



WiFi della città metropolitana di Roma Capitale: 10 anni di collaborazione tra CNR e un Ente territoriale di area vasta.[†]

Augusto Pifferi,^{*a} Giovanni Agostini,^a Massimiliano Catricalà^a

La Città metropolitana di Roma Capitale ha varato nel 2008 il "Piano Innovazione" per la diffusione delle reti WiFi e per la lotta al digital divide. Tra i progetti contenuti nel Piano, "WiFi-metropolitano" intende valorizzare e modernizzare il territorio provinciale, adottando soluzioni tecnologiche avanzate per il monitoraggio, il controllo e la salvaguardia delle aree, mediante sistemi a basso impatto ambientale. Con "WiFi-metropolitano" i più importanti luoghi di ritrovo del territorio provinciale sono dotati di punti di accesso ad Internet a banda larga, senza fili, per permettere ai cittadini/utenti di navigare gratuitamente in rete (1 ora al giorno e per un massimo di 300 MB).

Si tratta di un progetto per la diffusione di Internet gratis senza fili che per numero di abitanti coinvolti (circa 4 milioni di persone), superficie del territorio (5mila Km²) e Comuni interessati (121) è una rete tra le più vaste d'Europa. Nell'ottobre 2008 l'Area della Ricerca RM1 del CNR inizialmente e l'Istituto di Cristallografia poi hanno firmato il primo di una serie di accordi per la collaborazione nell'ambito del progetto.

Keywords: WiFiMetropolitano, WiFi libero, Hiperlan.



1 Introduzione

Nel 2008 l'allora Provincia di Roma, alla quale dal 1° gennaio 2015, è succeduta amministrativamente la Città metropolitana di Roma Capitale, la quale ha giurisdizione sull'intero territorio dell'ex provincia, composta di 121 comuni, ha lanciato l'ambizioso progetto di portare il WiFi libero e gratuito in ciascuno dei 121 comuni inclusi nel proprio territorio. Attualmente la rete WiFi della ex Provincia e della città di Roma sono confluite in un'unica rete. "WiFi-metropolitano"¹, la rete WiFi pubblica della Città metropolitana di Roma Capitale che vede coinvolti tutti i 121 comuni metropolitani, ha raggiunto recentemente quota 500.000 utenti registrati con più di 6.000 connessioni al giorno. Il primo iscritto risale al 17 novembre 2008, giorno in cui è stato inaugurato il primo hot spot presso la sede di Palazzo Valentini. Questa rete, per la connessione ad internet senza fili gratis, continua ad essere la più grande rete pubblica di WiFi in Europa: con 2.310 Access Point su 1.331 siti dislocati nelle principali aree pubbliche tra cui scuole, centri anziani, ospedali, biblioteche ed esercizi commerciali.

A partire dall'anno precedente, l'Area della Ricerca RM 1 del CNR aveva iniziato a stringere accordi per l'installazione di trasmettitori wireless per collegamenti WiFi nei comuni della Sabina romana e reatina e nell'area nord occidentale del territorio della ex Provincia di Roma per rispondere alla richiesta dei ter-

ritori contigui all'Area di colmare il profondo divario digitale di cui erano afflitti. E' stato quindi naturale, vista l'affinità degli obiettivi, che CNR e Provincia iniziassero un dialogo che si è concretizzato nell'ottobre del 2008 con la firma di un accordo tra Dipartimento di Progettazione Molecolare e Provincia di Roma proprio in coincidenza con l'avviamento del progetto che allora era denominato "Provincia WiFi". In questo accordo era previsto che il CNR installasse un primo gruppo di 14 Access Point forniti dalla Provincia collegandoli in internet attraverso la propria rete wireless nel territorio. Da allora questi accordi sono stati rinnovati di anno in anno (attualmente firmati tra la Città metropolitana di Roma Capitale ed Istituto di Cristallografia) arrivando ad un parco di Hot spot installati di 34 in continua crescita.

