LAN Technology

Wireless LAN Protocols

Arash Habibi Lashkari
PHD of Computer Science - Information Security
July 2010

Wireless LAN Protocols

Outlines:

- WLAN: Wireless LAN by IEEE 802.11 Protocols
- IEEE 802.1X: EAP over LAN (EAPOL) for LAN/WAN Authentication and key Management
- IEEE 802.15 and Bluetooth: WPAN Communications
- WiMAX: IEEE 802.16

Why Wireless?

- No cable plant
  - Lower cost!?
  - Rapid deployment
- Enhanced mobility
- Ad hoc relationships

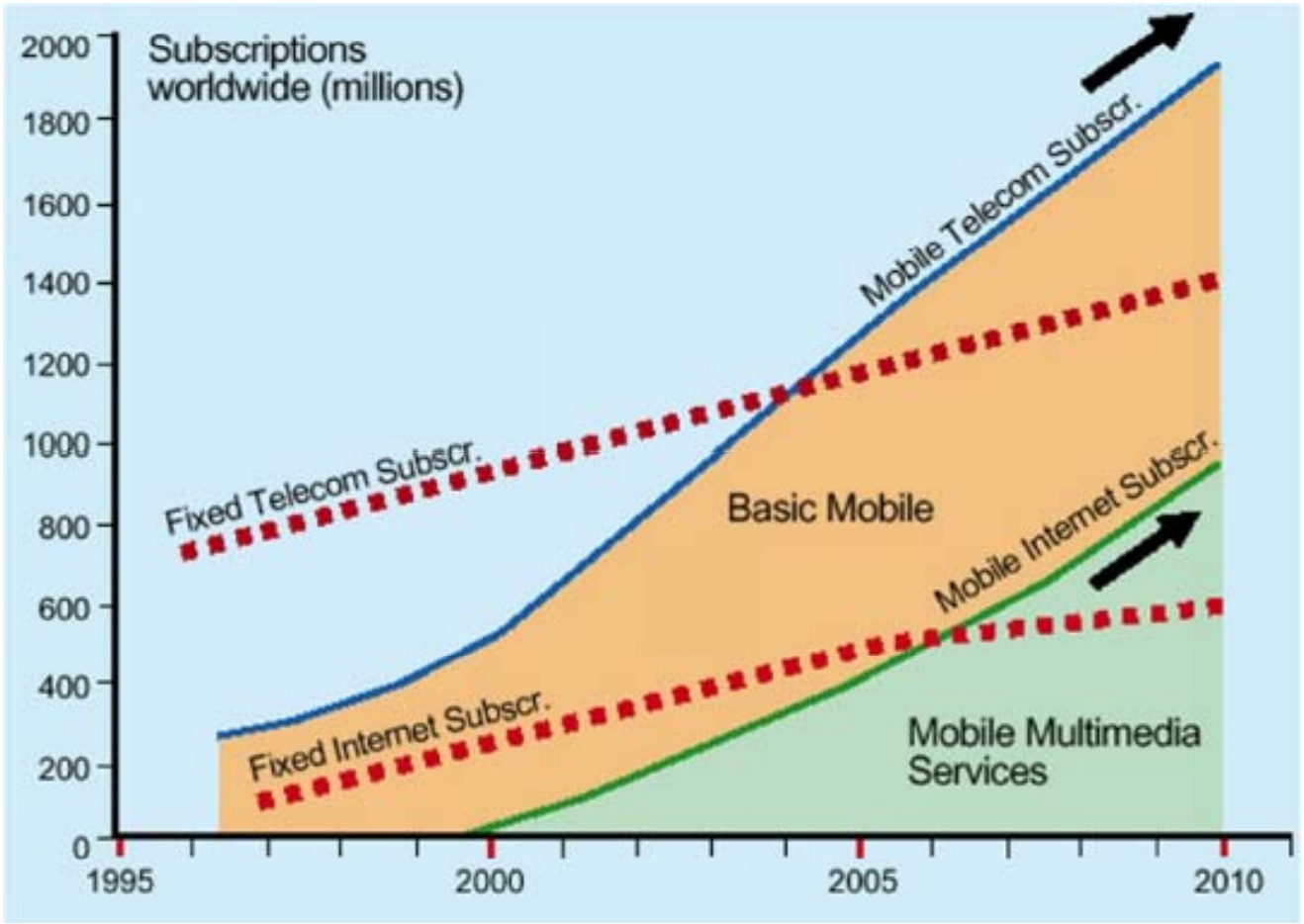
Why not Wireless

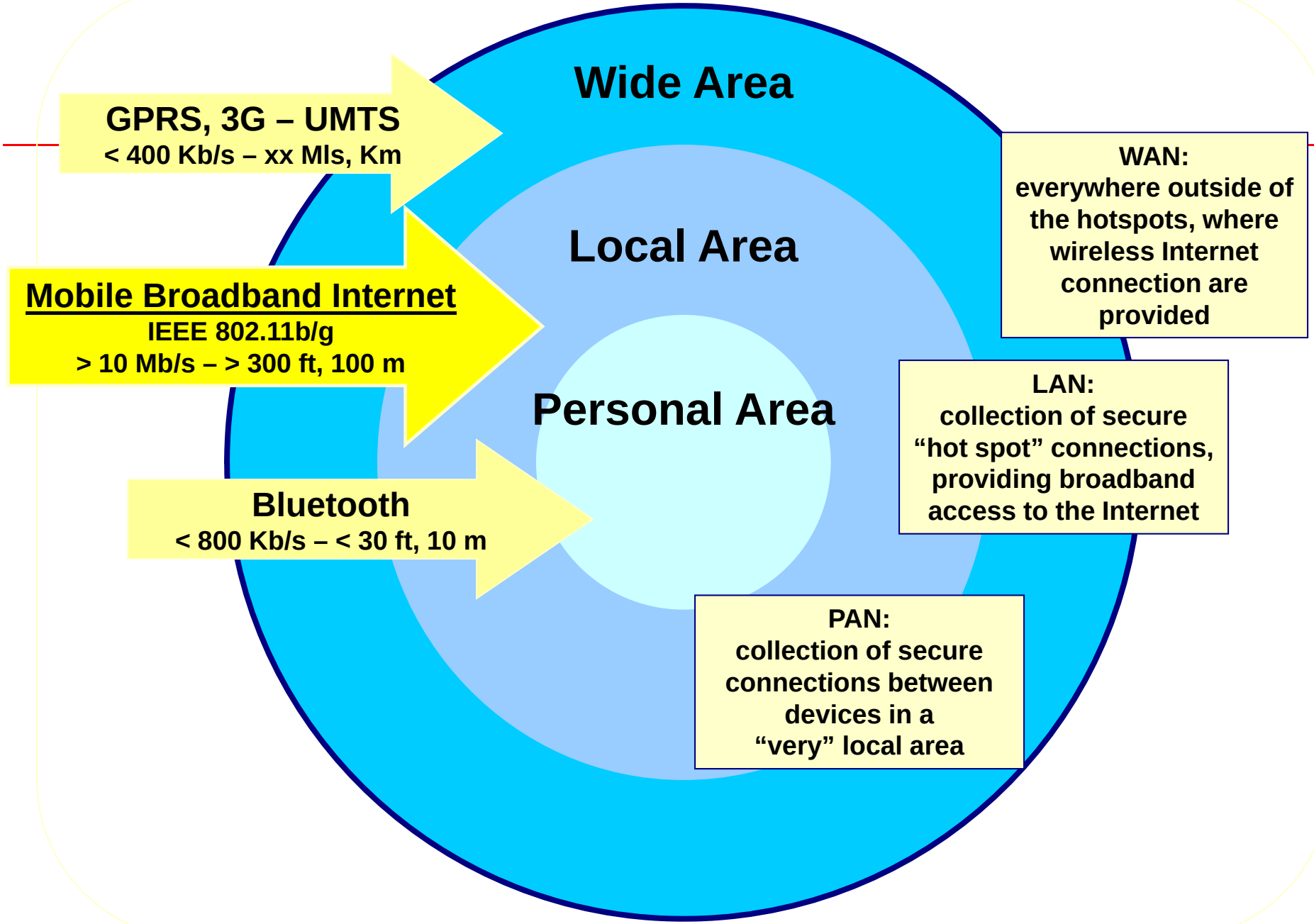
No physical security

Low throughput

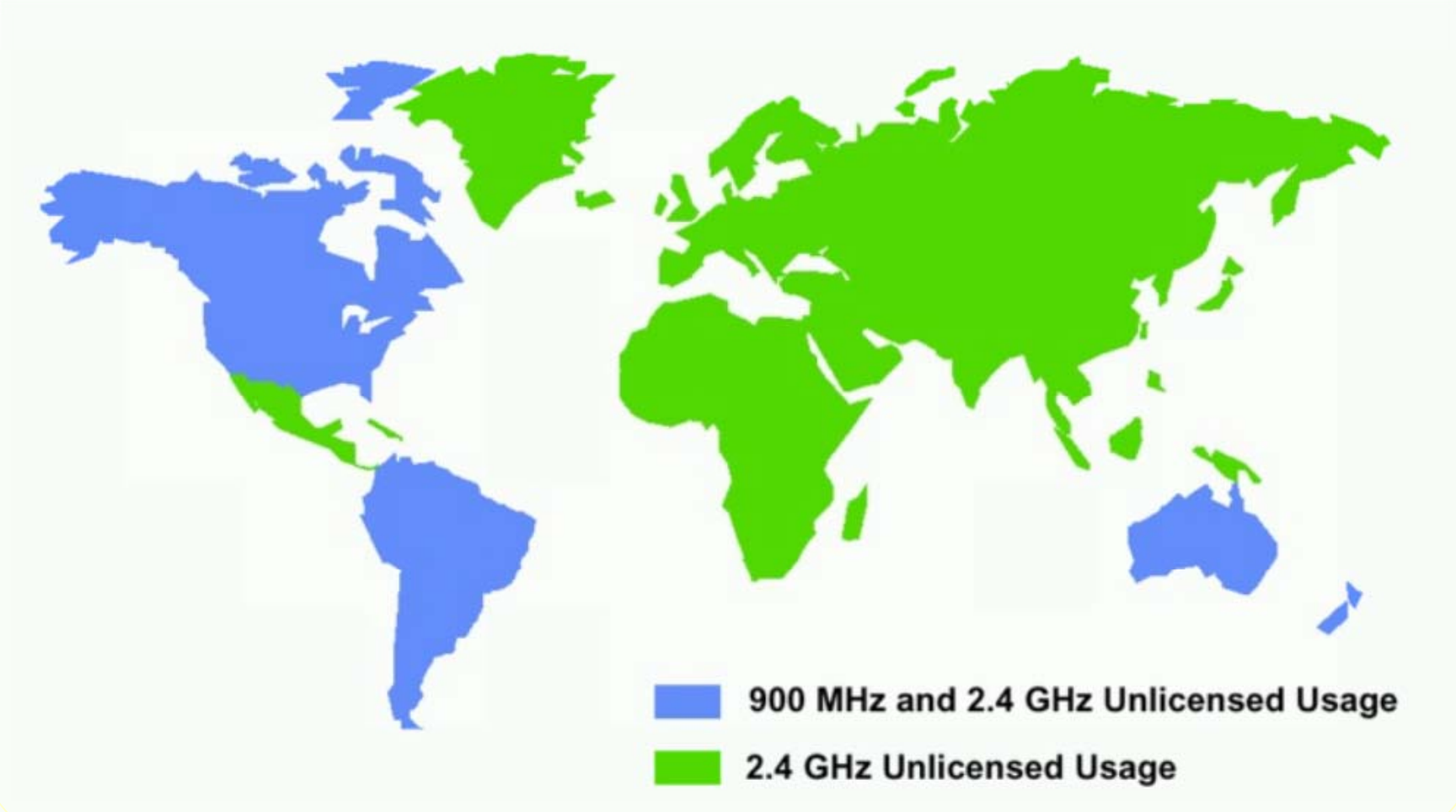
Unregulated, noisy bands

Are We Scared of Wireless?




Wide Area
Local Area
Personal Area
GPRS, 3G – UMTS
< 400 Kb/s – xx Mls, Km
Mobile Broadband Internet
IEEE 802.11b/g
> 10 Mb/s – > 300 ft, 100 m
Bluetooth
< 800 Kb/s – < 30 ft, 10 m
WAN:
everywhere outside of the hotspots, where wireless Internet connection are provided
LAN:
collection of secure "hot spot" connections, providing broadband access to the Internet
PAN:
collection of secure connections between devices in a "very" local area

Global RF Regulations



Wireless LAN Standards IEEE

- IEEE 802.11 group has developed and is continuing to develop WLAN standards
  - Supports both 802.11a and 802.11b radio standards
- 802.11 has chosen to use 802.1x to support access authentication
- Groups of interest for access control are:
  - 802.11i (charged with security improvements)
  - 802.11f (charged with roaming between Access Points)

WLAN Security Concerns

- Authentication
  - Risk of unauthorized access to corporate network from malicious users
- Privacy
  - Risk of eavesdropping on WLAN data traffic
- Encryption
  - One of the weakest point so far

WLAN Security Issues

- Focus on security for WLAN in the news
  - Especially with the successful attacks on WEP
    - Feb 2001: paper from Berkeley on “802.11 Security”
    - Aug 2001: paper by Fluhrer on “WEP weaknesses”
    - Aug 2001: AirSnort software (needs a large amount of data)
- WEP fixes are being worked on by the IEEE 802.11i standards group.
- Some vendors are implementing “improved” but non-standard methods
- Other Wireless methods have parallel issues:
  - Mobile Network (e.g. 3G or 4G Cellular)
  - Local Networks (e.g. Bluetooth)

Introduction to 802.1x

Trade articles call it:

- “Security protocol”
- “Security standard”
- “Authentication method “
- “User authentication protocol”

802.1x is a “Port Based Network Access Control” mechanism

Done at the time a user attaches to the network, not for each packet between STA and AP

Motivation and history for the development of 802.1x:

The increased use of 802 LANs in public and semi-public places

The need for per-port network control

The need for AAA (Authentication, Authorization, and Accounting)

The need to distribute dynamic encryption keys

Terminology in 802.1x

Port

Authenticator

Supplicant

Extensible Authentication Protocol (EAP)

Extensible Authentication Protocol Over LAN (EAPOL)

