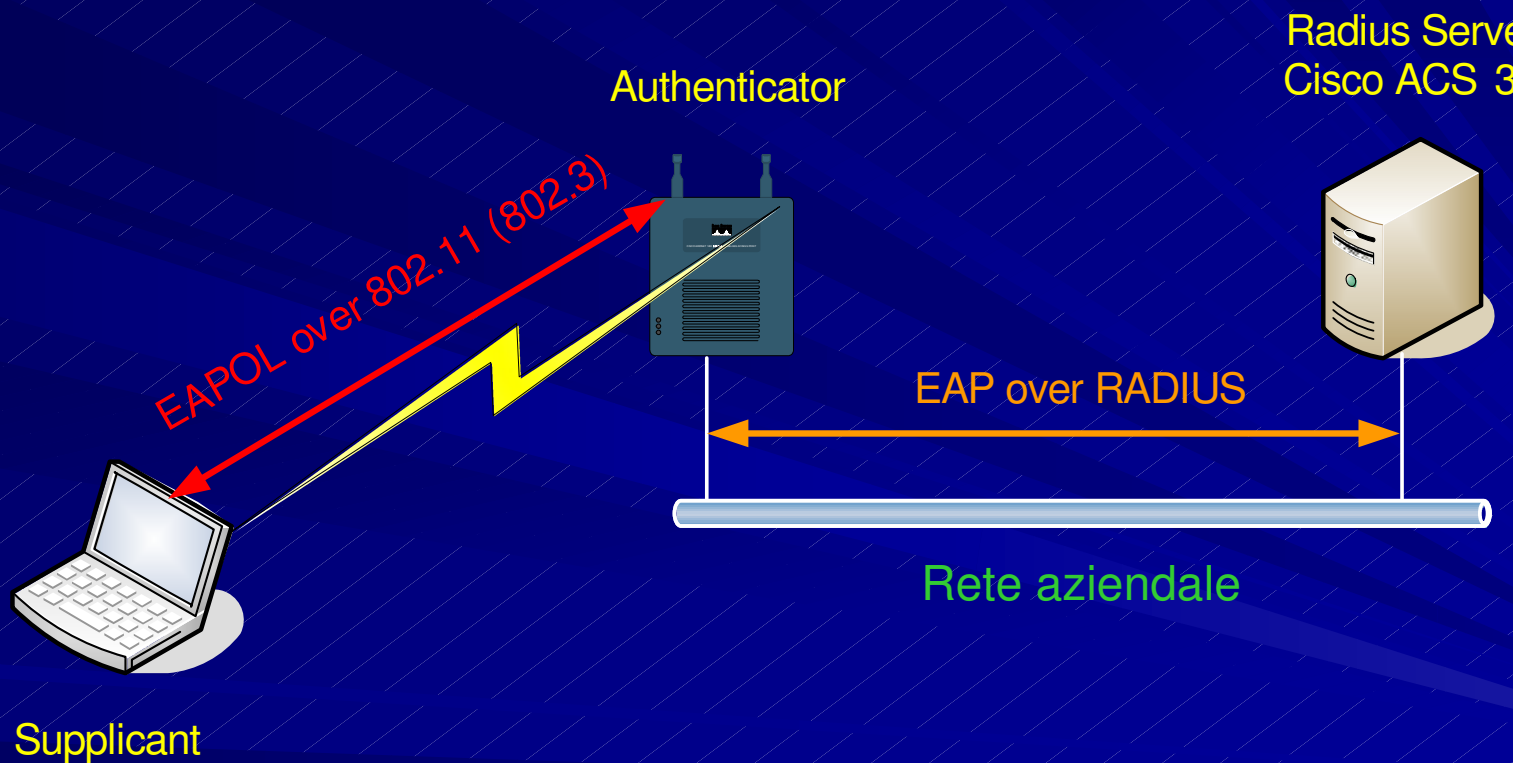
EAP

Nel nostro caso:

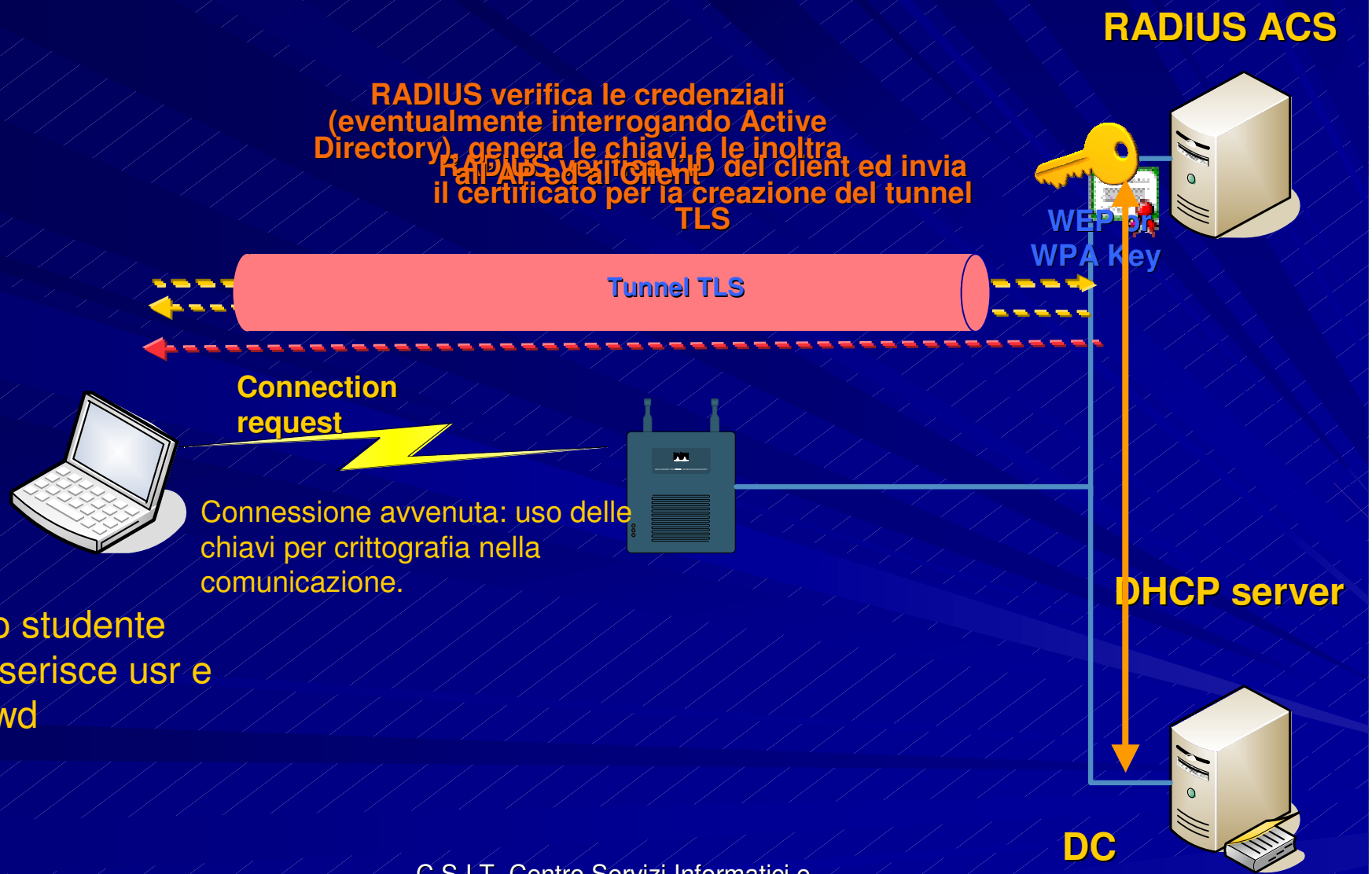
PEAP (studenti e docenti)

EAP-TLS (docenti)

Deployment della rete



PEAP


RADIUS ACS
RADIUS verifica le credenziali (eventualmente interrogando Active Directory), genera le chiavi e le inoltra all'AP ed al Client
RADIUS verifica l'ID del client ed invia il certificato per la creazione del tunnel TLS
WEP or WPA Key
Tunnel TLS
Connection request
Connessione avvenuta: uso delle chiavi per crittografia nella comunicazione.
Lo studente inserisce usr e pwd
DHCP server
DC

PEAP Vantaggi

- Gli utenti possono username e password utilizzate nei laboratori didattici. Non necessità del rilascio di certificati o smartcard a tutti gli utenti.
- Username e password vengono trasmesse attarverso un tunnel TLS cifrato.
- Per l'autenticazione basata su password viene usato MS-CHAPv2.
- Non vi sono pre-shared key.

  Le chiavi sono dinamicamente generate per ogni sessione e per ogni utente

EAP-TLS

- Ad ogni utente viene assegnato un certificato digitale (X509) impiegato nella fase d'autenticazione (no password, miglior metodo d'autenticazione)
- EAP-TLS consente la mutua autenticazione Client-Radius Server
- Obbliga all'installazione una Public Key Infrastructure
- Modalità di distribuzione del certificato agli utenti

