



# CASPUR

Consorzio interuniversitario per le Applicazioni di Supercalcolo Per Università e Ricerca

## Provinciawifi

Metro Ethernet e Wireless ISP Virtuali Open Source

Maurizio Goretti - Davide Guerri

---

# Cos'è CASPUR?

# Cos'è CASPUR?

Consorzio inter-Universitario

- ▶ CASPUR è un consorzio Interuniversitario per il calcolo scientifico di cui fanno parte tutte le Università pubbliche Romane



# Cos'è CASPUR?

## Rapporti con la Pubblica Amministrazione

---

- ▶ CASPUR da sempre ha stretti rapporti con la pubblica amministrazione centrale e locale



Avvocatura dello Stato



Comune di Roma

 Camera dei deputati



MINISTERO  
PER I BENI E  
LE ATTIVITÀ  
CULTURALI



PROVINCIA  
DI ROMA



Presidenza del Consiglio dei Ministri

# Cos'è CASPUR?

## Crocevia Internet italiana

---

### ▶ CASPUR ospita

- ▶ il PoP romano dei maggiori Carrier operanti in Italia
- ▶ La sede PoP GARR Roma
- ▶ Il punto di Interscambio NaMeX



- [BT Italia](#)
- [Cogent Communications](#)
- [Colt Telecom](#)
- [Eutelia](#)
- [Fastweb](#)
- [Global Crossing](#)
- [Infracom](#)
- [Interoute](#)
- [MC-link](#)
- [Retelit](#)
- [TATA Communications](#)
- [Telecom Italia](#)
- [Telefonica International](#)
- [Unidata](#)
- [Wind](#)

# Sommario

---

- ▶ **Federazione di reti Wi-Fi e Access Point Linux-based (GARR WS08)**
  - ▶ Dove eravamo rimasti
  - ▶ Cos'è successo dopo
- ▶ **Provinciawifi**
  - ▶ Il progetto
  - ▶ Il ruolo di CASPUR
  - ▶ Aspetti Tecnici
  - ▶ Aspetti Normativi
- ▶ **Altri progetti e sperimentazioni**
  - ▶ Rete Unica degli Atenei di Roma

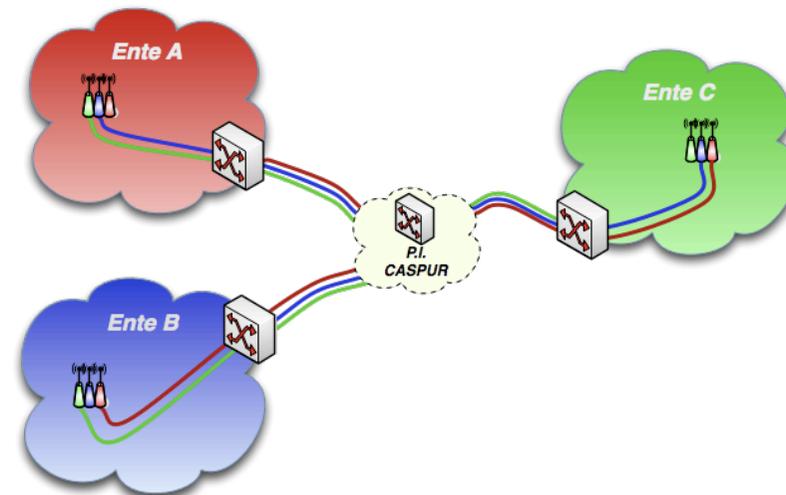
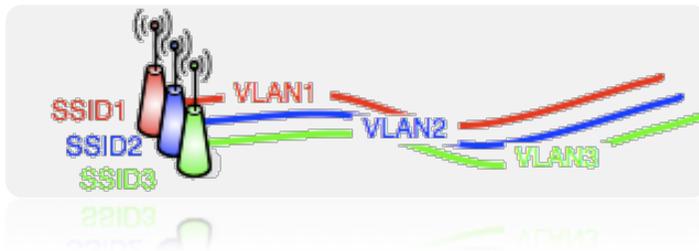
---

# Federazione di reti Wi-Fi e AP Linux-based

# Federazione di reti Wi-Fi e AP Linux-based

## Dove eravamo rimasti (GARR WS08) (1 / 4)

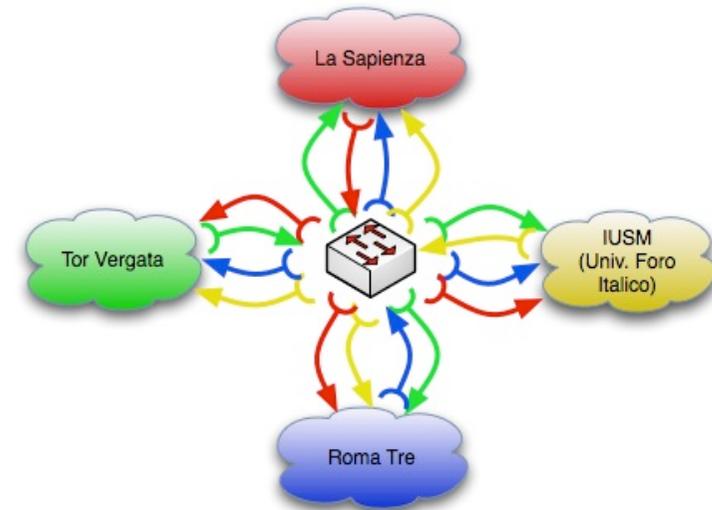
- ▶ Durante lo scorso Workshop GARR abbiamo presentato un modello di federazione di reti Wi-Fi basato su
  - ▶ multiple-SSID sugli apparati di accesso
  - ▶ alcuni servizi e strumenti gestiti, neutralmente, da CASPUR
    - ▶ Punto di interconnessione Layer 2 per reti Wi-Fi
    - ▶ Access Point con firmware personalizzato



# Federazione di reti Wi-Fi e AP Linux-based

Dove eravamo rimasti (GARR WS08) (2/4)

- ▶ Punto d'interconnessione L2 per reti Wi-Fi
  - ▶ un'infrastruttura di switching per l'interscambio di VLAN tra
    - ▶ gli atenei consorziati con il CASPUR (in particolare le 4 Università pubbliche di Roma)
    - ▶ enti esterni (e.g.: annuncio della rete Wi-Fi de "La Sapienza" sull'infrastruttura Romawireless)



# Federazione di reti Wi-Fi e AP Linux-based

Dove eravamo rimasti (GARR WS08) (3/4)

---

- ▶ **Access Point con firmware personalizzato**
  - ▶ Laddove non è possibile inoltrare il layer 2, abbiamo proposto l'utilizzo di AP progettati e realizzati da CASPUR
  - ▶ Anche attraverso la Rete pubblica, gli AP instaurano una VPN con il concentratore sito nel punto di interconnessione
    - ▶ le VPN sono in grado di incapsulare frame 802.1Q
    - ▶ è richiesta solo connettività Internet (anche con Firewall e NAT)
  - ▶ È possibile “annunciare” più di una rete mediante multiple-SSID
    - ▶ Ogni Virtual-AP è in bridging con una differente VLAN



