Security aspects in Mobile IPv6

IPv6 Italian Task Force

Torino, 6 luglio 2005

Implementazione del testbed MIPL6 (1/2)

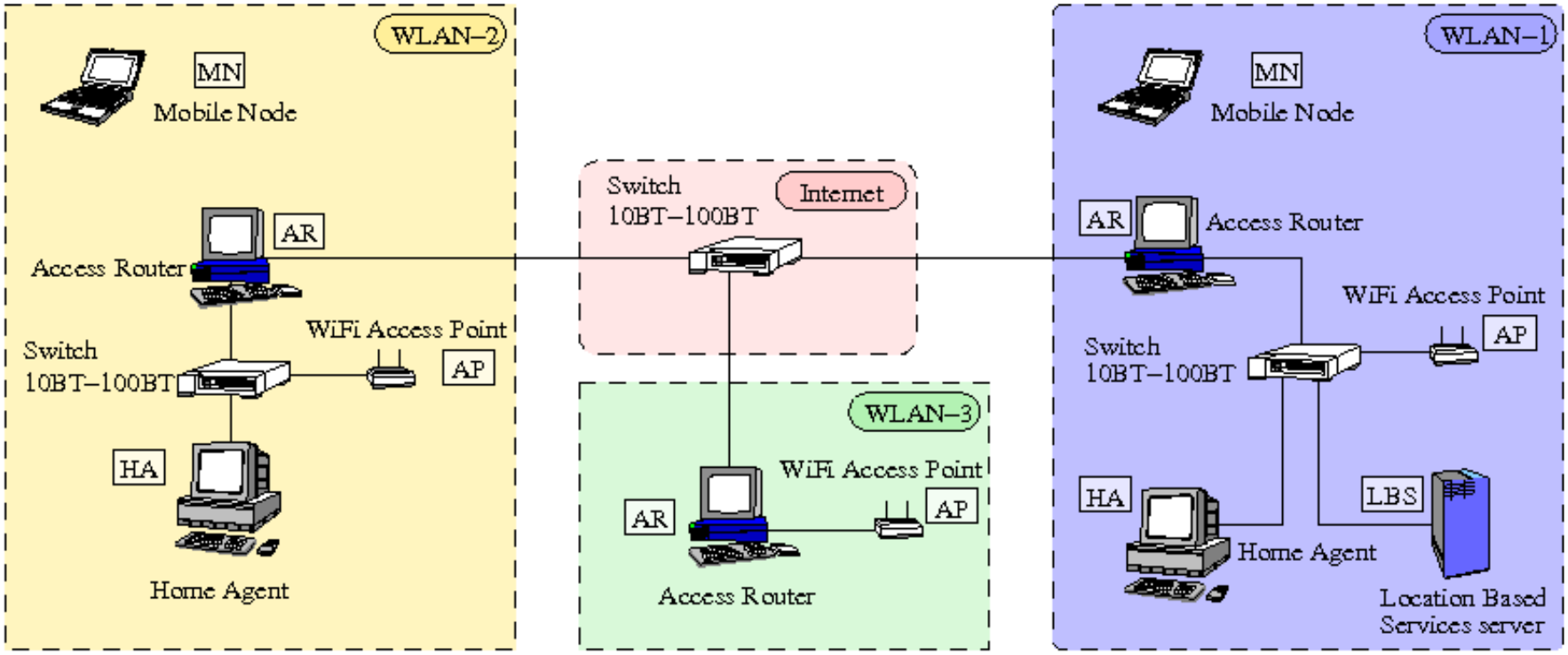
- Testbed Mobile IPv6 Wind
  - implementazione del Helsinki University of Technology (HUT) MIPL6 (Mobile IP for Linux IPv6) versione 1.0
  - patches per kernel Linux 2.4.22
  - utilities per debug/monitoring
- Access Points (AP): IEEE 802.11 WiFi
  - implementazione Open Source SW (OSS): HostAP su Laptop PC + PCcard wireless
  - prodotti commerciali: Cisco series 350 e Linksys
- PCcard wireless: IEEE 802.11 WiFi (MN)
  - prodotti commerciali: Cisco e Linksys

Implementazione del testbed MIPL6 (2/2)

- Elementi della rete Mobile IPv6 (PCs + GNU/Linux):
  - Home Agent (HA)
  - Access Router (AR)
  - Mobile Node (MN)
  - Correspondent Node (CN)