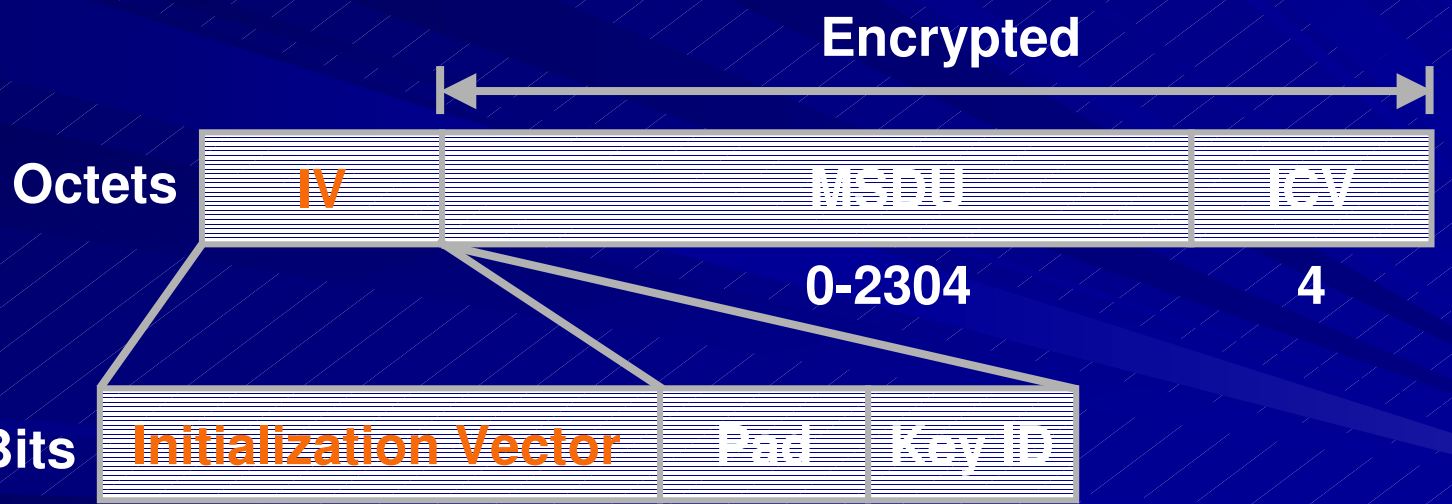
Chiavi di cifratura

Attualmente sono supportate sia le chiavi WEP che le chiavi WPA-TKIP

Chiavi di cifratura - WEP

WEP: algoritmo di cifratura RC4 che impiega chiavi ottenuto dalla combinazione della WEP (40 o 104 bit) + IV Initialization Vector di 24 bit a formare quindi chiavi a 64 o 128 bit,

IV cambia ad ogni pacchetto.



Chiavi di cifratura - WEP

WEP: algoritmo di cifratura RC4 che impiega chiavi ottenuto dalla combinazione della WEP (40 o 104 bit) + IV Initialization Vector di 24 bit a formare quindi chiavi a 64 o 128 bit,

IV cambia ad ogni pacchetto.

- Una debolezza nell'implementazione delle chiavi WEP da parte dell'RC4 genera alcuni IV detti deboli "weak" che "trasportano" con se informazioni sulla chiave impiegata.
- La cattura di un numero sufficiente di weak-IV (fino a 256 per ogni byte della chiave) permette di risalire alla chiave di cifratura.
- La "vita" di una chiave dipende dall'intensità del traffico, si parla comunque di:
  - minuti per chiavi a 40 bit
  - alcune ore per chiavi a 104 bit

Chiavi di cifratura WEP

- In 802.1x le chiavi sono dinamiche, generate ad ogni nuova autenticazione dell'utente.
- Le chiavi impiegate, nel nostro caso, sono a 104 bit (128 bit).
- L'AP chiede la riautenticazione dell'utente ogni 600 sec (con conseguente generazione di nuove chiavi), prima cioè che un attaccante catturi un numero sufficiente di weak-IV.

Chiavi di cifratura WPA-TKIP

Cerca di risolvere le debolezze delle WEP introducendo:

- IV a 48 bit (riduce i tempi di riuso del vettore)
- Per-packet key
- Message intergrity code (“Michael”)

Chiavi di cifratura

	WEP	WPA
Authentication	Mutual authentication through pre-shared secret (WEP key) or 802.1x	Mutual authentication through pre-shared secret (master key) or 802.1x
Keying	Global shared key or dynamic keying through 802.1x	Either global shared key or dynamic keying through 802.1x
Encryption	**RC4, with per-packet keys constructed by concatenating WEP key and random initialization vector**	**RC4, with per-packet keys constructed from hashed WEP key and serially increasing initialization vector**
Message Integrity	**32-bit CRC**	**32-bit CRC plus Message Integrity Code (MIC)**
Implementation	**Typically through RC4 chips in access point**	**In software, using existing hardware to perform RC4 processing**
The Good News	None	**Eliminates known WEP flaws, easy to upgrade enterprise access points and wireless clients**
The Bad News	Practically useless from a security perspective; difficult to deploy	Difficult and potentially expensive to deploy, degraded performance, not available for many environments, not a complete security architecture

