

Progettazione, realizzazione e gestione di una rete temporanea wired/wireless per l'accesso a Internet in occasione di un Meeting Internazionale

Alessandro Castellano¹, Giovanni Francesco Castriotta¹,
Giovanni Giuseppe Mandorino¹, Alessandro Sbrana²

Il XII incontro annuale della *Human Brain Mapping Organization* ha trasformato, per poco meno di una settimana, il Centro Congressi di Firenze in un campus universitario internazionale. Gli autori sono stati incaricati di progettare l'accesso a Internet per i partecipanti al meeting, realizzando, tra l'altro, la copertura wireless di buona parte dell'area del Centro Congressi e le procedure per l'accesso nel rispetto delle normative attualmente vigenti. Il documento descrive le principali problematiche affrontate e le soluzioni adottate in quanto applicabili al problema generale della progettazione e realizzazione di reti temporanee per l'accesso a Internet. In conclusione, alcune considerazioni a proposito delle economie realizzabili (pur garantendo soluzioni di qualità) grazie alla collaborazione inter- e intra-universitaria.

Introduzione

La diffusione dell'informatica personale e mobile, l'abitudine, ormai invalsa nei Paesi “sviluppati” in particolare negli ambienti a più elevato livello culturale, ad essere sempre e dovunque collegati alla Rete fa sì che la disponibilità dell'accesso a Internet sia considerata imprescindibile anche quando le circostanze ci portano a trascorrere pochi giorni lontano dal nostro normale ambiente di vita e di lavoro. Non paia perciò esagerato affermare che la predisposizione di un sistema di accesso a Internet di facile utilizzo e di buona qualità è tra le sfide che chi organizza happening di carattere scientifico-tecnologico si trova comunemente a dover affrontare, rappresentando l'indisponibilità di un servizio di questo genere un fattore immediatamente percepito dai convenuti come negativo. L'obbiettivo di questo documento è condividere l'esperienza fatta nell'allestimen-

1 Università di Pisa

2 Università di Firenze

to di una rete temporanea in occasione di un evento congressuale di dimensioni significative toccando, in particolare, gli aspetti suscettibili di riutilizzo in circostanze analoghe.

Ambiente di implementazione

Il Centro Congressi di Firenze è costituito da alcuni edifici in un ampio parco a poche decine di metri dalla stazione ferroviaria di Firenze Santa Maria Novella. Ogni anno ospita alcune decine di eventi congressuali di varia rilevanza.

Gli autori sono stati incaricati della progettazione, realizzazione e gestione dei servizi di rete locale e di accesso a Internet in occasione del XII Annual Meeting (il primo in Italia) della Human Brain Mapping Organization tenutosi a Firenze dall'11 al 15 giugno 2006.

Il Meeting ha ospitato circa 3000 studiosi e ricercatori provenienti (letteralmente) da tutti gli angoli della Terra che hanno impegnato l'area del Centro evidenziata in fig. 1 (in evidenza la posizione degli AP utilizzati), grosso modo