# Federazione di reti Wi-Fi e AP Linux-based

## Dove eravamo rimasti (GARR WS08) (4/4)

---

### ▶ Modello di federazione “link-layer”

#### ▶ PROs

##### ▶ Flessibilità

- Può essere utilizzato qualsiasi sistema di controllo dell'accesso alla rete

##### ▶ Controllo completo dell'AAA e del traffico L2 degli utenti da parte dell'ente d'appartenenza

- L'indirizzamento IP e le politiche di utilizzo della rete sono stabilite dall'ente cui la rete Wi-Fi appartiene (non quello dell'ente ospitante)

- **Reti Wi-Fi pubbliche ospitabili in sedi prive delle infrastrutture per l'identificazione degli utenti e la data retention a norma di legge**

#### ▶ CONs (...alcuni risolti)

##### ▶ Scalabilità

- Ethernet non è pensato per reti con estensione geografica
- Numero di ESSID limitati
- Necessità di apparati d'accesso con supporto per multiple-SSID (uno per afferente)

##### ▶ Sicurezza

- Più difficile il controllo rispetto ad una LAN, tuttavia non è obbligatorio “propagare” un singolo dominio di broadcast L2

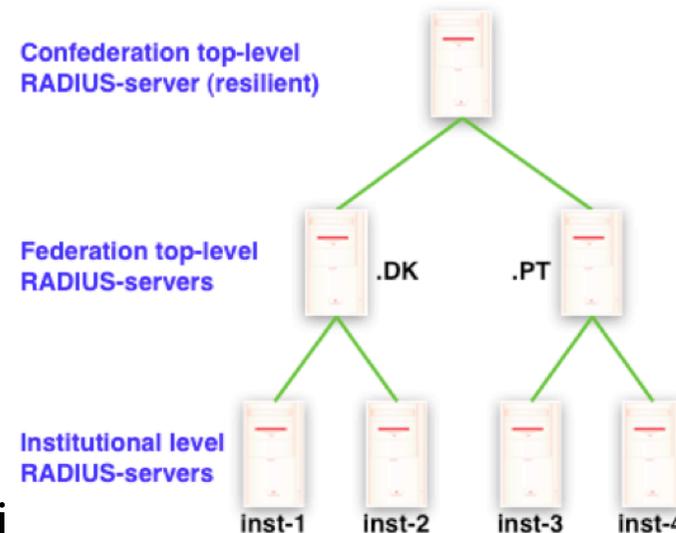
##### ▶ Costi/Fattibilità dell'afferire al punto d'interconnessione

# Federazione di reti Wi-Fi e AP Linux-based

## Ma non c'è già EDUROAM? (1/2)

### ▶ EDUROAM

- ▶ Progetto per la federazione delle reti Wi-Fi degli enti di ricerca
- ▶ Confederazione mondiale, riservata agli enti serviti dagli NRENs(\*)
- ▶ Basata su gerarchia di proxy RADIUS e 802.1x
  - ▶ Gli utenti si autenticano per mezzo di EAP (TLS, TTLS, PEAP, ...) sulla propria infrastruttura di autenticazione



(\*) "The use of eduroam is restricted to the closed community served by NRENs according to their national policies" -- *European eduroam confederation policy* [1]

# Federazione di reti Wi-Fi e AP Linux-based

## Ma non c'è già EDUROAM? (2/2)

---

- ▶ Il modello di federazione L2 proposto ha finalità e scope differenti
  - ▶ Propone un modello per il trasporto delle reti Wi-Fi
  - ▶ Lo scopo della federazione delle reti Wi-Fi degli atenei **non è solo** quello di fornire un servizio alle università consorziate con il CASPUR
- ▶ Ufficiale la convenzione dei 4 atenei pubblici di Roma con il CASPUR per
  - ▶ Annuncio reciproco delle rispettive reti Wi-Fi
  - ▶ **Accordi con realtà non accademiche**. In particolare:
    - ▶ Biblioteche Comunali di Roma (i.e.: Biblioteche Senza Filo)
    - ▶ Biblioteche Nazionali
    - ▶ Comune di Roma (i.e.: Romawireless)
    - ▶ Provincia di Roma (i.e.: Provinciawifi)
  - ▶ Altri accordi in cantiere
- ▶ Una rete la cui autenticazione è gestita dai meccanismi utilizzati da EDUROAM, può essere annunciata sugli AP proposti
  - ▶ Questa soluzione permetterebbe l'utilizzo dell'infrastruttura di autenticazione centrale della istituzione afferente ad EDUROAM
    - ▶ E.g.: distaccamenti, sedi remote, ...

---

# Cos'è successo dopo

# Federazione di reti Wi-Fi e AP Linux-based

## Evoluzione dell'infrastruttura (1 / 3)

---

- ▶ L'architettura si è “evoluta” anche per dare connettività nell'ambito di alcuni eventi e manifestazioni
  - ▶ Il link layer distribuito agli access point tramite le VPN viene utilizzato da una rete gestita mediante un captive portal
    - ▶ Il captive portal risiede su una macchina virtuale
    - ▶ Il captive portal e policy di firewalling sono personalizzate per lo specifico evento
    - ▶ Autorizzazione, Autenticazione ed Accounting sono gestiti tramite RADIUS
      - Con applicazioni ad-hoc per la generazione batch delle credenziali
  - ▶ Partendo da alcuni “template” la generazione dell'infrastruttura di rete e di autenticazione è estremamente rapida

# Federazione di reti Wi-Fi e AP Linux-based

## Evoluzione dell'infrastruttura (2/3)

---

- ▶ Anche per gli apparati di accesso ci sono state alcune evoluzioni
  - ▶ Sperimentati(\*) AP estremamente compatti e leggeri basati sul WiSoC Atheros (Atheros AR2317 @180Mhz, architettura MIPS)
    - ▶ OpenWRT con openVPN
    - ▶ Radio 802.11bg con supporto per il multiple-SSID



(\*) in collaborazione con Unidata S.p.A. Oggi in produzione per Provinciawifi e Romawireless.



---

# Provinciawifi

# Provinciawifi

## Il progetto

---

- ▶ Quest'ultimo modello, per la sua flessibilità, ha attirato l'attenzione della Provincia di Roma per il progetto di diffusione delle reti Wi-Fi sul territorio
  - ▶ In quanto risolve alcune problematiche introdotte dalla vigente normativa italiana in fatto di reti di accesso ad Internet per il pubblico.
- ▶ Il progetto, battezzato “Provinciawifi”, è al centro del “Pianoinnovazione” proposto dalla Provincia di Roma
  - ▶ Fornire connettività pubblica e gratuita in **121 Comuni**
  - ▶ Installare **500 hotspot** entro la fine del 2010
  - ▶ “Provinciawifi” vuole essere principalmente uno stimolo alla lotta al digital divide
- ▶ Per raggiungere questi obiettivi si è deciso di utilizzare anche infrastrutture di rete preesistenti
  - ▶ In alcuni casi gli AP utilizzano infrastrutture di rete derivate da progetti finanziati dalla Provincia
  - ▶ Più frequentemente gli AP utilizzano le reti dei Comuni
    - ▶ Reti non aperte al pubblico
    - ▶ E.g.: Punti Informazione Turistica, LAN degli uffici Municipali, ...

