IL SERVIZIO WIFE DELL'UNIVERSITÀ DEGLI STUDI DI FERRARA

Gianluca Mazzini, Cesare Stefanelli
Dipartimento di Ingegneria, Università di Ferrara
[gmazzini, cstefanelli]@ing.unife.it

Enrico Ardizzoni, Michele Lugli
Centro di Telematica, Università di Ferrara
[enrico, michele]@unife.it

WIFE è il servizio di connessione wireless a Internet realizzato all'Università di Ferrara per tutti gli studenti e per tutto il personale strutturato. WIFE utilizza la tecnologia Wi-Fi e permette il collegamento a Internet da tutte le biblioteche, le sale studio e le aule didattiche dell'Ateneo, per favorire l'accesso ai servizi Web di Ateneo (posta elettronica, iscrizione agli esami via Web, etc.) e per facilitare l'interazione tra gli studenti e i docenti. L'innovativa architettura dell'infrastruttura di WIFE è stata progettata per rendere estremamente semplice e sicuro il collegamento a Internet e per supportare la completa mobilità dei terminali.

1. Introduzione

L'enorme diffusione della tecnologia Wi-Fi ha contribuito a rendere pervasivo l'accesso alla rete Internet. Gli utenti dotati di terminali Wi-Fi possono accedere alla rete senza bisogno di collegamenti cablati, semplicemente collegandosi via radio, in una qualunque area dove sia presente la copertura Wi-Fi, come aeroporti, Internet café, biblioteche, etc. Questo facilita la fruizione di tutti i servizi Web, contribuendo significativamente alla loro diffusione ([1], [2], [4]).

L'Ateneo di Ferrara ha deciso di sfruttare la tecnologia Wi-Fi per permettere a tutti gli studenti e a tutto il personale strutturato (docente e tecnico amministrativo) di accedere alla rete Internet e in particolare ai servizi Web di Ateneo. Con questo fine è nato il servizio WIFE (WIreless FErrara) (www.unife.it/wife) progettato e realizzato dal Centro di Telematica (CDT) dell'Ateneo e dal Dipartimento di Ingegneria, con finanziamenti CampusOne (www.campusone.it). Il servizio WIFE è disponibile tramite una Wireless LAN (WLAN) che copre tutte le strutture dell'Ateneo (biblioteche, sale studio, aule didattiche, etc.), dislocate in tutta la città di Ferrara. Il servizio WIFE presenta alcune importanti caratteristiche, principali obiettivi definiti in fase di progetto:

- massima facilità di accesso. Gli utenti WIFE accedono senza bisogno di effettuare configurazioni ai loro terminali; tutte le operazioni di configurazione sono eseguite automaticamente;

- sicurezza del servizio. WIFE garantisce la sicurezza degli utenti del servizio e protegge anche gli utenti della rete cablata di Ateneo da possibili attacchi provenienti dalla WLAN. A questo fine l'accesso al servizio WIFE è

subordinato al superamento dell'operazione di autenticazione, che verifica l'identità dell'utente. Inoltre, il traffico della WLAN è logicamente separato dal traffico delle rete cablata di Ateneo;

- massimo supporto alla mobilità degli utenti e dei terminali, anche durante la fruizione del servizio;

- l'infrastruttura è gestita e manutenuta centralmente dal Centro di Telematica (per operazioni di configurazione, monitoraggio, accounting).

2. Architettura del servizio WIFE

I vari elementi che compongono l'infrastruttura di WIFE sono rappresentati nella Figura 1 che possiamo descrivere, per semplicità, considerando il percorso di un generico pacchetto. Il terminale mobile (WT) manda un pacchetto via radio a un Access Point (AP), da cui viene inoltrato al Router Terminale (RT), che lo inserisce in un tunnel fino al Router di Concentrazione (RC), collocato al CDT, per essere infine instradato su Internet. La macchina Cerbero ospita i servizi di configurazione e sicurezza (DHCP, DNS, Autenticazione, Proxy e Firewall) e il router RC-Unife, collegato in fibra ottica al GARR, fornisce la connettività a Internet. Si noti che nelle diverse facoltà sono presenti molti AP, al fine di ampliare la copertura del servizio. Ogni AP è collegato a un router RT per realizzare i tunnel con il CDT. Più AP possono essere collegati allo stesso router RT (fino a un massimo di 3) e in una Facoltà sono tipicamente presenti più router RT. Il collegamento tra AP e RT è realizzato tramite una rete privata, in modo da separare il traffico tra gli utenti WIFE e quelli della Facoltà; questa separazione permane anche a valle di RT grazie all'utilizzo di vari tunnel.