2 La rete wireless geografica

Nel 2007 il Servizio Reti dell'Area della Ricerca RM 1 dette vita ad un progetto di abbattimento del Digital Divide nel territorio della Sabina romana e reatina sulla spinta di esigenze manifestate dagli Enti locali. Infatti gli operatori di telecomunicazioni non avevano interesse a portare infrastrutture di telecomunicazioni digitali in zone a remissione di mercato e quindi in quest'area non erano disponibili connessioni digitali di adeguata qualità e performance. D'altra parte lo Stato aveva in atto un piano di digitalizzazione che obbligava i Comuni ad utilizzare procedure telematiche in sostituzione dell'ormai obsoleto "passaggio di carte". L'idea fu quella di realizzare una infrastruttura leggera, basata su tecnologie wireless che permettevano servizi di buona qualità. Non bisogna dimenticare che nel 2007 si era alle soglie del bando di gara per l'assegnazione delle frequenze del WiMax² (acronimo di **W**orldwide **I**nteroperability

^a C.N.R. Istituto di Cristallografia - UOS Monterotondo, via Salaria Km. 29,300, 00015 Monterotondo Scalo (RM), Italia.

Creative Commons Attribuzione - Non commerciale - Condividi allo stesso modo 4.0 Internazionale

[†] Rapporto tecnico IC-RM 2017/10 protocollato in data 03/08/2017 n. 1337

for Microwave Access). Il servizio reti aveva in prova degli apparati WiMax dell'Aperto networks che furono installati inizialmente nel comune di Torrita Tiberina (RM) e S.Oreste (RM) utilizzando frequenze di trasmissione a 3.7GHz destinate alla sperimentazione con questa tecnologia. Con l'assegnazione delle frequenze nel febbraio del 2008 fu necessario interrompere la sperimentazione WiMax e pertanto si optò per la tecnologia wireless HIPERLAN³ (HIGH PERFORMANCE Radio LAN) in banda libera a 5.4GHz. Rapidamente furono installati presso i comuni che avevano aderito al progetto CNR nuove stazioni base. In figura 1 è mostrata l'area geografica coperta dalla rete wireless nella sua attuale estensione (giugno 2017).

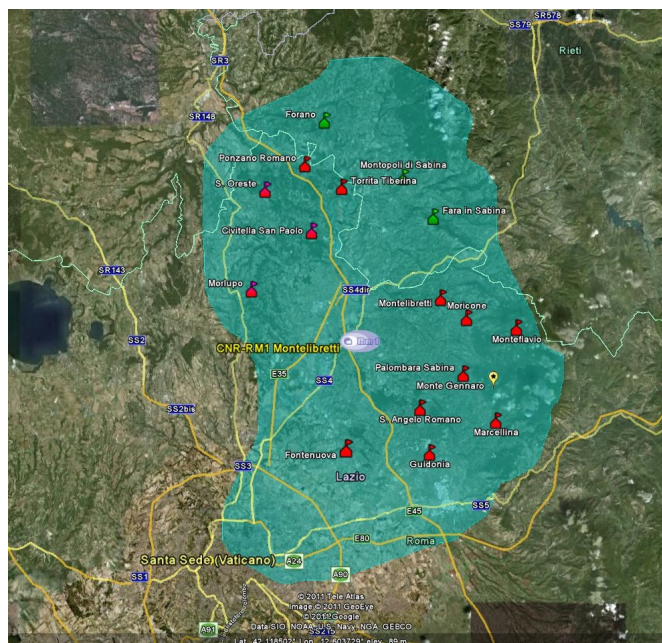


Fig. 1 Area geografica coperta dalla rete wireless dell'Istituto di Cristallografia

3 Gli Access Point della Città Metropolitana

Negli accordi è prevista da parte della Provincia di Roma (Città Metropolitana di Roma Capitale) la fornitura degli Access Point (AP) da installare nel luogo prescelto. Gli apparati utilizzati sono di marca Ubiquiti e devono essere riprogrammati con un firmware appositamente realizzato al fine di instaurare il tunnel VPN verso la rete del CASPUR (oggi CINECA)⁴ che opera come Ente per la gestione dei sistemi di monitoraggio e l'implementazione del software e del firmware. L'accesso fisico alla rete Internet viene assicurato dall'Internet Service Provider Fastweb.

