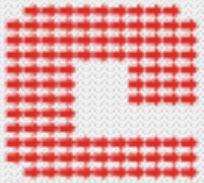


CASPUR

Consorzio interuniversitario per le Applicazioni di Supercalcolo Per Università e Ricerca

Federazione di reti Wi-Fi e Access Point Linux-based

Maurizio Goretti – Davide Guerri

CASPUR

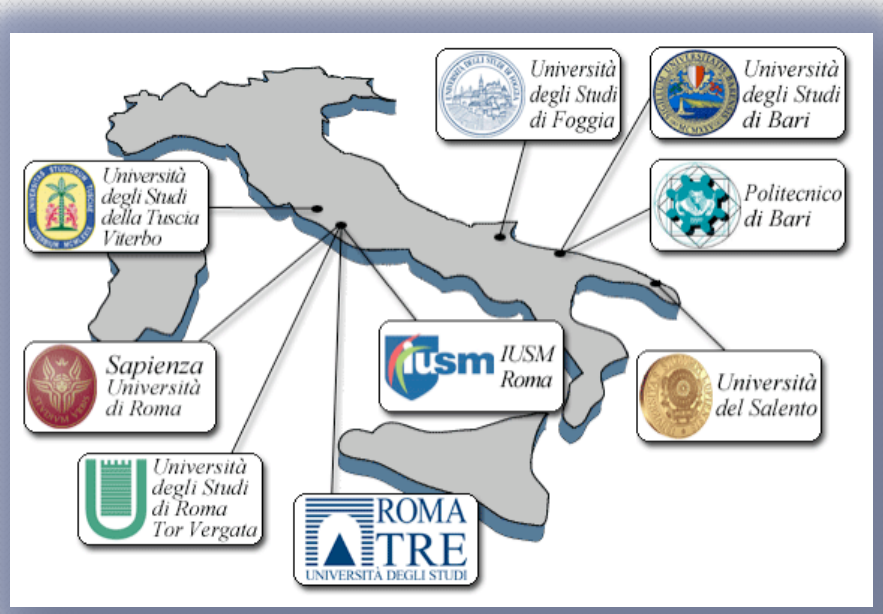
Sommario – Parte 1

- Cos'è CASPUR?
- Reti Wi-Fi a Roma
  - Federazione Sapienza-Romawireless
- Punto d'interconnessione
- Biblioteche senza Filo
- Attuali installazioni
- Sperimentazione e nuovi accordi

CASPUR

CASPUR e le Università

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



CASPUR

CASPUR e la Pubblica Amministrazione

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

ISFOL

MiBAC

AVVOCATURA DELLO STATO

Camera dei deputati

SPQR

Comune di Roma

Ministero dell'Università e della Ricerca
Piazza Kennedy, 20 - 00144 Roma - Tel. 0697721

CASPUR

CASPUR crocevia Internet

- PoP romano dei maggiori Carrier operanti in Italia
- Sede PoP GARR Roma
- Punto di Interscambio
- Nuova Rete Pubblica Amministrazione

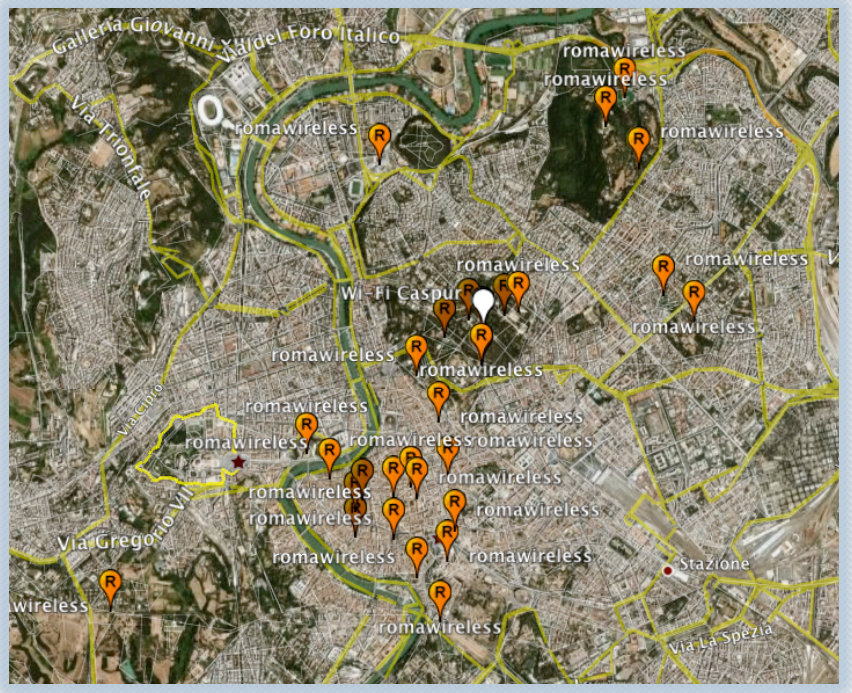
BT Italia
Cogent Comunications
Eutelia
Fastweb
Global Crossing
Infracom
Mclink
Retelit
Tata Communications
TelecomItalia
Unidata
Wind

