OpenWISP, una soluzione open source originale per la diffusione di servizi WiFi

Davide Guerri

CASPUR

Abstract. L'articolo presenta una soluzione originale sviluppata per permettere in modo semplice e versatile la diffusione di reti di accesso WiFi, anche tecnologicamente complesse, su connettività non dedicata ed eterogenea. Gli strumenti e le strategie utilizzate hanno permesso di implementare alcuni importanti progetti di diffusione di reti WiFi per il pubblico, principalmente promossi da Pubbliche Amministrazioni italiane. L'articolo propone inoltre una strategia per la semplice e veloce installazione di punti di accesso al servizio di roaming internazionale Eduroam in siti con limitate risorse tecnologiche.

1. Introduzione

La collaborazione fra il CASPUR e la Provincia di Roma per il progetto ProvinciaWiFi [1] ha permesso di implementare, in soli due anni, la più grande rete WiFi gratuita e aperta al pubblico mai realizzata in Italia e probabilmente la più grande d'Europa, con l'installazione di punti di accesso nei comuni del territorio provinciale di Roma. Le originali tecniche e gli strumenti utilizzati in questo contesto hanno mostrato il chiaro vantaggio di permettere la semplice e veloce diffusione di servizi di connettività pubblica su infrastrutture di rete che, per differenti ragioni di natura tecnica e legale, non avrebbero altrimenti potuto essere utilizzate per tale scopo. Inoltre questo approccio, abbracciando la filosofia della condivisione delle risorse tipica dei progetti open, permette a chiunque di contribuire alla crescita della rete, ospitando, senza alcun onere amministrativo e tecnologico, un punto di accesso.

Dall'esperienza acquisita sul campo, a seguito di un processo di reingegnerizzazione degli strumenti software utilizzati, è nata la suite software OpenWISP [2], che include quanto necessario per realizzare un servizio di connettività pubblica WiFi del tutto equivalente a quello utilizzato da ProvinciaWiFi. Come si vedrà, quest'ultimo servizio è solo uno dei possibili utilizzi degli strumenti presentati.

2. La suite di applicazioni OpenWISP

La suite OpenWISP comprende cinque applicazioni open source rilasciate con licenza GPLv3, utilizzabili congiuntamente o integrandone solo alcune con applicativi di terze parti, per realizzare e gestire l'infrastruttura tecnologica di un generico Wireless Internet Service Provider. OpenWISP, infatti, comprende quanto necessario per la gestione degli apparati di accesso WiFi e per la registrazione, identificazione, controllo degli accessi e *accounting* degli utenti finali del servizio.

2.1 OpenWISP User Management System

L'OpenWISP User Management System (OWUMS) è una delle applicazioni principali della suite poiché costituisce il punto di contatto degli utenti finali del servizio, che la utilizzano per auto-registrarsi, per gestire il proprio account e per consultarne le statistiche.

L'applicazione, sviluppata su framework Ruby on Rails, è strutturata in due sezioni principali: un *front-office*, che tipicamente viene reso accessibile anche dall'esterno della rete WiFi al quale è destinato, e un *back-office* utilizzabile dal personale tecnico per gestire il servizio ed espletare le procedure di helpdesk. Il front-office espone una ricca interfaccia web 2.0, in versione desktop e mobile che utilizza esclusivamente

Conferenza GARR_11 Selected Papers. Da 20 anni nel futuro. Bologna 8-10 novembre 2011
ISBN: 978-88-905077-3-1 © 2012 Associazione Consortium GARR

javascript al fine di garantire la massima compatibilità con tutti i recenti dispositivi mobili. Le operazioni effettuate sul front-office agiscono sulle tabelle di un DBMS relazionale, create e mantenute dal framework Ruby on Rails. Tali relazioni sono rese disponibili anche a un server RADIUS mediante opportune viste. Quest'ultimo servizio, interagendo con un Network Access Server (NAS) quale un *captive portal*, implementerà l'autenticazione, l'autorizzazione e l'accounting (AAA) per il servizio WiFi.

