



"ICT4University – WiFi SUD"
Regione CALABRIA
Università degli Studi "Mediterranea" di REGGIO CALABRIA
Progetto: Mediterrane@senzafili.plus: potenziamento di una rete wireless per
l'accesso sicuro degli studenti
17-lug-2008

Sezione 1 – Dati del proponente

Università proponente

Denominazione	Università degli Studi "Mediterranea" di REGGIO CALABRIA
Sede	Reggio di Calabria
Indirizzo postale	via Diana, 3
Indirizzo e-mail	bucca@unirc.it
Telefono	0965 872911
Fax	0965 332201
Sito web	www.unirc.it
Codice Fiscale	80006510806

Rappresentante legale

Cognome e nome	Giovannini Massimo
Qualifica	Rettore - Professore Ordinario
Telefono	0965 872911
Fax	0965 332201
Indirizzo e-mail	rettore@unirc.it

Referente di progetto

Cognome e nome	Buccafurri Francesco
Qualifica	Direttore del Centro Servizi Informatici di Ateneo (CESIAT) – Professore Ordinario
Telefono	0965 875302
Fax	0965 875247
Indirizzo e-mail	bucca@unirc.it

Sezione 2 – Sintesi del progetto

Identificazione e descrizione breve del progetto

Nome progetto	Mediterrane@senzafili.plus: potenziamento di una rete wireless per l'accesso sicuro degli studenti
Finalità progetto	Potenziamento dell'infrastruttura per l'accesso wi-fi della popolazione studentesca ai servizi on-line (compresi i servizi minimi di verbalizzazione elettronica degli esami e iscrizione on-line) e realizzazione di servizi di groupware per gli studenti.
Date inizio prevista	10/04/2008
Date fine prevista	09/10/2009

Struttura finanziaria del progetto

Valore totale del Progetto pari a:	592.611,77
Di cui a carico:	
1. Università	304.731,77
2. Finanziamento richiesto al Dipartimento	287.880,00
3. Altri soggetti pubblici o privati	0,00
4. Altri	0,00
N/A	

Dettaglio del finanziamento richiesto al Dipartimento

Finanziamento richiesto al Dipartimento:	287.880,00
Di cui:	
1. per servizi (compresi i servizi minimi)	58.000,00
2. per infrastrutture di rete	222.880,00
3. per piano di comunicazione agli studenti	7.000,00

Copertura della rete senza fili realizzata

Percentuale dell'area dell'Università coperta da rete senza fili prima prima del progetto	10.0
Percentuale dell'area dell'Università che si prevede sarà coperta da rete senza fili al completamento del progetto	90.0
Percentuale di studenti che si prevede saranno raggiunti dalla rete senza fili al completamento del progetto sul totale degli studenti iscritti	100.0
Numero studenti regolarmente iscritti all'ateneo	11116

Copertura e caratteristiche dei servizi minimi

Servizio per l'iscrizione online

Il servizio è già disponibile presso l'università?	NO
----------------------------------------------------	----

Descrizione sintetica	<p>NOTA: i servizi minimi di verbalizzazione elettronica degli esami e di iscrizione on-line (IOL) sono oggetto di attuazione di un progetto di Ateneo già avviato e non ancora concluso che prevede l'adozione della verbalizzazione elettronica degli esami attraverso l'uso della firma digitale e l'estensione della procedura studenti in uso in Ateneo (GISS) attraverso le funzionalità Web di segreteria didattica e segreteria studenti (inclusa la funzione di IOL). Con ampio anticipo sulla data di chiusura del presente progetto (presumibilmente prima dell'avvio del progetto – ciò dipende dai tempi di approvazione e di stipula della convenzione) pertanto i servizi minimi saranno presenti, anche se il progetto pilota prevede per la verbalizzazione elettronica degli esami di raggiungere solo il 10% della popolazione studentesca. E' prevista tuttavia un'azione di completamento/potenziamento del progetto pilota che è condizionata all'approvazione di una proposta di progetto prodotta dall'Ateneo nell'ambito dell'avviso "Campus Digitali", appartenente alla medesima iniziativa del presente progetto.</p>
-----------------------	---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

Servizio per la verbalizzazione elettronica degli esami

Il servizio è già disponibile presso l'università?	NO
Descrizione sintetica	<p>NOTA: i servizi minimi di verbalizzazione elettronica degli esami e di iscrizione on-line (IOL) sono oggetto di attuazione di un progetto di Ateneo già avviato e non ancora concluso che prevede l'adozione della verbalizzazione elettronica degli esami attraverso l'uso della firma digitale e l'estensione della procedura studenti in uso in Ateneo (GISS) attraverso le funzionalità Web di segreteria didattica e segreteria studenti (inclusa la funzione di IOL). Con ampio anticipo sulla data di chiusura del presente progetto (presumibilmente prima dell'avvio del progetto – ciò dipende dai tempi di approvazione e di stipula della convenzione) pertanto i servizi minimi saranno presenti, anche se il progetto pilota prevede per la verbalizzazione elettronica degli esami di raggiungere solo il 10% della popolazione studentesca. E' prevista tuttavia un'azione di completamento/potenziamento del progetto pilota che è condizionata all'approvazione di una proposta di progetto prodotta dall'Ateneo nell'ambito dell'avviso "Campus Digitali", appartenente alla medesima iniziativa del presente progetto.</p>
Qualora il servizio sia introdotto in modalità sperimentale, indicare la percentuale studenti che ne potranno usufruire (rispetto agli iscritti)	100.0

Copertura e caratteristiche degli eventuali altri principali servizi realizzati

Denominazione del servizio	Piattaforma di groupware per gli studenti
Descrizione sintetica	Realizzazione di una infrastruttura di groupware ad alta affidabilità con autenticazione basata su server LDAP dedicata agli studenti, interoperante con la procedura di gestione studenti denominata GISS già in uso all'Ateneo per la creazione automatica degli account
Percentuale studenti raggiunti dal servizio (rispetto agli iscritti)	100.0
Eventuali informazioni aggiuntive	Si prevede la creazione, gestione e messa in condivisione di calendari, documenti, rubriche, conversazioni in forma di instant messaging, strumenti VoIP, con piena capacità di integrazione ai più diffusi browser web (IExplorer, Firefox, Safari) e alle nuove tecnologie di comunicazione mobile (palmari, smartphone, etc.).

Denominazione del servizio	eduroam
Descrizione sintetica	eduroam (EDUcation ROAMing) è un'infrastruttura d'autenticazione, basata su una rete gerarchica e confederata di server RADIUS, che utilizza 802.1x.

Percentuale studenti raggiunti dal servizio (rispetto agli iscritti)	100.0
Eventuali informazioni aggiuntive	Gli utenti roaming che visitano un Istituto federato all'iniziativa potranno utilizzare la WLAN usando le medesime credenziali (username e password) che userebbero nella loro istituzione d'appartenenza, senza quindi la necessità di procedere ad ulteriori formalità presso l'istituto ospitante

Misure di sicurezza previste

Descrizione sintetica delle procedure previste per l'autenticazione e la gestione degli accessi alla rete	<ul style="list-style-type: none"> • 802.11i, Wi-Fi Protected Access 2 (WPA2), WPA, and Wired Equivalent Privacy (WEP) • 802.1X con Extensible Authentication Protocol (EAP), Protected EAP (PEAP), EAP con Transport Layer Security (EAP-TLS), EAP con Tunneled TLS (EAP-TTLS), LEAP • VPN (IP Security [IPSec] e Layer 2 Tunneling Protocol [L2TP]) • RADIUS (AAA) in alta affidabilità (HA) • Captive Portal • LDAP in architettura Master, Replica • Accesso ad Internet autenticato, autorizzato e registrato mediante 802.1X, RADIUS e Captive Portal
Descrizione sintetica di ulteriori misure di sicurezza previste	<ul style="list-style-type: none"> • Cisco NAC (Network Admission Control) Appliance (Clean Access) in alta affidabilità (HA)

Utilizzo di soluzioni Open Source e/o riuso di soluzioni disponibili

Soluzioni Open Source utilizzate nel progetto	CentOS, DHCP, DNS, NTP, FreeRADIUS, OpenLDAP, phpLDAPadmin, MySQL, phpMyAdmin, Webmin
Soluzioni già realizzate, anche da terzi, e riutilizzate nel progetto	Controller per AP Cisco WLC AIR-WLC4402-50-K9, sistema di controllo Cisco Wireless Control System (WCS-APLOC-50 / MCS-7825-H3-CCE1), trenta AP Cisco AIR-LAP1131AG-E-K9

Piano di comunicazione

Piano di comunicazione del progetto (ad esempio, bacheche dedicate, poster, depliant illustrativi, ecc.)	<p>L'avvio del progetto deve essere promosso da un piano di comunicazione che sappia trasferire le motivazioni e gli obiettivi del progetto, e la sua capacità e adeguatezza a rispondere alle attese e ai bisogni degli utenti (studenti e docenti) sottolineando i benefici derivanti dalla realizzazione del progetto.</p> <p>Tra le azioni di comunicazione si possono elencare:</p> <ul style="list-style-type: none"> produzione di materiale informativo; organizzazione di eventi; realizzazione di apposite sezione web dedicate ai servizi. <p>Il portale di Ateneo e quelli di facoltà sono il luogo fondamentale per la divulgazione del progetto.</p>
----------------------------------------------------------------------------------------------------------	-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

Sezione 3 – Scheda Progetto

Nome e descrizione del progetto

Mediterrane@senzafili.plus: potenziamento di una rete wireless per l'accesso sicuro degli studenti

Il presente progetto ha l'obiettivo di portare a completamento, estendere e potenziare il progetto già avviato dall'Università Mediterranea di Reggio Calabria per la realizzazione di una rete wireless di Ateneo e di alcuni servizi agli studenti (tra cui una piattaforma di groupware), grazie al finanziamento ottenuto attraverso analogo bando del Ministero per l'Innovazione e le Tecnologie (MIT) di concerto con il Ministero dell'Università, dell'Istruzione e della Ricerca (MIUR) e con il Ministero dell'Economia e della Finanza, attraverso decreto datato 6 dicembre 2005 (progetto denominato Mediterrane@senzafili).

Il progetto prevede, tra le azioni preliminari, la realizzazione delle infrastrutture di cablaggio in un edificio dell'Ateneo ad alta concentrazione di studenti (denominato lotto D), azione propedeutica alla realizzazione dei servizi wireless in quella sede.

Inoltre prevede la realizzazione di alcune delle misure di sicurezza previste nel progetto Mediterrane@senzafili (il sistema NAC – Network Access Control) ma non in esso finanziate.