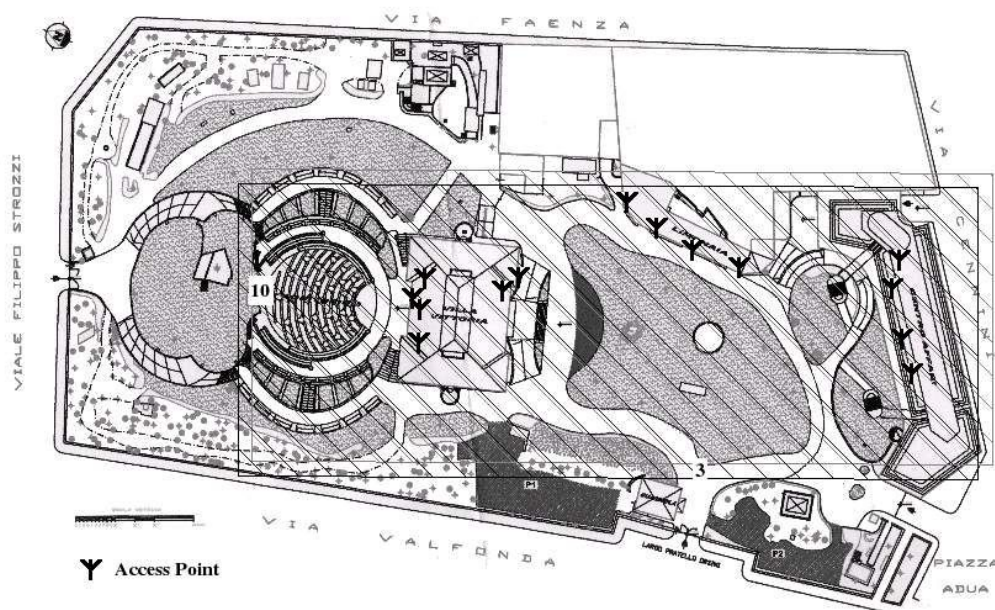


Fig. 1: Centro Congressi di Firenze. Evidenziata la zona interessata dalla rete wireless

approssimabile con un parallelogramma con lati di 100 e 175 mt circa. Le attività didattico-congressuali del Meeting hanno impegnato, principalmente l'edificio che la delimita a destra (Palazzo Affari), mentre l'edificio al centro dell'area evidenziata (Villa Vittoria) ospitava gli uffici destinati alle figure istituzionali presenti al convegno, ai meeting istituzionali, le aree attrezzate per la stampa e

per le attività individuali degli ospiti. Il clima mite e favorevole del giugno fiorentino incoraggiava e rendeva gradevole l'uso dell'ampio parco alberato e dell'anfiteatro (a sinistra nell'area evidenziata) per trascorrere gli intervalli tra un impegno e l'altro dal primo mattino al tardo pomeriggio. L'edificio a un solo piano (Limonaia) che delimita in alto l'area evidenziata era utilizzato per la registrazione e l'assistenza ai convegnisti.

I due edifici principali sono collegati da una coppia in fibra ottica multimodale. Un singolo link UTP cat 5 unisce Villa Vittoria alla Limonaia. Quasi tutte le stanze di Villa Vittoria dispongono di una singola presa di rete cablata in UTP: non si tratta di un vero e proprio cablaggio strutturato ma di una rete costituita da spezzoni interconnessi senza una logica apparente.

Specificità della progettazione e realizzazione reti temporanee

Una volta esaminato l'ambiente in cui va calata l'esperienza progettuale oggetto del documento passiamo in rassegna le principali specificità della progettazione e gestione reti temporanee da allestire per eventi congressuali, in particolare, vanno perseguiti i quattro classici obiettivi progettuali, anche se riletta alla luce del breve tempo di vita della rete. Tra questi, tre rivestono particolare importanza:

funzionalità e affidabilità: rispondere alle esigenze degli utilizzatori e deve funzionare correttamente per tutto il tempo dell'evento. Interruzioni del servizio superiori ai pochi secondi sono particolarmente mal tollerate e lasciano poco spazio a politiche di recupero;

adattabilità: permettere la connessione di una molteplicità di diversi tipi di client e supportare schemi di traffico non pienamente prevedibili a priori: quasi ciascun convegnista dispone di un portatile equipaggiato con i dispositivi diffusi nella propria regione di residenza. Anche se la standardizzazione aiuta, questo significa dover supportare il maggior numero possibile di protocolli della famiglia 802.11 (nel nostro caso, 802.11a/b/g), oltre ad essere pronti a modifiche in corso d'opera se le circostanze lo richiedono.

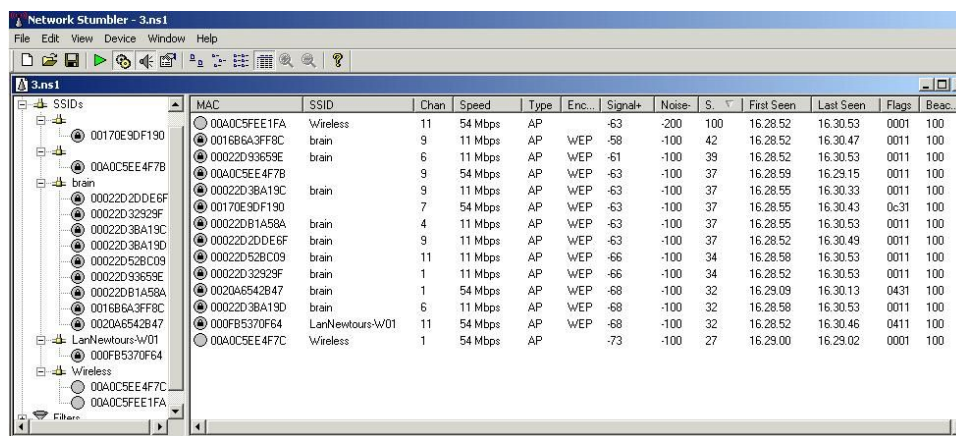
gestibilità: individuare e porre rimedio ad eventuali degrading delle prestazioni ed intervenire possibilmente prima che questo diventi evidente all'utenza