CASPUR

romawireless

Consorzio Roma Wireless

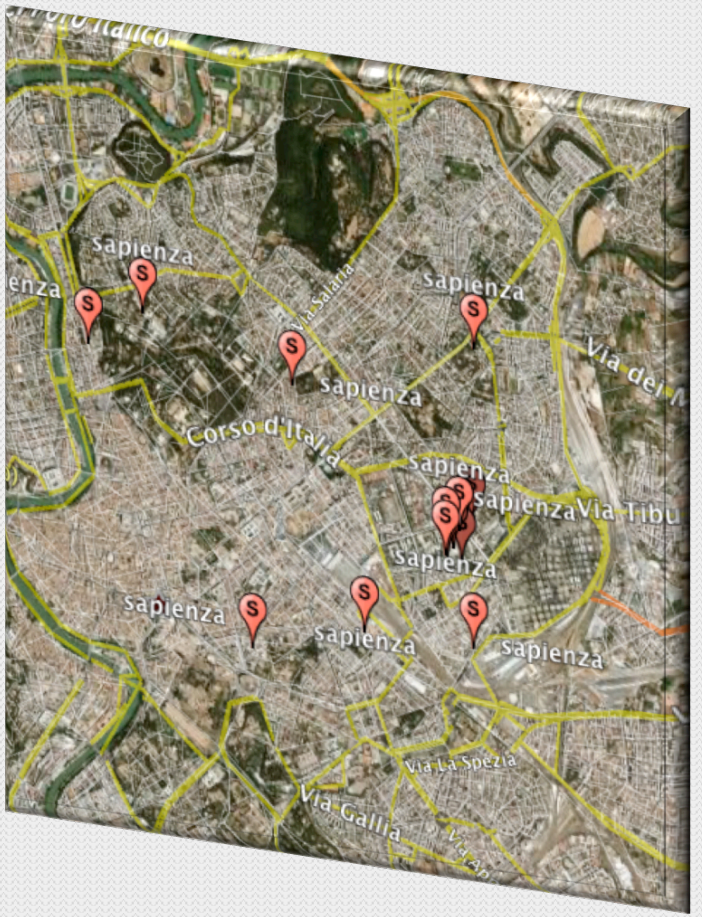
- Patrocinio del Comune di Roma
  - Wi-Fi nelle aree pubbliche di Roma
    - Ville Storiche
    - Centro città
- Circa 50 AP
- CASPUR consorziato



CASPUR

Sapienza Wireless

- Realizzazione di una infrastruttura Wi-Fi per l'Ateneo
  - Più di ***14300*** utenti totali
  - 40 AP
  - Oltre 1500 accessi medi giornalieri
  - Captive Portal



Federazione RomaWireless-Sapienza

- Accordo di Federazione
  - Utenti Sapienza accedono su AP RomaWireless
- Quale soluzione tecnica per la federazione?
  - Proxy Radius?
    - Ottima soluzione nel caso di organizzazioni omogenee (EDUROAM)
    - Qualche problema nel nostro caso….(continua…)

Federazione RomaWireless-Sapienza

Proxy radius problems

- Istituzioni di natura diversa possono non amare il passaggio dei dati dei propri utenti su proxy altrui
- Identificazione (L.155/2005 – “Pacchetto Pisanu”) di un utente nel caso di violazioni di legge
  - Incrociare log appartenenti ad istituzioni diverse
    - Indirizzi IP di una organizzazione
    - Utenti di un’altra

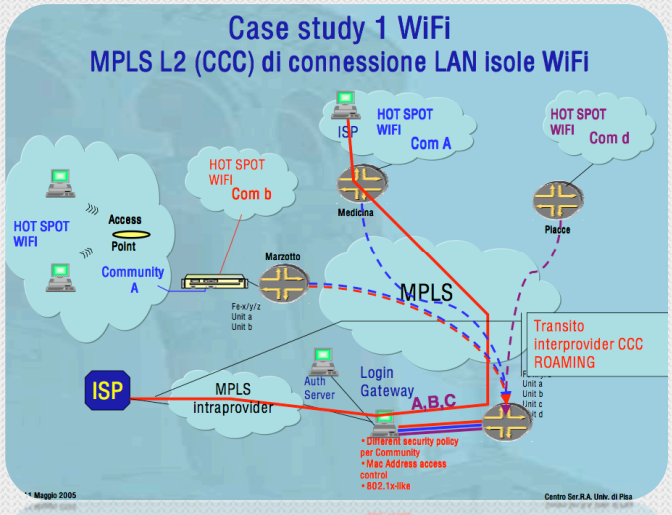
E quindi?

- In un mondo ideale vorrei che al posto dell'access point delle realtà con cui mi federo ci fosse il mio
  - Io controllo il sistema di autenticazione
  - Vengono assegnati i miei indirizzi
- Uso una infrastruttura esterna come se fosse la mia

CASPUR

L'esperienza del Centro Serra

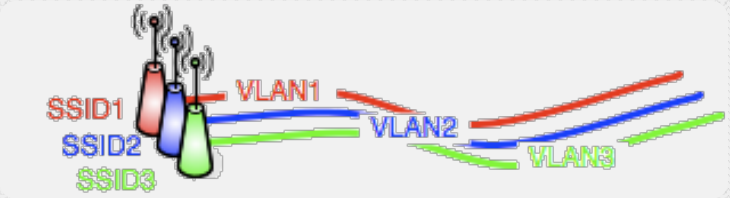
- Nel 2005, alla conferenza GARR di Pisa, ci fu una presentazione del Centro Serra
- Usavano la virtualizzazione degli AP
  - Multi ESSID -> VLAN
- … e quella della rete
  - MPLS/xWDM