- L’architettura del testbed Mobile IPv6 con i suoi vari elementi e’ illustrata nella Figura sequente

MIPv6 based LAN-WLAN testbed

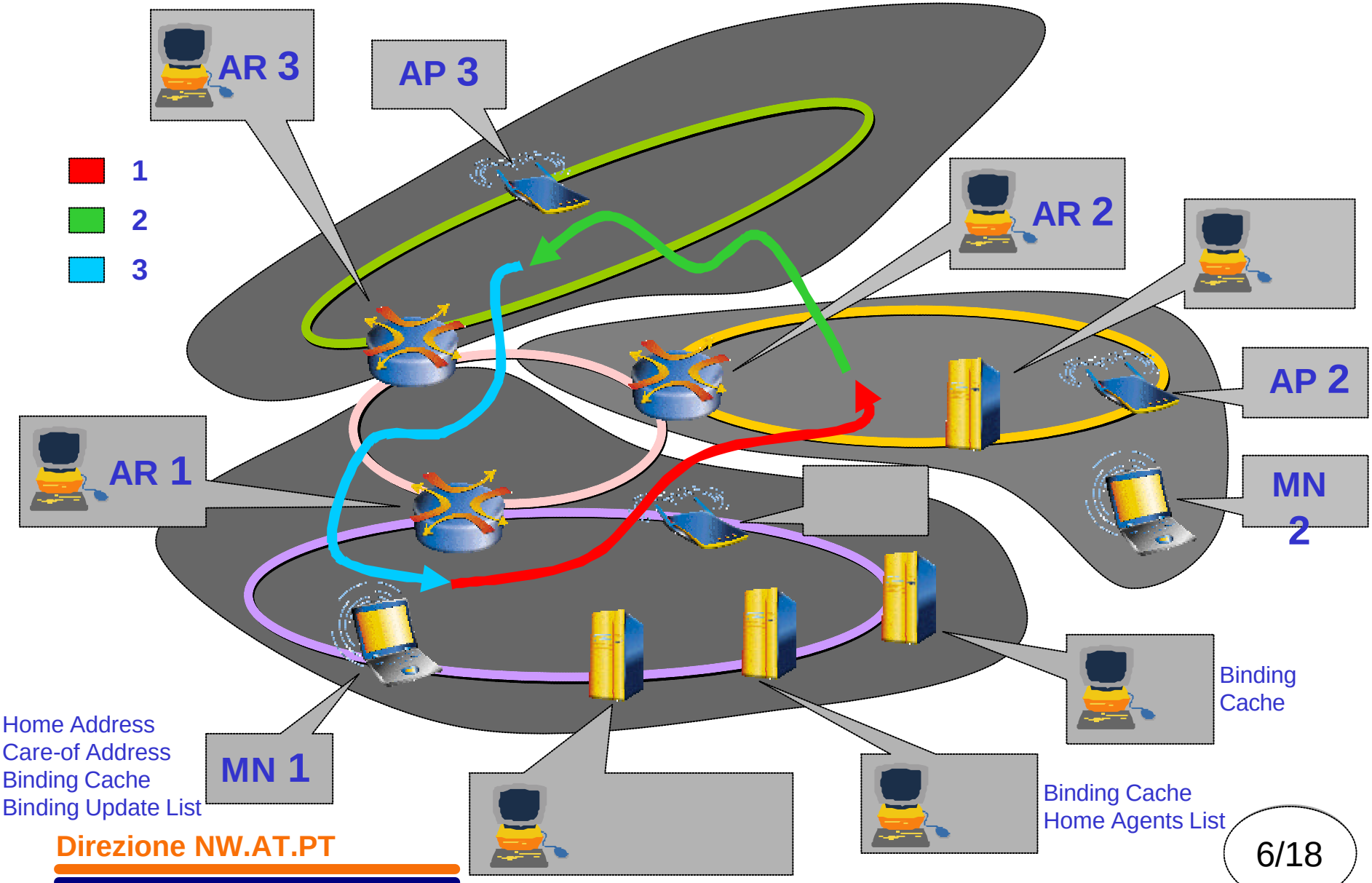


Tests realizzati

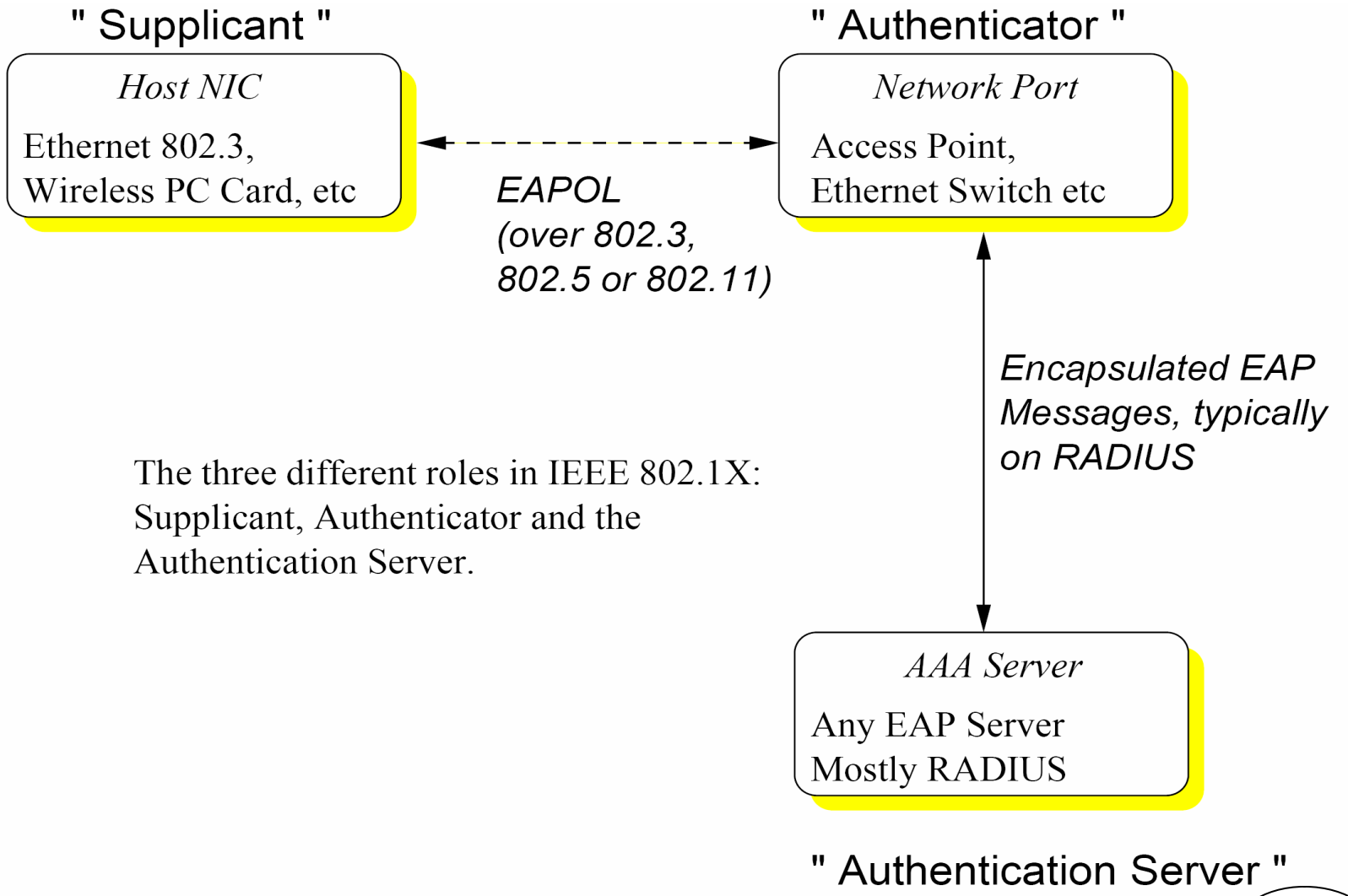
Il testbed MIPL6 ha permesso lo studio di:

- **Mobilita' seamless** tra 3 diverse reti Mobile IPv6 con Handoff orizzontale e studio della continuità della sessione
- **Accesso a servizi in mobilita'**
  - real-time: VoIP e Multimedia Streaming
    - Servizi telefonici basati su VoIP6 con User Agents (UA) OSS "Linphone" e "6Voice"
    - Streaming audio IPv6 OSS "Icecast" + client-player "mp123",
    - Streaming video/audio IPv6 con OSS "VideoLAN"
  - non-realtime: tipicamente Web Browsing, File Transfer, LBS
    - Servizi di localizzazione basati su Location Based Services (LBS) server geografici
- **Verifica e misura del QoS audio** end-to-end con metodologie MOS equivalenti anche durante Handoff orizzontale

