0912386 7 RST 3 EFG 8 TUV 3 EFG

www.unipa.it

Infrastruttura di rete della Università degli studi di Palermo

Dott. Massimo Tartamella

Centro Universitario di Calcolo

La realtà informatica universitaria

- **Il sistema di rete universitario (costituito da 100 collegamenti) collega circa 5500 risorse tra cui:**
  - 200 server Linux con funzioni di: web, mail, proxy, dns, dhcp, nfs, ftp, log, mrtg, file & printer, backup, tftp, vpn, firewall, natting, ids, controllo vulnerabilità, antivirus, ldap, radius, ntp, Oracle 8.1.7 e 10g DB & AS
  - 300 apparecchiature di rete: switch, router, access point
  - 4500 stazioni di lavoro: Personal Computer con Windows, workstation con sistemi operativi Unix oriented, etc.
  - 6.496 utenti su @unipa.it e 30.185 utenti su @studenti.unipa.it a marzo 2008 (gli studenti che frequentano sono complessivamente circa 50.000)

Connessioni in rete .. segue

- Il CUC è collegato alla rete Internet a 155 Mbps in tecnologia ATM (tramite nodo GARR in fibra ottica nello stesso edificio)
- 42 connessioni a 1000 Mbps in fibra ottica:
  - 1 CUC - Steri
  - 1 CUC - San Antonino
  - 20 CUC – Edifici in Parco d'Orleans
  - 20 Infosys – Edifici in AOUP (Facoltà di Medicina)
- 10 connessioni 100 Mbps in fibra ottica:
  - DPDS/Giurisprudenza, Geodesia/Fisiologia, Steri/Scia e 8 in via Archirafi (Dip. Di Matematica – ed. di via Archirafi)