Inoltre:

- la rete è **temporanea**: deve restare in funzione per un periodo di tempo limitato, spesso molto breve. Deve essere facile da installare e rimuovere in tempi molto stretti (gli stessi ambienti possono essere riutilizzati a distanza di un giorno da altri) e deve essere presentare

Accesso alla rete locale

È comodo, oltre che appropriato, scomporre l'accesso ad una rete wireless infrastrutturata, basata su una pila TCP/IP, in una operazione di *associazione* tra client wireless e AP e in una di assegnazione al client dei parametri che gli permettano di configurazione TCP/IP. Mentre l'ultima operazione viene svolta in modo standard e consolidato con l'uso del protocollo DHCP, la prima richiede operazioni di configurazione da effettuare sul client, che diventano particolarmente complesse e, talvolta, penose anche per i più esperti se vanno effettuate su macchine che montano front-end mai visti in precedenza e il cui sistema operativo e tastiera sono in coreano o in cirillico. Questa, insieme alle altre considerazioni sviluppate sopra, ha determinato le scelte fatte nella realizzazione della regione di accesso wireless alla rete: (a) ridondanza spinta all'estremo, con ogni punto della zona di interesse coperto dal segnale di tre o più AP (vedi fig. 3); (b) semplificazione massima della configurazione per l'accesso alla rete wireless (WEP a 64bit senza autenticazione, SSID e key della rete uguali e facili da ricordare).



The screenshot shows the Network Stumbler interface with a list of detected wireless networks. The table below represents the data shown in the main window.

MAC	SSID	Chan	Speed	Type	Enc...	Signal+	Noise-	S	First Seen	Last Seen	Flags	Beac...
00A0C5FEE1FA	Wireless	11	54 Mbps	AP		-63	-200	100	16.28.52	16.30.53	0001	100
001686A3FF8C	brain	9	11 Mbps	AP	WEP	-58	-100	42	16.28.52	16.30.47	0011	100
00022D93659E	brain	6	11 Mbps	AP	WEP	-61	-100	39	16.28.52	16.30.53	0011	100
00A0C5EE4F7B	brain	9	54 Mbps	AP	WEP	-63	-100	37	16.28.59	16.29.15	0011	100
00022D38A19C	brain	9	11 Mbps	AP	WEP	-63	-100	37	16.28.55	16.30.33	0011	100
00170E90F190	brain	7	54 Mbps	AP	WEP	-63	-100	37	16.28.55	16.30.43	0c31	100
00022D81A58A	brain	4	11 Mbps	AP	WEP	-63	-100	37	16.28.55	16.30.53	0011	100
00022D20DE6F	brain	9	11 Mbps	AP	WEP	-63	-100	37	16.28.52	16.30.49	0011	100
00022D52BC09	brain	11	11 Mbps	AP	WEP	-66	-100	34	16.28.58	16.30.53	0011	100
00022D93659E	brain	1	11 Mbps	AP	WEP	-66	-100	34	16.28.52	16.30.53	0011	100
0020A6542B47	brain	1	54 Mbps	AP	WEP	-68	-100	32	16.29.09	16.30.13	0431	100
001686A3FF8C	brain	6	11 Mbps	AP	WEP	-68	-100	32	16.28.58	16.30.53	0011	100
0020A6542B47	LanNewtours-W01	11	54 Mbps	AP	WEP	-68	-100	32	16.28.52	16.30.46	0411	100
00A0C5EE4F7C	Wireless	1	54 Mbps	AP		-73	-100	27	16.29.00	16.29.02	0001	100

Fig. 3: Output di Network Stumbler nella posizione "3" di fig. 1 (SSID 'brain')

Vale la pena osservare che, anche se originariamente non previsto, è emersa subito, a seguito di richieste di numerosi convegnisti, l'esigenza di allestire un'area cablata (abbiamo messo a disposizione oltre 40 punti di accesso) attraverso cui poter connettere i portatili privi di scheda wireless. Allo stesso modo, molto successo hanno riscosso le 16 postazioni fisse predisposte all'accesso pubblico: fuori dalla sala in cui erano collocate la fila superava spesso i 30 minuti.