Obiettivi e ambito del progetto

L'obiettivo è quello di portare a completamento una infrastruttura di copertura wireless per le sedi d'Ateneo che sia in grado di fornire:

- flessibilità completa nell'accesso alla rete e ai suoi servizi, utilizzando una logica di aree di più ampia copertura possibile ed il roaming tra diversi punti di accesso
- utilizzo di una architettura AAA (autenticazione, autorizzazione e accounting) RADIUS centralizzata per la definizione e gestione dei profili di accesso
- cifratura delle comunicazioni wireless, utilizzando i più recenti standard di sicurezza, per garantire massima riservatezza ai dati trasmessi
- supporto dello standard 802.1x e VPN in grado di aumentare la sicurezza intrinseca della soluzione e di regolamentare l'accesso delle utenze alla rete wireless Wi-Fi
- accesso alla rete attraverso NAC (Network Access Control)
- utilizzazione di profili d'utenza e differenziazione per i diversi tipi di accesso (p.es. ospiti, studenti, docenti, personale tecnico-amministrativo, eventi, ecc.)
- compatibilità dell'infrastruttura con i più diffusi apparati e standard disponibili in commercio, per abilitare una vasta ed eterogenea utenza quale quella universitaria alla fruizione dei servizi
- elevate funzionalità di Network e Security Management, per l'ausilio all'esercizio quotidiano di rete
- elevate prestazioni in termini di qualità e quantità di banda trasmissiva messa a disposizione delle singole utenze
- impulso ai servizi di E-learning
- facilitazioni ai servizi minimi di verbalizzazione elettronica degli esami e sportello virtuale delle segreterie didattiche e studenti

La soluzione proposta avrà caratteristiche generali di modularità tali da poter essere agevolmente estesa a eventuali nuovi edifici del Campus di Ateneo nonché offrire la possibilità di estendere la copertura agli spazi aperti comuni dell'intero complesso d'edifici delle sedi e del Campus (non oggetto dell'intervento previsto nel presente progetto).

Finalità e risultati attesi dal progetto

La finalità principale è quella di consentire alla popolazione universitaria (studenti, docenti, personale tecnico-amministrativo, ospiti) un accesso facile, sicuro ed ubiquitario ai servizi resi disponibili dalla Rete di Ateneo, alla connessione alla rete GARR per fini didattici o di ricerca, ad un metodo di condivisione delle informazioni più diretto e proficuo.

Rispetto al progetto originario, del quale il presente rappresenta un potenziamento, le finalità attese risultano di scala superiore, in quanto la copertura wireless che si intende raggiungere riguarderà la quasi totalità delle aule e dei luoghi frequentati dagli studenti, compresi gli edifici di nuova costruzione (lotto D).

L'esigenza della fruibilità dell'accesso alla rete da parte degli studenti è in rapida crescita nell'Ateneo di Reggio Calabria, anche per il fatto che, parallelamente alla esecuzione di questo progetto, l'Ateneo sta mettendo in atto un progetto per la realizzazione dei servizi di verbalizzazione elettronica degli esami e di segreteria studenti/didattica on-line (servizi minimi, secondo il bando relativo al presente progetto), con iniziativa autonoma e possibilità di completamento/potenziamento nell'ambito del bando "Campus Digitali".

La realizzazione del presente progetto comporterà un aumento della produttività e soddisfazione di tutte le categorie d'utenza coinvolte nel progetto, grazie alla possibilità fornita dalla tecnologia wireless. In quest'ottica è altrettanto facilmente prevedibile un incremento della

fruizione dei servizi interni già disponibili ed un successivo, naturale sviluppo di nuovi strumenti, grazie all'accelerazione consentita dalla facilità d'accesso e di sfruttamento degli stessi.

Ulteriori applicazioni potranno poi essere veicolate per mezzo della connettività allargata, quali per esempio modalità didattiche real-time (chat, forum, newsgroup), reperimento di testi ed informazioni in tempo reale, gruppi di studio "virtuali" tra studenti che risiedono in diverse sedi o in diverse Facoltà, spazi di discussione dedicati a materie d'insegnamento o d'approfondimento, distribuzione di materiale didattico su piattaforme di ultima generazione (p.es. podcasting su Apple iPod®).

Il progetto darà quindi notevole impulso ai servizi di e-learning, e alle altre iniziative progettuali dell'Ateneo che sono orientate alla fruizione on-line da parte degli studenti. Per il corpo docente e tecnico-amministrativo la possibilità di accesso alle proprie risorse anche al di fuori dello studio o dell'ufficio risulterà in una maggiore libertà di movimento, contemporaneamente incrementando l'efficacia del tempo dedicato alle attività lavorative quotidiane.

Caratteristiche dei servizi / Procedure di sicurezza

Una qualsiasi infrastruttura wireless pone particolari problematiche di sicurezza connesse alla natura stessa del mezzo radio, utilizzato per la trasmissione dati.

Gli accessi di tipo wireless richiedono, infatti, una gestione molto più complessa delle procedure di sicurezza, in considerazione del fatto che una infrastruttura di questo tipo risulta essere, per definizione, molto più vulnerabile rispetto ad un'infrastruttura cablata.

Le maggiori debolezze possono riassumersi nei seguenti punti:

- accesso condiviso al mezzo trasmissivo da parte degli utenti, con conseguente facilità ad acquisire informazioni riservate. Gli utenti sono quindi maggiormente esposti a rischi quali, anzitutto, l'intercettazione delle credenziali personali e la violazione della privacy
- difficoltà a localizzare fisicamente l'utente wireless
- difficoltà a circoscrivere con precisione il raggio di copertura di un Access Point. Ciò è spesso legato alle caratteristiche architettoniche della struttura in cui un Access Point è installato, con il conseguente rischio di far accedere alla rete utenti "abusivi" che operano al di fuori delle sedi istituzionali.

Per queste ragioni, all'interno delle strutture di Ateneo raggiunte dal servizio, l'accesso degli utenti dovrà necessariamente essere regolato da un solido sistema di autenticazione, oltre che di sicurezza, che garantisca sia la fruizione esclusiva alle persone autorizzate sia la protezione delle credenziali d'accesso. Altrettanto importanti dovranno essere i meccanismi di gestione della rete e del canale radio in senso lato (mappe radio del campus, autoconfigurazione radio per reazione ad interferenze, servizi opzionali di localizzazione, etc.).

I sistemi più diffusi per il controllo dell'accesso alle reti wireless si basano sul meccanismo di autenticazione IEEE 802.1x, originariamente ideato per reti cablate ed in seguito adattato per l'utilizzo su reti wireless (802.1x/EAP).

Considerate le finalità istituzionali cui è destinata la rete wireless di Ateneo, è stata dunque prestata particolare attenzione all'attivazione di meccanismi che garantiscano un alto grado sia di sicurezza sia di affidabilità (HA) dei servizi - di rete e applicativi - che si intendono veicolare anche attraverso di essa.

E' stata quindi individuata una architettura ridondata di gestione, controllo e autenticazione centralizzata.

L'architettura hardware individuata utilizza un apparato denominato Wireless LAN Controller (WLC), in alta affidabilità, a cui tutti gli AP dovranno associarsi (previo controllo delle autenticazioni) in grado di gestirne la configurazione qualora se ne presentasse la necessità.

Gli AP dialogano con il controller mediante un protocollo denominato Lightweight Access Point (LWAPP) che definisce un meccanismo di tunneling del traffico e della messaggistica di controllo per l'impostazione delle operazioni run-time.

Per avere un controllo puntuale ed effettivo dell'infrastruttura si è poi individuata una piattaforma hardware/software necessaria alla pianificazione, configurazione e gestione delle reti wireless centralizzate, denominata Wireless Control System (WCS), già acquisita dall'Ateneo.

L'importazione all'interno del WCS delle mappe relative alle zone di copertura wireless permette, grazie ad una funzionalità di planning integrata in fase di progettazione, la valutazione della copertura e potenza del campo elettromagnetico generato dagli AP. Il WCS è in grado di fornire la distribuzione del campo wireless irradiato in funzione della geometria e della consistenza dei materiali presenti nell'ambiente in cui viene ospitato l'AP, facilitando in questo modo il posizionamento dei diversi AP all'interno degli ambienti.

Il WCS ricopre, allo stesso tempo, un ruolo centrale nel monitoring del funzionamento delle connessioni wireless, poiché dotato di strumenti di controllo e monitoraggio quali, ad esempio:

- un quadro sinottico contenente il numero di AP attivi ed il numero di client wireless serviti da ciascun AP
- la distribuzione effettiva del campo wireless in ciascuna zona
- il posizionamento del client wireless all'interno di ciascuna zona
- il controllo sui tentativi di accesso non autorizzato in senso lato (AP non autorizzati, utenti non autorizzati, attacchi, tentativi di intrusione, etc.)

L'architettura di sicurezza è basata su NAC (Network Access Control), Radius ed LDAP.

Nell'ambito di una LAN wireless, la soluzione NAC non dovrebbe essere considerata un'alternativa alla autenticazione basata su 802.1x/EAP. I

servizi di controllo d'accesso e di bonifica offerti dalla soluzione NAC sono complementari, e forniscono misure di sicurezza aggiuntive al controllo d'accesso offerto intrinsecamente da 802.1x/EAP.

Sebbene l'architettura NAC possa essere utilizzata come punto di controllo e rafforzamento di sicurezza degli accessi alla rete locale, questa non può, da sola, fornire la necessaria confidenzialità dei dati trasmessi (privacy).

Per questa ragione è necessario utilizzare 802.1x/EAP integrandolo a WPA/WPA2, l'interazione dei quali assicura la confidenzialità dei dati riducendo al contempo potenziali minacce di sicurezza.

Gli utenti si identificano utilizzando le medesime credenziali per l'accesso ai servizi di posta elettronica (username /password), in un form web che appare automaticamente all'interno di un browser.

Una volta che un utente wireless si sia autenticato ed abbia ottenuto l'accesso alla parte wireless della rete, l'architettura NAC applica un aggiuntivo livello di sicurezza al fine proteggere ulteriormente l'accesso alla parte wired della rete, fino a quando non siano soddisfatte le seguenti condizioni:

- l'utente finale è stato verificato/autenticato. Sebbene questo processo sia ridondante per l'accesso wireless (perché ripete ciò che è già stato realizzato mediante autenticazione 802.1x/EAP), questa fase è necessaria per l'accesso tramite le reti wired.

- la periferica dell'utente finale (computer, pda, terminale voip, etc.) supera con esito positivo gli eventuali, ulteriori controlli di conformità alle politiche di sicurezza, ad esempio il controllo che sul client dell'utente sia in esecuzione la versione più recente di un software anti-virus, etc.

Il progetto prevede RADIUS (Remote Authentication Dial-In User Server/Service) come meccanismo di autenticazione.

Un server FreeRadius, in alta affidabilità, che è destinato al controllo degli accessi, dialoga con un directory server Open LDAP (Lightweight Directory Access Protocol), anch'esso in alta affidabilità, contenente le credenziali ed alcune informazioni relative a studenti, dipendenti e ad altre categorie di utenza dell'Ateneo, quali ad esempio assegnisti di ricerca, dottorandi, docenti a contratto, collaboratori occasionali, etc.

Tale soluzione, aderente agli standard attualmente più diffusi, si è già dimostrata estremamente affidabile e molto versatile nel controllo degli accessi applicato alla rete cablata.

Un'ulteriore fase di controllo è prevista nel momento in cui l'utente accede alla rete GARR. Anche in questa fase la sessione dell'utente viene tracciata in un file di log, nel pieno rispetto della normativa vigente in materia di privacy e di sicurezza nell'accesso ad Internet. Attraverso i record di accounting è possibile stabilire l'orario d'inizio e di fine delle sessioni wireless o wired di un qualsiasi utente.