Connessioni in rete .. segue

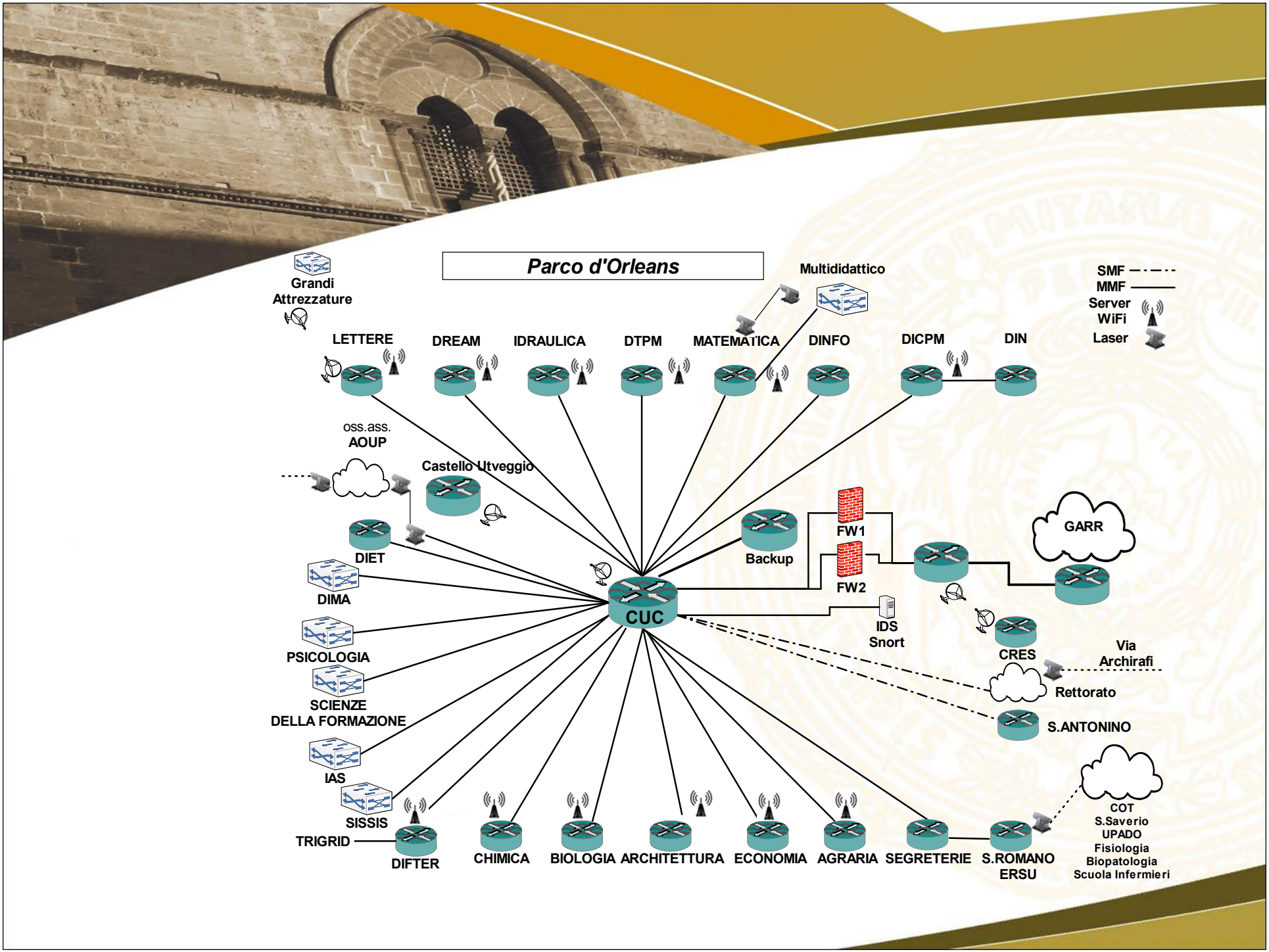
- 12 connessioni attraverso ponti ottici a 100 Mbps:
  - DIET – Oss. Astr. – AOUP – Steri - Archirafi
  - Santi Romano – San Saverio – Giurisprudenza
  - Santi Romano – COT via Veneziano
  - Santi Romano – Patologia – Scuola Infermieri
- 2 connessioni attraverso ponti ottici a 10 Mbps:
  - Santi Romano – Upado, “San Saverio”/Geologia-Fisiologia
- 16 connessioni a 54 Mbps via radio:
  - Steri/”Città e Terr.-Storia e Progetto Arch.”, “Ex-Scia”/Geografia, Matematica/”Presidenza Farmacia”, Matematica/Biblioteca, Giurisprudenza/”Scienze politiche”, Steri/Giurisprudenza, “Santi Romano”/”Via Toti”, Dermatologia/”Via Bergamo”, Dermatologia/”Nutrizione Umana”, CUC/Utveggio/IMI/Laloggia/Cervello, CUC/”Grandi Attrezzature”, “San Saverio”/Edison, “San Saverio”/Divisi
- 2 connessioni a 11 Mbps via radio:
  - Giurisprudenza/Architettura, Steri/SESOF)