Chiavi di cifratura

Perché sono mantenute sia WEP che WPA

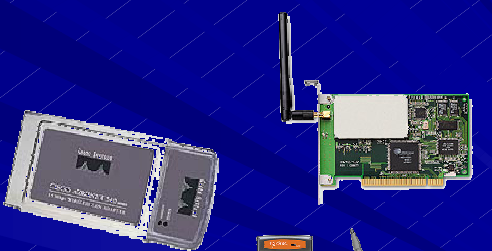
- Al momento della progettazione della rete (giugno 2003) le schede wireless e i SO più diffusi supportavano solo WEP.
- L'uso di WPA comporta aggiornamenti software e firmware (Windows XP SP2 per esempio) che alcuni utenti non hanno ancora effettuato.
- Le chiavi WEP verranno dismesse entro il 31/12/2005

Deployment della rete

riassumendo, le principali componenti sono:

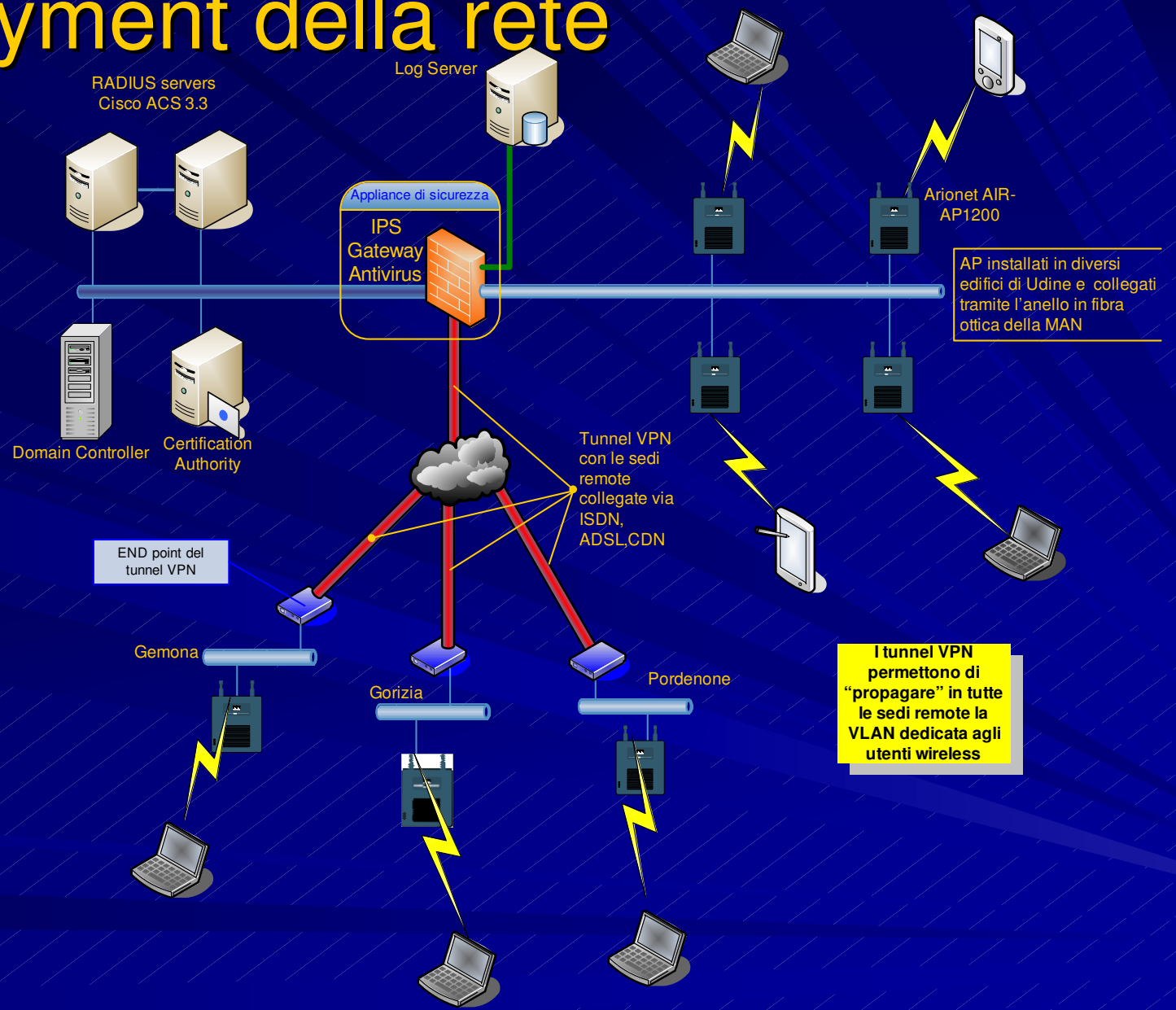
- Dispositivi end-user: PC dotati di scheda di rete wireless (Windows XP SP1 o SP2, Windows 2000 SP3/4, Mac OSX), Pocket PC ecc. con supporto 802.1x e chiavi WEP o WPA