Mobilita’ nel testbed MIPv6 LAN-WLAN

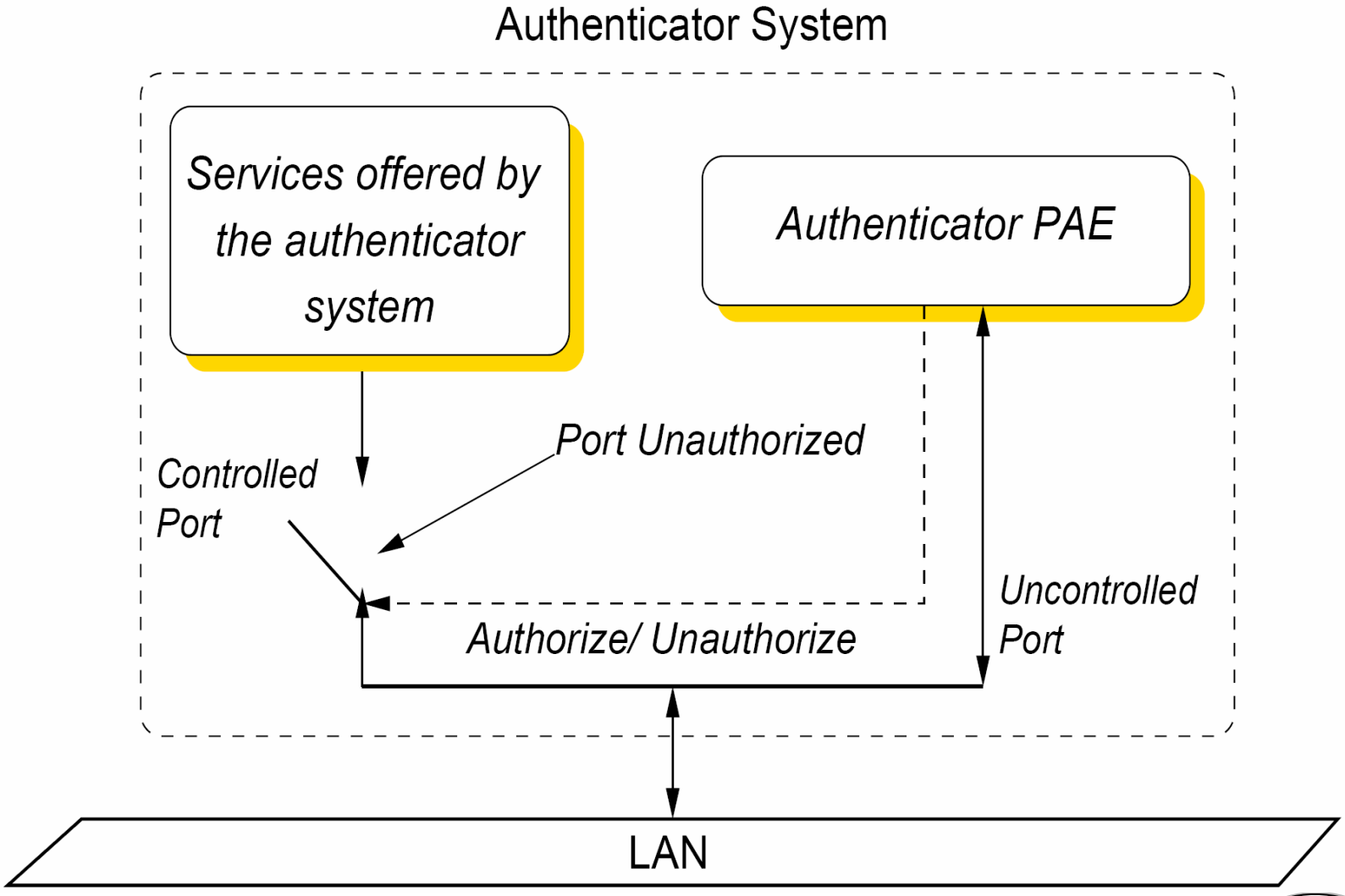


Controllo di Accesso con IEEE 802.1x



The three different roles in IEEE 802.1X: Supplicant, Authenticator and the Authentication Server.