Ogni Access Point instaura almeno due VPN con il centro servizi di Città Metropolitana di Roma Capitale. La prima VPN, "di setup", necessaria solo durante la fase di avvio dell'apparato consente il recupero di alcuni parametri di funzionamento:

SSID reti Wi-Fi pubblicate

VPN "d'esercizio" da utilizzare

La seconda VPN, "d'esercizio", è utilizzata per incapsulare tutto il traffico dati degli utenti (Wi-Fi). Tutto il traffico delle VPN è cifrato e gli end-point di queste VPN sono mutuamente autenticati. A tal fine si utilizza la cifratura SSL con certificati X509. Questo richiede la verifica di validità temporale dei cer-

tificati ed è quindi necessario che la data interna degli AP sia corretta.

La sincronizzazione della data interna degli AP richiede sempre almeno una di queste porte:

UDP 123(ntp)

TCP 80(htpdate)

La VPN "di setup" utilizza sempre la porta TCP 1194. La VPN "d'esercizio" utilizza il protocollo TCP e UDP e le porte comunicate dal sistema di autoprovisioning della configurazione attraverso la prima VPN instaurata. Tipicamente vengono usati i seguenti range di porte:

tcp e udp range 1198 - 1200

tcp e udp range 12128 - 12130

Gli AP utilizzati per il servizio WiFimetropolitano sono molto flessibili e permettono di essere impiegati anche in presenza di reti con NAT/firewall a patto che i protocolli e le porte citate in precedenza siano utilizzabili in uscita dalla rete ospitante. Per semplificare, il funzionamento degli AP richiede che:

Sia permesso tutto il traffico proveniente dagli AP e diretto verso le reti 194.242.230.0/24 e 151.0.255.64/27

La porta UDP 123 (Network Time Protocol) oppure la porta TCP 80 (HTPDATE).

Non è richiesta l'apertura di porte verso l'AP

Ai fini della sicurezza tutto il traffico degli utenti è incapsulato nella VPN "d'esercizio" e viene visto su internet con l'IP di Città Metropolitana di Roma Capitale. La rete ospitante è utilizzata solo per la configurazione iniziale dell'AP, sincronizzazione dell'ora e VPN "di setup" in cui il traffico IP sorgente è uguale all'IP dell'AP sulla rete ospitante e l'IP destinazione è l'IP del centro servizi.

Il meccanismo di autenticazione degli AP è molto semplice; una volta programmato il firmware e connesso alla rete pubblica l'apparato fa una chiamata verso un determinato server con il quale instaura il protocollo VPN. A questo punto chi si collega con il proprio terminale sulla rete wireless viene reindirizzato verso il portale della Città Metropolitana ove può essere effettuata la registrazione per fornire la propria identità e creare una nuova utenza o se già registrati, inserendo user e Password, si può iniziare la navigazione.

4 Installazione tipo

Per la connessione alla rete WWAN (Wireless Wide Area Network) gestita dall'Istituto ogni Access Point della Provincia viene connessa ad un'antenna del tipo SXT 5 (figura 2) per collegamenti alla stazione base fino a 8-10 Km. Per distanze superiori fino a 15-17Km si utilizzano delle antenne Mikrotik del tipo QRT 5 (figura 3).



Fig. 2 Antenna Mikrotik SXT 5



Fig. 3 Antenna Mikrotik QRT 5 e scheda router interna

L'accesso alla rete avviene con protocollo PPPoE che riceve le credenziali e configura le caratteristiche della connessione da un server Radius per l'autenticazione, l'autorizzazione e l'accounting (AAA). Sono stati perciò predisposti profili di accesso per ognuno dei punti Provincia WiFi controllati dall'Istituto (figura 4).