Interconnessione alla rete pubblica

Passando all'altra estremità della rete (la connessione a Internet), considerando il numero dei partecipanti previsto, ci è apparso immediatamente evidente che la connessione disponibile presso il Centro Congressi (HDSL a 1Mbps, da condividere con gli uffici del Centro) avrebbe fornito una banda penalizzante per quanto avessimo potuto ottimizzarne l'uso. Di fronte ai costi (e ai tempi) richiesti dagli ISP per fornire un accesso temporaneo di poco più performante, dopo una breve indagine sul territorio, abbiamo individuato una struttura dell'Università di Firenze, servita dalla rete in FO dell'Ateneo a poco più di 200mt di distanza dal Centro Congressi e lungo la line-of-sight del Belvedere di Villa Vittoria: la realizzazione di un ponte radio (Hiperlan) era tecnicamente fattibile. Interpellati dal presidente del comitato organizzativo locale (docente presso l'Università di Pisa) i gestori della rete di Ateneo di Firenze sono stati immediatamente disponibili a collaborare mettendo a disposizione del Meeting una connessione wired nella struttura da noi identificata e concedendo 2 indirizzi IP pubblici. In questo modo abbiamo potuto allestire un ponte radio in tecnologia hiperlan con una banda utile di circa 50Mbps (sia pure half duplex). Questa circostanza si è rivelata determinante: per gran parte del tempo del Meeting il traffico in ingresso alla nostra rete temporanea si è mantenuto al di sopra dei 4Mbps raggiungendo e superando, per periodi di tempo significativi i 6Mbps (vedi fig. 4)

Controllo e logging degli accessi

Ci resta da affrontare il tema di come si fa a permettere, in tempi ragionevoli nelle condizioni date, l'accesso ad Internet a circa 3000 persone, attraverso un servizio wireless, nel rispetto del “Decreto Pisanu” (decreto Min. Interno 16 agosto 2005, in particolare artt. 3 e 4,) e, dove applicabile, del “Codice per la protezione dei dati personali” e con l'uso di 2 soli indirizzi IP pubblici.

La soluzione è in una combinazione di misure tecnologiche ed organizzative.

La tecnologia del *captive portal* ci aiuta nel compito di attribuire il traffico diretto ad Internet, che attraversa il confine della nostra rete privata, univocamente ad un client della rete stessa ed al suo utilizzatore, che ottiene la possibilità di accedere alla rete pubblica solo a fronte della presentazione di opportune credenziali.

La tecnica del NAT ci permette di ricondurre un numero praticamente illimitato (alcune migliaia) di indirizzi IP con significato locale (di solito appartenenti ai range riservati per uso privato) ad un unico indirizzo visibile dalla rete pubblica.

La gestione, esclusivamente su supporto cartaceo, delle associazioni tra l'identità personale e le credenziali usate per ottenere l'accesso alla rete pubblica ci permette di trattare, con mezzi informatici, esclusivamente informazioni anonime.

Nei giorni precedenti il meeting sono stati predisposti account anonimi (non attribuiti a nessun individuo) in numero sufficiente per dotarne tutti i partecipanti. Le credenziali (userId e password) relative a questi account sono state stampate, insieme alle norme di utilizzo (in Inglese), su fogli trattati in maniera tale che solo una parte dello stampato sarebbe rimasta visibile. Nella parte visibile compariva lo userId (non la password) ed era previsto uno spazio per l'annotazione dei dati personali e l'acquisizione della firma di colei/colui a cui l'account sarebbe stato consegnato. Al momento della consegna questa parte veniva compilata e archiviata, mentre la parte contenente lo userId, la password e le norme di utilizzo restava nelle mani del partecipante al meeting. Tutto secondo il modello (anche se con un livello di segretezza molto minore) che molti di noi hanno sperimentato per l'acquisizione del PIN del bancomat.