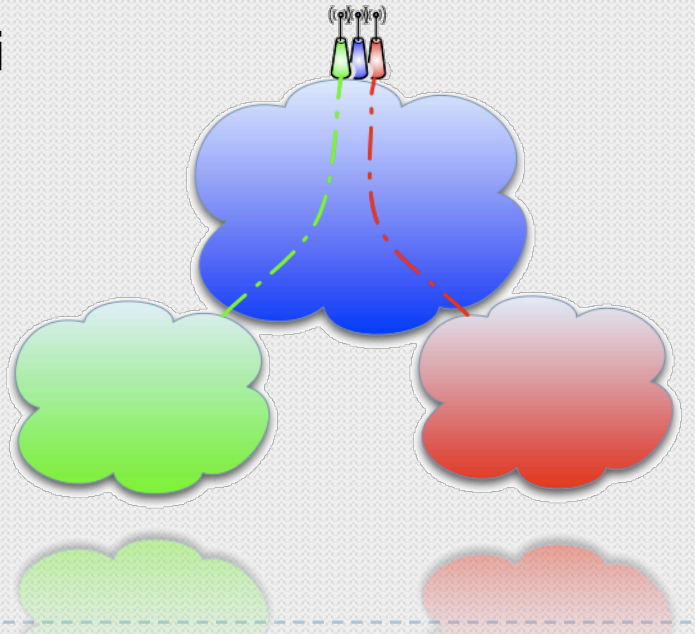
- Per poter permettere a più organizzazioni di poter utilizzare lo stesso AP come se fosse il proprio
- AP distribuiti sulla rete metropolitana di Pisa

L'esperienza del Centro Serra
Virtualizzazione degli AP

- Un AP annuncia una rete Wi-Fi tramite un ESSID
- Alcuni AP possono annunciare più reti, ovvero ESSID multipli ed associare un ESSID ad una VLAN



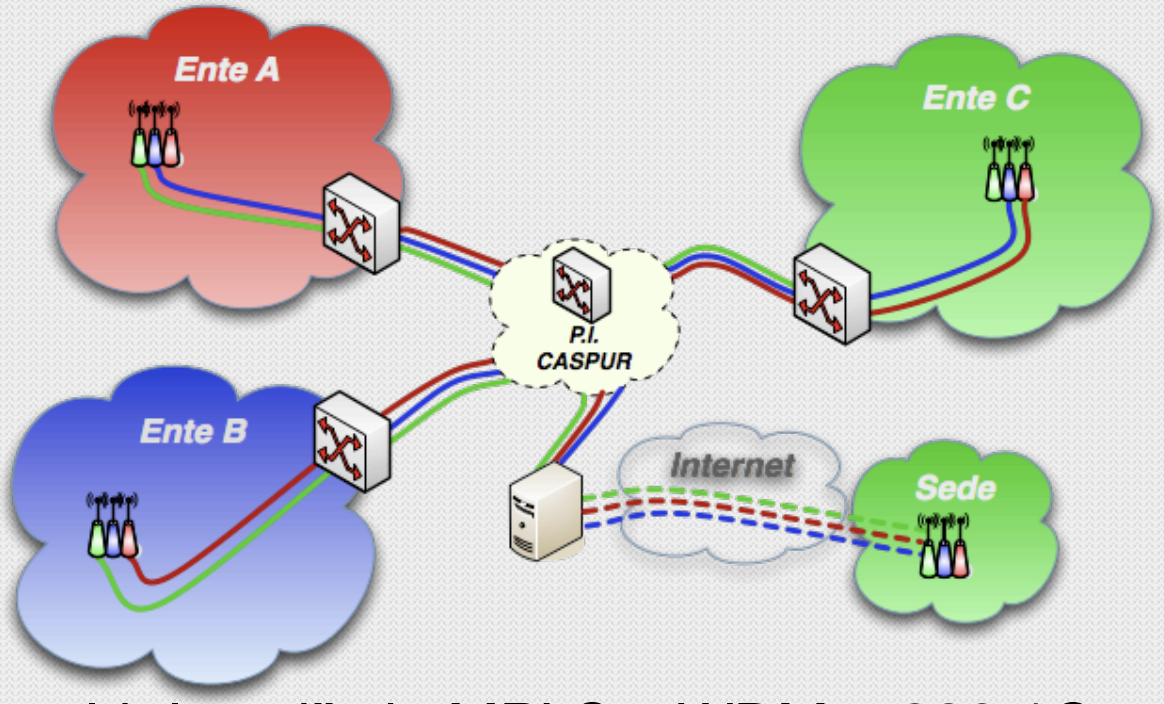
- Se la rete trasporta le VLAN, sono in grado di "remotizzare" la mia rete Wi-Fi
- Posso chiedere ad un AP ospitante di ospitare il mio AP
- Porto il mio livello 2 (Ethernet) sull'AP
  - Uso il mio metodo di autenticazione
  - Fornisco i miei indirizzi IP



Problemi

- Gli AP erano ancora solo quelli di fascia alta
- Non sempre la rete è in grado trasportare il livello 2
  - Difficoltà locali nel trasporto delle VLAN
  - Non disponibilità di infrastruttura MPLS capillare
- … a meno di non incapsulare il livello 2 tramite una VPN dall'AP al Punto di Interconnessione Wi-Fi
  - OpenVPN
  - Necessità di AP personalizzabili (*e.g.*: Linux Based)

Punto Interconnessione Wi-Fi



- Livelli 2 “multiplexati” via MPLS, xWDM o 802.1Q
  - Quando possibile
- Tunnel OpenVPN incapsulanti 802.1Q
  - Come alternativa

Access Point home made

- HW dedicato
  - Basso costo
- SW personalizzato
  - Multi ESSID, openVPN
  - Possibilità di personalizzazioni infinite
- Facile installazione su reti ospitanti grazie ad openVPN