Inoltre, per l'accesso ad Internet da parte dell'utenza wireless, potrà essere definita una ulteriore policy (port filtering), che rende disponibili soltanto alcuni servizi, negando implicitamente il resto delle applicazioni disponibili su Internet (ad esempio il peer-to-peer).

La fase di autorizzazione ai vari servizi disponibili on line è gestita a livello applicativo con la definizione dei profili di accesso. Infatti, le varie applicazioni implementano un sistema di profilatura che consente di modellare gli accessi sulla base dei privilegi accordati alle diverse categorie di utenti.

Infine, un ulteriore livello di sicurezza è rappresentato dall'infrastruttura della Server Farm centralizzata che prevede l'utilizzo di sistemi in alta affidabilità (HA). In questo contesto, la disponibilità dei servizi WEB Authentication, RADIUS, DHCP, DNS e LDAP deriva dalla ridondanza hardware e software dei server che li ospitano.

Sulla piattaforma sopra descritta verranno poi resi disponibili, oltre ai servizi minimi (iscrizione online e verbalizzazione elettronica degli esami), due nuovi servizi, da cui potrà trarre immediato beneficio in primis la comunità studentesca.

Il primo, eduroam (EDUCation ROAMing) è un'infrastruttura basata su una rete gerarchica e confederata di server RADIUS, che utilizza 802.1x. Gli utenti roaming che visitano un Istituto federato all'iniziativa saranno in grado di utilizzare la WLAN usando le medesime credenziali (username e password) che userebbero nella loro istituzione d'appartenenza, senza quindi la necessità di procedere ad ulteriori formalità presso l'istituto ospitante.

Eduroam consente agli utenti delle istituzioni accademiche confederate l'accesso sicuro a Internet presso qualsiasi altra istituzione parimenti confederata.

Il secondo è una collaboration suite innovativa, ZIMBRA, basata su piattaforma open source su tecnologia Ajax, sviluppata con l'intento di rendere più agevole e customizzata - grazie all'impiego di diverse tecnologie, non ultime quelle dedicate alla sicurezza, operanti indifferentemente su server Linux e MAC - proprio la collaborazione aziendale, intesa come scambio di informazioni dei più svariati generi tra utenti appartenenti ad una stessa comunità.

In sintesi quindi, l'infrastruttura possiede i seguenti requisiti di massima:

- web authentication per l'utente dotato di client con funzionalità IEEE 802.11b/g. Tale modalità semplifica molto la fase di setup/startup; l'utente deve preoccuparsi unicamente di attivare un browser ed impostare/inserire le proprie username e password

- controllo centralizzato degli accessi con backend di autenticazione LDAP. Ciò consente di ridurre gli oneri gestionali legati a soluzioni d'autenticazione locali, e di mantenere un unico database centrale degli utenti autorizzati alla fruizione del servizio

- software ed hardware centralizzato per la configurazione, la gestione ed il monitoraggio degli Access Point con riduzione dei costi di gestione del servizio, considerato che non vi è necessità di presidio nelle strutture periferiche.

Questo progetto è stato sviluppato nell'ottica di integrare, estendere (considerando anche le strutture periferiche) e potenziare l'infrastruttura wireless di Ateneo, rafforzandone le misure di sicurezza, soprattutto a seguito della recente inaugurazione e messa in uso del complesso edilizio denominato Corpo D (c.d. 3° Lotto) all'interno Campus Universitario.

Si tratta di un nuovo complesso edilizio deputato principalmente ad ospitare in spazi più adeguati e funzionali tutte quelle attività che coinvolgono la partecipazione studentesca, a cominciare da quelle di didattica, laboratorio, seminari ed espositive, per finire (in maniera sicuramente non esaustiva) con quelle relative agli organi di rappresentanza studentesca e quelle di tipo ricreativo e/o culturale che la coinvolgeranno direttamente.

In questo senso si dovrà parimenti tener conto del prevedibile incremento nel tempo del numero di utenti, direttamente connesso alla crescita dell'Ateneo stesso, anche nelle sue sedi periferiche.

Prima di procedere con l'esposizione della soluzione di massima, si ritiene opportuno descrivere l'infrastruttura di rete attualmente disponibile (cfr. progetto Re.B.US – Rete Broadband di CampUS, di cui all'Avviso 901/2003, PON 2000-2006 “Ricerca Scientifica, Sviluppo Tecnologico, Alta Formazione” Misura II.2 “Società dell'Informazione per il Sistema Scientifico Meridionale” Azione a – Infrastrutture di rete locale) e quella di imminente realizzazione (cfr. progetto Mediterraneo@senza.fili, di cui al decreto attuativo DIT 6.12.2005).

Attuale infrastruttura wired

L'architettura di massima della rete di Campus dell'Università Mediterranea di Reggio Calabria è articolata in tre livelli: un livello di accesso, uno di distribuzione ed uno di core (lo schema logico è riportato nella figura A).

Il livello d'accesso è costituito da switch Cisco 3750 / 3650 layer 3.

Il livello di distribuzione è composto da switch Cisco 4507-R layer 3.

Il livello di core è costituito da due switch Cisco 6509-E layer 3.

L'edge router è un Cisco 7606.

Le dorsali ridondate in fibra ottica sono in tecnologia 10GbE.

La Server Farm possiede un proprio livello di distribuzione/accesso con switch Cisco 6509-E, popolato con scheda firewall WS-SVC-FWM-1-K9 e scheda Content Switching/SSL WS-X6066-SLB-S-K9.

Gli edge firewall sono due Cisco ASA5520-AIP10-K9 in HA.

Infrastruttura wireless in corso di realizzazione

Nell'ambito del progetto Mediterraneo@senza.fili sopraccitato, l'Ateneo, attraverso il CESIAT, sta sviluppando l'installazione in alcune sedi, ed in particolare negli spazi comuni destinati alla didattica e alle attività “di massa”, di 30 Access Point per la connessione wireless alla rete di Ateneo da parte della popolazione studentesca, del personale docente e di quello tecnico-amministrativo.

Nella figura B è rappresentata, integrata alla rete di Campus, la rete wireless (oggetto del progetto Mediterraneo@senza.fili) che è in corso di realizzazione.

Con riferimento alle nuove esigenze sopraccennate, si rende necessario un complessivo potenziamento sia dell'estensione della copertura wireless sia di quella delle attrezzature ad essa pertinenti.

Si ritiene quindi indispensabile offrire una percentuale di copertura assai più ampia e pervasiva, tenendo conto della rapida espansione delle attività didattiche (lezioni tradizionali e/o su piattaforme e-learning, seminari, mostre, etc.) e della condivisa – oltre che necessaria – volontà di offrire agli studenti servizi tradizionali ed innovativi attraverso una infrastruttura wireless molto più efficiente e sicura.

In riferimento a quanto appena esposto, l'Ateneo si è poi già autonomamente attivato per la realizzazione di una infrastruttura di telecomunicazioni (cablaggio strutturato, apparati per la LAN d'edificio e interconnessione in fibra ottica al backbone di Campus) destinata a consentire la fruibilità wired/wireless dei servizi di rete ed applicativi nel complesso edilizio Corpo D / 3° Lotto.

E' di imminente realizzazione il cablaggio strutturato CAT6 dell'edificio (per un totale di 196 PDL pari a 392 punti rete), ed i necessari apparati di networking d'accesso, distribuzione (LAN di edificio) e interconnessione al backbone di Campus sono stati recentemente acquisiti dall'Ateneo.

Il complesso edilizio Corpo D / 3° Lotto si sviluppa in altezza su sette quote.

Gli interventi infrastrutturali di cablaggio strutturato individuati come necessari, riguardano solamente le aree ed i livelli indicati nella illustrazione sottostante, e precisamente:

Zona A (Aule, studi, uffici)

- Livello -2, Building Distribution (BD)

- livello -2, servito dal rack FD-A.-2
 - livello 0, servito dai rack FD1-A.0 ed FD2-A.0
 - livello +1, servito dal rack FD-A.+1
 - livello +2, servito dal rack FD-A.+2
- Zona B (Aula Magna)
- Livello +2, servito dal rack FD-B.+2
- Zona C (Biblioteca)
- livello -2, servito dal rack FD-C.-2

Nella figura C si riporta sinteticamente la topologia del cablaggio strutturato dell'edificio in corso di realizzazione.

Le attrezzature di networking, già acquisite dall'Ateneo, necessarie a garantire la piena funzionalità della nuova rete di edificio e la sua completa integrazione con quella esistente, sono state individuate in sette switch di accesso (FD) ed uno di distribuzione (BD) per la LAN di edificio, nonché in quelle necessarie all'interconnessione in fibra ottica al Centro Stella di Campus (ER-CESIAT – POLO GARR) e quindi al backbone di Ateneo ed alla rete GARR.

Nella figura D si riporta sinteticamente la topologia della LAN di edificio in corso di realizzazione.

Nella figura E viene evidenziato l'inquadramento topologico della LAN del Corpo D / 3° Lotto in quella complessiva di Campus.

I nuovi Access Point verranno attestati all'infrastruttura di rete wired di edificio e la loro attivazione avverrà tramite la configurazione di specifiche VLAN sugli apparati d'accesso. In questo modo sarà possibile realizzare la completa integrazione dei nuovi apparati della rete wireless all'interno dell'infrastruttura di rete esistente nel Campus.

Per tre sedi periferiche dell'Ateneo, e precisamente: il Dipartimento di Scienze Storiche, Giuridiche, Economiche e Sociali (DSSGES), il Centro Orientamento di Ateneo (UniOrienta) e la Segreteria Studenti e Biblioteca della Facoltà di Giurisprudenza, sarà utilizzata la tecnologia H-REAP (Hybrid Remote Edge Access Point).

H-REAP permette di configurare e controllare gli AP collocati in una sede periferica attraverso un controller centralizzato, quindi senza necessità di acquistare ed installare un controller per ciascuna sede. Risulta essere una soluzione affidabile qualora il numero di AP locali sia piccolo.

Un AP in modalità H-REAP può essere configurato affinché commuti il traffico di utente sulla rete locale di edificio (piuttosto che trasmetterlo al controller centralizzato attraverso il tunnel LWAPP), con ciò consentendo che tale traffico possa essere indirizzato, ad esempio, verso la connessione Internet di ciascuna struttura decentrata.

Viceversa per la Facoltà di Giurisprudenza, che verrà dotata di un numero più ampio di AP, è prevista la riutilizzo in locale del controller Cisco AIR-WLC4402-50-K9 (al momento utilizzato come controller centralizzato di Campus).

Il controller periferico e quello in alta affidabilità centralizzato verranno gestiti dal sistema Wireless Control System (WCS), che dovrà di conseguenza essere adeguato al maggior numero di AP attivi.

Nella figura F viene rappresentato lo schema logico dell'infrastruttura WLAN sulla WAN di Ateneo, evidenziando i flussi di traffico di utente (blu) e i flussi di controllo tra AP e WLC (rosso) e quelli tra WLC e WCS (nero).