# Provinciawifi

## Il ruolo di CASPUR (1/3)

---

- ▶ **La Provincia di Roma, verso la fine del 2008, ha chiesto a CASPUR**
  - ▶ la progettazione e la messa in produzione dell'infrastruttura di rete, di sicurezza e dei servizi per “provinciawifi”
  - ▶ Il coordinamento tecnico degli enti incaricati delle installazioni
  - ▶ La gestione tecnica di tutta l'infrastruttura
- ▶ **L'ISP gestito da CASPUR (INROMA) è diventato anche un W-ISP**
  - ▶ Prendendosi quindi carico degli oneri derivanti dalle vigenti normative in fatto di reti Wi-Fi pubbliche

# Provinciawifi

## Il ruolo di CASPUR (2/3)

---

- ▶ Nei primi tre mesi di affidamento, prima dell'inaugurazione di Provinciawifi, CASPUR ha progettato e realizzato
  - ▶ Il prototipo di un firmware per gli apparati di accesso, derivato dall'esperienza pregressa
  - ▶ il prototipo dell'infrastruttura centrale
    - ▶ Concentrazione delle VPN
    - ▶ Captive Portal su infrastruttura di virtualizzazione
    - ▶ Sistema di auto-registrazione degli utenti
  - ▶ Il prototipo dell'infrastruttura di monitoraggio degli AP
- ▶ Contestualmente, CASPUR ha coordinato l'installazione dei primi 45 apparati (30 da interno e 15 da esterno)

# Provinciawifi

## Il ruolo di CASPUR (3/3)

---

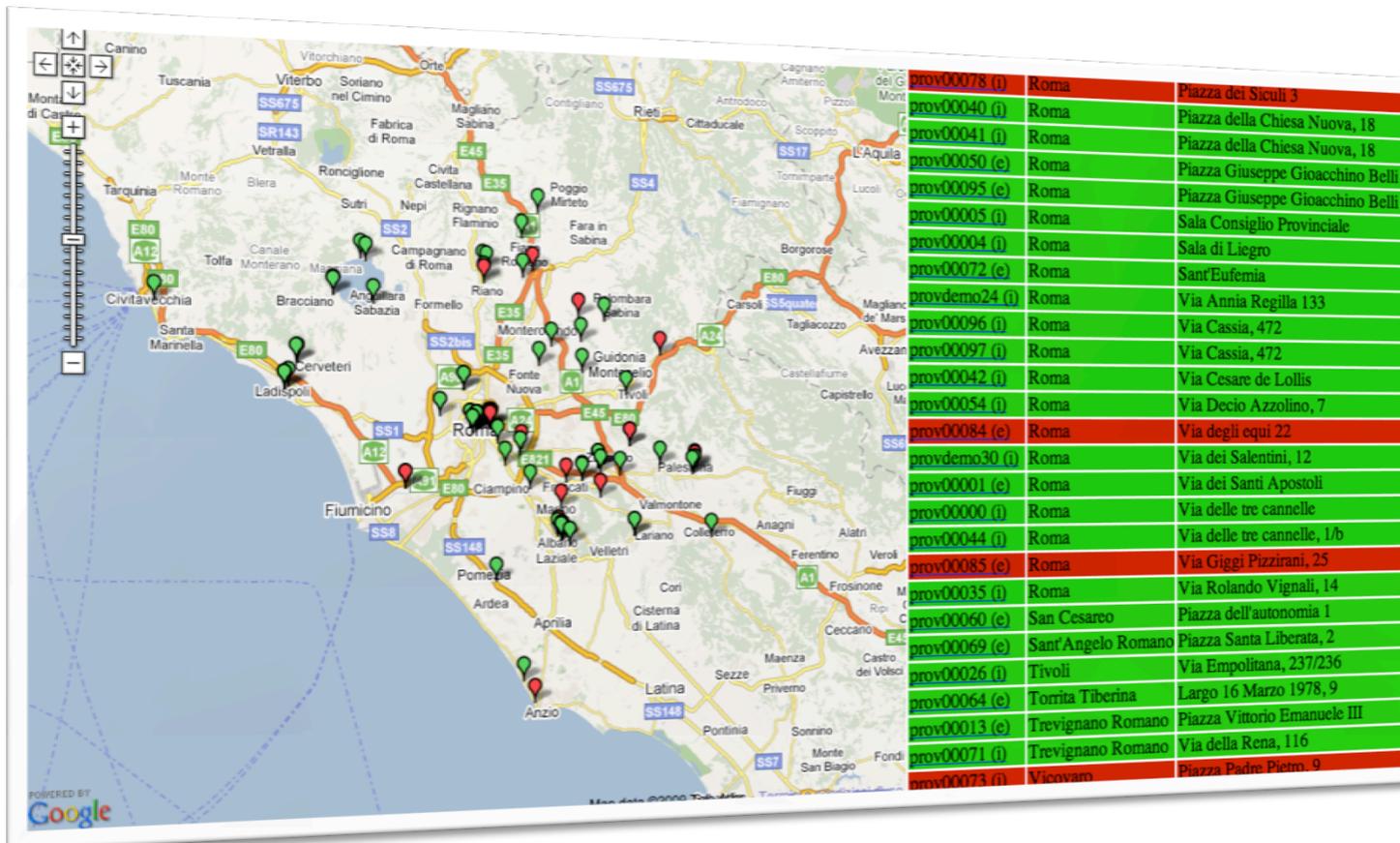
### ▶ Oggi

- ▶ Tutti i sistemi centrali sono stati ridonati con clustering per HA
- ▶ Per far fronte all'elevato numero di AP da installare e mantenere
  - ▶ Formalizzazione delle procedure per la gestione degli aspetti tecnici e amministrativi legati alla distribuzione/manutenzione degli apparati di accesso
  - ▶ Realizzazione di un sistema di autoprovisioning dei parametri di configurazione degli apparati di accesso
  - ▶ Progettazione di un firmware in grado di rendere estremamente semplice l'installazione e la gestione degli apparati
- ▶ E' stato inoltre istituito un helpdesk di secondo livello
  - ▶ Supporto alle installazioni
  - ▶ Risoluzione delle problematiche tecniche specifiche dell'infrastruttura