Prima di concedere l'accesso alla rete pubblica ad un particolare client, il *captive portal* interviene a richiedere e verificare userId e password associando poi, in modo univoco, la userId all'indirizzo IP (e al MAC) utilizzato nell'occasione. La fornitura di credenziali autorizzate permette, fino al momento della deregistrazione esplicita o allo spirare di un timeout (di alcune ore), a quella macchina (rappresentata dall'associazione tra IP e MAC) di accedere liberamente alla rete pubblica. Tutti gli eventi rilevanti, in particolare l'avvenuta associazione tra userId e indirizzo IP e la cessazione di questa associazione (e della possibilità di accedere alla rete pubblica fino ad una nuova) vengono registrati in un apposito log.

Strumenti utilizzati

Passate in rassegna le funzionalità implementate ci appare opportuno dedicare poche righe a citare almeno i nomi degli strumenti che ce ne hanno permesso la realizzazione:

- CaptivePortal, DHCP Server e NAT: PfSense 1.0-RC1 (www.pfsense.org) montato su Pentium III 700Mhz
- Radius Server, per la gestione degli account e la raccolta dei log, FreeBSD + freeRadius montato su Pentium III 700Mhz;
- AP di vari costruttori: Linksys, Proxim/Lucent, Hawking e Intel.

La fig. 4 presenta una delle funzionalità statistiche messe a disposizione dall'interfaccia di gestione di PfSense, quella che permette di verificare

l'andamento del traffico su una interfaccia nell'arco di un dato intervallo di tempo.

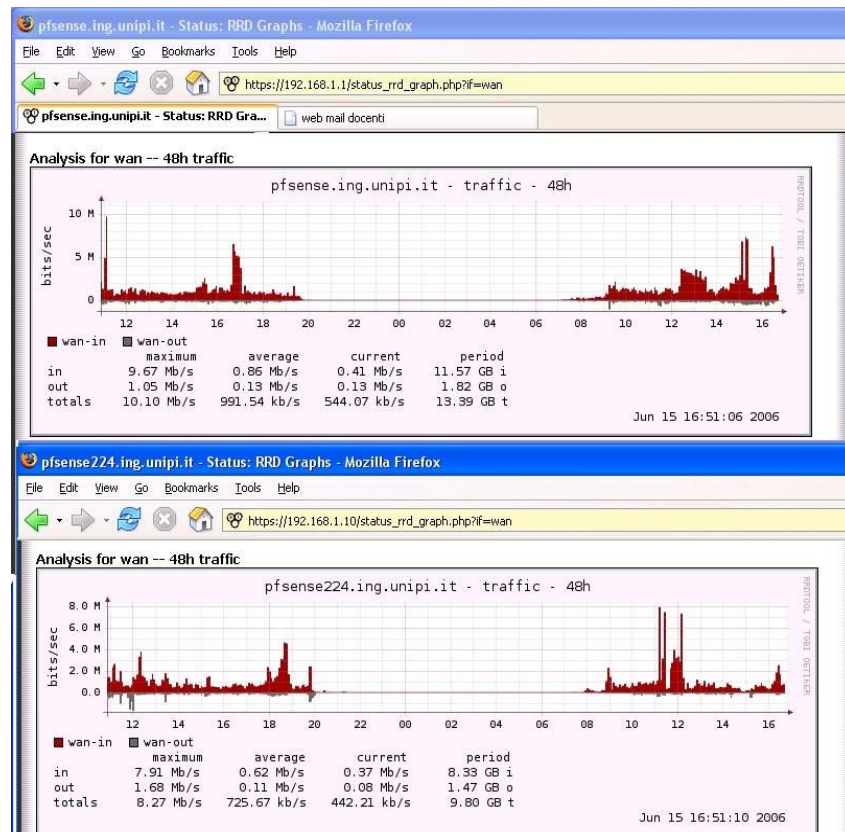


Fig. 4: statistiche del traffico Internet (ultime 30 ore del meeting, due CP in parallelo)

Problematiche specifiche degli strumenti

Solo poche righe, anche qui, per indicare le limitazioni o i punti di particolare attenzione per coloro che si trovassero ad affrontare in futuro un'esperienza simile.

Detto che, anche per le reti temporanee – specie per quelle outdoor, vanno valutate attentamente le condizioni ambientali di esercizio (non solo la presenza di pioggia o fulmini ma anche la temperatura dell'ambiente e la dissipazione del calore generato dagli apparati), ci soffermeremo più in dettaglio sui problemi che sono emersi nella nostra applicazione in conseguenza, soprattutto, del numero elevato di fruitori.