Sull'infrastruttura wireless appena descritta, come precedentemente accennato, saranno resi disponibili, oltre ai servizi minimi (iscrizione online e verbalizzazione elettronica degli esami) i nuovi servizi eduroam e Zimbra:

L'architettura di eduroam si basa su una serie di tecnologie (e di accordi reciproci tra istituzioni, enti, etc.) che consentono all'utente roaming di poter "accendere il pc ed essere on-line".

Eduroam assicura un alto livello di sicurezza poiché l'autenticazione di ciascun utente viene effettuata presso l'istituzione di appartenenza dello stesso, attraverso il suo metodo di autenticazione specifico.

L'autorizzazione per l'accesso alle risorse di rete locale è invece richiesta all'istituzione ospitante.

Per fornire questo strumento, eduroam è stato costruito secondo uno schema gerarchico confederato.

Il servizio di Confederazione, che si trova gerarchicamente più in alto, è costruito su servizi di roaming nazionali, gestiti dagli operatori nazionali di roaming (NROs) (nella maggior parte dei casi NREN). I servizi nazionali di roaming possono avvalersi di altri soggetti, ad esempio, confederazioni di campus, comunali, regionali, etc.

Per il trasporto della richiesta (e della necessaria risposta) di autenticazione di un utente dalla istituzione visitata alla istituzione di appartenenza viene utilizzato un sistema gerarchico di server RADIUS.

Generalmente, ogni ente utilizza un server RADIUS, che a sua volta è collegato ad un backend d'autenticazione locale.

Ciascun server RADIUS locale è collegato ad un server RADIUS nazionale, che a sua volta è collegato ad un server RADIUS europeo (o transcontinentale).

Poiché gli utenti usano nomi utente nel formato "UTENTE@REALM" (in cui REALM è il nome di dominio DNS dell'istituzione di appartenenza, spesso sotto forma di istituzione.tld, dove tld è il codice di dominio di primo livello dello stato), il server RADIUS può usare queste informazioni per indirizzare la richiesta tramite la struttura gerarchica fino a raggiungere l'istituto d'appartenenza.

Utilizzando l'apposito metodo EAP, viene quindi stabilito un tunnel protetto (EAP-TTLS e PEAP) dal computer dell'utente verso il suo istituto di appartenenza, attraverso il quale sono veicolate le informazioni di autenticazione (nome utente/password etc.). Parimenti può essere utilizzato un sistema di autenticazione reciproco mediante certificati X.509 (EAP-TLS). I tre metodi di autenticazione citati stabiliscono un tunnel TLS protetto a partire dal dispositivo dell'utente fino al suo server di autenticazione.

Il secondo servizio è basato su una collaboration suite innovativa, ZIMBRA, costruita su piattaforma open source in tecnologia Ajax, sviluppata con l'intento di rendere più agevole e customizzata – grazie all'impiego di diverse tecnologie, non ultime quelle dedicate alla sicurezza, operanti indifferentemente su server Linux e MAC – proprio la collaborazione e comunicazione aziendale, intese come scambio di informazioni dei più svariati generi tra utenti appartenenti ad una stessa comunità.

Sulla infrastruttura appena descritta si procederà quindi, nell'ambito di questo progetto, a:

- potenziare in modo capillare la copertura wireless estendendola a tutto il Campus Universitario e le sue sedi periferiche, attraverso l'acquisizione di nuovi Access Point, apparati wireless, di networking, e dei server per i necessari servizi di rete (si noti in questa direzione la scelta di applicazioni Open Source descritte con maggiori dettagli nell'apposita sezione)
- rafforzare le misure di sicurezza mediante WEB Authentication (NAC), RADIUS ed LDAP
- assicurare, sull'intera infrastruttura wireless, la piena fruibilità dei servizi minimi (iscrizione online e verbalizzazione elettronica degli esami)
- realizzare nuovi servizi di comunicazione e collaborazione dedicati principalmente alla comunità studentesca
- rafforzare l'affidabilità di tutti i servizi erogati attraverso soluzioni in HA (con ridondanza hardware e software)

La rete wireless di Ateneo utilizzerà DHCP per assegnare gli indirizzi IP sia agli Access Point (su VLAN di management) sia ai client wireless (VLAN di utente). Anche tale fondamentale servizio di rete verrà installato in alta affidabilità.

Analogamente vale per i servizi di rete DNS ed NTP.

Anche i servizi applicativi verranno installati in alta affidabilità.

Più in dettaglio le nuove acquisizioni riguarderanno, di massima:

- 160 access point
- switch d'accesso necessari agli AP per la connessione alla rete wired
- due controller wireless in alta affidabilità (HA)
- hardware di networking per l'integrazione dell'infrastruttura al Centro Stella di Campus
- server in alta affidabilità destinati ai vari servizi di rete (DHCP, DNS, LDAP, RADIUS, etc.)
- server in alta affidabilità destinati ai servizi da offrire alla popolazione studentesca nell'ambito di realizzazioni connesse alla necessità di comunicazione e interscambio/condivisone di dati di vario genere
- software di supporto/integrazione/monitoring
- servizi professionali (interni e/o esterni all'Ateneo) necessari ad assicurare, sull'intera infrastruttura wireless, la piena fruibilità dei servizi minimi (iscrizione online e verbalizzazione elettronica degli esami)
- acquisto di licenze software
- servizi professionali (interni e/o esterni all'Ateneo), quali ad esempio servizi di progettazione, consulenza, implementazione servizi di rete e nuovi servizi agli studenti, servizi di sviluppo esterno, risorse interne, etc. e di gestione.

Le sedi presso cui il servizio verrà attivato sono: le quattro Facoltà, le Aule Magne, il III Lotto, il Rettorato, il Dipartimento di Scienze Storiche, Giuridiche, Economiche e Sociali c/o Palazzo Sarlo - Via Tommaso Campanella n. 38/A, gli Uffici Amministrativi – con particolare riguardo alle Macro Aree Servizi agli Studenti (MCA III), il Centro Orientamento di Ateneo (UniOrienta) - Via San Marco n. 3, e la Segreteria Studenti e Biblioteca della Facoltà di Giurisprudenza – Piazza S. Stefano da Nicea, nella frazione Archi.

Approccio e Piano di realizzazione

Il progetto prevede un piano di realizzazione articolato in 9 task.

Si noti che essendo il progetto di potenziamento e completamento di un progetto di Ateneo già in atto, la durata complessiva indicata nei dati sintetici del progetto è maggiore dei 12 mesi previsti dal bando per il completamento dal momento della stipula della convenzione, includendo tutte le attività del progetto non concluse alla data di pubblicazione dell'avviso sulla G.U. (come previsto nell'art. 1 del bando). Essa assume dei tempi di approvazione e stipula della convenzione di circa 3 mesi dalla scadenza del bando, comportando quindi una durata complessiva del progetto di 18 mesi dalla pubblicazione del bando sulla G.U.

In particolare, il progetto è stato avviato il 10 Aprile 2008. Alla data di scadenza del bando sono pertanto stati eseguiti i primi 3 mesi e 10 giorni di attività. Le attività proseguiranno durante la fase di approvazione e stipula della convenzione, di cui si presume una durata di 2 mesi e 20 giorni. A questo punto saranno state svolte attività per 6 mesi. Il progetto proseguirà per ulteriori 12 mesi (così come previsto dal bando)

fino alla data del 9/10/2009, raggiungendo così una durata complessiva di mesi 18. Si veda anche il diagramma di GANTT in allegato.

Task a – Attività di comunicazione.

Sin dall'inizio della realizzazione del progetto sarà svolta una pervasiva attività di comunicazione che consisterà tra l'altro in:

- predisposizione di materiale informativo (poster e/o cartelli)
- seminari divulgativi presso le strutture interessate dal servizio
- predisposizione delle pagine web sui siti di Ateneo e di Facoltà contenenti informazioni sui nuovi servizi e realizzazioni

Al momento dell'attivazione del servizio verranno affissi i poster e/o i cartelli predisposti in tutte le sedi interessate e verrà svolta una adeguata campagna di informazione attraverso gli strumenti di comunicazione interna (newsletter, notiziario, etc.).

Successivamente all'avvio del servizio verranno organizzati seminari divulgativi rivolti soprattutto agli studenti e sarà costantemente svolta una attività di monitoraggio per verificare il grado di utilizzo effettivo e di gradimento del servizio.

Durata: dall'inizio al termine del progetto.

Task b - Individuazione delle aree wireless nelle sedi coinvolte dal progetto.

Sono previste tre distinte attività:

- 1- individuazione delle aree, all'interno di ciascuna sede, in cui attestare gli Access Point. Tale attività verrà svolta tenendo conto della dislocazione delle aule e degli spazi in cui sono concentrate le attività didattiche e nelle quali gli utenti possono usufruire di arredi (sedute, tavoli, etc.) che consentano loro di utilizzare uno strumento personale per l'accesso alla rete
- 2- sopralluoghi mirati, per verificare l'esistenza delle condizioni ambientali, strutturali, impiantistiche e architettoniche necessarie per includere nel progetto ciascun'area individuata
- 3- pianificazione degli interventi tecnici necessari a porre rimedio, laddove se ne verifichi la necessità, alle carenze impiantistiche riscontrate nel corso dei sopralluoghi descritti nell'attività precedente

Durata: 1 mese dalla fine dei Task e ed f.

Task c – Realizzazione della nuova Infrastruttura.

Questa fase prevede, da parte della ditta aggiudicataria, l'installazione dei nuovi apparati centrali (wireless controller), la loro configurazione, e la relativa attestazione e attivazione degli Access Point nelle sedi universitarie preindividuate, nonché la loro integrazione della nuova infrastruttura con le reti wireless e wired esistenti tramite la configurazione degli apparati di rete locali, switch layer 2 o 3 e l'attivazione di Vlan "ad hoc".

Sarà di seguito cura dell'Ateneo procedere alle necessarie attività di collaudo.

Durata: 8 mesi dal completamento del Task b.

Task d – Attività di verifica finale e "tuning" del sistema.

Una volta completata la fornitura ed effettuato il collaudo del sistema il servizio verrà attivato. Sarà di seguito realizzata un'attività di monitoraggio tesa a verificare il buon funzionamento dell'infrastruttura in ogni sua componente (HW/SW) nel rispetto dei requisiti e vincoli tecnici di progetto, con particolare attenzione alla sicurezza ed alle prestazioni. Ciò permetterà anche di realizzare in maniera tempestiva tutti gli interventi necessari per l'ottimizzazione del sistema (tuning).

Durata: 3 mesi dal termine del Task c.

Task e– Cablaggio lotto D

In questa fase verrà effettuato il cablaggio strutturato (incluso acquisto ed installazione) degli apparati attivi del lotto D del Campus di Feo di Vito, che ospita aule della Facoltà di Architettura e della Facoltà di Giurisprudenza.

Durata: 6 mesi dall'inizio del progetto.

Task f – Sistema di Controllo dell'accesso alla rete (NAC)

In questa fase viene installato, configurato e messo in esercizio il sistema NAC (network access control) che rappresenta il sistema scelto per il controllo dell'accesso alla rete.