# Provinciawifi

## Lo stato del sistema (1/2)

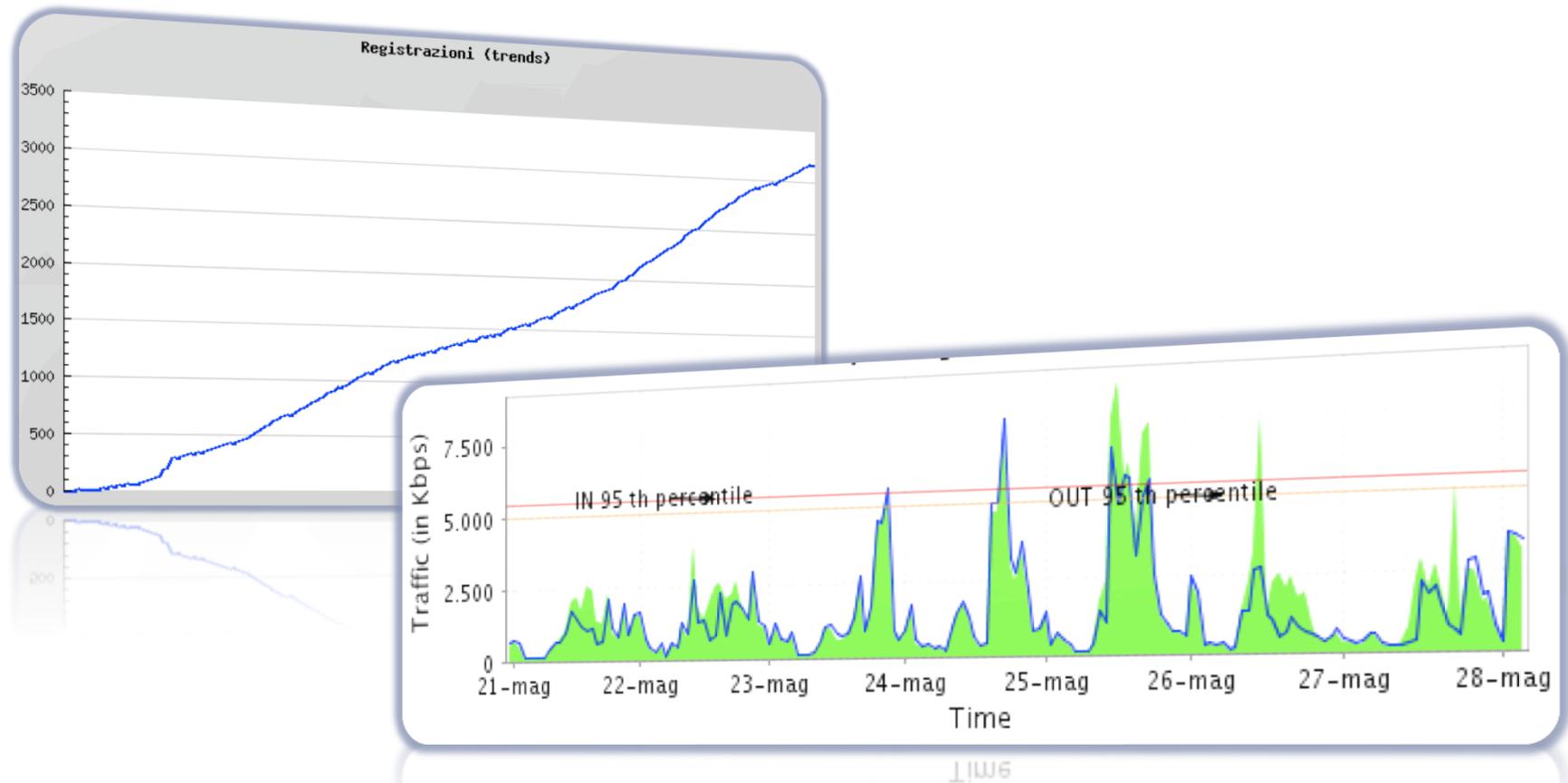
- ▶ Dopo circa 8 mesi
  - ▶ Sono stati installati quasi 120 hotspot in circa 40 Comuni



# Provinciawifi

## Lo stato del sistema (2/2)

- ▶ 3200 utenti registrati, in forte crescita
- ▶ 5Mbps di banda media con picchi “sostenuti” fino a 10Mbps



# Provinciawifi

## Aspetti Tecnici

---

- ▶ **Panoramica sugli elementi più interessanti dell'architettura**
- ▶ **Per l'utente**
  - ▶ Autoprovisioning credenziali di accesso
  - ▶ Sistema di AAA
- ▶ **Per gli operatori**
  - ▶ Autoprovisioning attivazione Access Point
  - ▶ Sistema di monitoraggio
  - ▶ Aspetti di sicurezza
- ▶ **Strumenti utilizzati**

# Provinciawifi

## Architettura – Autoprovisioning delle credenziali

---

- ▶ Ogni utente può registrarsi in autonomia con un sistema di autoprovisioning delle credenziali derivato da Romawireless
  - ▶ Oltre ai dati anagrafici, viene richiesto l'inserimento del numero di telefonia mobile di chi effettua la registrazione
  - ▶ Per attivare l'utenza è necessario effettuare una chiamata, dal numero inserito, verso un numero di telefonia fissa (utenza VoIP associata ad un'istanza di Asterisk)
    - ▶ Asterisk (mediante alcuni script AGI) controlla il numero del chiamante
    - ▶ Se quest'ultimo risulta valido, l'utenza viene attivata e le credenziali vengono registrate sul backend del server RADIUS che si occupa dell'autenticazione e dell'accounting.
  - ▶ Non c'è alcuna risposta alla chiamata dell'utente → l'attivazione è completamente gratuita
- ▶ Il sistema è coerente con la normativa Italiana (decreto Pisanu)

# Provinciawifi

## Architettura – AAA

---

- ▶ L'autenticazione è basata su Captive Portal
  - ▶ Quest'ultimo utilizza un server RADIUS che, a sua volta, ha un database come backend
- ▶ Viene gestito l'accounting al fine di forzare alcune policy di utilizzo del servizio
  - ▶ Per ogni utente, ogni giorno, la navigazione è limitata a 300 Mbyte trasferiti *oppure* un'ora
    - ▶ Se vengono trasferiti più di 300 Mbyte in meno di un'ora, allo scadere dell'ora l'utente è disconnesso
    - ▶ Altrimenti l'utente può rimanere online fino al trasferimento di 300 Mbyte
- ▶ È possibile l'autenticazione su base MAC address
  - ▶ Non è richiesta l'apertura di un browser
  - ▶ Utile per l'autenticazione automatica di alcuni strumenti “di servizio”

# Provinciawifi

## Architettura – Autoprovisioning attivazione AP

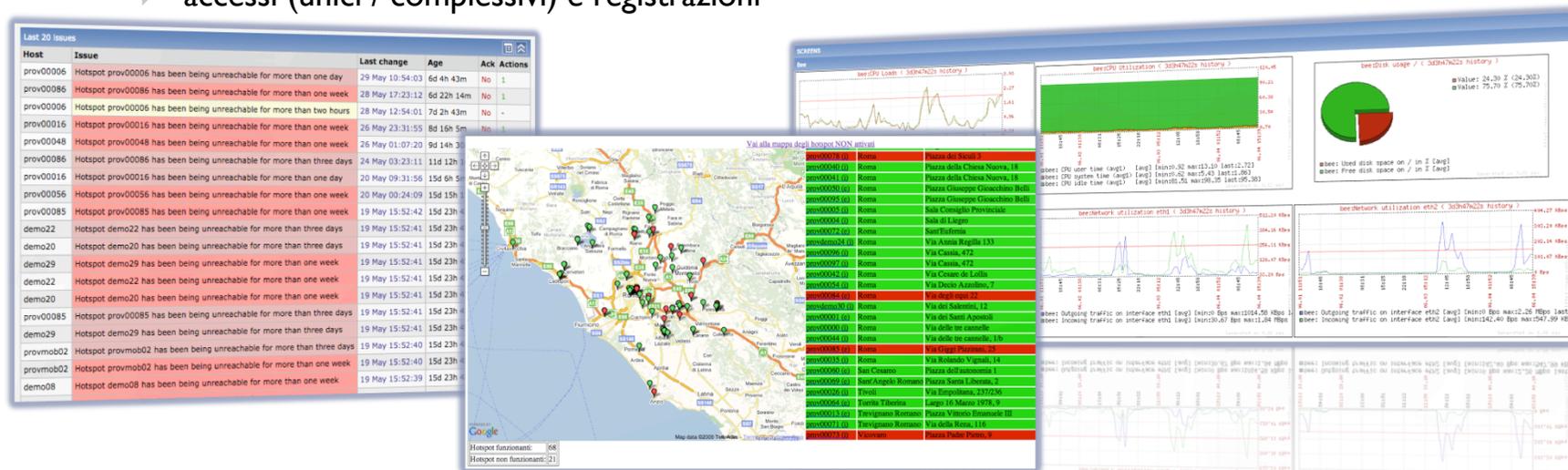
---

- ▶ Mediante una semplice interfaccia WEB l'operatore inserisce la posizione geografica ed il tipo (interno/esterno) dell'apparato che intende installare
  - ▶ Come risultato ottiene un codice di attivazione
  - ▶ Nel database degli hotspot attivabili viene automaticamente inserito il nuovo apparato, configurato in base ad un template
- ▶ Durante la fase d'installazione, l'operatore configura l'AP con il codice di attivazione
  - ▶ Ad ogni riavvio l'AP si collega in VPN al sistema centrale, scaricando la propria configurazione (generata dal database di cui sopra)
    - ▶ SSID annunciati
    - ▶ VLAN propagate nella VPN
    - ▶ IP di gestione
    - ▶ Etc.
- ▶ Ad esclusione del codice di attivazione, gli AP sono “stateless”
  - ▶ Ad ogni riavvio scaricano nuovamente la configurazione dal sistema centrale