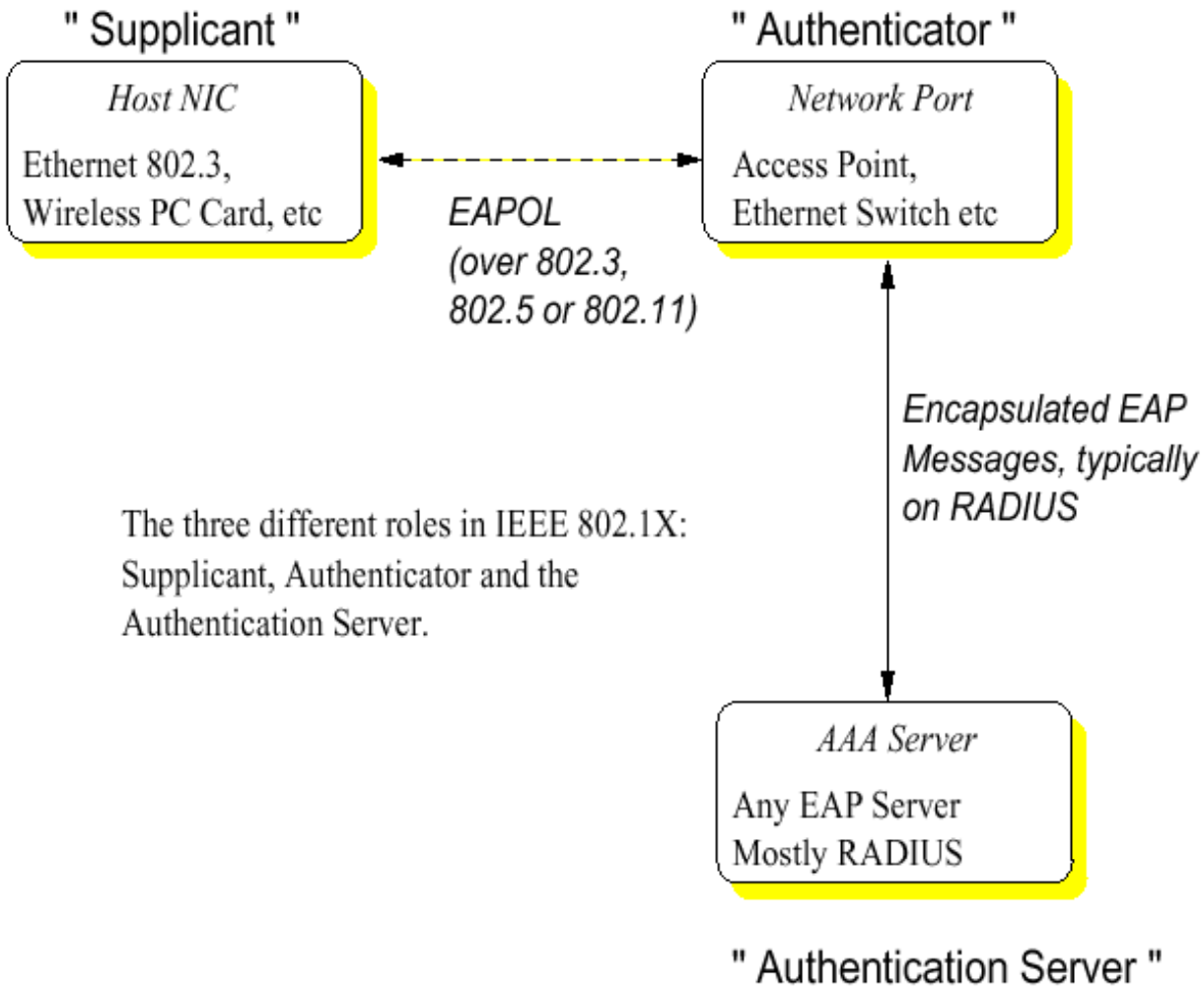
RADIUS

Mutual Authentication

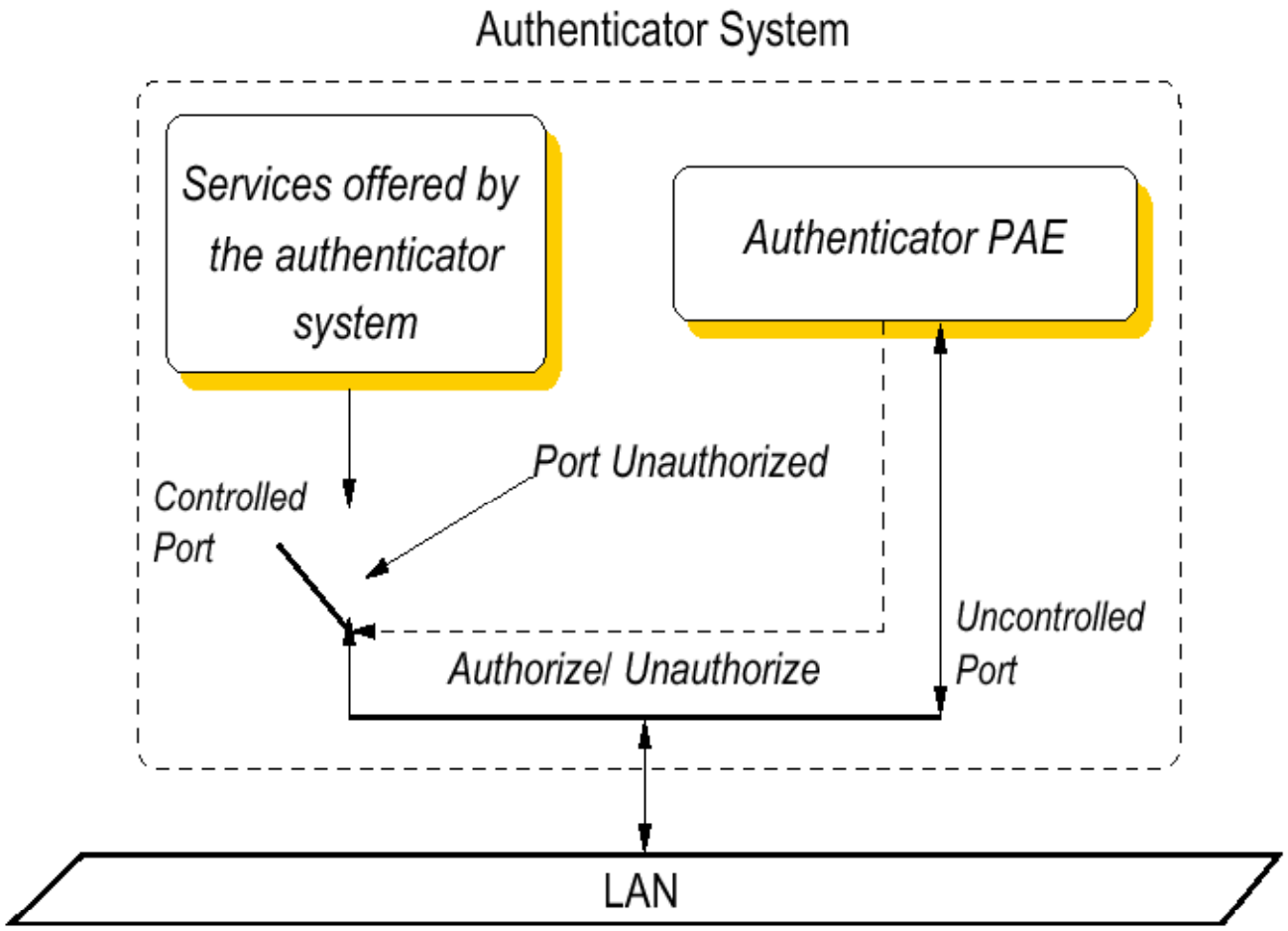
The authentication method used between the Supplicant and the RADIUS should do mutual authentication:

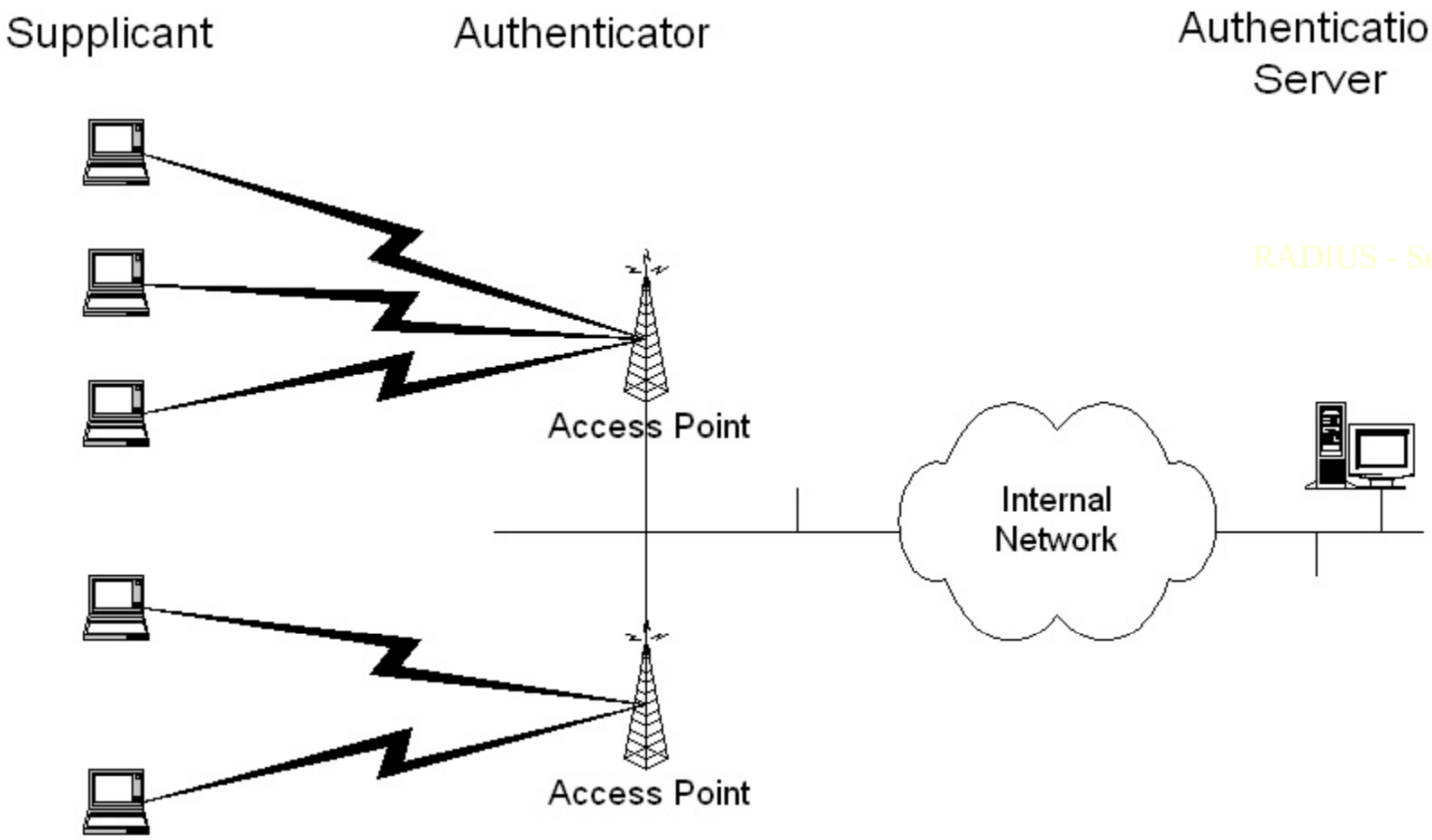
- Supplicant authenticates to RADIUS and RADIUS authenticates to Supplicant
- User is known to service provider, service provider is known to user