Durata: 6 mesi dall'inizio del progetto.

Task g - Monitoraggio

Durante tutte le fasi del progetto è prevista un'azione di monitoraggio che permetterà di verificare eventuali criticità, ritardi, compensazioni.

Durata: dall'inizio alla fine del progetto

Task h – procedure tecnico-amministrative

Questa attività riguarda tutte le attività amministrative previste nel progetto, corrispondenti alla stesura di disciplinari di gara, capitolati speciali d'appalto, richieste preventivo, ordini, rendicontazioni, collaudi, pagamenti, etc.

Durata: dall'inizio alla fine del progetto

Vedi figura: GANTT

Utilizzo di soluzioni Open Source e riuso di soluzioni già disponibili

CentOS (Community enterprise Operating System) è un sistema operativo concepito per fornire una piattaforma enterprise per chiunque intenda utilizzare GNU/Linux ad un livello superiore. Si tratta di una distribuzione Linux che deriva da Red Hat Enterprise (sempre Linux), con cui cerca di essere completamente compatibile. Red Hat Enterprise Linux è composta interamente da software libero, ma è resa disponibile in una forma usabile (come CD-ROM di binari) solo a pagamento. Come richiesto dalla GNU General Public License e dalle altre licenze, tutto il codice sorgente è reso disponibile pubblicamente dalla Red Hat. Gli sviluppatori di CentOS usano questo codice per creare un prodotto molto simile a Red Hat Enterprise Linux rendendolo disponibile gratuitamente per il download e l'uso, senza però il supporto offerto da Red Hat. Sostanzialmente la differenza tra Red Hat e CentOS risiede principalmente nell'assenza di assistenza (il vero/principale motivo per cui si paga), e il cambio del logo, dato che Red Hat è un marchio registrato.

I servizi di rete DHCP, DNS ed NTP saranno implementati utilizzando le versioni Open Source dell'ISC (Internet Systems Consortium, Inc.).

Per RADIUS verrà utilizzato FreeRADIUS, una delle principali OpenSource di RADIUS. Il software, giunto ormai alla versione 1.1.2, è rilasciato sotto licenza GNU/GPL. Offre tutte le funzionalità dei software commerciali ed attualmente supporta i database LDAP, MySQL, PostgreSQL ed Oracle. Inoltre gestisce le autenticazioni tramite i protocolli EAP (EAP-MD5, EAP-SIM, EAP-TSL, EAP-TTSL, EAP-PEAP), MSCHAP, MSCHAPV2, Cisco LEAP, oltre ai classici PAP e CHAP.

Per LDAP verrà utilizzato OpenLDAP, un software libero, open source, implementazione del Lightweight Directory Access Protocol (LDAP) sviluppato dal progetto OpenLDAP. Viene rilasciato sotto una sua propria licenza chiamata OpenLDAP Public License.

Sarà anche utilizzato phpLDAPadmin (pla), un software scritto in PHP destinato a gestire l'amministrazione di server LDAP via Web. E' distribuito con la licenza GNU/GPL.

Come sistema di gestione dei dati, verrà utilizzato MySQL, un Database management system (DBMS) relazionale, composto da un client con interfaccia a caratteri e un server, entrambi disponibili sia per sistemi Unix come GNU/Linux che per Windows. MySQL supporta la maggior parte della sintassi SQL e si prevede in futuro il pieno rispetto dello standard ANSI. Possiede delle interfacce per diversi linguaggi, compreso un driver ODBC, due driver Java e un driver per Mono e .NET. Il codice di MySQL è di proprietà della omonima società, viene però distribuito con la licenza GNU/GPL oltre che con una licenza commerciale.

Come strumento destinato a gestire l'amministrazione di MySQL via Web, verrà utilizzato phpMyAdmin. Si tratta di uno strumento scritto in codice PHP, in grado di creare e cancellare basi di dati, creare / cancellare / modificare tabelle, cancellare / modificare / aggiungere campi, eseguire qualsiasi istruzione SQL, gestire chiavi sui campi, gestire privilegi, esportare dati in vari formati. E' oggi disponibile in 55 lingue. E' distribuito con la licenza GNU/GPL.

Per la configurazione generale dei server ed i servizi di base da essi erogati, verrà utilizzato Webmin: uno strumento di configurazione web based per sistemi operativi OpenSolaris, Linux e altri sistemi Unix-like. Con esso è possibile configurare, ad esempio, gli utenti, le quote disco, svariati servizi, file di configurazione, etc., oltre a configurare e controllare molte applicazioni OpenSource, come ad esempio il server HTTP Apache, PHP, MySQL, etc.

Webmin è in gran parte basato su Perl, in esecuzione con il suo proprio processo e server web, e può essere configurato per l'utilizzo di SSL se OpenSSL è installato con ulteriori aggiunte di moduli Perl.

È costruito su moduli che hanno un'interfaccia per i file di configurazione e il server Webmin. Ciò rende facile aggiungere nuove funzionalità.

Proprio per il suo design modulare, è possibile per chiunque scrivere plug-in per la configurazione del desktop.

Webmin permette anche il controllo di molte macchine attraverso una singola interfaccia, o mediante login webmin su altri host sulla stessa sottorete o LAN.

Webmin è rilasciato sotto licenza BSD.

Zimbra Collaboration Suite (ZSC) è una soluzione Open Source dedicata alla comunicazione e collaborazione Server (anche con Web Client, in tecnologia AJAX): offre infatti la gestione e la messa in condivisione di calendari, documenti, rubriche, conversazioni in forma di instant messaging, strumenti di comunicazione VoIP pienamente compatibili con SIP, con totale capacità di integrazione ai più diffusi browser web (

IEplorer, Firefox, Safari) e alle nuove tecnologie di comunicazione mobile (palmari, smartphone, etc.).

Non da ultimo, Zimbra è anche un server di posta elettronica con interfaccia web client fluida e intuitiva, attraverso cui gestire la messaggia in entrata e in uscita, con facilità di personalizzazione e piena tutela dell'utente contro Spam e Virus.

Zimbra include anche una tecnologia open source denominata Zimlet, che rende facile e rapida la personalizzazione dei moduli di condivisione e produzione delle informazioni direttamente dal client web dell'utente (mash-up).

Zimbra è disponibile anche con licenza commerciale con specifiche versioni (Network Standard / Professional Edition) che includono ulteriori funzionalità avanzate, quali ad esempio la possibilità di backup/restore di una o più mailbox, la sincronizzazione in modalità "over-the-air push" di mail, contatti, e calendario per client Palm, Symbian, Windows Mobile 5 e Blackberry, la configurazione cluster in alta affidabilità, il mail-storage a due livelli con trasferimento automatico dei messaggi più vecchi su memoria di massa meno performante e più economica, il supporto tecnico specialistico telefonico e via web, l'accesso alla Knowledge Base, etc.

Saranno riutilizzati il controller WLC Cisco AIR-WLC4402-50-K9, il sistema di controllo Cisco Wireless Control System (WCS-APLOC-50 / MCS-7825-H3-CCE1), trenta AP Cisco AIR-LAP1131AG-E-K9.

Iniziative e Piano di comunicazione

1. Obiettivi, Strategia e Target del Piano di Comunicazione

L'Obiettivo primario del presente Piano di Comunicazione è quello di strutturare un modello di promozione delle nuove attività che si andranno ad erogare, attraverso un sistema di comunicazione integrata finalizzata a creare informazione diffusa, rispetto al target primario di fruitori costituito dagli studenti dell'Ateneo. Accanto a questo, si ritiene opportuno articolare il Piano anche riguardo ad un ulteriore sub-obiettivo, quale quello di creare attenzione diffusa rispetto alle innovazioni del modello organizzativo che l'Università sta introducendo, al fine di far emergere le peculiarità dell'Ateneo su scenari molto ampi, riguardo all'attenzione che la stessa attribuisce ai fattori di customer-relationship. È noto che il livello di partecipazione soggettiva nei confronti di un servizio dipende strettamente non solo dall'utilità, dall'interesse personale ma anche dal tipo di rapporto, di relazione e di reputazione, riconosciuta al soggetto erogatore. In questa direzione, azioni di informazione adeguatamente svolte, oltre a favorire la diffusione di conoscenze specifiche, favoriscono un importante processo di consolidamento del soggetto istituzionale che ha il ruolo di attore primario nel sistema complessivo di gestione del processo e, nella fattispecie, dei servizi offerti attraverso l'infrastruttura wi-fi alla popolazione studentesca.

In sintesi, l'obiettivo primario del Piano di comunicazione è Comunicare in maniera efficace le nuove modalità operative e la conseguente rimodulazione strategica delle azioni. Ciò si perseguirà con l'attuazione di una opportuna strategia, finalizzata a:

- dare massima visibilità alla innovazione introdotta, attraverso una comunicazione coinvolgente, trasmettendo un'immagine di forte impatto, associata a capacità organizzativa e gestionale.
- Mettere in risalto gli indirizzi di riferimento presso i quali poter ottenere ulteriori informazioni, ed i luoghi dove poter trovare materiali informativi.
- Comunicare in sintesi, ma con efficacia, i contenuti tecnici delle singole attività programmate e fornire con chiarezza ed in maniera esaustiva tutte le informazioni utili per fruire al meglio dei servizi offerti dal progetto;

Ciò dovrà tradursi nel consolidamento del modello di customer relationship in chiave manageriale e nel rafforzamento del ruolo di centralità delle attività di relazione one-to-one nella gestione del sistema complesso della comunicazione.

Ferma restando dunque la finalità primaria di tutta la Campagna di Comunicazione, facilmente identificabile con l'esigenza di portare a conoscenza del maggior numero possibile di studenti l'avvio del nuovo sistema organizzativo, ad essa si affiancheranno alcuni "sotto-obiettivi" altrettanto facilmente individuabili,.

- Divulgare con la massima chiarezza la portata dell'evento e le innovazioni di servizio apportate Informando il maggior numero possibile di potenziali fruitori;
- Porre al centro dell'attenzione il cliente/fruitor effettivo e quello potenziale;
- Amplificare la "cassa di risonanza" dell'iniziativa;
- "Utilizzare" l'importanza dell'iniziativa per creare valore aggiunto sul brand complessivo dell'Ateneo;
- Adottare un linguaggio di comunicazione opportunamente orientato al target di riferimento, puntando a realizzare un'attività di comunicazione efficace per i differenti tipi di pubblico, interno ed esterno (opinione pubblica, decisori locali, autorità, ecc.);

Veicolare la diffusione di informazioni attraverso i servizi interattivi.

In sintesi, la strategia degli obiettivi e delle azioni del Piano mira a realizzare un servizio che diffonda informazione, conoscenze, modalità di interazione.

2. La Strategia Creativa e le Scelte Grafico-Visive

Le azioni di comunicazione verranno realizzate facendo ricorso a strumenti di comunicazione differenziati per funzione, al fine di raggiungere più efficacemente gli obiettivi prefissati.