# Provinciawifi

## Architettura – Sistema di monitoraggio

- ▶ Basato su Zabbix
  - ▶ Monitoraggio disponibilità e prestazioni dei sistemi centrali
  - ▶ Monitoraggio disponibilità di tutti gli apparati di accesso
  - ▶ Autodiscovery dei nuovi apparati installati ed applicazione di template per il monitoraggio
  - ▶ Allarmistica
- ▶ Composto da alcuni strumenti “fatti in casa”
  - ▶ Mappa (Google maps API) con la situazione di tutti gli hotspot
  - ▶ Statistiche e reportistica
    - ▶ numero di stazioni collegate su ciascun apparato (autenticate e non)
    - ▶ accessi (unici / complessivi) e registrazioni



# Provinciawifi

## Architettura - Sicurezza

---

- ▶ Ogni client, dal livello 2, è connesso esclusivamente al captive portal
  - ▶ “Client isolation” sugli access point
  - ▶ Filtri link layer sul concentratore che vietano il traffico tra VPN differenti
  - ▶ Mantenimento dell’associazione tra IP e MAC address per i client autenticati
- ▶ Gli accorgimenti implementati non risolvono tutti i problemi derivanti dall’avere una rete “open”
  - ▶ Tuttavia l’utenza deve essere quanto più “allargata” possibile

# Provinciawifi

## Strumenti utilizzati

- ▶ Tutti gli strumenti utilizzati sono rigorosamente Open Source
  - ▶ AccessPoint con firmware basato su **openWRT** (*Kamikaze*)
  - ▶ VPN: **openVPN** in modalità L2 e multi-client
  - ▶ Virtualizzazione: **KVM** (Kernel-based Virtual Machine)
    - ▶ incluso nel Kernel Linux dalla versione 2.6.20
  - ▶ Firewall/Captive Portal: **pfSense**
  - ▶ Monitoraggio: **Zabbix**
  - ▶ Storage Area Network (filesystem delle VMs) **openFiler**
  - ▶ DBMS **MySQL** (con replica circolare dei DB),
  - ▶ Clustering **Heartbeat2**
  - ▶ (Piccola) area di storage distribuito mediante OCFS2 su **DRBD**



# Provinciawifi

## Aspetti Normativi

---

- ▶ Oltre alle problematiche tecniche, la fornitura di un servizio al pubblico richiede l'ottemperanza a varie normative Italiane.
- ▶ In particolare, i seguenti aspetti sono tutti regolati da specifiche norme
  - ▶ Installazione di apparati Wi-Fi su suolo pubblico
  - ▶ Attivazione (radio) di apparati Wi-Fi per connettività Internet al pubblico
  - ▶ Identificazione degli utenti del servizio

# Provinciawifi

## Aspetti Normativi – Installazione Hotspot

---

- ▶ L'installazione degli hotspot su suolo pubblico in un Comune deve essere autorizzata da quest'ultimo
  - ▶ D. Lgs. 259/2003 “*Procedimenti autorizzatori relativi alle infrastrutture di comunicazione elettronica per impianti radioelettrici*” [2]
  - ▶ In particolare, l' art. 87 richiede la produzione di una “**Denuncia di inizio attività**” per impianti con potenza in antenna inferiore a 20 watt”
  - ▶ Quest'ultimo documento deve contenere
    - ▶ Informazioni logistiche degli apparati
    - ▶ Tipologia e caratteristiche tecniche delle antenne installate
    - ▶ Fotografie del sito, con simulazione post-operam

# Provinciawifi

## Aspetti Normativi – Attivazione Servizio Pubblico

---

- ▶ L'attivazione di hotspot Wi-Fi pubblici è regolamentata dal Decreto Ministeriale 28 maggio 2003 [3] (e successive modifiche)
  - ▶ *“Condizioni per il rilascio delle autorizzazioni generali per la fornitura al pubblico dell'accesso radio LAN alla rete ed ai servizi di telecomunicazione”*
  - ▶ Solo gli operatori precedentemente autorizzati dal Ministero delle Comunicazioni possono installare hotspot che erogano un servizio al pubblico.
  - ▶ Entro 30 giorni, ogni hotspot attivato deve essere dichiarato al Ministero

# Provinciawifi

## Aspetti Normativi – Identificazione Utenti (Pisanu)

---

- ▶ Decreto-legge 27 luglio 2005, n. 144, convertito, con modificazioni, dalla legge 31 luglio 2005, n. 155 [4]
  - ▶ Art. 6: Nuove norme sui dati del traffico telefonico e telematico
    - ▶ “[...] Le predette imprese<sup>(\*)</sup> adottano tutte le necessarie misure affinché venga **garantita l'acquisizione dei dati anagrafici riportati su un documento di identità**, nonché del tipo, del numero e della riproduzione del documento presentato dall'acquirente, ed assicurano il corretto trattamento dei dati acquisiti.”

(\*) fornitori di una rete pubblica di comunicazioni o di un servizio di comunicazione elettronica accessibile al pubblico

# Provinciawifi

## Aspetti Normativi – Identificazione Utenti (Pisanu)

- ▶ Parere ufficiale del Ministero dell'Interno alla procedura di autenticazione con telefono mobile
  - ▶ "[...] per quanto concerne il punto relativo all'identificazione dell'utente che si connette alle reti di comunicazione elettronica attraverso la tecnologia wireless, si reputa condizione sufficiente, per soddisfare i requisiti previsti dalla normativa vigente, l'utilizzo del telefono mobile quale mezzo per attivare le procedure necessarie ad ottenere le credenziali di accesso alla rete stessa, in quanto consente l'identificazione, **seppur indiretta**, dell'utente suddetto."