L'identificazione degli utenti costituisce uno strumento estremamente utile per la gestione di un servizio WiFi, anche dal punto di vista della sicurezza, permettendo il corretto utilizzo delle risorse. Su OWUMS la registrazione iniziale degli utenti può avvenire mediante tre differenti meccanismi, di seguito esposti.

2.1.1 Verifica di possesso di un'utenza di telefonia mobile

Secondo quanto riportato in un parere fornito dal Ministero dell'Interno in risposta ad una specifica richiesta da parte dell'associazione provider indipendenti (AssoProvider), è ammessa un'identificazione indiretta degli utenti di un servizio WiFi, ovvero senza obbligo di acquisizione di un documento d'identità, purché questa sia basata sulla verifica di possesso di un'utenza di telefonia mobile italiana [3]. L'applicazione OWUMS implementa tale verifica tramite acquisizione dell'identificativo chiamante (Caller-ID o CID): le credenziali dell'utente saranno abilitate solo se, entro un periodo di tempo configurabile, quest'ultimo effettuerà una chiamata telefonica ad un numero di rete fissa, associato tramite VoIP all'applicazione, dall'utenza telefonica inserita in fase di registrazione.

2.1.2 Transazione economica tramite carta di credito

L'applicazione OWUMS consente anche l'identificazione affidabile degli utenti che si auto-registrano sul sistema per mezzo della verifica di possesso di una carta di credito

2.1.3 Acquisizione della copia di un documento d'identità

Il terzo metodo di identificazione degli utenti del servizio segue pedissequamente quanto era prescritto dalla normativa italiana fino alla fine del 2010: tramite la supervisione di un operatore, opportunamente istruito, l'applicazione OWUMS permette l'upload della scansione di un documento d'identità che rimarrà associato all'account dell'utente.

2.2 OpenWISP Manager e Firmware

Il management dei punti di accesso di un servizio WiFi è un aspetto estremamente delicato della gestione di un Wireless ISP. Il controllo di apparati con hardware eterogeneo ma con configurazione uniforme e potenzialmente mutevole nel tempo è stata una delle criticità riscontrate durante la gestione del progetto ProvinciaWiFi. La scelta del *firmware* per gli apparati di accesso è caduta inevitabilmente su openWRT, open source e leader nel settore delle distribuzioni specifiche per *wireless router* [4]. Il grande vantaggio di utilizzare openWRT in un contesto quale quello presentato è stato individuato anche nella presenza di un sistema integrato di configurazione in grado di agire su ogni aspetto fondamentale del sistema, lo Unified Configuration Interface (UCI). Tale sistema, pur essendo limitato alla configurazione locale, permette un buon livello di astrazione dallo specifico hardware utilizzato e consente l'utilizzo di molteplici funzionalità avanzate, quali Bridging Linux 802.1d, Virtual Local Access Network (VLAN) tagging 802.1Q, Virtual Access Point (VAP) multipli su singola scheda radio, Virtual Private Network (VPN) ed il Port Based Network Access Control basato su 802.1X con, ad esempio, WPA o WPA2 in modalità *enterprise*.

Per remotizzare il funzionamento di UCI e permettere l'amministrazione centralizzata di una moltitudine di apparati d'accesso, installati anche su reti con connettività eterogenea e su un'importante estensione territoriale, è stato sviluppato un sistema di *configuration management* che potesse controllare senza sforzo e tramite una comoda interfaccia grafica migliaia

di access point, anche contemporaneamente.

L'applicazione Ruby on Rails denominata OpenWISP Manager (in breve OWM) implementa proprio un sistema di configuration management UCI-oriented, in grado di modellare la configurazione degli access point mediante template che ne descrivono le caratteristiche essenziali. Ogni access point è dunque istanza di un *template* e rimane ad esso collegato: qualunque modifica effettuata sul template sarà applicata anche alle sue istanze, ma rimarrà possibile la personalizzazione di alcune delle caratteristiche di ogni singola istanza, finalizzata al *finetune* dell'access point ad essa associato.