L'idea fondante è quella di attuare una comunicazione informativa correlata ad un forte impatto visivo, adeguata a coinvolgere razionalmente ed emotivamente il potenziale fruitore dei servizi e creare, con lo stesso, un forte feeling in grado di garantire una continuità efficace del

rapporto. Al tempo stesso, l'immagine utilizzata deve rispecchiare il carattere di istituzionalità dell'evento e l'autorevolezza del soggetto proponente. Per questo motivo si privilegeranno colori forti, che riprendono quelli istituzionali dell'Ateneo, resi più caldi, e dunque attenuati nel loro rigore, dalla presenza di alcuni "sprazzi" di colori più vivaci. Occorre comunque non discostarsi dalla linea stilistica dell'Ateneo, e da essa trarre autorevolezza e, conseguentemente, affidabilità. Dunque scelte cromatiche nel segno di una continuità moderata, impreziosita da immagini forti.

Caratteristiche della comunicazione del progetto saranno la chiarezza, la sintesi, la capillarità della diffusione ed il forte impatto.

Il "tono" della comunicazione sarà chiaro ed autorevole, ma al tempo stesso giovanile, con lo scopo di creare un forte grado di attenzione nei confronti dell'iniziativa.

Il linguaggio utilizzato sarà estremamente semplice, diretto, concreto, chiaro, convincente.

L'immagine punterà molto sulla valenza del Progetto nel complesso, sulla qualità ed autorevolezza della proposta grafico visiva, con una particolare valorizzazione di alcuni segni grafici rilevanti.

Essa vuole trasmettere l'idea di qualcosa di estremamente serio ed affidabile, ma, al tempo stesso semplice, poco complesso, finalizzato ad una crescita reale dei servizi a supporto degli studenti, e, più in genere, dell'organizzazione complessiva dell'Ateneo.

L'articolazione della campagna prevede una serie di azioni di comunicazione, integrate tra loro. Queste azioni saranno supportate da una massiccia campagna di informazione attuata chiedendo la fattiva collaborazione dei giornali e delle televisioni locali.

3. Le Linee d'intervento della Campagna di Comunicazione

Azioni e timing

E' bene però fare attenzione che buona parte dei soggetti che rientrano nel nostro pubblico target è costituito da un segmento della popolazione che, in relazione in particolare all'età, è in grado di "interpretare" a fondo, anche solo istintivamente, un sistema di comunicazione "promozionale". Ad essi non si giunge dunque attraverso forme e/o mezzi tradizionali, ma utilizzando quelli che meglio di ogni altro possono creare "contatti" diretti, snelli, veloci, efficaci.

Pertanto la pianificazione mezzi risulta strutturata in forma relativamente semplice.

La prima fase, definita «ad alto impatto», prevede l'utilizzo massiccio di mezzi di comunicazione "classici" e sarà orientata a creare un forte effetto emotivo sulla popolazione-target.

La seconda fase, definita «di mantenimento», prevede un utilizzo molto meno massiccio dei mezzi di comunicazione classici, limitandosi a sostenere l'effetto richiamo ed informativo. Esso potrà essere supportata da strumenti innovativi quali sms-remember dedicati ed e-mail mirate.

Le attività di promozione, diffusione e valorizzazione prevedono:

Seminario di presentazione del progetto, durante il quale verranno illustrati il programma delle attività, gli obiettivi perseguiti, i risultati attesi, le prospettive di sviluppo. Saranno invitati a partecipare i potenziali beneficiari diretti delle iniziative progettuali ed i soggetti con responsabilità programmatiche.

Realizzazione di info point, da posizionare nelle aree di maggior flusso delle differenti facoltà, dove sarà distribuito tutto il materiale informativo e, in alcune fasce orarie di particolare affluenza, verranno somministrati dei brevi questionari finalizzati a verificare da un lato (soprattutto in una prima fase) il livello di interesse da parte dei destinatari finali, dall'altro (in un momento successivo) il livello di conoscenza e la valutazione del servizio.

Produzione e distribuzione di materiale informativo, in particolare si prevede di realizzare una brochure informativa (15.000 copie), di un opuscolo (1.000 copie), da distribuire in fase di presentazione dell'iniziativa e successivamente, rilasciare sia presso degli Info point opportunamente istituiti che nei principali luoghi di ritrovo degli studenti (biblioteche, aree attrezzate, luoghi di ristoro, ecc). Strumento di comunicazione diretto e di diffusione veloce di informazioni, il pieghevole informativo consente al messaggio di raggiungere il target in tempi relativamente brevi.

Produzione e distribuzione di locandine, volantini ed altro materiale Promo-pubblicitario

Si prevede la realizzazione di locandine formato cm. 35x50 (circa 500), volantini bifacciali formato cm.15x20, flyers di sintesi formato cm. 10x15, da distribuire in tutti i punti di maggiore frequenza degli studenti e dei docenti.

Diffusione Spot Radio in Onda sulla Radio d'Ateneo

Mezzo altamente affine al target, veloce nella fruizione del messaggio, è un media determinante per ottimizzare il successo delle campagne di comunicazione. Garantisce continuità alla pianificazione a costi leggeri, permettendo una forte reiteratività del messaggio.

Diffusione delle informazioni attraverso i media; Verranno elaborate e diffuse note e comunicati stampa ai giornali locali, a quelli specializzati ed agli organi di informazione televisivi e radiofonici.

Diffusione di un rapporto finale contenente la descrizione dei risultati conseguiti, della strategia e delle modalità d'intervento che hanno permesso di raggiungerli e delle opportunità di sviluppo legate all'introduzione del sistema. Le copie del rapporto saranno rese disponibili on line.

Struttura finanziaria del progetto

--

Vedi figura: Piano Finanziario

Eventuali ulteriori informazioni

NOTA: Si noti che essendo il progetto di potenziamento e completamento di un progetto di Ateneo già in atto, la durata complessiva indicata nei dati sintetici del progetto è maggiore dei 12 mesi previsti dal bando per il completamento dal momento della stipula della convenzione, includendo tutte le attività del progetto non concluse alla data di pubblicazione dell'avviso sulla G.U. (come previsto nell'art. 1 del bando).

Essa assume dei tempi di approvazione e stipula della convenzione di circa 3 mesi dalla scadenza del bando, comportando quindi una durata complessiva del progetto di 18 mesi dalla pubblicazione del bando sulla G.U.

In particolare, il progetto è stato avviato il 10 Aprile 2008. Alla data di scadenza del bando sono pertanto stati eseguiti i primi 3 mesi e 10 giorni di attività. Le attività proseguiranno durante la fase di approvazione e stipula della convenzione, di cui si presume una durata di 2 mesi e 20 giorni. A questo punto saranno state svolte attività per 6 mesi. Il progetto proseguirà per ulteriori 12 mesi (così come previsto dal bando) fino alla data del 9/10/2009, raggiungendo così una durata complessiva di mesi 18. Si veda anche il diagramma di GANTT in allegato.