Porte dell'Authenticator



Elementi tipici di IEEE 802.1x

❖ Elementi di IEEE 802.1x:

- Authentication Server: AAA server RADIUS (Remote Authentication Dial In User Service)
  - provvede agli aspetti di AAA della rete
- Authenticator: elemento lato AP
  - elabora le richieste di accesso e in caso di utilizzo di un RADIUS server le trasmette a quest'ultimo
    - **fa da tramite ai messaggi RADIUS tra il client e AAA server**
- Supplicant: elemento lato client
  - richiede autorizzazione di accesso alla rete

Aggiunta degli elementi per AAA (1/2)

Al testbed esistente sono stati aggiunti alcuni elementi SW che permettono l'implementazione e lo studio degli aspetti di **Authentication, Authorization e Accounting (AAA**) della rete Mobile

- Server RADIUS e AAA
  - Principali funzioni del server Radius nell'architettura AAA:
    - **Authentication**: identificazione dell'utente
    - **Authorization**: autorizzazione al rilascio delle risorse
    - **Accounting**: generazione di log degli accessi per tariffazione, configurazione e manutenzione

Aggiunta degli elementi per AAA (2/2)

- Versioni di server RADIUS implementate/testate nel testbed MIPv6 Wind:
  - OSS: “freeradius” (IPv4)
  - Commerciale: “Radiator+Radar” (IPv4+IPv6)
- Alternativa a RADIUS: il nuovo protocollo Diameter

Controllo dell'accesso alla rete wireless

- Standard IEEE 802.1x "Port Access Control"
  - disponibilita' di SW "Supplicant" OSS e la relativa semplicita'/facilita' di installazione
  - 802.1x può essere utilizzato anche per il controllo dell'accesso alle rete wired (LANs):
    - in questo caso si farà uso di una diversa implementazione del "supplicant"

“Supplicant” IEEE 802.1x

- Implementazione di IEEE 802.1x Supplicant con OSS “xsupplicant” su un Laptop PC

- Certificati: commerciali e privati

  - Certificati commerciali non disponibili
    - costi e tempo di acquisizione
    - prime prove con certificati privati (creati manualmente in modo autonomo con utilities di “freeradius”)

  - Possibilità di utilizzo dei certificati Free di “Radiator”

  - Metodi implementati e provati: PEAP, TTLS (TLS)

Il Network Access Server (NAS)

❖ NAS (Network Access Server)

- Il NAS costituisce il **punto di accesso alla rete**
  - NAS nel caso di una WLAN: **Authenticator + Access Point**
- Implementazioni NAS provate:
  - Commerciali: Cisco 350 series
  - OSS: “HostAP”
    - **si e’ dimostrato più funzionale per i nostri scopi di studi, verifiche e implementazioni essendo “aperto”**
- Possibili evoluzioni di “HostAP” verso IPv6 previste nei prossimi mesi

❖ HostAP

- NAS (Authenticator + AP bridge) OSS
  - Elementi costituenti: driver, daemon e utilities
  - Requisiti hardware: PCcard wireless con chipset Prism2, -2.5 o -3 (tipo utilizzato: Linksys WPC11)

- Alcuni dei metodi EAP supportati
  - EAP-TLS
  - EAP-PEAP
  - EAP-TTLS
  - EAP-SIM
  - EAP_PAX (experimental)

Palmare “Communicator” Nokia 9500

- Tests di autenticazione con il palmare “Communicator” Nokia 9500
  - Accesso alla rete WiFi con meccanismi di autenticazione e encryption tramite AP:
    - Commerciali: Cisco series 350 e/o Linksys
    - OSS: “HostAP”
- I meccanismi di encryption provati finora sono sostanzialmente secondo WiFi Protected Access (WPA):
  - evoluzione con chiavi dinamiche del meccanismo di encryption originale di IEEE 802.11, Wire Equivalent Privacy (WEP)

Evoluzioni e sviluppi futuri

- Patch di “HostAP” per IPv6
- Utilizzo e test di Radiator + Radar in IPv6
- Passaggio da AAA server RADIUS a Diameter
- Implementazione della versione 2.0 di MIPL6
- Utilizzo di IEEE 802.11i / RSN (WPA2)
- Tests di Handover verticale con Nokia 9500
- Introduzione di altre tecnologie di accesso per l’estensione del “web” nel nostro testbed:
  - Power Line Communications (PLC)
  - IEEE 802.16 WiMAX
- Ulteriori test di servizi e AAA con i nuovi scenari

Roberto Bertoldi

WIND Telecomunicazioni S.p.A.
Viadotto XXV Aprile 9,
10015 Ivrea (TO), Italy

http://www.wind.it
e-mail: **roberto.bertoldi@mail.wind.it**