Ad oggi gestiamo 34 access point sul territorio provinciale, distribuiti nei comuni e località di:

- Acquaviva di Nerola (1)
- Civitella San Paolo (1)
- Cretona (1)
- Fonte Nuova (3)
- Guidonia (4)
- Montorio Romano (1)
- Marcellina (1)
- Monteflavio (1)
- Montecelio (1)
- Montelibretti (1)
- Moricone (2)
- Morlupo (2)
- Nerola (1)
- Palombara Sabina (3)
- Prco dei Monti Lucretili (1)
- Ponzano Romano (1)
- Santa Lucia di Fontenuova (1)
- Sant'Oreste (2)
- Scuola di Cavalleria dell'Esercito di Montelibretti (2)
- Stazzano (1)
- Torrita Tiberina (1)
- Villa dei Quintili (Appia antica) (1)

oltre ad un concentratore installato presso l'Area della Ricerca RM1 del CNR che consente l'accesso alla rete della Provincia in tutti gli edifici dell'Area dotati di router wireless centralizzati.

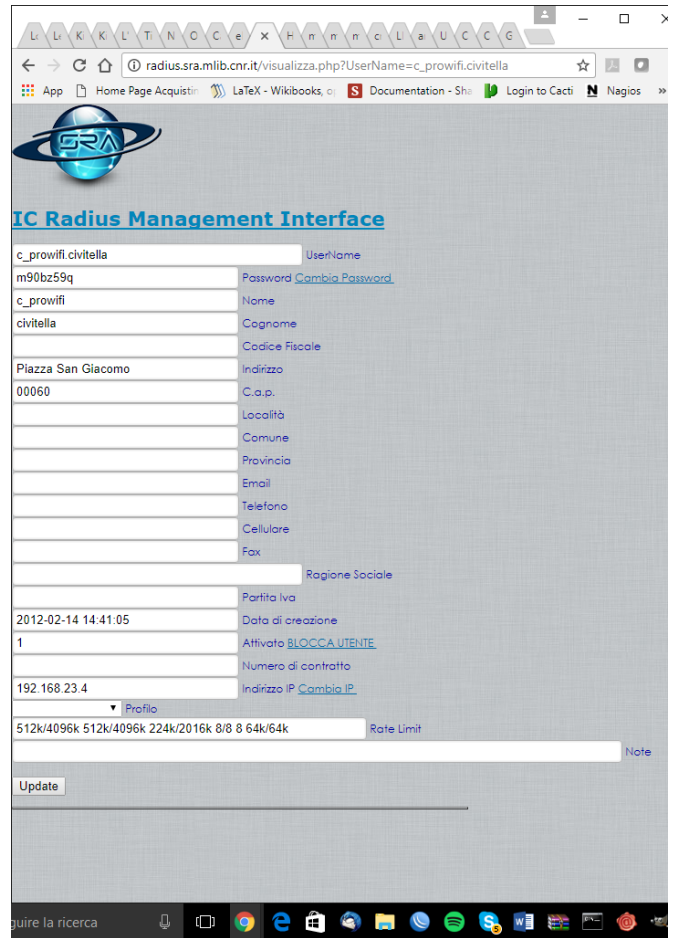


Fig. 4 Profilo Radius

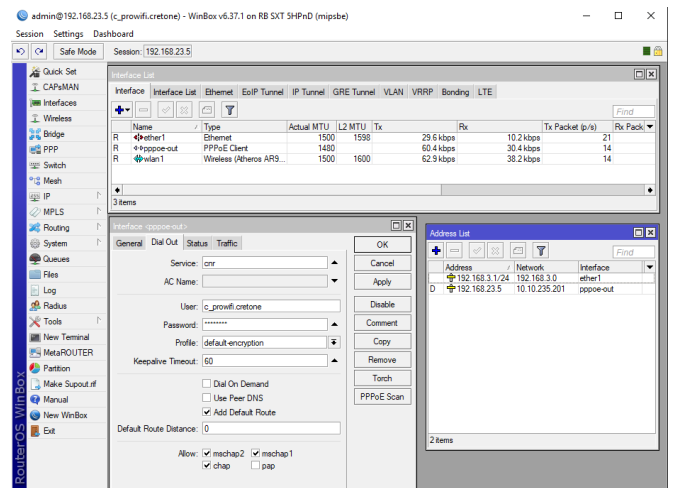


Fig. 5 Esempio di configurazione della routerboard Mikrotik

5 Test di funzionamento post installazione

Al termine dell'installazione in situ degli apparati, se l'AP non ha la configurazione adeguata (sia localmente sia lato server centrali) o se è stato alimentato ma non collegato alla rete, entra in uno stato denominato di "setup" che perdura fino a che l'apparato non riesce a scaricare (dai server centrali) la propria configurazione. In questo stato l'AP annuncia l'ESSID "owf-00:11:22:33:44:55" ove il codice numerico di suffisso a "owf-" corrisponde al MAC address dell'interfaccia ethernet dell'apparato. Tale codice è tipicamente riportato sulle etichette dell'ap-

parato stesso al quale è possibile associarsi inserendo l'apposita password. La configurazione della scheda Wi-Fi del computer utilizzato per l'installazione deve prevedere l'ottenimento dei parametri di rete via DHCP. Dopo la corretta associazione, l'AP fornirà un indirizzo IP del tipo: 172.22.33.x. Per ottenere l'Accesso all'interfaccia WEB dell'AP occorre aprire un browser (Internet Explorer, Chrome, Firefox, Opera, Safari, etc..) e scrivere nella barra degli indirizzi: http://172.22.33.1:8080/. Premendo invio, il browser visualizzerà un menù che permetterà una delle seguenti operazioni:

- Access Point Information - Informazioni generali apparato
- Connectivity Settings - Configurazione connettività apparato
- Site Test - Test sito
- Status Log - Log apparato
- Reboot Device - Riavvio apparato

Generalmente è sufficiente utilizzare la sola funzione Connectivity Settings per configurare la modalità con la quale l'AP acquisisce i parametri di rete. Tuttavia, in caso di problemi è possibile consultare i log in Status Log ed effettuare un test del sito (Site Test) per cercare di individuare le cause del malfunzionamento.

6 Monitoraggio e controllo

Il controllo dello stato di funzionamento degli Access Point avviene grazie a due sistemi complementari. Le antenne wireless (CPE) vengono costantemente interrogate dal sistema di monitoraggio Open Source Zabbix⁵ installato sui server dell'Istituto di Cristallografia. In parallelo la Città metropolitana mantiene sotto controllo gli Access Point con il proprio sistema di monitoraggio basato sul progetto Open Source OpenWisp⁶, piattaforma indicata per il controllo di apparati wireless di Internet Service Provider. L'abbinamento di questi due sistemi indipendenti di monitoraggio fornisce preziose indicazioni in caso di down di un "sistema". Infatti se l'eventuale guasto è da attribuirsi al link fornito dalla CPE vedremo sui sinottici l'allarme sia per l'apparato wireless su Zabbix sia l'allarme sul sistema OpenWisp. Questa è una situazione ambigua in quanto l'indicazione ricevuta è che sicuramente l'apparato wireless di collegamento alla rete ha problemi, ma non si ha indicazione sullo stato reale dell'Access Point. Nel caso in cui si abbia un allarme solo sul sistema OpenWisp, fatti gli opportuni controlli sul funzionamento del routing, si può intervenire sull'apparato di diffusione wireless locale. In un progetto in cui i dispositivi sono distribuiti in un territorio molto vasto queste informazioni sono di estrema importanza in quanto consentono di ottimizzare e/o programmare le uscite dei tecnici per la risoluzione dei guasti e per le manutenzioni.