La gerarchia di oggetti che descrive ogni access point, modellata tramite OWM, è tradotta in una configurazione UCI, scaricata ed eseguita dagli apparati di accesso. Periodicamente, ogni access point verifica lo stato di aggiornamento delle informazioni ricevute dal server OWM e, se necessario, provvede a scaricare nuovamente la sua configurazione.

L'insieme delle applicazioni che risiedono sugli access point, che realizzano i meccanismi sopra riportati, è denominato OpenWISP Firmware (OWF). L'OWF si occupa anche di realizzare e curare la disponibilità di un canale di comunicazione sicuro, mediante una VPN realizzata con il software openVPN [5] tra l'access point e il server OWM. Tale canale, denominato setup-VPN, è utilizzato dagli apparati di accesso per richiedere la propria configurazione e consente il monitoraggio e la gestione dell'apparato da parte degli operatori.

Infine, per semplificare l'installazione degli access point, l'OWF espone un'interfaccia web minimale attraverso la quale è possibile inserire alcune informazioni essenziali per la configurazione di rete, in funzione di quanto richiesto dal sito ospitante e per effettuare il *troubleshooting* delle più comuni problematiche in fase di *deployment* dell'apparato.

La sequenza delle operazioni implementate dall'OWF per ottenere la configurazione da un server OWM è riportata in figura 1. Poiché la setup-VPN è originata dall'access point, lo svolgimento dei processi legati al *configuration management* è garantito anche se l'apparato viene installato dietro ad un firewall o ad un dispositivo che implementa il NAT, a patto che le comunicazioni originate dall'access point possano raggiungere il server OWM.

La configurazione *runtime* tipica di un access point consiste nel veicolare all'interno di una VPN più VLAN 802.1Q. Ogni VLAN sarà poi opportunamente collegata ad un VAP tramite un bridge 802.1d. Poiché tutte le VPN sono realizzate con flussi UDP o TCP, tale configurazione permette la propagazione di reti WiFi multiple (ad esempio dedicate rispettivamente a servizi di connettività pubblica e a servizi municipali) su connettività preesistente, quale una semplice ADSL, anche in presenza di firewall o NAT.

2.3 OpenWISP Geographic Monitoring

Per assicurare l'opportuno livello di qualità e disponibilità di un servizio WiFi è necessario avere un adeguato strumento di monitoraggio. L'OpenWISP Geographic Monitoring (OWGM) è stato sviluppato per rispondere alle esigenze maturate nel corso della gestione

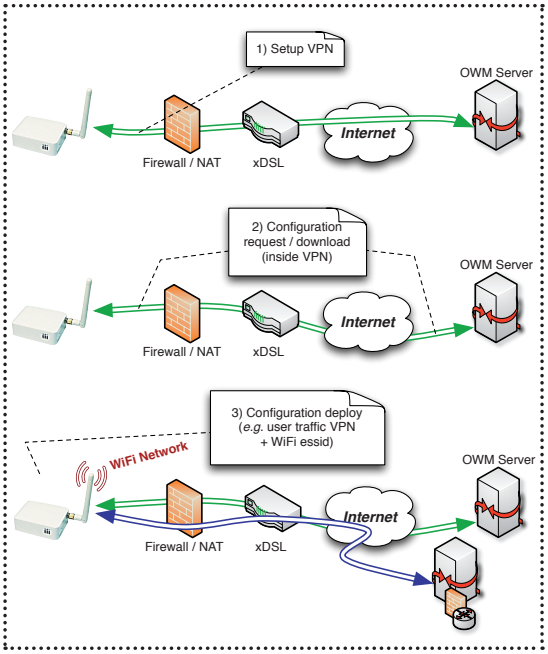

Fig. 1 Sequenza delle operazioni implementate dall'OWF per ottenere la configurazione da un server OWM

di numeri molto elevati di apparati di accesso. OWGM permette la visualizzazione dello stato della rete tramite differenti livelli di dettaglio: ad alto livello, con una mappa realizzata mediante la terza versione delle API di Google Maps, mostrando lo stato degli access point anche suddividendoli in *cluster* ove necessario; a livello intermedio, attraverso statistiche di disponibilità percentuale dei singoli apparati di acceso rispetto ad un arbitrario periodo di osservazione; e a basso livello, permettendo l'analisi dettagliata dei singoli apparati in termini di disponibilità e numero di utenti collegati.