2011.116

R: 0654220926 P. 2/3

- Cellucci  
- Proto

MOD. 4 P



*Ministero dell'Interno*

DIPARTIMENTO DELLA PUBBLICA SICUREZZA

DIREZIONI CENTRALI PER LA POLIZIA STRADALE, FERROVIARIA, DELLE COMUNICAZIONI E PER I REPARTI SPECIALI DELLA POLIZIA DI STATO  
SERVIZIO POLIZIA POSTALE E DELLE COMUNICAZIONI

n. 2000/89/44-F.320/3668 Roma, 27 novembre 2007

OGGETTO: Decreto Legislativo n. 144/05, convertito con modificazioni con legge n. 155/05.  
Connessione a internet wireless

ALLA ASSOCIAZIONE PROVIDER INDIPENDENTI  
c/o NETFLY s.r.l.  
via G. Cucci, 32

84014 NOCERA INFERIORE

Con riferimento alla nota datata 5 novembre 2007, increte l'oggetto si rappresenta che per quanto concerne il punto relativo all'identificazione dell'utente che si connette alle reti di comunicazione elettronica attraverso la tecnologia *wireless*, si reputa condizione sufficiente, per soddisfare i requisiti previsti dalla normativa vigente, l'utilizzo del telefono mobile quale mezzo per attivare le procedure necessarie ad ottenere le credenziali di accesso alla rete stessa, in quanto consente l'identificazione, **seppur indiretta**, dell'utente suddetto

Si reputa, però, **condizione necessaria**, che la messaggeria sia veicolata attraverso l'utilizzo di uno SIM/USIM, rilasciata all'utente rispettando le disposizioni relative all'identificazione dello stesso, previste dall'art. 55 del D-Lgs. N. 259/03 - Codice delle Comunicazioni Elettroniche, che prevede l'identificazione completa dell'utente prima dell'attivazione del servizio, **con esclusione**, quindi, di SIM/USIM rilasciate da paesi stranieri.

# Provinciawifi

## Prossimo futuro

---

- ▶ Personalizzazione delle Captive Pages in base alla posizione geografica (e.g.: pubblicazione news/avvisi specifici del Comune)
  - ▶ Già oggi l'infrastruttura è in grado di determinare da dove è connessa ogni stazione, ancora prima dell'autenticazione dell'utente...
  - ▶ ...cosa piuttosto complessa nel Layer 2 e per l'architettura proposta
- ▶ Utilizzo di CAPWAP[5] per la gestione centralizzata di alcuni parametri degli apparati
  - ▶ Protocollo standard (e.g.:RFC3990) per la configurazione ed il provisioning di Access Point Wireless. Versione "standard" del CISCO LWAP
  - ▶ È in sperimentazione la soluzione Open Source realizzata dall'Istituto per le Applicazioni del Calcolo del CNR e l'Università Campus Bio-Medico di Roma

---

# Altri progetti e Sperimentazioni

# Rete Unica degli Atenei di Roma

## Il progetto

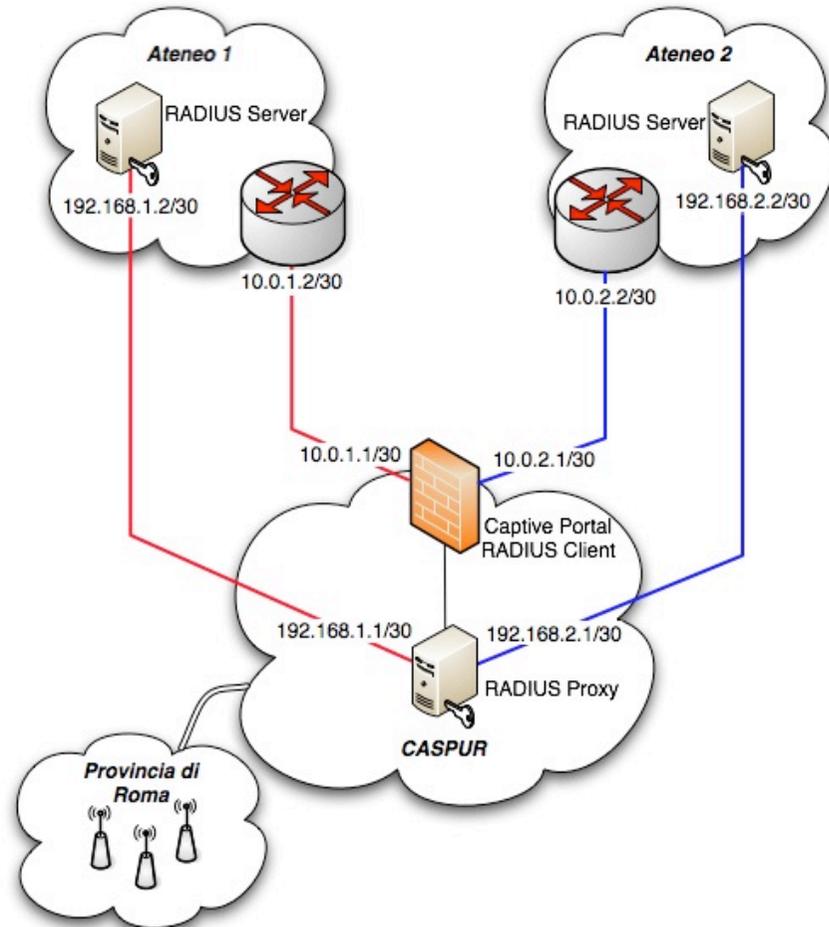
---

- ▶ In base ad un accordo tra gli Atenei pubblici di Roma e la Provincia di Roma, l'infrastruttura Wi-Fi di Provinciawifi pubblica una rete unica per i quattro Atenei di Roma
- ▶ La sfida
  - ▶ Mantenere l'indirizzamento pubblico di proprietà dei singoli Atenei
    - ▶ Utile per garantire il raggiungimento di alcune risorse con accesso garantito da ACL (e.g.: editoria elettronica)
  - ▶ Mantenere le policy di accesso ad Internet dei singoli Atenei
- ▶ Come fare con una sola rete Wi-Fi a disposizione?
  - ▶ La scelta di prodotti Open Source si è rivelata vincente
    - ▶ Personalizzazione del codice di autenticazione e di firewalling del Captive Portal

# Rete Unica degli Atenei di Roma

## Architettura

- ▶ **Autenticazione/Accounting**
  - ▶ inoltra delle credenziali utente da un proxy RADIUS “centrale” verso i RADIUS dei singoli atenei, in base al realm utilizzato.
  - ▶ Logging degli accessi/accounting sono gestiti dall’ateneo cui l’utente appartiene
- ▶ **Traffico degli utenti**
  - ▶ Analogamente a Provinciawifi le stazioni, su tutto il territorio, sono direttamente connesse al captive portal
  - ▶ Mediante policy routing “dinamico”, in base al realm, il traffico è inoltrato verso l’infrastruttura di routing dell’ateneo di competenza
  - ▶ Firewalling/NAT/logging sono gestiti da quest’ultimo