CASPUR

Punto di Interconnessione Wi-Fi

- Pertecipano al P.I. Wi-Fi
  - Uniroma1 (Fibra I.R.U)
  - Uniroma2 (openVPN -> Fibra I.R.U. + xWDM)
  - Uniroma3 (Fibra I.R.U. + CWDM)
  - RomaWireless Unidata (Fibra I.R.U. + DWDM + MPLS)
  - Biblioteche di Roma (OpenVPN -> HDSL -> Hyperlan)
- CASPUR riveste un ruolo neutrale

CASPUR

Biblioteche senza filo

- Nato da una idea di CASPUR e Università “La Sapienza” di Roma
  - Prorettore Prof. Renato Masiani
  - Resp. Tec. Marco Cavallo
- Wi-Fi delle Università nelle biblioteche pubbliche di Roma
  - Biblioteche Comunali
  - Biblioteche Nazionali
- Attiva Uniroma3 (Prof A.Neri, dott. P. Cursi)
- In fase di attivazione Uniroma2 (Prof A.Desideri, dott D.Genovese)

CASPUR

Attuali installazioni

- Biblioteche senza Filo
  - 3 Biblioteche comunali
    - Ostia, Primavalle e Marconi
    - Tutte le biblioteche attive entro Giugno 2008 (circa 40)
  - Attive oggi 2 Biblioteche Nazionali
    - Alessandrina
    - Vallicelliana

- Accordo Sapienza - RomaWireless
  - Villa Borghese
    - Casa del Cinema
    - Museo Canonica
    - Casino Orologio

CASPUR

Sperimentazioni e nuovi accordi

- Il punto di interconnessione Wi-Fi permette accordi tra singoli afferenti
- Accordi tra università
  - Uniroma3 annuncia sperimentalmente Uniroma1 sui suoi AP
- Contatti tra RomaWireless e le altre Università di Roma
- Proxy Radius neutrale gestito da CASPUR

Parte 2

CASPUR

Sommario – Parte 2

- Federazione *link-layer* di reti Wi-Fi
  - PROs & CONs
- Soluzione Tecnica
  - Punto d'interconnessione
  - Estensione geografica del *link layer*
    - Architettura sistema
    - Concentratore
    - Apparati di accesso
  - Lo stato della sperimentazione
  - Ulteriori Sviluppi

CASPUR

Federazione *link layer* di reti Wi-Fi

Federazione *link-layer* di reti Wi-Fi

PROs & CONs

- Problemi intriseci del modello
  - Necessità di apparati d'accesso Wi-Fi con supporto per *multiple-ESSID*
  - Scalabilità
    - Numero di ESSID limitati
    - Estensione di un singolo dominio di broadcast di L2
  - Sicurezza

Federazione *link-layer* di reti Wi-Fi

PROs & CONs – cont'd

- Vantaggi del modello
  - L'indirizzamento IP è dell'ente cui la rete Wi-Fi appartiene e **non** quello dell'ente ospitante
    - Reti Wi-Fi pubbliche ospitabili in sedi prive delle infrastrutture per la *data retention* a norma di legge
  - Possibilità di replicare ***esattamente*** la rete di un ente presso le altre entità afferenti alla federazione
    - Reti "open" con autenticazione basata su captive portal
    - WPA/WPA2 personal (anche se non adatti a reti con numerosi AP…)
    - WPA/WPA2 enterprise (802.1x)

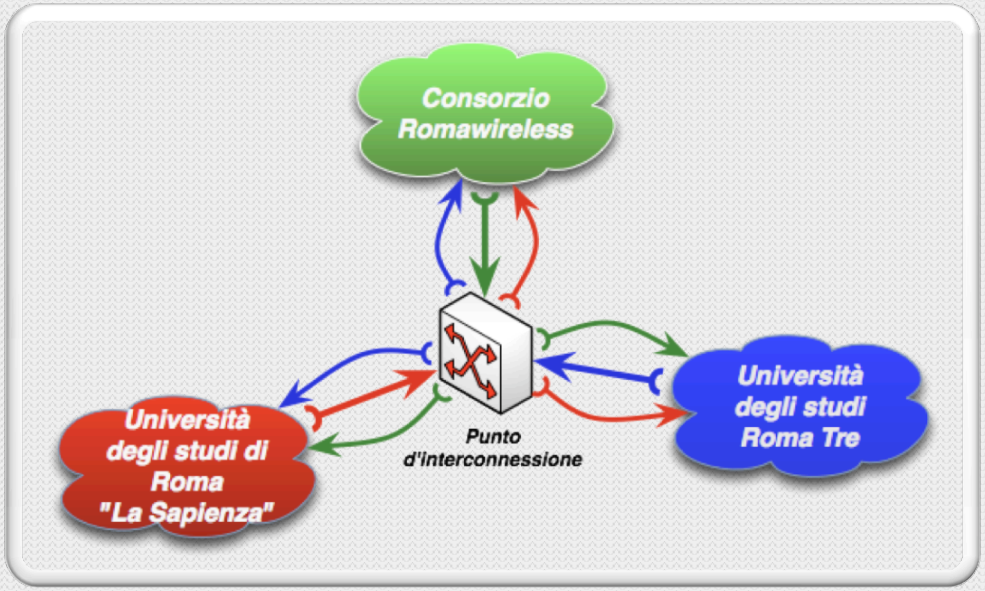
CASPUR

Soluzione Tecnica

Soluzione tecnica
Punto d'interconnessione

- Il punto d'interconnessione per la federazione "*link layer*" delle reti Wi-Fi
  - È fondamentalmente un centro stella (switch) incaricato di smistare opportunamente il traffico 802.1Q (VLAN) degli afferenti