Per consentire l'esportazione dell'elenco geo-referenziato degli access point, utilizzabile ad esempio per mostrare agli utenti finali la posizione dei punti di accesso al servizio, OWGM consente l'emissione di un *feed* di tipo Geographic Really Simple Syndication (GeoRSS) [6], personalizzabile nei contenuti descrittivi mediante l'interfaccia web dell'applicazione.

2.4 OpenWISP Captive Portals Manager

Attualmente, è tipico che le reti WiFi aperte al pubblico presentino un controllo degli accessi basato su captive portal. Le motivazioni di questa scelta, in contrapposizione a quanto offerto dallo stato dell'arte dei protocolli, dagli algoritmi e dai meccanismi crittografici implementati da 802.1X quando utilizzato da WPA/WPA2 in modalità *enterprise*, va ricercata nella semplificazione delle procedure e delle competenze necessarie per il grande pubblico ad utilizzare il servizio. Benché le applicazioni della suite OpenWISP permettano l'utilizzo di standard con alti livelli di sicurezza, tutte le installazioni effettuate sono state dotate di un portale di accesso web verso il quale avviene la redirezione forzata del protocollo HTTP fino all'avvenuta autenticazione.

Il panorama open source presenta alcune interessanti soluzioni per la realizzazione di captive portal, tuttavia, fondamentalmente per esigenze di personalizzazione e integrazione, si è scelto di realizzare un'implementazione *ad hoc*: l'OpenWISP Captive Portals Manager (OWCPM). OWCPM supporta, tra le altre funzionalità, la gestione di captive portal multipli, l'utilizzo di un server RADIUS per autenticare gli utenti del servizio e per autorizzarli in modo differente nell'utilizzo della rete e per implementare l'accounting.

2.5 OpenWISP MiddleWare

L'ultima applicazione è l'OpenWISP MiddleWare (OWMW), che costituisce il collante tra le applicazioni della suite, mediante un livello d'astrazione che espone un'interfaccia di tipo RESTful. Mediante OWMW, è inoltre possibile esportare verso applicazioni di terze parti alcune informazioni, come ad esempio quelle sulla posizione geografica degli access point o degli utenti attivi.

3. Risultati

3.1 Le reti WiFi gestite da OpenWISP

La suite OpenWISP è oggi utilizzata per gestire alcune delle principali reti wireless italiane. Oltre a ProvinciaWiFi, che può essere considerata come il motore di tutti i progetti esposti nel presente articolo, alla fine del 2011 OpenWISP è alla base dei servizi WiFi delle città di Genova e Torino e delle Province di Grosseto, Prato, Pistoia e Gorizia. Il totale degli access point gestiti nell'ambito dei vari progetti è, sull'intero territorio nazionale, superiore alle 1.200 unità, per oltre 160 mila utenti complessivi.

3.2 OpenWISP e Eduroam

Eduroam (Education Roaming) realizza un servizio di accesso in *roaming*, con elevati standard di sicurezza, tramite una federazione mondiale di comunità di ricerca e istruzione. Dal punto di vista tecnico, Eduroam è implementato mediante meccanismi, protocolli e algoritmi di WPA/WPA2 Enterprise per l'accesso alla rete e ad una gerarchia di *proxy* RADIUS per la validazione delle credenziali degli utenti in roaming [7].