Caratteristiche fondamentali del'infrastruttura di WIFE sono il meccanismo di creazione della WLAN (con un triplo livello di Network Address Translation - NAT) e i servizi dell'infrastruttura di autenticazione, configurazione e gestione.

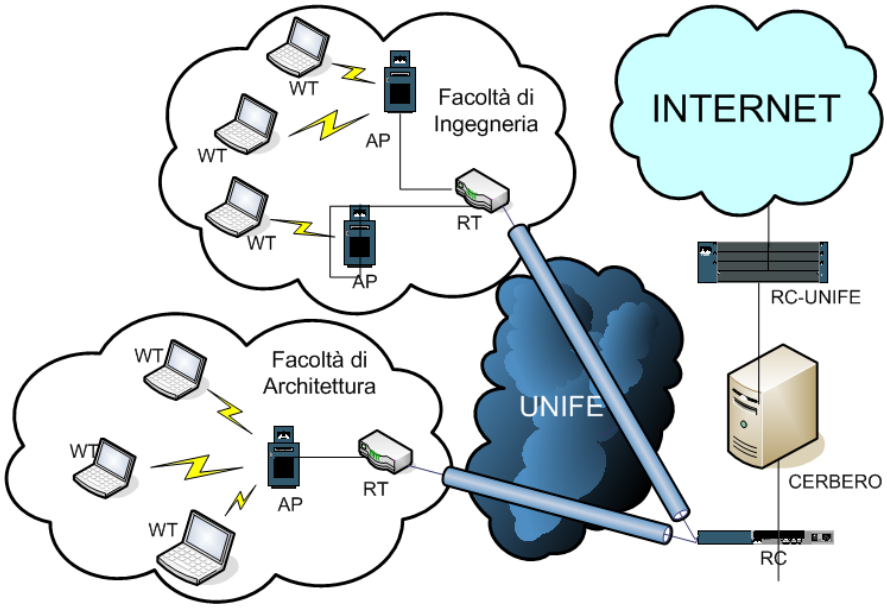

Figura 1. Architettura e componenti del servizio WIFE

2.1. Il routing di WIFE

La WLAN di Ateneo riservata al traffico WIFE è realizzata con un meccanismo di NAT che fornisce una traslazione degli indirizzi IP sorgenti. In particolare, il meccanismo di NAT è stato progettato sia con lo scopo di garantire la sicurezza del servizio che di favorire la mobilità dei terminali tra i vari AP.

Gli indirizzi IP assegnati al servizio WIFE appartengono alla rete di classe A 14.0.0.0/8, che pur non essendo definita privata [6][7], è stata considerata come tale in quanto utilizzabile solo da provider di telefonia per trunk interni (la rete 10.0.0.0/8 è assegnata agli host collegati alla rete fissa). L'idea di base è di avere una numerazione non dipendente dal particolare AP al quale si è collegati e consentire quindi un facile supporto alla mobilità dell'utente senza interruzioni sul collegamento. Inoltre, ogni hot spot è identificato con un numero, A > 1.

La Figura 2 descrive l'architettura con tre livelli di NAT del servizio WIFE, dove il primo livello consente di passare dal generico indirizzo 14.0.X.Y/16 a un indirizzo 14.A.X.Y/16, che identifica l'RT a cui il WT è correntemente collegato in modo da avere un riferimento per il percorso di ritorno. Il secondo livello di NAT è introdotto con lo scopo di eliminare la dipendenza dell'indirizzo dal tunnel [12] utilizzato e quindi dalla posizione del WT all'interno della VPN; in questo livello si ha una traslazione da 14.A.X.Y/16 a 14.0.X.Y/16. Con questo meccanismo viene definito il percorso dei pacchetti dal Router di Concentrazione (ovvero quello proveniente da Internet) verso gli host wireless.