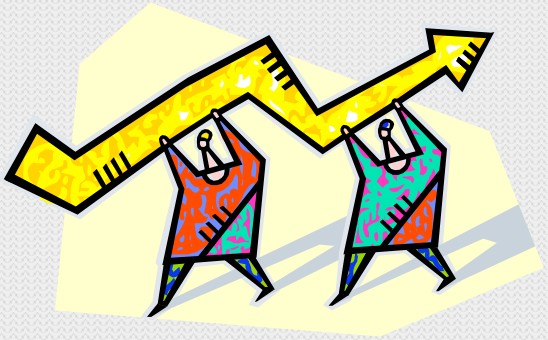
- Attualmente il centro stella è realizzato mediante
  - Uno switch Gigabit RubyTech
  - Uno switch Fast-Ethernet HP Procurve



Soluzione tecnica

Punto d'interconnessione (cont'd)

- Le VLAN (anche più d'una per ogni afferente) possono pervenire al punto d'interconnessione mediante collegamento:
  - Fisico (fibra/UTP)
    - Attualmente è richiesto che il segmento terminale del collegamento sia 100Base-TX (RJ-45)
  - Logico (incapsulamento)
    - MPLS
    - VPN L2 (su IP/IPv6)



Soluzione tecnica

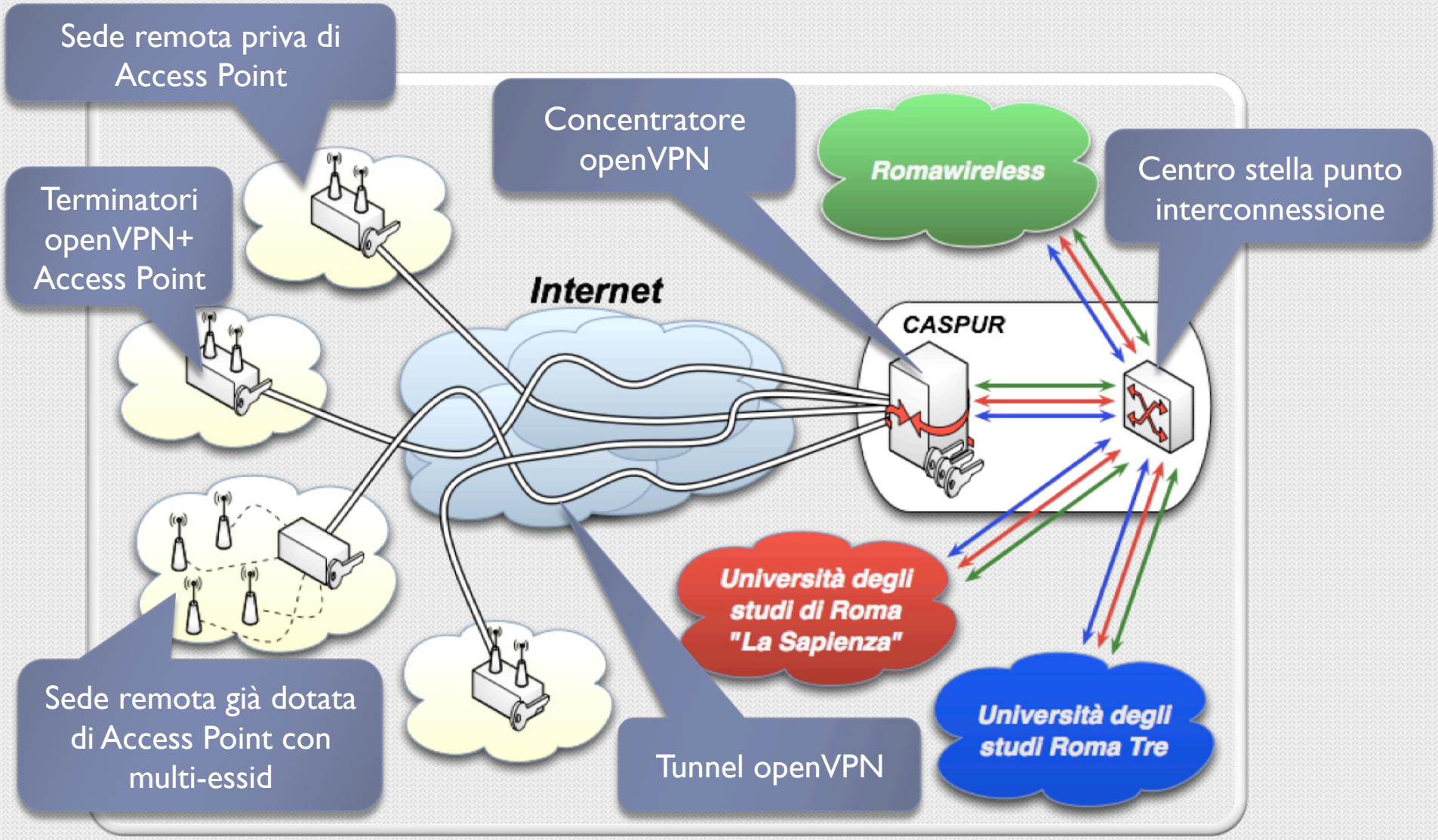
Estensione geografica del link layer

- Al fine di consentire l'estensione geografica del link layer anche in sedi non "fisicamente" raggiungibili via ethernet, CASPUR ha realizzato un'infrastruttura *ad hoc*
  - Tunnel ***openVPN***, incapsulanti 802.1Q
  - Apparati d'accesso estremamente personalizzabili e capaci di ***multiple-ESSID***
- Le caratteristiche principali di questa infrastruttura sono
  - Utilizzo ***esclusivo*** di strumenti software ***open-source***
  - Hardware dai ***costi contenuti***