Nella seconda metà del 2011 è stata avviata una collaborazione tra il GARR, coordinatore per la federazione italiana Eduroam, la Provincia di Roma e CASPUR. La collaborazione era finalizzata a capire se le tecnologie uti-

lizzate per Eduroam fossero fruibili attraverso gli access point di ProvinciaWiFi e, in caso affermativo, iniziare una sperimentazione su un sottoinsieme di questi ultimi apparati. Il setup elaborato per la sperimentazione è riportato in figura 2. Questo ha previsto, oltre a quanto necessario per annunciare le reti WiFi della Provincia di Roma, l'inoltro di due VLAN 802.1Q: una per veicolare il traffico IPv4 e IPv6 degli utenti autenticati e l'altra per permettere la comunicazione tra l'*authenticator* 802.1X (nella fattispecie il *daemon hostapd*) e il proxy RADIUS Eduroam di GARR.

La sperimentazione si è conclusa positivamente, anche se i risultati hanno indicato la necessità di aggiornare il firmware OWF degli apparati in produzione per poter risolvere alcuni *bug* e supportare propriamente WPA/WPA2 con 802.1X. Alla fine del 2011 un piccolo nucleo di apparati ProvinciaWiFi annuncia Eduroam mediante connettività ADSL, in luoghi utilizzati da potenziali utenti del servizio di roaming mondiale. Dato l'intrinseco livello di sicurezza, i requisiti d'installazione richiesti per Eduroam non sono facilmente realizzabili da tutte le istituzioni potenzialmente interessate al servizio e comunque potrebbero insorgere delle difficoltà per sedi distaccate con risorse tecniche limitate. Uno dei vantaggi fondamentali che si ottiene utilizzando Eduroam con l'architettura proposta, è invece quello di permettere una veloce e semplice installazione di apparati di accesso ovunque vi sia disponibilità di connettività IP verso il *datacenter* dell'istituzione interessata alla promozione della federazione.

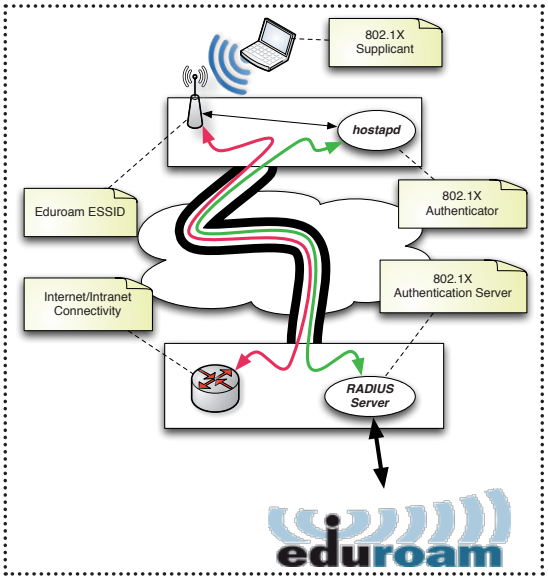

Fig. 2 Setup elaborato per la sperimentazione dell'integrazione di ProvinciaWiFi e Eduroam

Riferimenti bibliografici

[1] ProvinciaWiFi, http://www.provincia.roma.it/percorsitematici/innovazione-tecnologica/progetti/4035

[2] OpenWISP application suite http://www.openwisp.org

[3] Parere del Ministero dell'Interno, prot. n.300D/89/44lF.320/3668 del 27/11/2007 http://www.scribd.com/doc/54536635/Autenticazione-Parere-Ministero-Delle-Comunicazioni-1

[4] OpenWRT, https://openwrt.org

[5] OpenVPN, http://www.openvpn.net

[6] GeoRSS, http://wikipedia.org/wiki/GeoRSS

[7] Eduroam, http://www.eduroam.it

Davide Guerri
davide.guerri@gmail.com

Laureato in Informatica, ha conseguito il master in "Sicurezza dei sistemi e delle reti" de "La Sapienza" di Roma. Ha progettato l'infrastruttura tecnologica di ProvinciaWiFi, è ideatore e lead developer della suite OpenWISP e CTO dei servizi WiFi offerti da CASPUR alle P.A. È CTO dell'IX-WiFi.