- Access Point: componente d'accesso tra la rete cablata ed i vari dispositivi wireless (PC, PDA,ecc…). Nel nostro caso si impiega Cisco AP AIRONET 1200



- Server di controllo per l'accesso: server RADIUS Cisco ACS3.3, Certification Authority, Active Directory, DHCP server

Deployment della rete

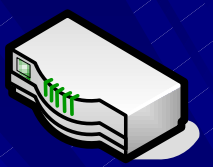


Deployment della rete

- L'utenza wireless viene concentrata in una sola sottorete (VLAN)
- Gli indirizzi IP vengono assegnati via DHCP
- Tutto il traffico da e verso i client wireless viene filtrato da un firewall

Deployment della rete

Appliance di sicurezza: features

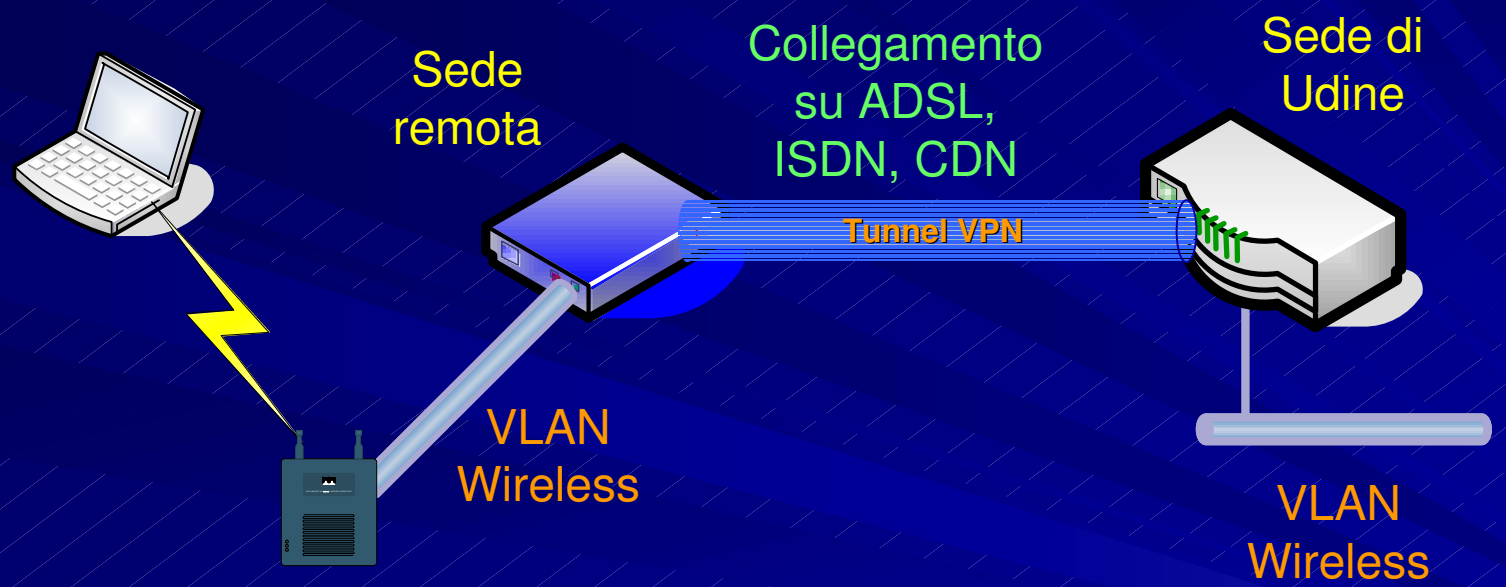


- Firewall:stateful filtering

11/14/2005 23:06:10.384	Notice	Network Access	TCP connection dropped	158.110.XXX.XXX, 3263, X1	158.110.XXX.XXX, 445, X0	TCP SMB	4 (WAN->LAN)	
11/14/2005 23:05:52.688	Info	Network	TCP stateful inspection: Invalid flag; TCP packet dropped	219.129.XXX.XXX, 80, X1	158.110.XXX.XXX, 46606, X3			
305	11/14/2005 23:15:49.832	Alert	Intrusion Prevention	Possible port scan dropped	217.169.XXX.XX, 80, X1	158.110.XXX.XXX 1883, X3	TCP scanned port list, 1878, 1879, 1881, 1880, 1882	
306	11/15/2005	Alert	Security	Gateway Anti-Virus Alert: MhtRedir.ITS.data.1	66.98.XXX.XX, 80,	158.110. XXX,XXX		=WAN)
307								
295	11/11/2005 11:29:36.048	Alert	Intrusion Prevention	Anti-Spyware Prevention Alert: CoolWebSearch ActiveX component download (Browser HiJacker), Danger Level: High	207.68.XXX.XX, 80, X1	158.110.XXX.XXX 4544, X0		
296	11/11/2005 11:29:35.320	Alert	Intrusion Prevention	IPS Prevention Alert: ICMP Echo Reply, Priority: Low	66.98.XXX.XXX, 8, X1	158.110.XXX.XXX 768, X3		
297	11/11/2005 11:29:30.480	Debug	Network Access	Broadcast packet dropped	158.110.XXX.XXX, 67, X1	255.255.255.255, 68	Protocol:68	