CASPUR

Soluzione tecnica

Estensione geografica del link layer - Architettura sistema



CASPUR

Soluzione Tecnica::Concentratore

CASPUR

Soluzione tecnica

Estensione geografica del link layer – Concentratore

- Il concentratore è un server linux (Ubuntu 7.10)
  - Raccoglie le VPN relative agli apparati di accesso
  - Smista opportunamente le VLAN 802.1Q provenienti dal punto d'interconnessione e dagli apparati di accesso
- A breve l'apparato di concentrazione sarà ridondato
  - Il modello consente in modo estremamente semplice l'implementazioni di configurazioni ***High Availability*** e/o ***Load Balancing*** per la raccolta delle VPN

Soluzione tecnica

Estensione geografica del link layer – Ottimizzazioni

- Il traffico ***inter-vpn*** è vietato con filtraggio tramite ***ebtables*** (*i.e.*: link layer firewall) sul concentratore
  - È permesso esclusivamente il traffico da e verso il punto d'interconnessione
    - Le sedi coperte dal servizio sono isolate fra loro (per ogni rete Wi-Fi)
- È possibile filtrare ulteriormente il traffico, ad esempio:
  - Permettendo soltanto alcuni protocolli, quali IP/ARP e/o IPv6
    - Riduzione del traffico "non necessario"
    - Mitigazione di alcuni attacchi L2 (tipicamente DoS) alle implementazioni di alcuni protocolli di controllo (e.g.: CDP/LLDP, STP, …)

Soluzione tecnica

Estensione geografica del link layer – Ottimizzazioni (cont'd)

- Al fine di garantire integrità e riservatezza delle comunicazioni incapsulate in openVPN
  - Ogni tunnel è cifrato
    - Per mezzo di AES-128-CBC
  - Gli end-point di ogni tunnel sono autenticati
    - Crittografia asimmetrica (via TLS-RSA, certificati X509)
    - PKI interamente gestita tramite openSSL
      - È possibile la revoca dei certificati ad esempio in caso di furto di uno degli apparati

CASPUR

Soluzione tecnica

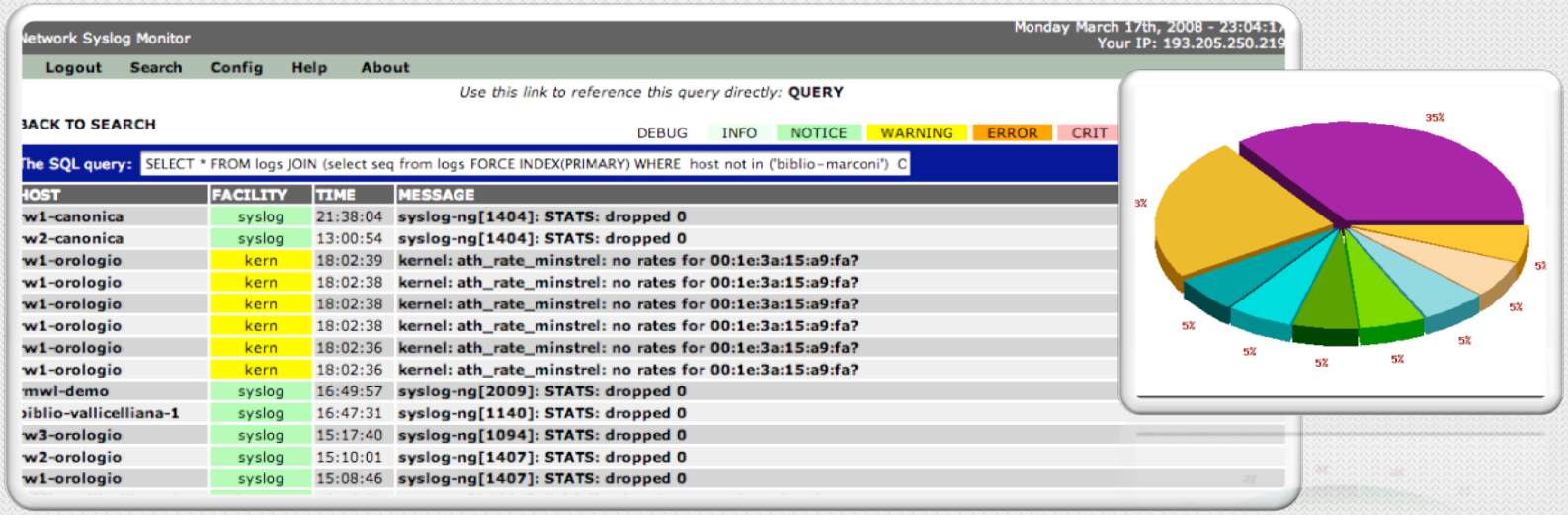
Estensione geografica del link layer – Sistema di monitoraggio

- Gli apparati sono monitorati costantemente mediante agenti software ZABBIX dotati di appositi script
- La “telemetria” è raccolta da un server centrale ZABBIX
  - Utenti connessi su ogni ESSID, utilizzo memoria, CPU, traffico di rete, servizi attivi, modifica dei file di sistema,…
  - Gestione allarmistica e notifica via e-mail (IM, SMS, ..)