Al fine di verificare l'identità degli utenti e di attuare politiche di controllo, il router RC è connesso al firewall Cerbero, a sua volta collegato alla rete cablata di Ateneo tramite un'ulteriore interfaccia di rete. Su questa macchina, a seguito del superamento dell'operazione di autenticazione, viene eseguito un terzo livello di NAT su un singolo IP pubblico. Il terzo livello di NAT è basato su port overloading, dove coppie costituite da indirizzo IP sorgente e porta sorgente prima dell'operazione di NAT vengono mappate su una nuova porta sorgente dopo l'operazione di NAT.

Si osservi che il primo e il secondo livello di NAT consentono di mantenere la connessione anche in situazioni di passaggio tra diversi AP, anche se questi sono collegati a diversi RT, e quindi fanno capo a diversi tunnel. Questo è possibile in quanto le porte degli RT verso gli AP hanno sempre lo stesso indirizzo IP (fissato sempre a 14.0.0.1) e lo stesso MAC, in modo da avere un unico default gateway (fornito dal DHCP agli utenti, come descritto nel seguito).

Gli AP sono tipicamente dispositivi di layer 2 ma includono spesso caratteristiche di layer 3; in ogni caso, gli AP necessitano di un indirizzo IP per la gestione. Inoltre, ciascun AP richiede un router RT per instradare il traffico alla VPN. Per ridurre il numero di router, più AP (al massimo 3) possono essere collegati allo stesso RT, con la fascia di IP 14.0.0.4*A/30 per il loro indirizzamento. Tale fascia di IP è stata esclusa dal pool dinamico del DHCP, in modo che indirizzi IP del tipo 14.0.0.Y non vengano mai assegnati agli host wireless. Il primo AP connesso ha indirizzo 14.0.0.4*Y; gli eventuali secondo e terzo AP rispettivamente indirizzi 14.0.0.4 * Y + 1 e 14.0.0.4 * Y + 2.

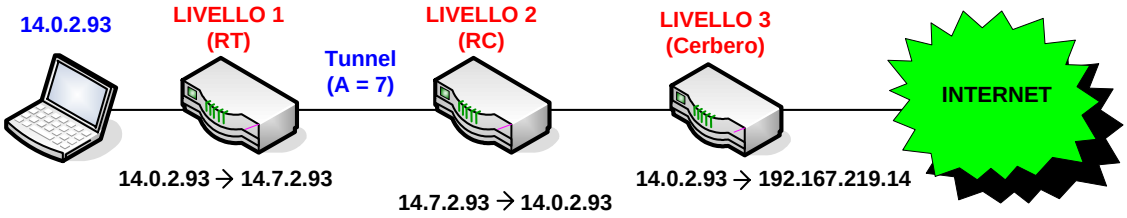

Figura 2. I 3 livelli di NAT del servizio WIFE

2.2. I servizi dell'infrastruttura di WIFE

Il servizio WIFE è fornito da un'infrastruttura composta da molti servizi e componenti in parte realizzati specificatamente per WIFE in parte ottenuti integrando alcuni servizi già presenti in Ateneo, come descritto nel seguito.

Dynamic Host Configuration Protocol (DHCP). Il DHCP [10] viene utilizzato per assegnare i parametri di configurazione ai terminali mobili. In particolare, in WIFE, il DHCP è utilizzato per la totale e automatica configurazione del terminale mobile, senza nessun intervento dell'utente.

Domain Name System (DNS). Il server DNS [11] assolve sia alla funzione di cache per le richieste provenienti dai terminali mobili, sia alla funzione di name server primario per le zone ".wifi" e "14.in-addr.arpa". Nelle due zone sono ora mappati tutti gli apparati di rete dell'infrastruttura WIFE e in futuro verranno inseriti i terminali mobili degli utenti per migliorare i servizi di localizzazione.

Autenticazione. Il meccanismo di autenticazione è basato sul captive portal NocatAuth (http://nocat.net). Per poter navigare, il generico utente WIFE deve aprire un browser e tentare di accedere a un indirizzo qualunque. Indipendentemente dall'indirizzo richiesto, tutti gli utenti non ancora abilitati sono automaticamente ridiretti a un server interno, verso una pagina di autenticazione protetta tramite SSL/TLS (https://...), dove inseriscono le proprie credenziali. NocatAuth autentica gli utenti via IMAP direttamente sui server di posta del Centro di Telematica. Agli utenti autorizzati viene inviata una pagina html (in una nuova finestra) che mantiene autenticato il terminale mobile fornendo identificativi di autenticazione ogni 5 minuti. Ad autenticazione avvenuta il browser viene diretto verso la pagina da visualizzare, servendo la richiesta originale che ha lanciato il processo. Le procedure che gestiscono l'autenticazione interagiscono strettamente con il firewall descritto nel seguito.