7 Conclusioni

Il progetto della rete WiFi libera della Città Metropolitana di Roma Capitale, con l'abolizione delle Province, si è fuso con l'analogo progetto del Comune di Roma. Il "WiFimetropolitano" ha allargato i suoi confini per permettere a tutti l'accesso al web utilizzando ovunque le stesse credenziali (USER ID e PASSWORD) e poter consentire alle Amministrazioni pubbliche, che non hanno il WiFi, di costruire una propria rete anche grazie alla piattaforma Open Source messa a disposizione di tutti gli Enti Locali dalla Città metropolitana di Roma Capitale.

Host	Description	Last check	Last value	Change	History
Montecelio	- other - (2 Items)				
	ICMP Link	08 Jul 2015 15:27:39	1	-	Graph
	ICMP Roundtrip	08 Jul 2015 15:27:40	9.67 ms	-0.56 ms	Graph
Monte Flavio	- other - (2 Items)				
	ICMP Link	08 Jul 2015 15:27:57	1	-	Graph
	ICMP Roundtrip	08 Jul 2015 15:27:28	67.27 ms	+36.82 ms	Graph
Montelibretti	- other - (2 Items)				
	ICMP Link	08 Jul 2015 15:27:43	1	+1	Graph
	ICMP Roundtrip	08 Jul 2015 15:27:44	6.63 ms	+6.62 ms	Graph
Montorio	- other - (2 Items)				
	ICMP Link	08 Jul 2015 15:27:38	1	-	Graph
	ICMP Roundtrip	08 Jul 2015 15:27:09	4.27 ms	-9.53 ms	Graph
Moricone	- other - (2 Items)				
	ICMP Link	08 Jul 2015 15:27:43	1	-	Graph
	ICMP Roundtrip	08 Jul 2015 15:27:14	24.14 ms	+5.49 ms	Graph
Morlupo	- other - (2 Items)				
	ICMP Link	08 Jul 2015 15:27:51	1	-	Graph
	ICMP Roundtrip	08 Jul 2015 15:27:22	15.01 ms	-1.57 ms	Graph
Nerola	- other - (2 Items)				
	ICMP Link	08 Jul 2015 15:28:06	1	-	Graph
	ICMP Roundtrip	08 Jul 2015 15:27:07	10.64 ms	-17.77 ms	Graph
Palombara Comune	- other - (2 Items)				
	ICMP Link	08 Jul 2015 15:27:40	1	-	Graph
	ICMP Roundtrip	08 Jul 2015 15:27:11	9.35 ms	-1 ms	Graph
Palombara Pit	- other - (2 Items)				
	ICMP Link	08 Jul 2015 15:28:01	1	-	Graph
	ICMP Roundtrip	08 Jul 2015 15:27:32	8.13 ms	-3.84 ms	Graph
Ponzano	- other - (2 Items)				
	ICMP Link	08 Jul 2015 15:27:45	1	-	Graph
	ICMP Roundtrip	08 Jul 2015 15:27:16	13.23 ms	-1.59 ms	Graph
S. Oreste biblioteca	- other - (2 Items)				
	ICMP Link	08 Jul 2015 15:27:53	1	-	Graph
	ICMP Roundtrip	08 Jul 2015 15:27:24	13.57 ms	+2.23 ms	Graph
Stazzano	- other - (2 Items)				
	ICMP Link	08 Jul 2015 15:27:41	1	-	Graph
	ICMP Roundtrip	08 Jul 2015 15:27:12	12.15 ms	+5.65 ms	Graph
Torrita	- other - (2 Items)				
	ICMP Link	08 Jul 2015 15:27:42	1	-	Graph
	ICMP Roundtrip	08 Jul 2015 15:27:13	10.75 ms	-0.41 ms	Graph