Connessioni in rete

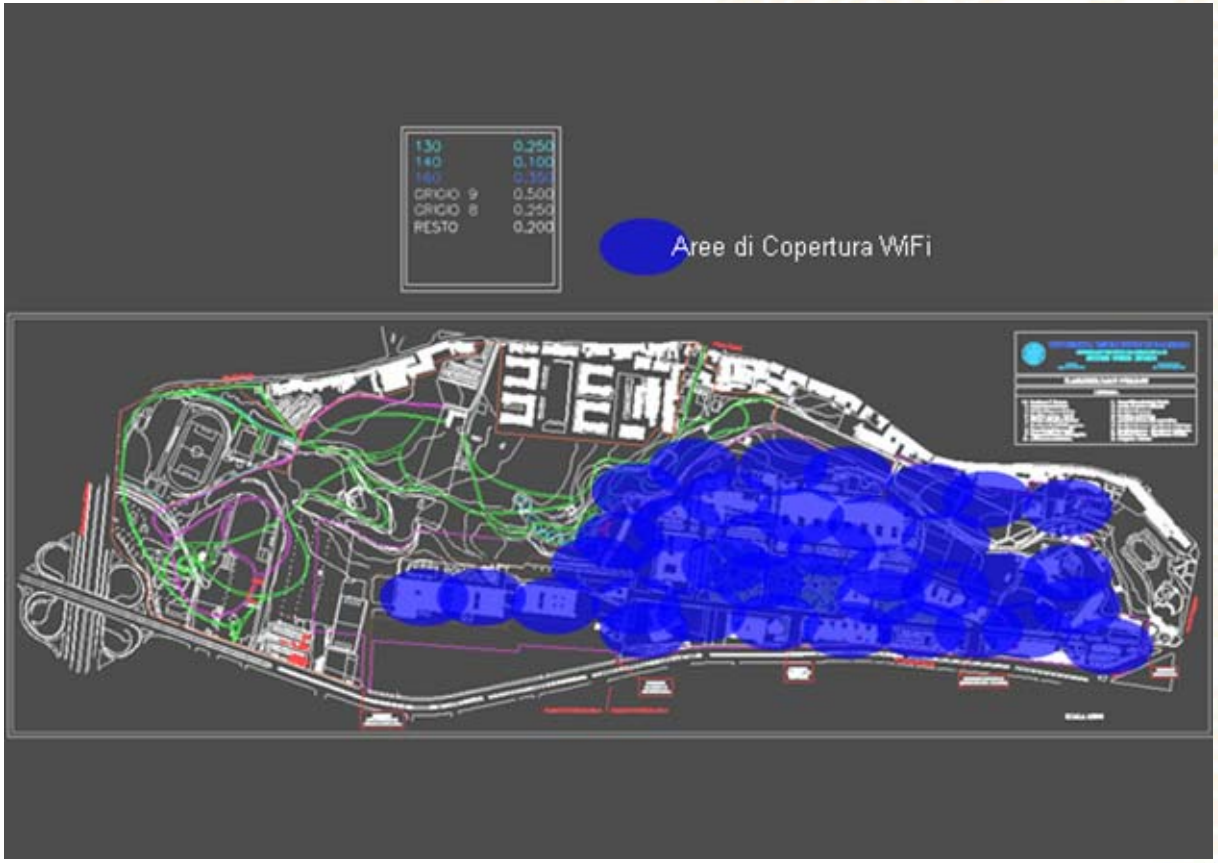
- HDSL Wind: 4 link, tra cui Polo-TP e CUPA-AG
- HDSL Telecom: 2 Link, Marsala-TP e Villa Genualdi-AG
- ADSL Telecom: 5 link
- ADSL FastWeb: 2 link
- CDN Telecom: 3 link (verranno a breve dismessi)
- Accessi analogici/ISDN: 30
- Possibilità di collegamento in VPN da ADSL/HDSL/UMTS/GPRS/EDGE/… (circa 100 utenze differenti giornaliere)

Progetti di calcolo distribuito

- TRIGRID, presso il DIFTER (Dipartimento di Fisica e Tecnologie Relative), parco d'Orleans, già operativo
- COMETA, presso il dipartimento di Fisica, via Archirafi
- Geogrid, presso il CUC
- Progetti vari presso il DINFO (Dipartimento di ingegneria INFOrmatica), parco d'Orleans