Firewall. La presenza di un firewall si rende necessaria per garantire un elevato livello di sicurezza e di controllo nell'uso del servizio WIFE. In particolare, si è scelto di installare un firewall statefull di tipo *packet filtering*, per un filtraggio sulla base di regole ACL (Access Control List). Il filtraggio viene fatto sui servizi, tramite il numero di porta, utilizzando il pacchetto standard Netfilter, disponibile su tutti i sistemi Linux. Quando una nuova sessione utente viene autorizzata, il firewall abilita il meccanismo di NAT per un set predeterminato di porte tcp/udp. È possibile definire classi differenti di utenti con particolari privilegi in termini di servizi abilitati, quote di traffico o tempo di navigazione. Infine, il firewall e il

sistema di autenticazione terminano ogni sessione che non abbia avuto una conferma all'autenticazione entro un tempo prefissato, pari a 5 minuti.

Web Proxy. Per migliorare le prestazioni, WIFE fa uso di un Web Proxy "trasparente" installato appositamente per eseguire il caching delle pagine web richieste dagli utenti della WLAN.

3. Monitoraggio

Il servizio WIFE integra funzionalità di monitoraggio e controllo progettate per tenere traccia di tutti gli accessi al servizio, per rilevare la disponibilità e la continuità del servizio e per raccogliere le statistiche sul traffico complessivo generato. Il monitoraggio viene effettuato su tutti i router RT e fa uso del tool mrtg (i dati sono disponibili in Internet all'URL http://cerbero.unife.it).

I dati raccolti dal sistema di monitoraggio mostrano che gli obiettivi di progetto, in particolare la facilità di accesso, sono stati ampiamente raggiunti, come è dimostrato dal rapido incremento del numero di utenti che ne stanno facendo uso. In particolare, la Figura 3 riporta l'andamento del numero degli utenti collegati a WIFE dalla sua attivazione, mentre la Figura 4 mostra l'occupazione di banda complessiva, in ingresso e in uscita, relativa allo stesso periodo.