Deployment della rete

Deployment della rete



802.1x per il wired

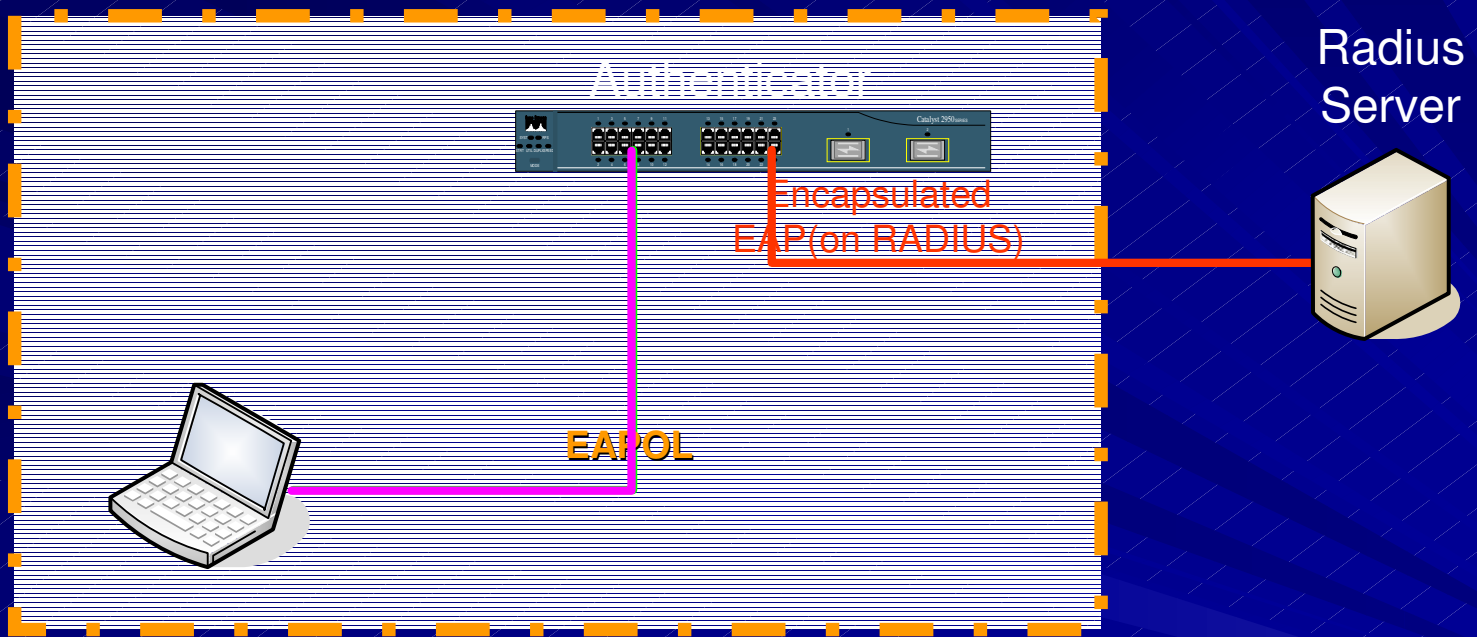
Autenticazione degli utenti mobili che utilizzano i punti rete cablati all'interno del campus

Authentication Authorization Accounting

- Utenti del convitto della Scuola Superiore
- Docenti che necessitano di connessione presso le aule didattiche