Accesso alla rete pubblica

PfSense, arrivato da pochi giorni alla versione 1.0-RC3, si è dimostrato abbastanza efficiente (e poco esigente in termini di risorse) nello svolgere le funzioni di Router/NAT, DHCP e firewall. Purtroppo non altrettanto performante nello svolgere le funzioni di captive portal: se vi aspettate che diverse decine di persone utilizzino questa funzionalità, praticamente, in contemporanea, converrà prevedere la presenza di più istanze di pfSense che, comunque, sono facilmente configurabili per lavorare in parallelo al servizio della stessa rete fisica. È sufficiente, infatti, configurare il servizio DHCP (magari svolto dalle stesse istanze di pfSense) per dirigere i client a cui fornisce i parametri di configurazione TCP/IP ad utilizzare in modo bilanciato, anche solo grossolanamente, come default gateway le diverse istanze presenti.

Per quanto attiene ai protocolli applicativi supportati, ricordate che qualunque NAT tool richiede specifiche configurazioni (e non sempre queste sono sufficienti) per trattare con protocolli che prevedono un ruolo attivo, nell'apertura di connessioni, da parte di server presenti al di là della sua interfaccia pubblica: non solo ftp in modalità attiva, ma anche, ad esempio, PPTP.

Accesso alla rete locale

Le problematiche emerse nel gestire l'accesso wireless alla rete locale sono da ricondurre principalmente ad un unico aspetto, anche se visto da punti di vista diversi:

- come i client scelgono l'AP a cui associarsi quando ne vedono più d'uno: Windows XP, ad esempio, per default preferisce quelli che dichiarano un protocollo capace di maggiore banda, mentre la qualità (SNR) del segnale ricevuto è considerata una variabile di secondo ordine;
 - il livello di controllo disponibile sul numero di client accettati da ciascun AP: questo numero, per quanto elevato, non è illimitato e, in una rete come quella descritta sopra in cui un elevato numero di client è concentrato in uno spazio ristretto, non è indifferente se (e come) l'AP vi permette di gestire il raggiungimento di (o, addirittura meglio, l'avvicinamento a) questo limite;
- È, infine, ovvia (al punto che quasi non la citeremmo) la necessità di dimensionare e ridondare adeguatamente il servizio DHCP e l'infrastruttura di distribuzione tra gli AP ed il core della rete.

Conclusioni

Prima di lasciare la parola, per una valutazione dei risultati conseguiti ai nostri committenti, ci appare utile riferire alcuni dati relativi alle dimensioni e al funzionamento della rete: tempo di installazione (compreso il ponte radio) 3 persone per 10 ore; numero di access point utilizzati: 16, di cui 8 con 2 moduli wireless; giorni di funzionamento 5; traffico in ingresso 43Gb, in uscita 8Gb circa; utenti realmente serviti 1200 (non tutti i presenti hanno chiesto di ottenere l'accesso a Internet); tempo di smantellamento 2 persone per 7 ore.

Il punto di vista del committente

“La velocità delle connessioni è stata buona e la copertura wireless dell'area del Centro Congressi è stata eccellente. A parte qualche problema di connettività che si è verificato il primo giorno del convegno, nei giorni successivi il servizio è risultato affidabile e funzionale. Al momento della registrazione al servizio, alcuni nostri collaboratori hanno fornito agli iscritti le informazioni necessarie per la connessione, nel rispetto delle normative attualmente vigenti.[...]”

L'informazione a proposito dell'esistenza di competenze/capacità realizzative in merito ad un servizio di questo tipo interno all'Ateneo è attualmente scarsa o inesistente. Si ritiene che sarebbe più che giustificata la stabilizzazione di una piattaforma tecnologica interna per la realizzazione di un servizio per l'accesso wireless a Internet da utilizzarsi ogni volta che l'Ateneo organizza un convegno.

A fronte di un servizio di elevata qualità e prestazioni, il costo sostenuto è stato circa di un terzo rispetto a quello relativo alle migliori offerte dei vari fornitori commerciali a cui ci eravamo rivolti.” (*Lorenzo Sani*, Comitato Organizzatore Locale del 12th Annual Meeting of Human Brain Mapping).