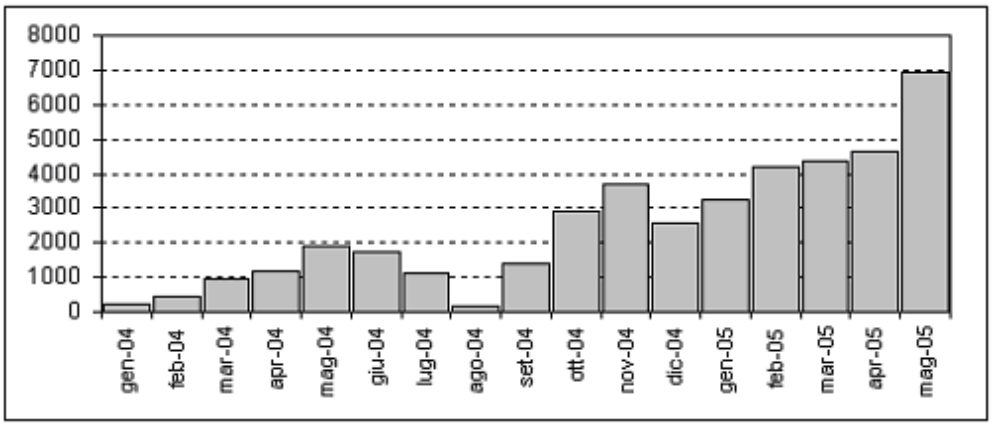

Figura 3. Numero di utenti (mensile) collegati al servizio WIFE

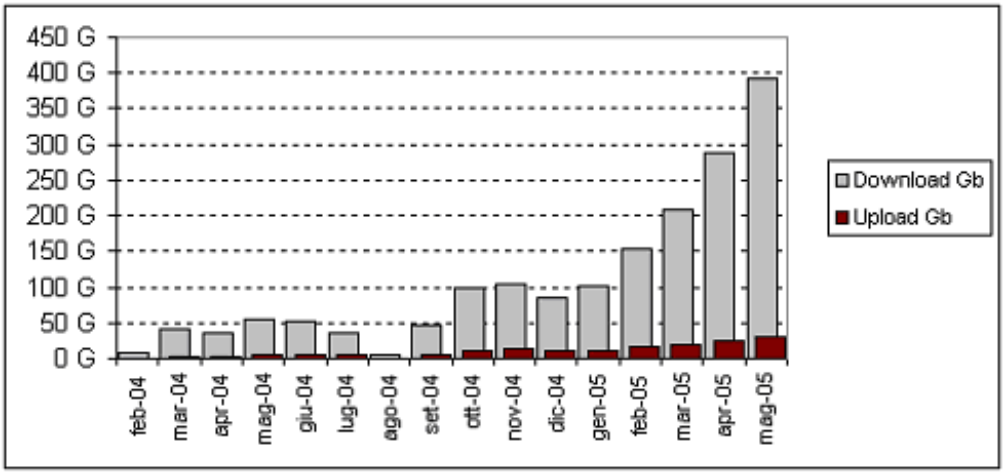

Figura 4. Traffico in uscita e in ingresso relativo al servizio WIFE

4. Conclusioni e sviluppi futuri

L'Ateneo di Ferrara è il primo in Italia ad avere realizzato un servizio di accesso wireless alla rete Internet disponibile in tutte le sue strutture didattiche dislocate in tutta la città. Il servizio WIFE è stato attivato all'inizio del 2004 e viene utilizzato da un numero sempre crescente di studenti, distribuito tra tutte le facoltà, indice di una buona penetrazione, un'elevata semplicità di utilizzo, un'ottima stabilità, buone prestazioni e sicurezza. La disponibilità di un'infrastruttura dislocata su tutto l'Ateneo sta stimolando lo sviluppo di nuovi servizi, come ad esempio innovativi servizi location-aware, che considerano la posizione fisica dello studente per fornire nuovi servizi di comunicazione, di collaborazione e di consultazione di materiale didattico. Infine, il recente disegno di legge sulla liberalizzazione dell'utilizzo di Wi-Fi al di fuori del fondo, apre nuove interessanti prospettive al sistema presentato, candidandolo ad avere impatti importanti sulla città. In questa ottica, un accordo con il Comune di Ferrara ha portato all'avvio di una prima sperimentazione, che vede l'estensione del servizio WIFE agli utenti della principale biblioteca comunale.

Riferimenti bibliografici

[1] P. Bellavista, A. Corradi, C. Stefanelli, *The Ubiquitous Provisioning of Internet Services to Portable Devices*, IEEE Pervasive Computing, Vol. 1, No. 3, pages 81-87, July-September 2002.

[2] M. S. Corson, J. P. Macker, V. D. Park, *Mobile and Wireless Internet Services: Putting the Pieces Together*, IEEE Communications Magazine, Vol. 39, No. 6, 2001, 148-155.

[3] N. Davies, H.-W. Gellersen, *Beyond Prototypes: Challenges in Deploying Ubiquitous Systems*, IEEE Pervasive Computing, Vol. 1, No. 1, 2002, 26-35.

[4] D. Estrin, D. Culler, K. Pister, G. Sukhatme, *Connecting the Physical World with Pervasive Networks*, IEEE Pervasive Computing, Vol. 1, No. 1, 2002. 59-69.

[5] J. Hightower, G. Borriello, *Location Systems for Ubiquitous Computing*, Computer, Vol. 34, No. 8, 2001, 57-66.

[6] J. Reynolds, J. Postel, RFC on Assigned Numbers

[7] IANA, RFC on Special-Use IPv4 Addresses

[8] K. Egevang, P. Francis, RFC on The IP Network Address Translator (NAT)

[9] S. Srisuresh, M. Holdrege, RFC on IP Network Address Translator (NAT) Terminology and Considerations

[10] S. Alexander, R. Droms, RFC on DHCP Options and BOOTP Vendor Extensions

[11] P. Mockapetris, RFC on Domain names - conceps and facilities

[12] C. Perkins, RFC on IP Encapsulation within IP

[13] R. Want, B. Schilit, *Expanding the Horizons of Location-aware Computing*, Computer, Vol. 34, No. 8, 2001, 31-34.