Fig. 6 Zabbix monitor

Hostname	Site di installazione	Indirizzo	Città	Mac address	Gruppo	Pubblicato	Preferito	Stato
CNR_BorgoMera	Piazza Palmiro Togliatti	Piazza Palmiro Togliatti	Montebretti	08:15:56:74:39:59	CNR	✓	✖	🟢
CNR_CivitaPaola	Piazza San Giacomo	Piazza San Giacomo	Civitate San Paolo	08:27:22:24:7a:67	CNR	✓	✖	🟢
CNR_Civione	Civione	Via Alessandro Manzoni	Fiorenza Sabina	01:9f:db:37:31:90	CNR	✓	✖	🟢
CNR_FondNuova	Piazza delle rose - Santa Lucia	Piazza delle Rose	Fonte Nuova	08:27:22:24:7a:68	CNR	✓	✖	🟢
CNR_FondNuova2	Municipio	Fonte Padre Pio	Fonte Nuova	08:27:22:4f:45:43	CNR	✓	✖	🟢
CNR_Guidonia1	Municipio	Piazza Matteotti	Guidonia Montecelio	08:27:22:24:7a:65	CNR	✓	✖	🟢
CNR_Guidonia2	Comando di Polizia Municipale	Viale Roma 145	Guidonia Montecelio	01:9f:db:37:2a:90	CNR	✓	✖	🟢
CNR_Guidonia3	Municipio	Piazza Matteotti	Guidonia Montecelio	24:84:3c:4f:ed:5c	CNR	✓	✖	🟢
CNR_Guidonia4	Istituto comprensivo Giovanni XXIII	Piazza Cole Orto	Guidonia Montecelio	08:72:51:0f:44:2a	CNR	✓	✖	🟢
CNR_Marcellina	Piazza Cesare Battisti	Piazza Cesare Battisti	Marcellina	08:27:22:4d:7a:c0	CNR	✓	✖	🟢

Fig. 7 Open Wisp

le. Per questo nel 2010, grazie ad un Protocollo di Intesa tra la Città metropolitana (allora Provincia di Roma), il Comune di Venezia e la Regione Sardegna, è nata “Free ItaliaWiFi” una federazione nazionale delle reti WiFi pubbliche a cui, ad oggi, hanno aderito 81 Amministrazioni. Per il prossimo futuro si sta studiando la possibilità di far aderire le reti libere locali di alcuni comuni gestite con progetti speciali dall’Istituto di Cristallografia al più ampio progetto di Free ItaliaWiFi con il notevole vantaggio per l’utenza di poter usare una sola credenziale per una delle reti WiFi libera più vaste d’Europa.

Riferimenti

- 1 <http://www.cittametropolitanaroma.gov.it/homepage/wifi-metropolitano>.
- 2 <https://it.wikipedia.org/wiki/WiMAX>.
- 3 <https://it.wikipedia.org/wiki/HIPERLAN>.
- 4 <https://www.cineca.it/it>.
- 5 <https://www.zabbix.com>.
- 6 <http://openwisp.org>.

Appendice

Localizzazione degli Access Point della Città Metropolitana gestiti dall'Istituto di Cristallografia.



Acquaviva di Nerola - Piazza Santa Teresa



Civitella San Paolo - Piazza S. Giacomo



Cretone - Belvedere



Monteflavio - via delle Grazie e Centro convegno



Montorio Romano - via 4 Novembre



Marcellina - Piazza Cesare Battisti



Fontenuova - Piazza Padre Pio



Fontenuova (Santa Lucia) - Piazza delle Rose



Fontenuova (Santa Lucia) - Parrocchia Santa Lucia



Guidonia - Piazza Matteotti



Guidonia - via Roma presso Comando Vigili



Guidonia Loc. La Botte - Piazza Colle Grato



Montecelio - Convento di San Michele, Museo



Montelibretti - Piazza della Repubblica



Moricone - Piazza Sante Aureli e Biblioteca



Morlupo - Piazza Armando Diaz e Biblioteca



Nerola - corso Umberto I



Palombara Sabina - Ente Parco Monti Lucretili e PIT Provincia



Palombara Sabina - Piazza Vittorio Veneto



Ponzano Romano - via XX settembre



Sant'Oreste - Piazza Cavalieri Caccia e Biblioteca



Stazzano - via Colle Stretto



Torrita Tiberina - Largo 16 Marzo 1978



Parco dell'Appia antica - Villa dei Quintili