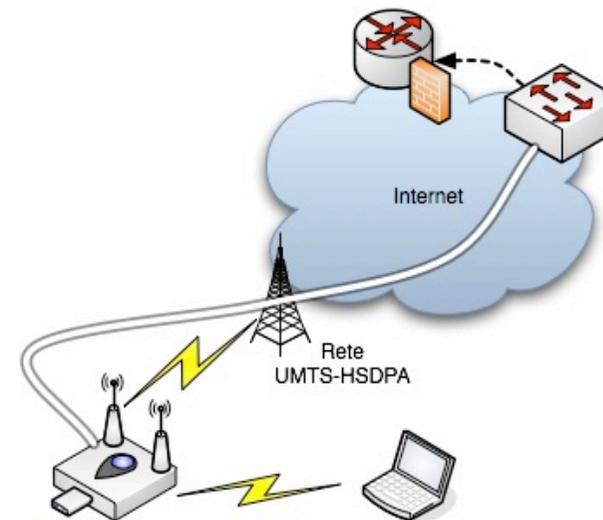
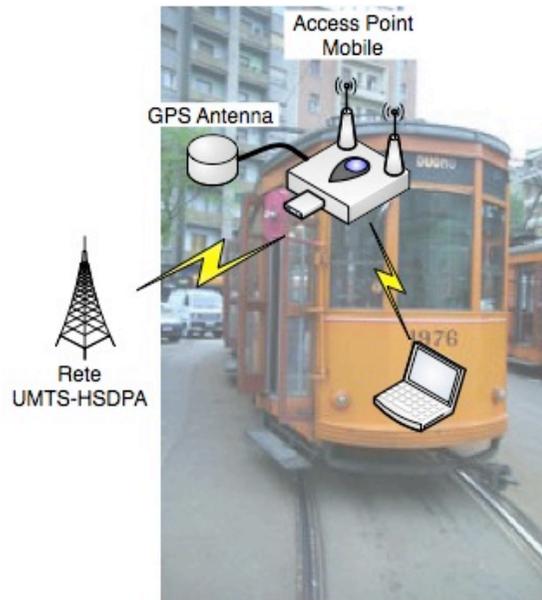


# Federazione di reti Wi-Fi e AP Linux-based

## Altri progetti e sperimentazioni

### ▶ Trambus - Progetto

- ▶ In collaborazione con Unidata S.p.A. installazione di Access Point basati su OpenWRT su alcuni mezzi di trasporto pubblico
  - ▶ Connettività degli AP via HSDPA/UMTS
  - ▶ Gli utenti all'interno del mezzo si connettono tramite Wi-Fi
- ▶ Il "trasporto" è realizzato mediante VPN L2 (OpenVPN)
  - ▶ La connettività Internet delle stazioni è garantita da apparati centralizzati

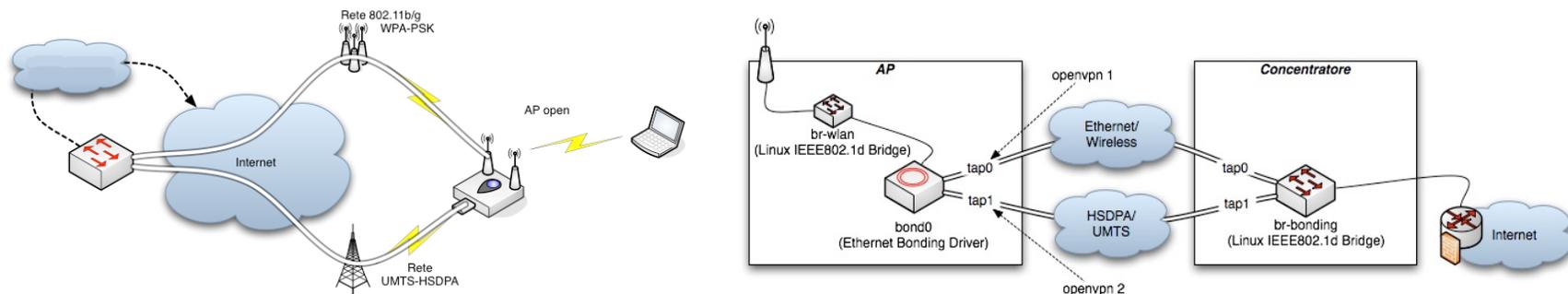


# Federazione di reti Wi-Fi e AP Linux-based

## Altri progetti e sperimentazioni

### ▶ Trambus – Sperimentazione

- ▶ Connettività HSDPA/UMTS per fornire connettività all'interno del mezzo in movimento
- ▶ Connettività Wi-Fi per fornire connettività all'interno del mezzo in sosta (fermate/capolinea)
- ▶ Handoff verticale Wi-Fi  $\leftrightarrow$  UMTS/HSDPA
  - ▶ Senza che le applicazioni sulle stazioni perdano connettività



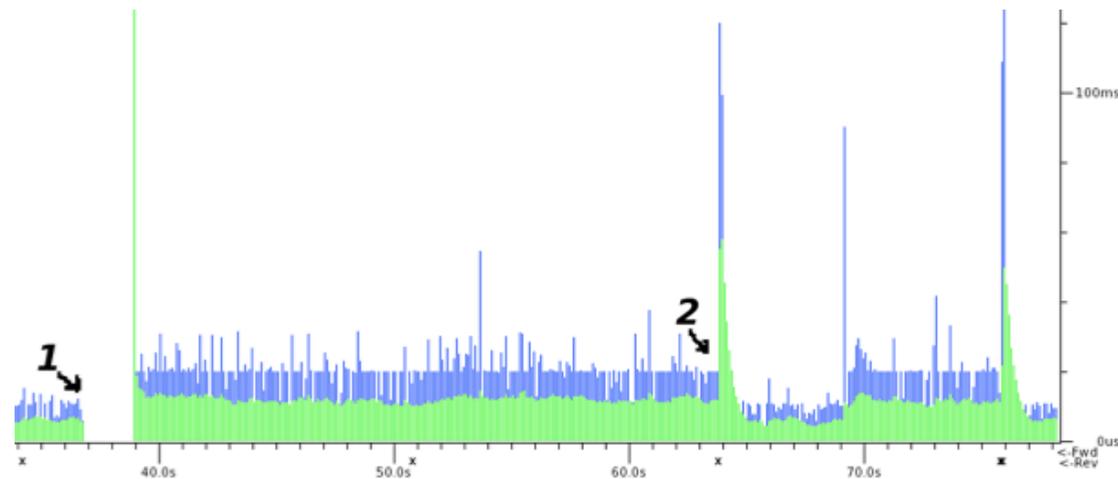
Architettura basata su due VPN L2 (openVPN) “aggregate” mediante bonding Linux (modalità active/backup)

# Federazione di reti Wi-Fi e AP Linux-based

## Altri progetti e sperimentazioni

---

- ▶ Handoff verticale Wi-Fi  $\leftrightarrow$  HSDPA
  - ▶ Unbuffered Audio Streaming – Unreliable Transport
    - ▶ Chiamata VoIP (codec GSM 06.10 )
  - ▶ Istogramma blu: latenza, Istogramma verde: jitter (variazione statistica del ritardo).