802.1x Architecture

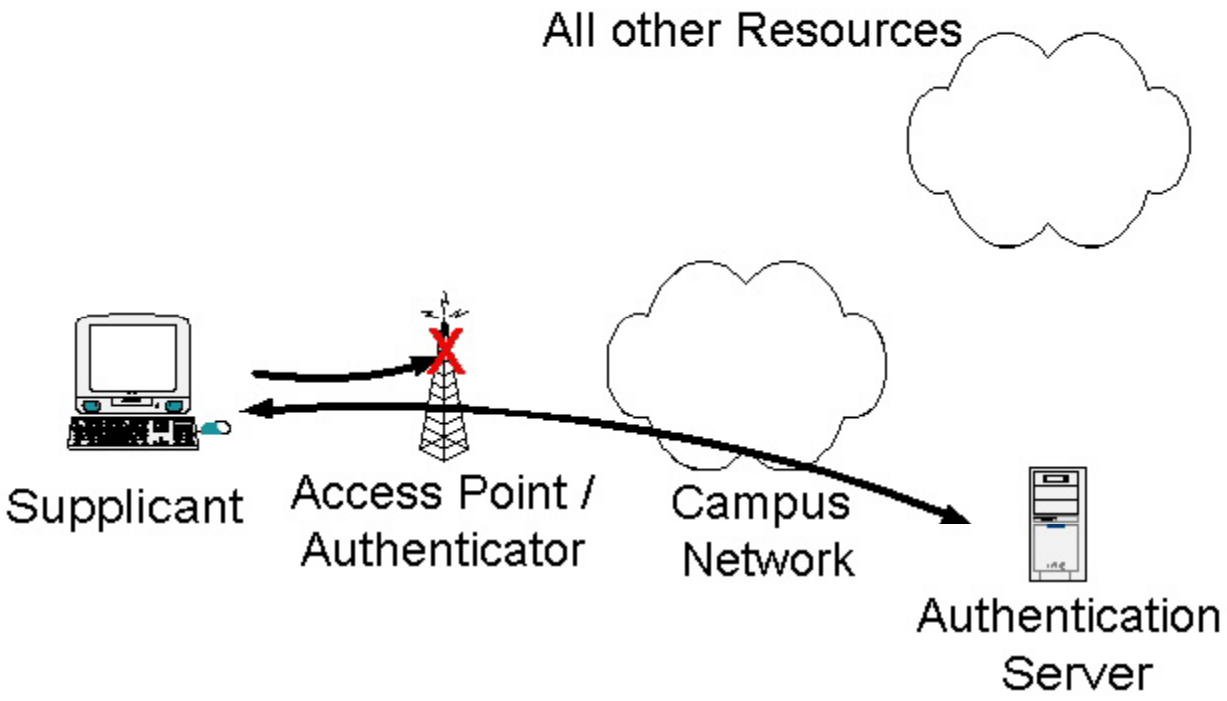


Port Based Authenticator

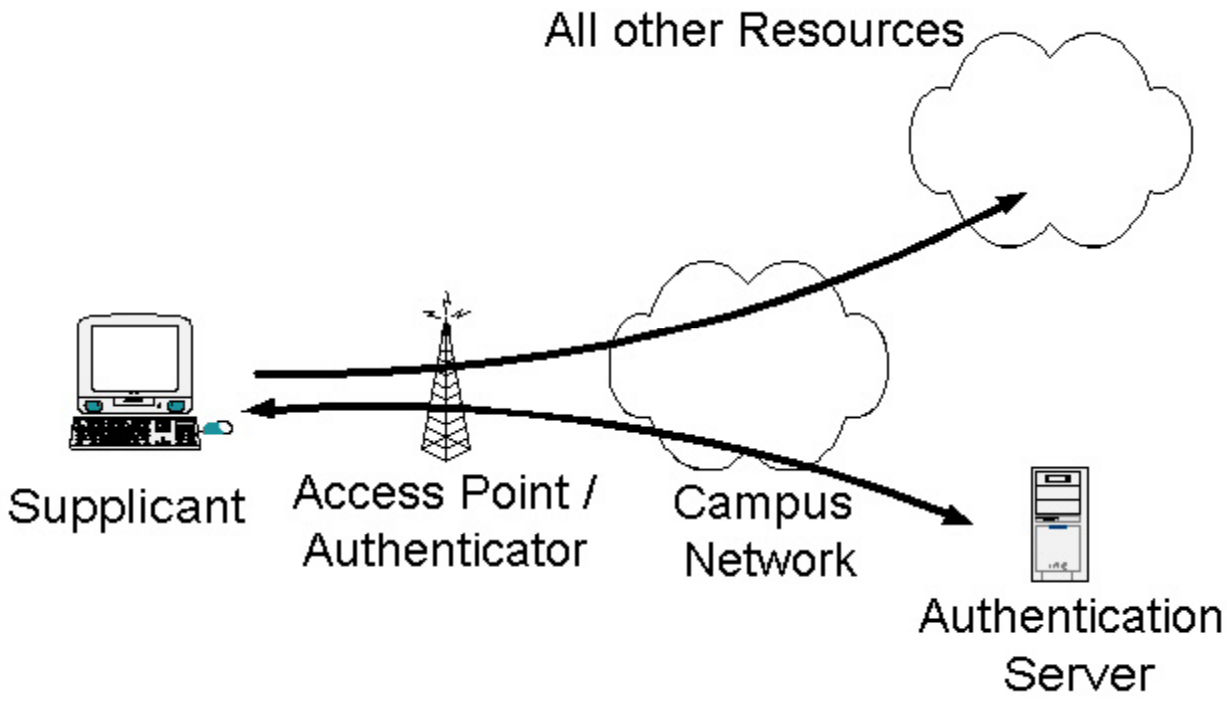


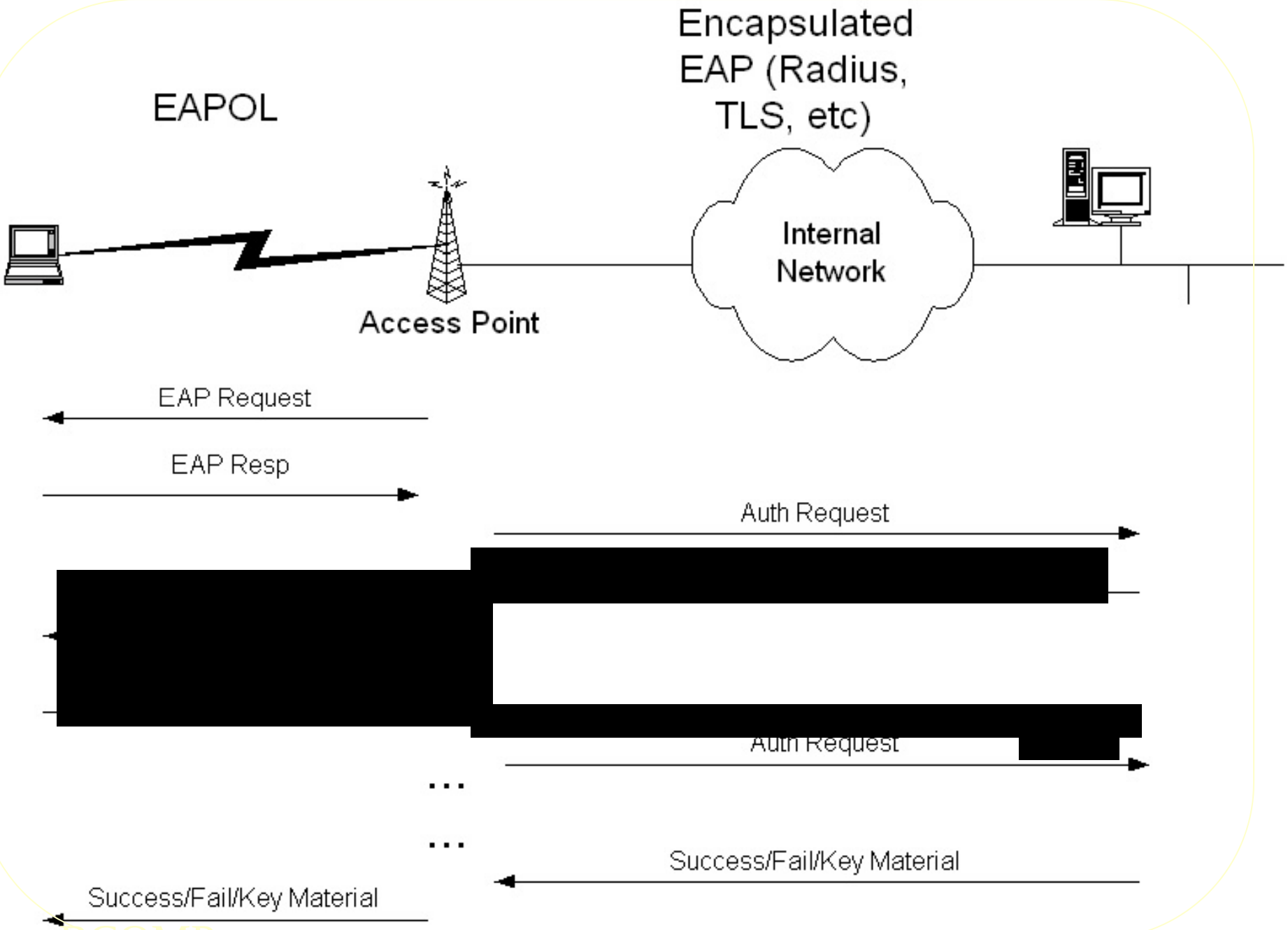


Pre-Authentication State Scenario



Post-Authentication State Scenario




Encapsulated
EAP (Radius,
TLS, etc)
EAPOL
Internal
Network
Access Point
EAP Request
EAP Resp
Auth Request
Auth Request
Success/Fail/Key Material
Success/Fail/Key Material