Soluzione Tecnica

Estensione geografica del link layer – Sistema di monitoraggio (cont'd)

- E' gestita la raccolta centralizzata dei log di tutti gli apparati di accesso
  - syslog-ng
  - php-syslog-ng
    - backend mysql e interfaccia web per ricerche nello storico



CASPUR

Soluzione Tecnica::Apparati di Accesso

Soluzione tecnica

Estensione geografica del link layer – Apparati di accesso

- Ogni apparato di accesso
  - Instaura una VPN con il concentratore
  - Riceve/invia trame 802.1Q da/nella VPN
  - Implementa ESSID 802.11a/bg multipli
    - Limite ***teorico*** del driver = 64
  - Ricopre il ruolo di autenticator per 802.1X per gli ESSID di reti WPA/WPA2 enterprise
  - Si occupa del bridging tra 802.11 e ethernet 802.1Q
    - Bridge separato per ogni ESSID-VLAN
  - Se necessario, può limitare la banda massima da dedicare al servizio Wi-Fi
    - Traffic shaping dati in ingresso alla VPN

CASPUR

Soluzione tecnica

Estensione geografica del link layer – Apparati di accesso – Hardware

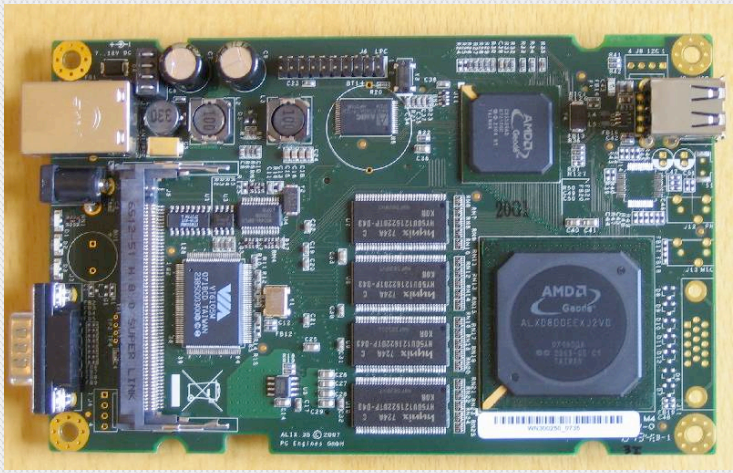
PCEngines ALiX

- AMD Geode LX @433/500Mhz
  - Architettura x86
- 128/256MB RAM
- Storage su CompactFlash
- 2 slot miniPCI
- Fino a 3 interfacce ethernet

- 2 Interfacce USB2 (*opt*)
- Uscita VGA (*opt*)
- Audio I/O (*opt*)

Atheros AR5212

- 802.11 a/bg
- H/W encryption support: WEP AES AES_CCM TKIP
- Code H/W per beacons/traffico e per QoS (WME)



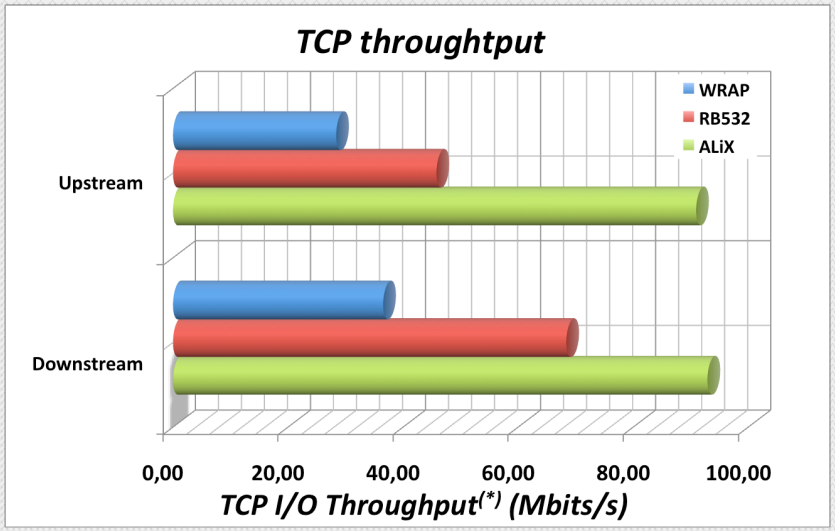
Immagini per gentile concessione di Pascal Dornier (www.pcengines.ch)

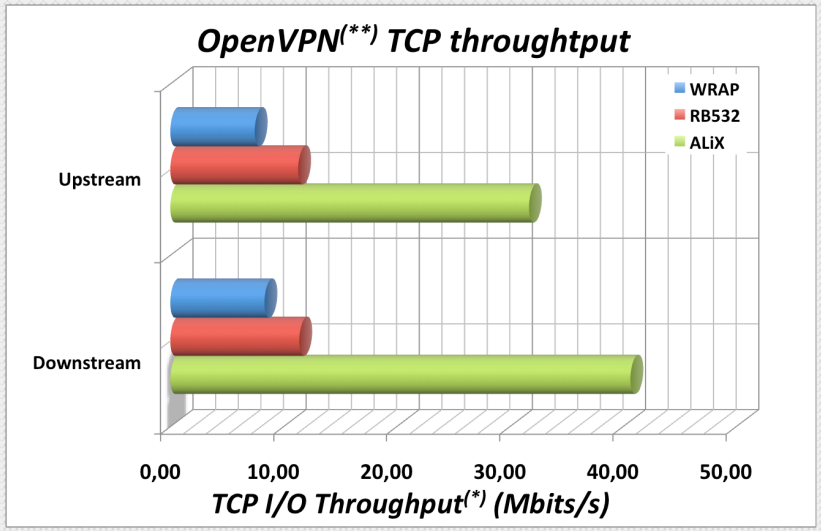
CASPUR

Soluzione tecnica

Estensione geografica del link layer – Apparati di accesso – Hardware (cont'd)