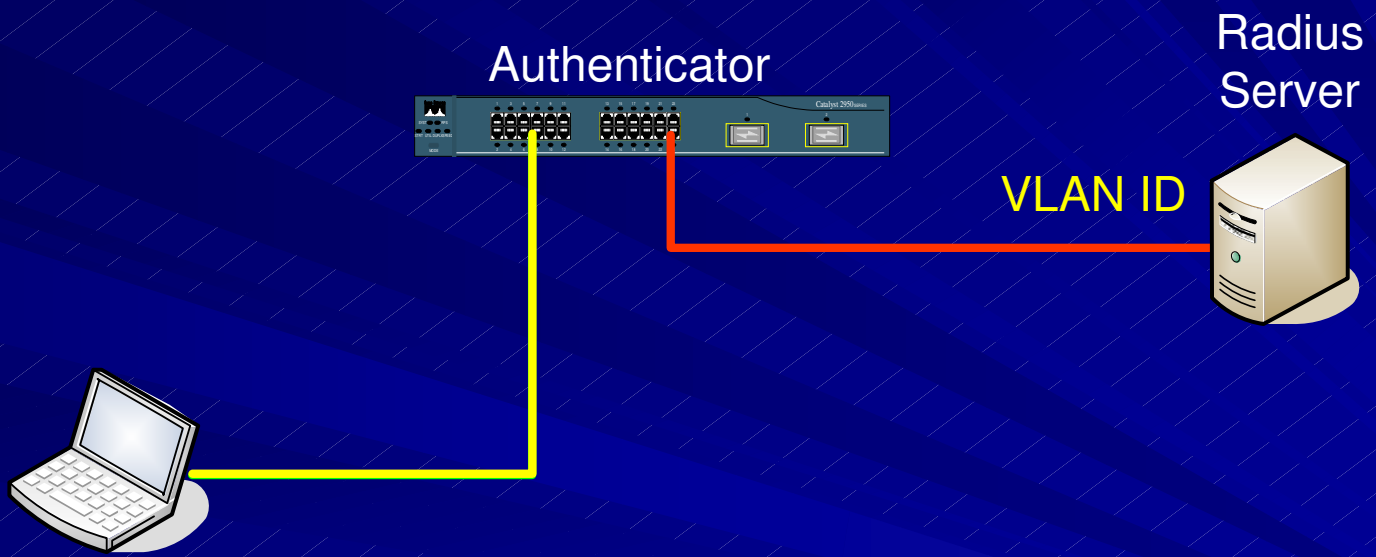
802.1x per il wired

Convitto Scuola Superiore



802.1x per il wired

Aule didattiche

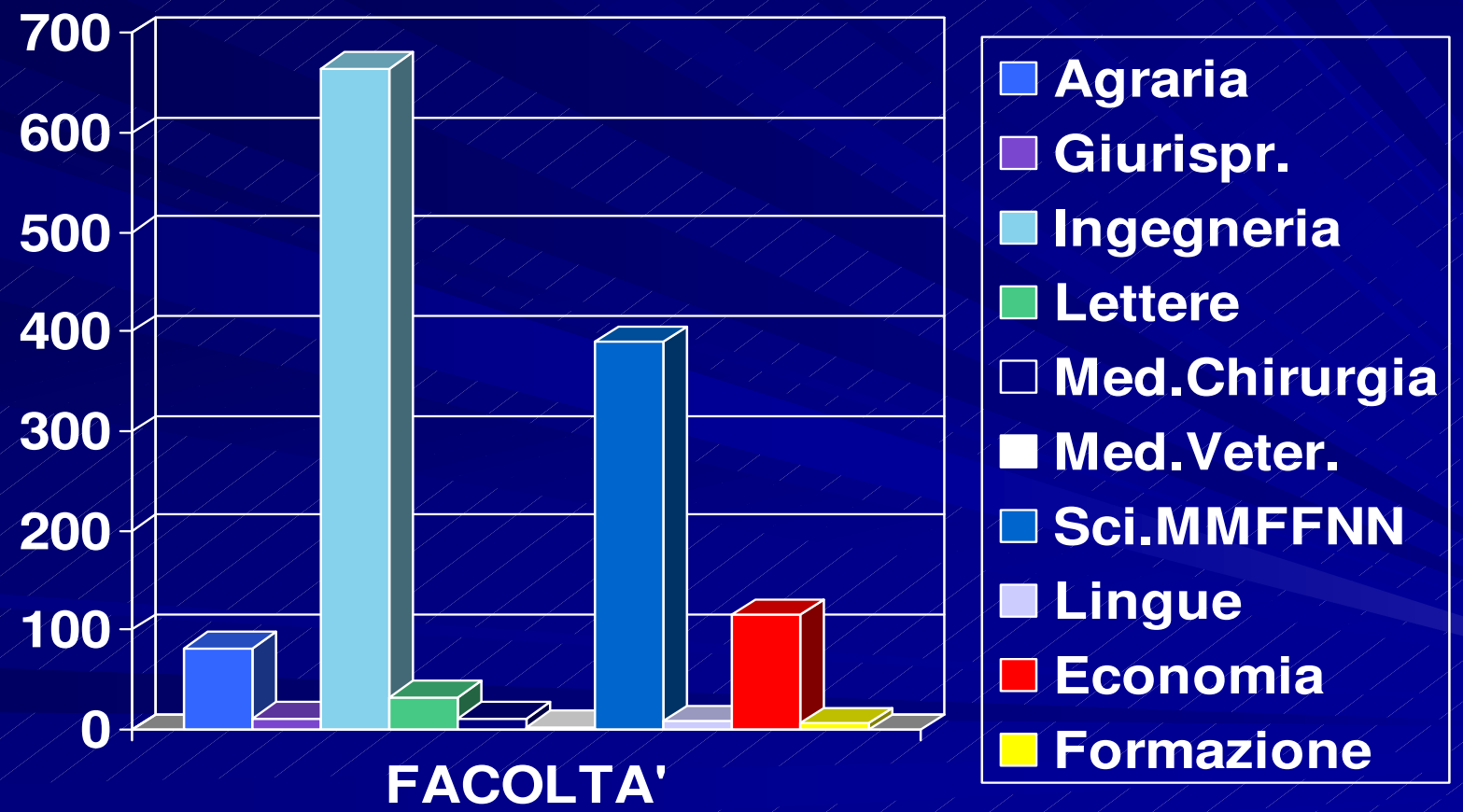


Considerazioni finali

- schieramento di una certification Authority per la distribuzione di certificati PKCS12 al fine di permettere l'estensione dell'uso del protocollo EAP-TLS anche agli studenti
- soppressione delle chiavi WEP entro il 31/12/2005
- Sperimentazione dei nuovi apparati ARUBA
- schieramento del dispositivo Cisco WLSE
- Schieramento delle VPN-SSL
- …

Utenti del servizio Wi-Fi

Totale utenti: ***circa 1400***



Fattori di successo (1/3)

- Politici/Organizzativi:
  - Progetto fortemente voluto dalla dirigenza fin dal 2002.
  - Gli studenti ottengono più postazioni ad accesso libero per collegarsi in rete. Quest'anno (*2005*) hanno richiesto la copertura di ogni sede universitaria.
  - Meccanismo di creazione automatizzata delle credenziali di accesso ai sistemi informatici e loro distribuzione stile "busta bancomat" all'atto dell'immatricolazione

Fattori di successo (2/3)

- Tecnologici
  - Utilizzate credenziali “sensibili” per l’autenticazione degli studenti (sono legate alla gestione della carriera).
  - Limitazione della potenza e della copertura RF e chiusura del servizio contestuale con la chiusura degli edifici.
  - Introduzione di un sistema di Firewall/IPS per evitare spiacevoli sorprese

Fattori di successo (3/3)

- Iniziative collaterali:
  - Attivazione contestuale alla partenza del servizio di una convenzione per l'acquisto agevolato di PC dotati di scheda Wi-Fi (siamo all'inizio del 2003 e non molti PC portatili avevano la scheda) preconfigurato per collegarsi in rete wireless.