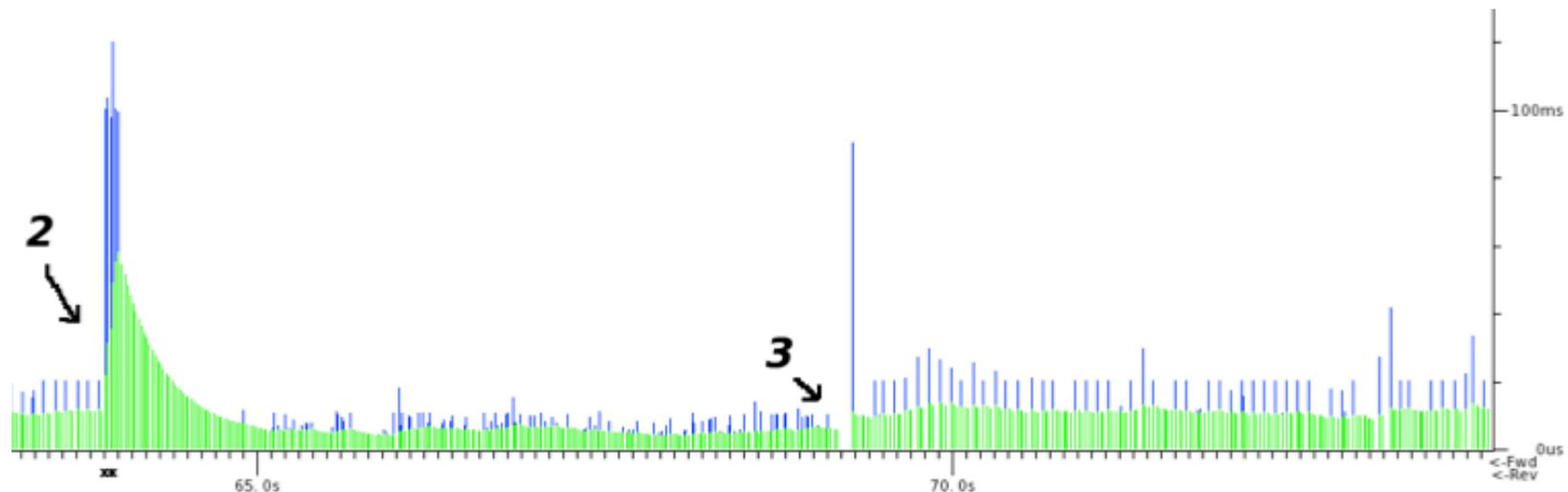


- 1) Caso Peggioro, Handoff Wi-Fi  $\rightarrow$  HSDPA non ancora utilizzato: “silenzio” di c.a. 2,3s
- 2) Handoff HSDPA  $\rightarrow$  Wi-Fi: nessuna perdita di pacchetti

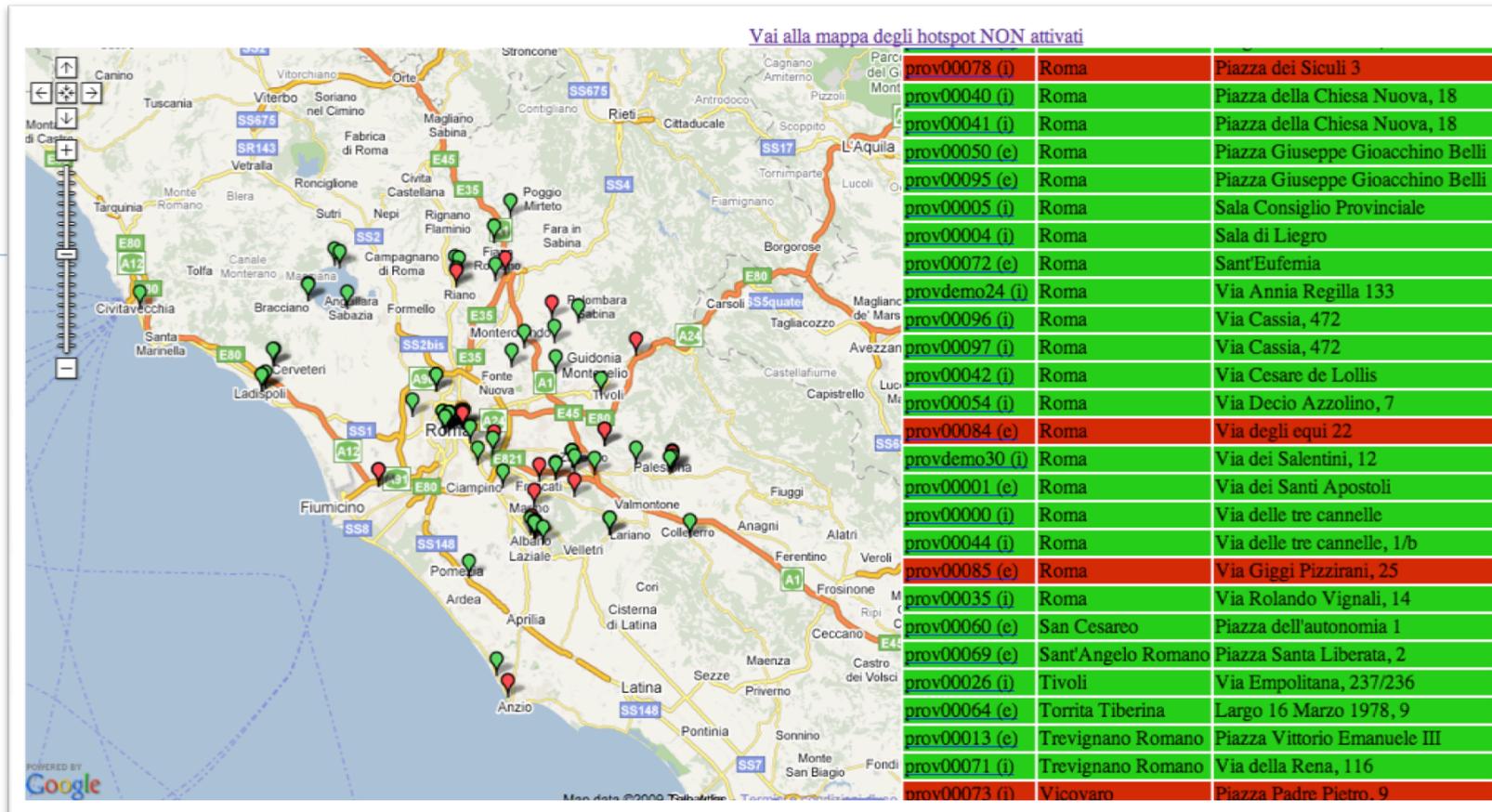
# Federazione di reti Wi-Fi e AP Linux-based

## Altri progetti e sperimentazioni

- ▶ Handoff verticale Wi-Fi  $\leftrightarrow$  HSDPA
  - ▶ Unbuffered Audio Streaming – Unreliable Transport
    - ▶ Chiamata VoIP (codec GSM 06.10 )
  - ▶ Istogramma blu: latenza, Istogramma verde: jitter



3) Secondo Handoff Wi-Fi  $\rightarrow$  HSDPA: “silenzio” < 0,5s



# Fine

d.guerri@caspur.it  
 m.goretti@caspur.it  
 wireless@caspur.it

# Riferimenti e approfondimenti

---

- [1] European eduroam confederation policy - <http://www.eduroam.org/downloads/docs/GN2-07-328-eduroam-policy-for-signing-Final2-2.pdf>
- [2] Codice delle comunicazioni elettroniche - <http://www.parlamento.it/leggi/deleghe/03259dl.htm>
- [3] Regolamentazione dei servizi Wi-fi ad uso pubblico - [http://www.interlex.it/testi/dm\\_wifi.htm](http://www.interlex.it/testi/dm_wifi.htm)
- [4] Conversione in legge, con modificazioni, del decreto-legge 27 luglio 2005, n. 144, recante misure urgenti per il contrasto del terrorismo internazionale - <http://www.camera.it/parlam/leggi/05155l.htm>
- [5] Control And Provisioning of Wireless Access Points (capwap) - <http://www.ietf.org/html.charters/capwap-charter.html>

---

Federazione di reti Wi-Fi e Access Point Linux-based – GARR Workshop 2008

<http://www.garr.it/eventiGARR/ws08/presentazioni/sessione4/FRW-GARRWS08-final.pdf>

---

Performance Analysis of OpenVPN on a Consumer Grade Router

<http://www.cse.wustl.edu/~jain/cse567-08/ftp/ovpn.pdf>