Figura A

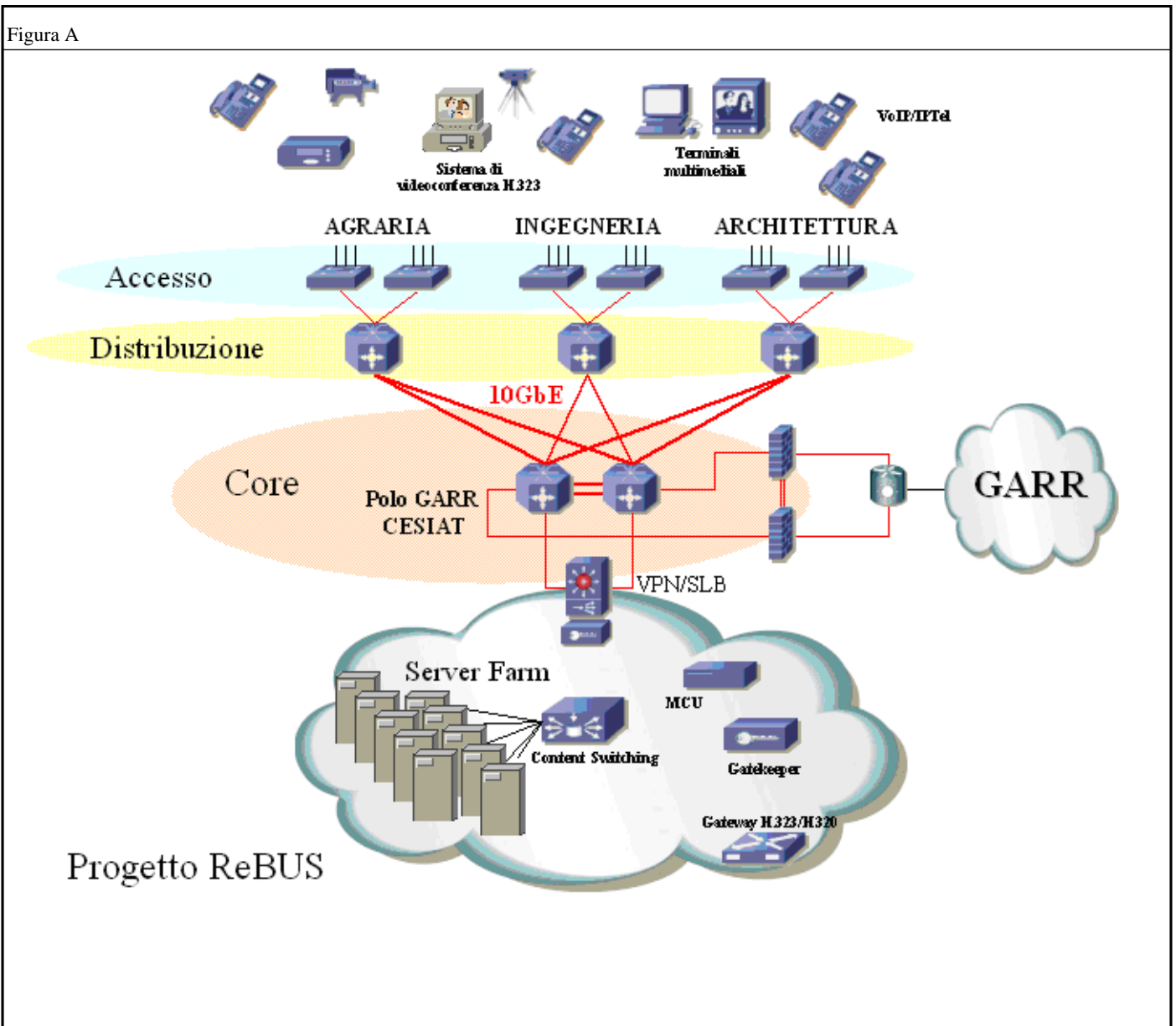


Figura B

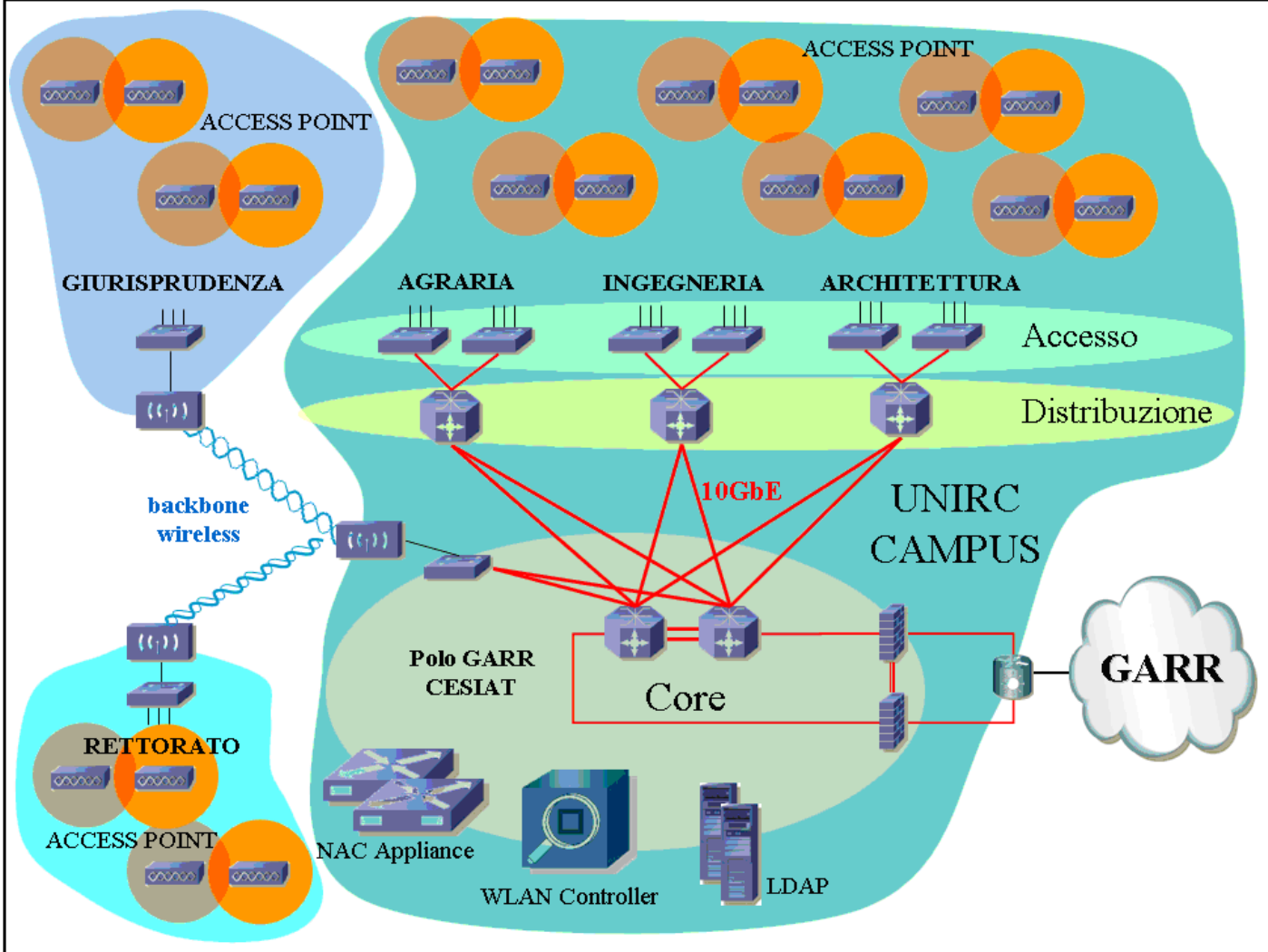


Figura C

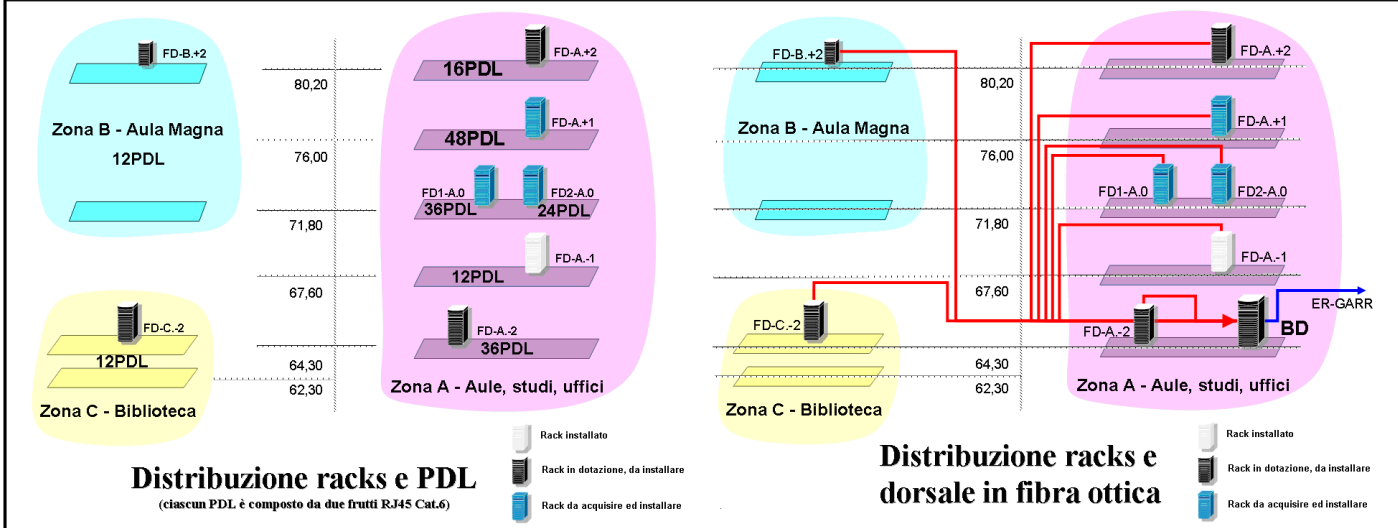


Figura D

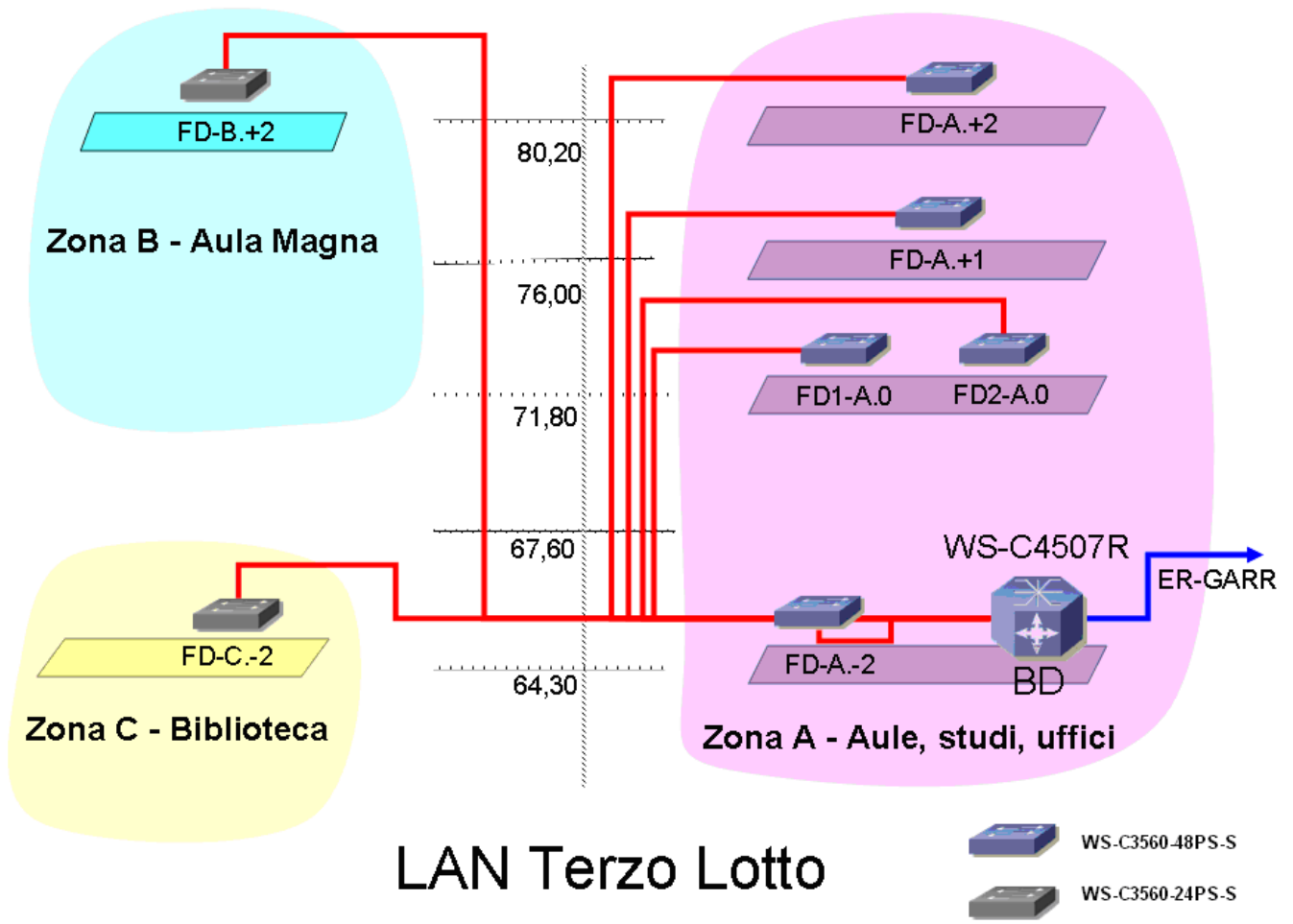


Figura E

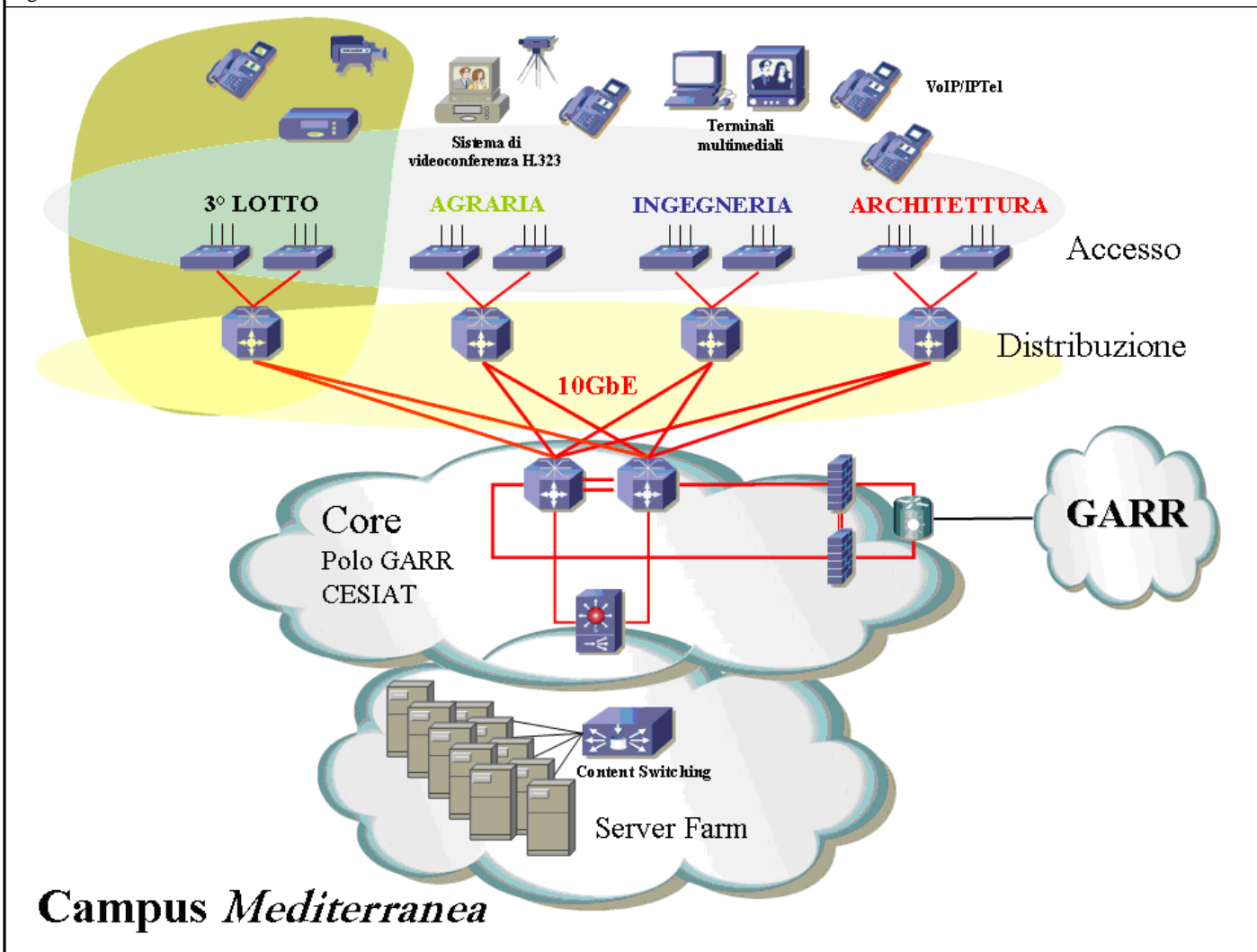


Figura F

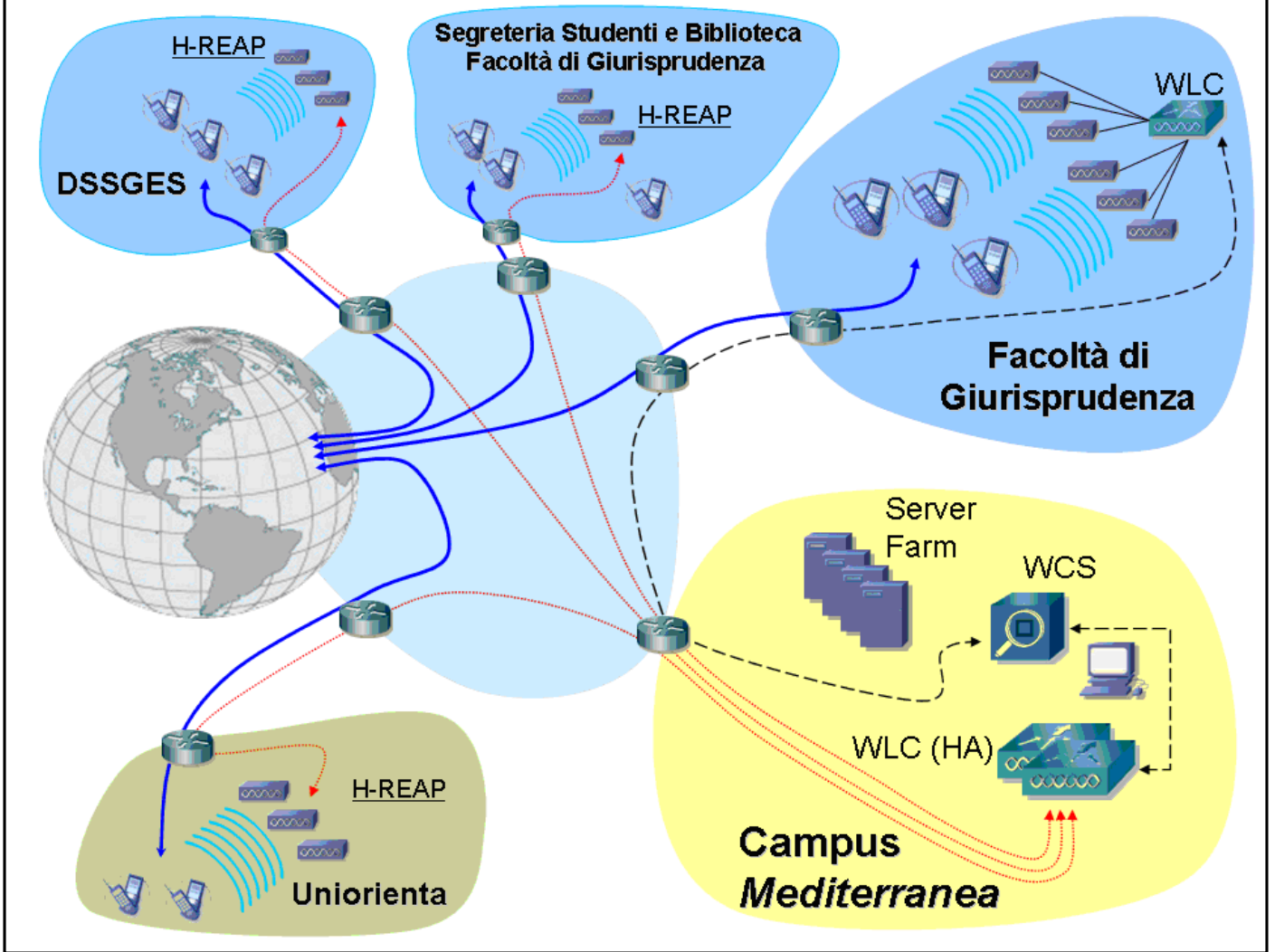
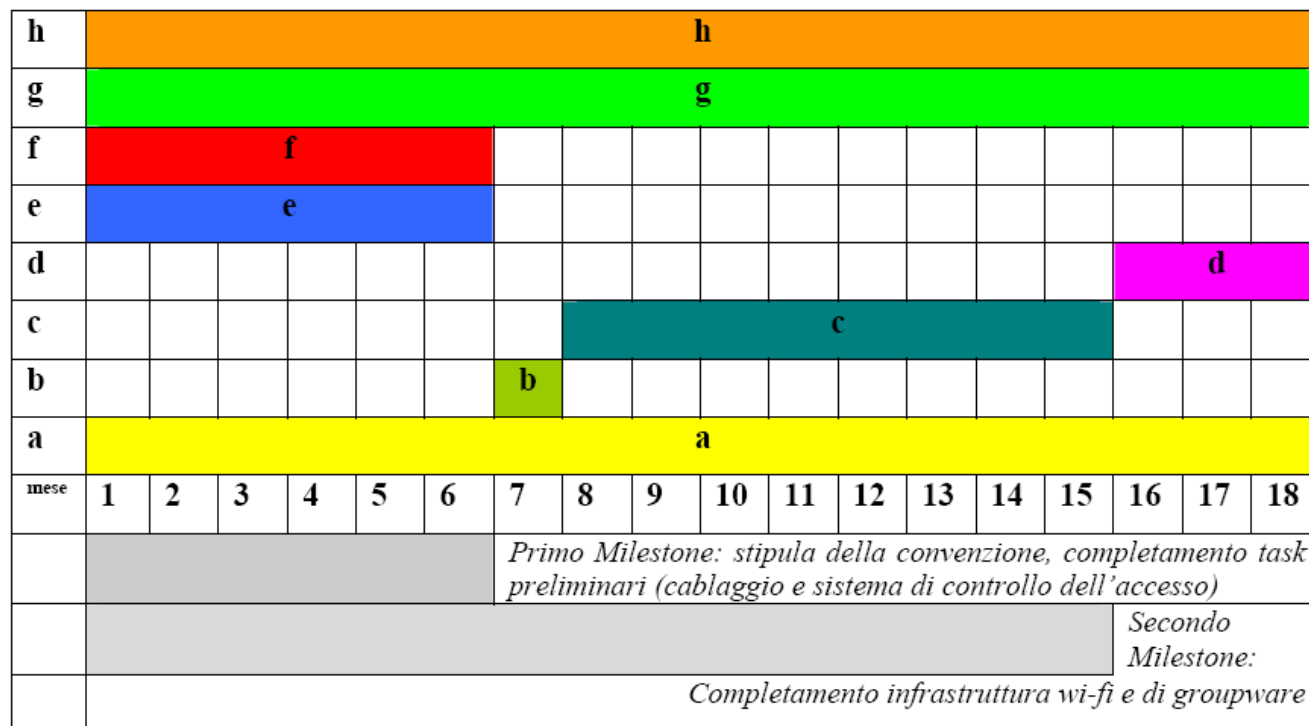


Diagramma di GANTT



Legenda

h	<i>Procedure Tecnico-Amministrative</i>
g	<i>Monitoraggio</i>
f	<i>Sistema NAC</i>
e	<i>Cablaggio lotto D</i>
d	<i>Monitoraggio e tuning</i>
c	<i>Realizzazione nuova infrastruttura</i>
b	<i>Individuazione delle aree wireless nelle sedi coinvolte dal progetto</i>
a	<i>Attività di comunicazione</i>

Ente finanziatore	Descrizione		Costi
Università Mediterranea di Reggio Calabria	Reti di connettività	20 Access Point, Piattaforma NAC, Corpo D (cablaggio strutturato, apparati, attrezzature networking d'interconnessione al backbone di Campus)	€ 287.076,00
	Servizi	server servizi applicativi studenti, costi indiretti sviluppo software integrazione/monitoring	€ 12.655,77
	Piano di Comunicazione agli Studenti	costi indiretti	€ 5.000,00
	Totale		€ 304.731,77
Dipartimento per l'Innovazione e le Tecnologie	Reti di connettività	140 Access Point, WLC in HA, upgrade WCS, switch d'accesso, server servizi di rete (RADIUS, DNS, DHCP, LDAP) in HA, attrezzature networking, server servizi applicativi studenti in HA	€ 222.880,00
	Servizi	Software Zimbra Collaboration Suite, servizi professionali (interni e/o esterni all'Ateneo) necessari ad assicurare, sull'intera infrastruttura wireless, la piena fruibilità dei servizi minimi (iscrizione online e verbalizzazione elettronica degli esami), acquisti di licenze software, servizi professionali (interni e/o esterni all'Ateneo) di progettazione, consulenza, implementazione dei servizi di rete e dei nuovi servizi dedicati agli studenti, servizi di sviluppo esterno, risorse interne, etc. e di gestione	€ 58.000,00
	Piano di Comunicazione agli Studenti		€ 7.000,00
	Totale		€ 287.880,00
Totale Complessivo			€ 592.611,77