  - Successivamente: attivazione iniziativa per concedere scheda Wi-Fi in comodato d'uso gratuito.

Criticità emerse (1/2)

- Tecniche/Logistiche
  - Necessità di adeguamento dell'impianto elettrico per consentire la ricarica delle batterie
  - Difficoltà di installazione e gestione degli access-point

Criticità emerse (2/2)

- Operative
  - Problemi legati al tempo impiegato nel supporto agli utenti
  - Difficoltà di attivazione e gestione dell'accordo a tre fra Ateneo, Istituto di Credito, produttore di PC

Riferimenti

- An Initial Analysis of the IEEE 802.1X Standard
  Authors: Arunesh Mishra, William A.Arbaugh (Department of Computer Science University of Maryland)
- 802.1X - Port Based Network Access Control
  http://www.ieee802.org/1/pages/802.1x.html
- “Extensible Authentication Protocol (EAP)”
  http://www.rfc-archive.org/getrfc.php?rfc=3748
- PPP EAP-TLS Authentication Protocol
  http://www.ietf.org/rfc/rfc2176.txt
- Protected EAP Protocol (PEAP)
  http://ietfreport.isoc.org/all-ids/draft-josefsson-pppext-eap-tls-eap-06.txt
- Protected EAP Protocol (PEAP) Version 2
  http://ietfreport.isoc.org/all-ids/draft-josefsson-pppext-eap-tls-eap-10.txt
- Wireless_parte2.ppt
  http://download.microsoft.com/download/2/f/2/2f2f8362-aab9-448d-bc8d-110422af7430/Wireless_parte2.ppt

Riferimenti

- “Wi-Fi Protected Access:Strong, standards-based, interoperable security for today’s Wi-Fi networks)”
  http://www.wi-fi.org/membersonly/getfile.asp?f=Whitepaper_Wi-Fi_Security4-29-03.pdf
- EAP-TLS Deployment Guide for Wireless LAN Networks
  http://www.cisco.com/warp/public/cc/pd/sqsw/sq/tech/acstl_wp.pdf
- Wepcrack
  http://sourceforge.net/projects/wepcrack