- ***Perché ALiX ?***
  - **TCO** ***~120€*** per ***O(10) pezzi***
    - *i.e.:* MoBo + Radio + Storage (CF) + Case + Antenne
  - **Dimensioni** (MoBo) 100x160 mm
  - **Prestazioni** bus e CPU





Confronto tra PCEngines WRAP, MikroTik RouterBoard 532A e PCEngines ALiX

(*) Misurazioni effettuate con ***iperf*** (ethernet crossover cable tra "client" e "server")

(**) openVPN con cifratura ***AES-128-CBC***

Soluzione tecnica

Estensione geografica del link layer – Apparati di accesso – Software

- Personalizzazione della distribuzione GNU/Linux ***OpenWRT***
  - Utilizzo del ***trunk svn compilato ad-hoc*** (Kamikaze)
    - Kernel Linux >= 2.6.22 (attualmente 2.6.24)
    - Driver wi-fi Madwifi-ng (attualmente snapshot 0.9.4)
    - 1000+ applicazioni/librerie open-source disponibili nel *buildroot*
  - Collaborazione attiva con gli sviluppatori (@IRC freenode.net #openwrt) per la risoluzione di alcuni bug (troubleshooting/patches submission)
  - Adattamento/configurazione e scrittura script per il monitoraggio
- Stiamo valutando l'utilizzo della distribuzione ZeroShell
  - In collaborazione con Fulvio Ricciardi (INFN) unico autore e mantainer

Soluzione tecnica

Estensione geografica del link layer – Ottimizzazioni apparati di accesso

- Per ogni ESSID è implementato l'isolamento delle stazioni (*i.e.*: ***client separation***)
  - Consente di limitare il traffico sulla singola radio
    - *e.g.*: non permette il file sharing tra le stazioni associate allo stesso ESSID
  - Mitiga gli effetti dei tipici attacchi L2 (*e.g.*: ARP poisoning)
- *Diversity* con determinazione automatica del ruolo delle antenne (*i.e.*:TX/RX)
- Determinazione automatica e ***per pacchetto*** della potenza di trasmissione

CASPUR

Lo stato della sperimentazione

CASPUR

Lo stato della sperimentazione

Apparati di accesso installati

- Sono attualmente installati i seguenti apparati realizzati da CASPUR
  - **Villa Borghese** (“Casino” dell’orologio e Museo Canonica, zona Piazza di Siena)
    - 5 Apparati Wi-Fi terminatori openVPN
    - 1 Apparato “concentratore” (serve altri access point multiple-ESSID)
  - **Biblioteca Nazionale Alessandrina**
    - 1 Apparato Wi-Fi terminatori openVPN
      - **26 utenze** contemporanee su più ESSID
      - ***100+ accessi*** al giorno
      - Throughput di ***2+ Mbit/s*** di picco giornaliero (downstream verso l’apparato)
  - **Biblioteca Nazionale Vallicelliana**
    - 2 Apparati Wi-Fi terminatori openVPN

CASPUR

Lo stato della sperimentazione

Apparati di accesso installati (cont'd)

- Sono attualmente installati i seguenti apparati (cont'd)
  - **Biblioteche comunali di Roma**
    - 1 Apparto "concentratore" installato presso il CED della Biblioteca Marconi di Roma
      - Serve gli access point multiple-ESSID di 3 sedi (a breve c.a. 40)
      - "Esporta" verso il punto d'interconnessione il livello 2 della rete Wi-Fi delle Biblioteche Comunali di Roma
  - **Università degli studi di Roma Tor Vergata**
    - 1 Apparato "concentratore" installato presso il CED dell'Università
      - "Esporta" verso il punto d'interconnessione il livello 2 della rete Wi-Fi dell'Università

CASPUR

Ulteriori Sviluppi

Sperimentazione – R&D

Ulteriori Sviluppi
Sperimentazione e R&D

- CASPUR è impegnato nella sperimentazione di diverse possibilità di utilizzo delle piattaforme embedded citate
  - Firewall IPv6 (attualmente in produzione)
  - ThinClient (*e.g.*: STB Multicast basato su VLC) in collaborzione con Unidata SPA
  - VoIP PBX
  - "Nagios"-Box
  - Con il firmware ZeroShell (http://www.zeroshell.net) si ha un "*appliance*" ***facilmente configurabile*** (*i.e.*: web interface) in grado di erogare molteplici servizi
    - Server RADIUS
    - Captive Portal
    - Firewall, Router, Bridge 802.1d, HTTP Proxy con antivirus, Traffic Shaper, gestione QoS, …
    - Terminazione VPN L2TP over IPsec e openVPN, …
    - Server DNS
    - PKI (X509)

Ulteriori Sviluppi

Sperimentazione e R&D (cont'd)

- Alcuni fronti di ricerca e sviluppo aperti
  - Vertical Handoff (UMTS/Wi-Fi/Ethernet) in collaborazione con il *Campus Biomedico Universitario* di Roma e Unidata SPA
    - primi risultati promettenti
  - Realizzazione di un sistema di gestione centralizzato per l'amministrazione delle MiniMotherboard con firmware OpenWRT
  - VANET (Vehicular Ad-Hoc NETwork)
    - IEEE 802.11p
    - Position-based Routing

Fine

(Q&A)

wireless@caspur.it

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