Noi aggiungiamo soltanto che alcuni dei fattori chiave per ottenere il risparmio evidenziato sono stati: (a) collaborazione tra strutture diverse dell'Ateneo pisano che hanno dato al loro personale la possibilità di lavorare assieme su uno specifico obiettivo; (b) utilizzo di professionalità qualificate presenti all'interno dell'Ateneo caratterizzate da un *bassissimo costo del lavoro*; (c) la disponibilità dell'amministrazione dell'Università di Firenze a fornire la connessione a Internet; (d) utilizzo di hardware già detenuto dal Centro Servizi Informatici della Facoltà di Ingegneria e *considerato obsoleto* per altri scopi; (e) utilizzo di software, di qualità, *non soggetto a pagamento di licenze*.

Ringraziamenti

Riteniamo doveroso ringraziare qui tutti coloro, e sono tanti, che hanno reso possibile la realizzazione del lavoro descritto in questo documento. In particolare:

il prof. Pietro Pietrini e i dott. Emiliano Ricciardi e Lorenzo Sani dell'Azienda Ospedaliero-Universitaria Pisana per averci affidato l'incarico di provvedere alla copertura wireless e alla connessione a Internet per HBMO Meeting 2006;

la prof.ssa Gigliola Vaglini e la dott.ssa Daniela Dorbolò del Centro Servizi Informatici della Facoltà di Ingegneria dell'Università di Pisa per aver aderito alla proposta del prof. Pietrini sostenendo attivamente l'opportunità di una collaborazione tra strutture universitarie diverse, consentendo ad uno di noi di partecipare al progetto e di utilizzare nella sua realizzazione risorse del CSIFI temporaneamente disponibili;

il dott. Renato Tamburrini del Dipartimento VI – Sistema Bibliotecario, Archivistico e Museale dell'Università di Pisa, per aver consentito la partecipazione di uno di noi al progetto;

i responsabili del C.s.i.a.f. dell'Università degli Studi di Firenze, che hanno fornito l'accesso a Internet per il meeting;

tutto lo staff del comitato organizzatore locale che ci ha, più che validamente, affiancato nel supporto agli utenti durante il meeting, permettendoci di concentrare la nostra attenzione soprattutto nel monitoraggio, gestione e adeguamento dell'infrastruttura;

i colleghi del Dipartimento VI – Sistema Bibliotecario, Archivistico e Museale e del CSIFI, sul cui lavoro quotidiano ha pesato la nostra assenza dagli uffici.

Profili biografici degli autori

Alessandro Castellano (a.castellano@ing.unipi.it), laureato in Ingegneria delle Telecomunicazioni, lavora dal 1996 nel settore informatico. Dopo essere stato coordinatore dei servizi tecnici presso una azienda pisana del settore, dal 2001 è responsabile dei sistemi IT presso il Dipartimento di Ingegneria Meccanica, Nucleare e della Produzione dell'Università di Pisa.

Giovanni Francesco Castriotta (g.castriotta@adm.unipi.it), laureato in Ingegneria Informatica, ha lavorato come sistemista presso il CSIFI e presso il Dipartimento di Ingegneria dell'Informazione: Elettronica, Informatica, Telecomunicazioni dell'Università di Pisa. Attualmente gestisce i sistemi informatici e di rete delle biblioteche dell'Ateneo.

Giovanni Giuseppe Mandorino (g.mandorino@ing.unipi.it), laureato in Scienze dell'Informazione, ha lavorato alla progettazione e realizzazione di sistemi di gestione e controllo di Reti e Sistemi informatici presso Tecsiel e Sodalìa dal 1991 al '98. Nel 1995 è stato delegato dell'Italia alla plenaria del comitato ISO JTC1/SC21 per la standardizzazione del Systems Management. Passato alle dipendenze dell'Università di Pisa, dopo una breve parentesi nel 2001 in Marconi Communications, si occupa, presso il CSIFI, della gestione e sviluppo dei servizi e sistemi di rete della Facoltà di Ingegneria.

Alessandro Sbrana (alessandro.sbrana@unifi.it), laureato in Economia e Commercio e Master in Auditing e Controllo Interno, lavora presso l'Università degli Studi di Firenze. E' stato sistemista presso l'Università di Pisa. Radioamatore (IK5MIC) dal 1985, la passione per le reti informatiche lo colpisce nei primi anni '90 quando diviene amministratore del primo radio-gateway italiano ubicato presso l'Istituto CNUCE del C.N.R di Pisa. Da anni è impegnato nella realizzazione di reti di comunicazioni alternative per la protezione civile. Ha ideato VicoNET, la prima rete wireless municipale autorizzata dal Ministero delle Comunicazioni.