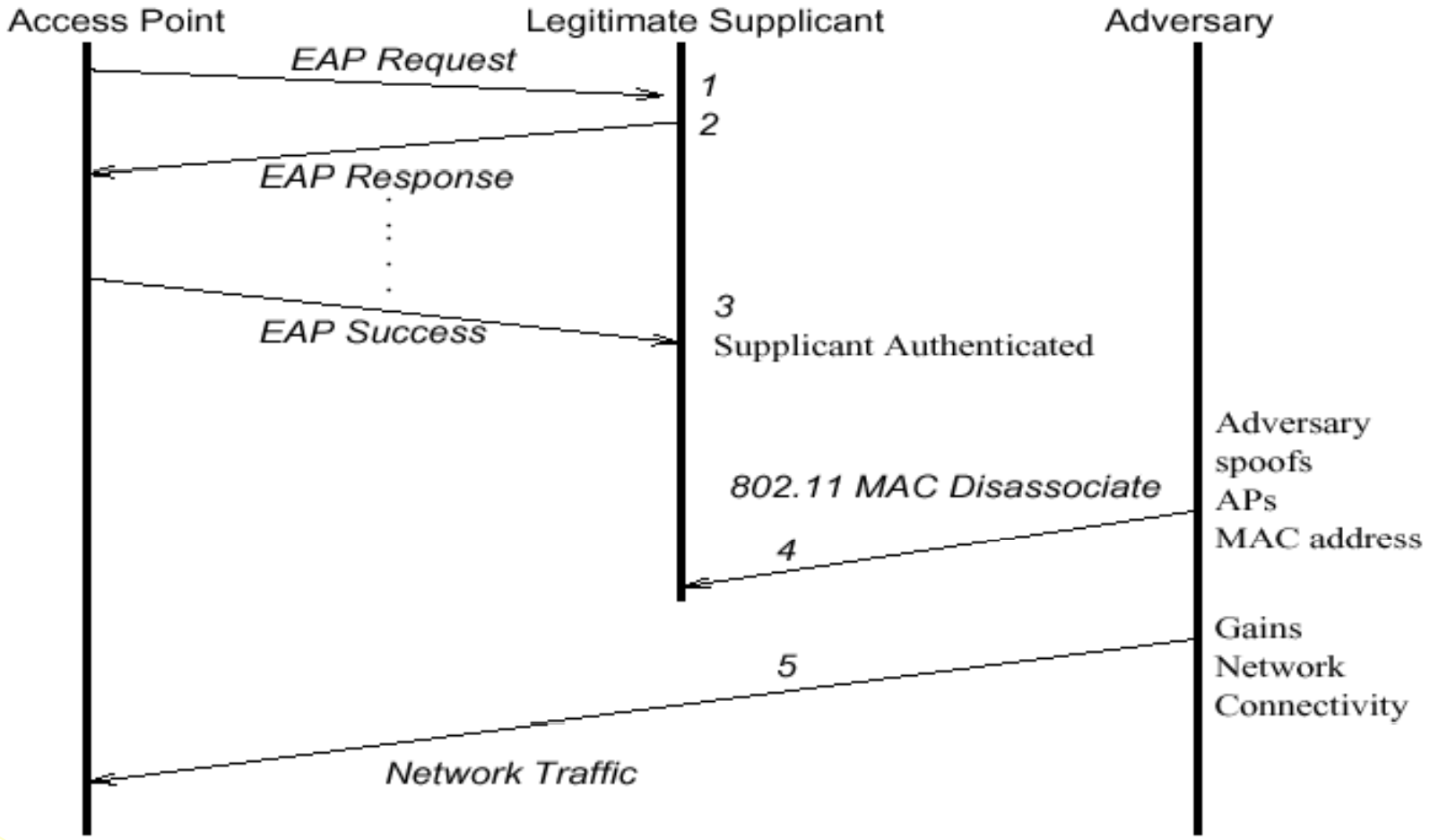
Advantages of using 802.1x in WLAN

- Control at the Network Edge
- Dynamic Session Key Management
- Low Overhead
- Utilizes Open Standards

Disadvantage:

- Hijacking
  - Send disassociate message to client. AP is in the dark

Session Hijack Attack



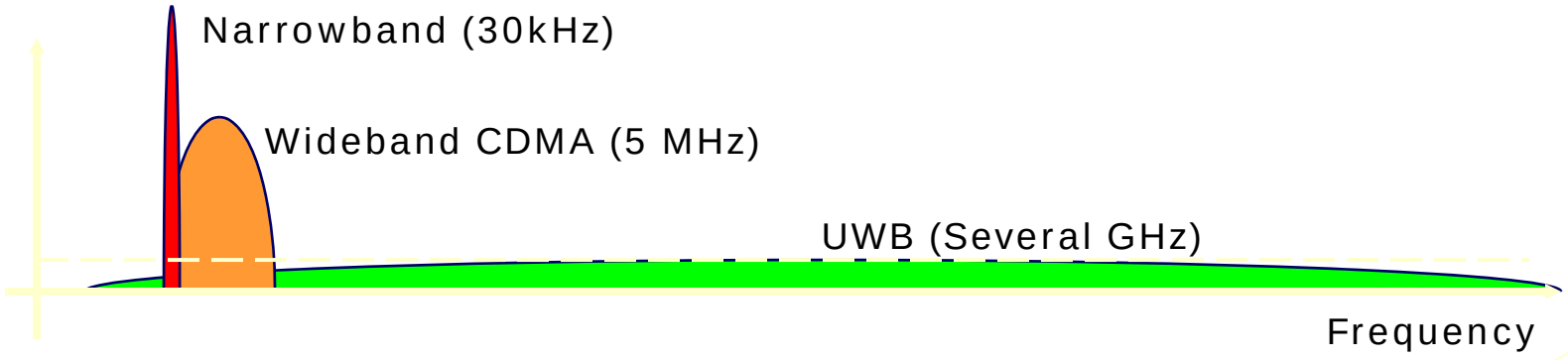
Wireless Future

Gigabit MM Wave Communication

- Rapid frequency expansion above 100 GHz
- Sensitive for weather conditions

UWB (Ultra-WideBand)

- Low Power
- Bluetooth
- Interference problem



Questions