Parco d'Orleans
Grandi Attrezzature
Multididattico
SMF
MMF
Server
WiFi
Laser
LETTERE
DREAM
IDRAULICA
DTPM
MATEMATICA
DINFO
DICPM
DIN
oss.ass. AOUP
Castello Utveggio
DIET
DIMA
PSICOLOGIA
SCIENZE DELLA FORMAZIONE
IAS
SISSIS
TRIGRID
DIFTER
CHIMICA
BIOLOGIA
ARCHITETTURA
ECONOMIA
AGRARIA
SEGRETERIE
S.ROMANO
ERSU
COT
S.Saverio
UPADO
Fisiologia
Biopatologia
Scuola Infermieri
CUC
Backup
FW1
FW2
IDS Snort
GARR
CRES
Via Archirafi
Rettorato
S.ANTONINO

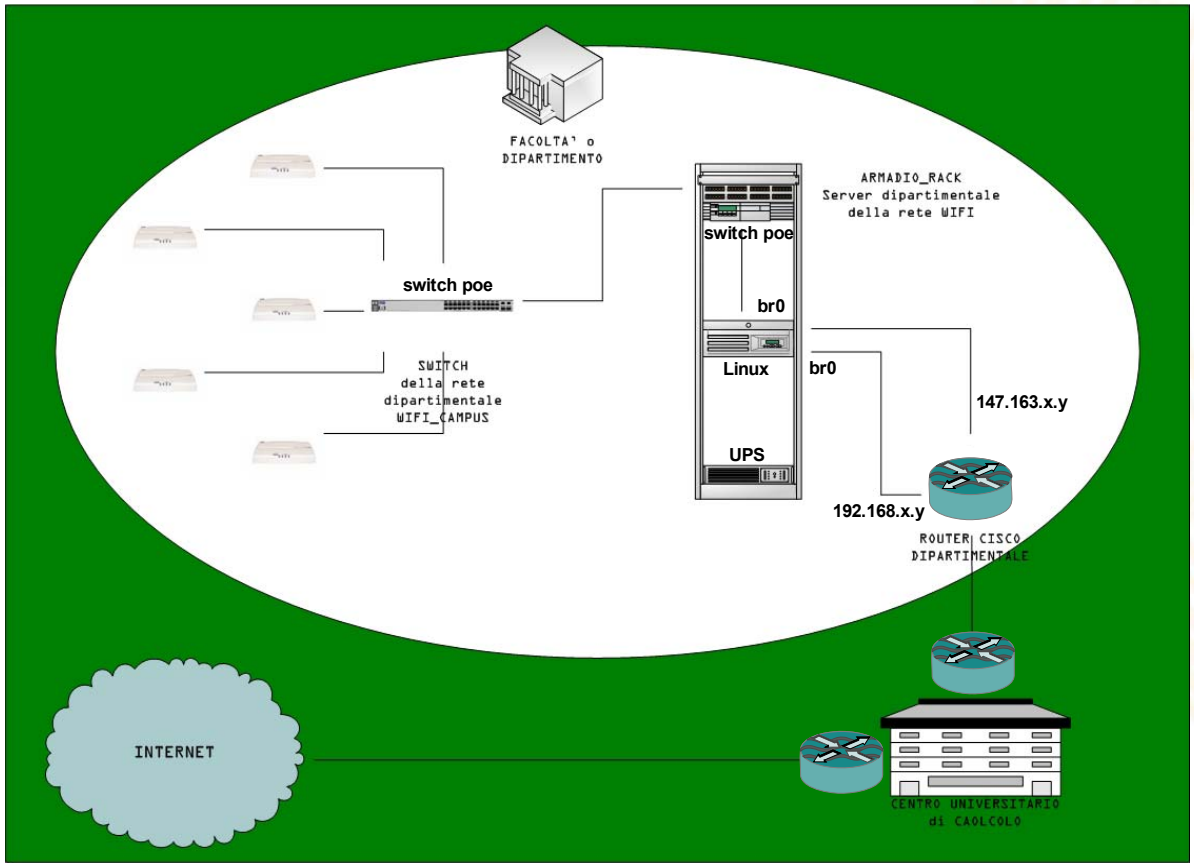
Rete wireless di Parco d'Orleans

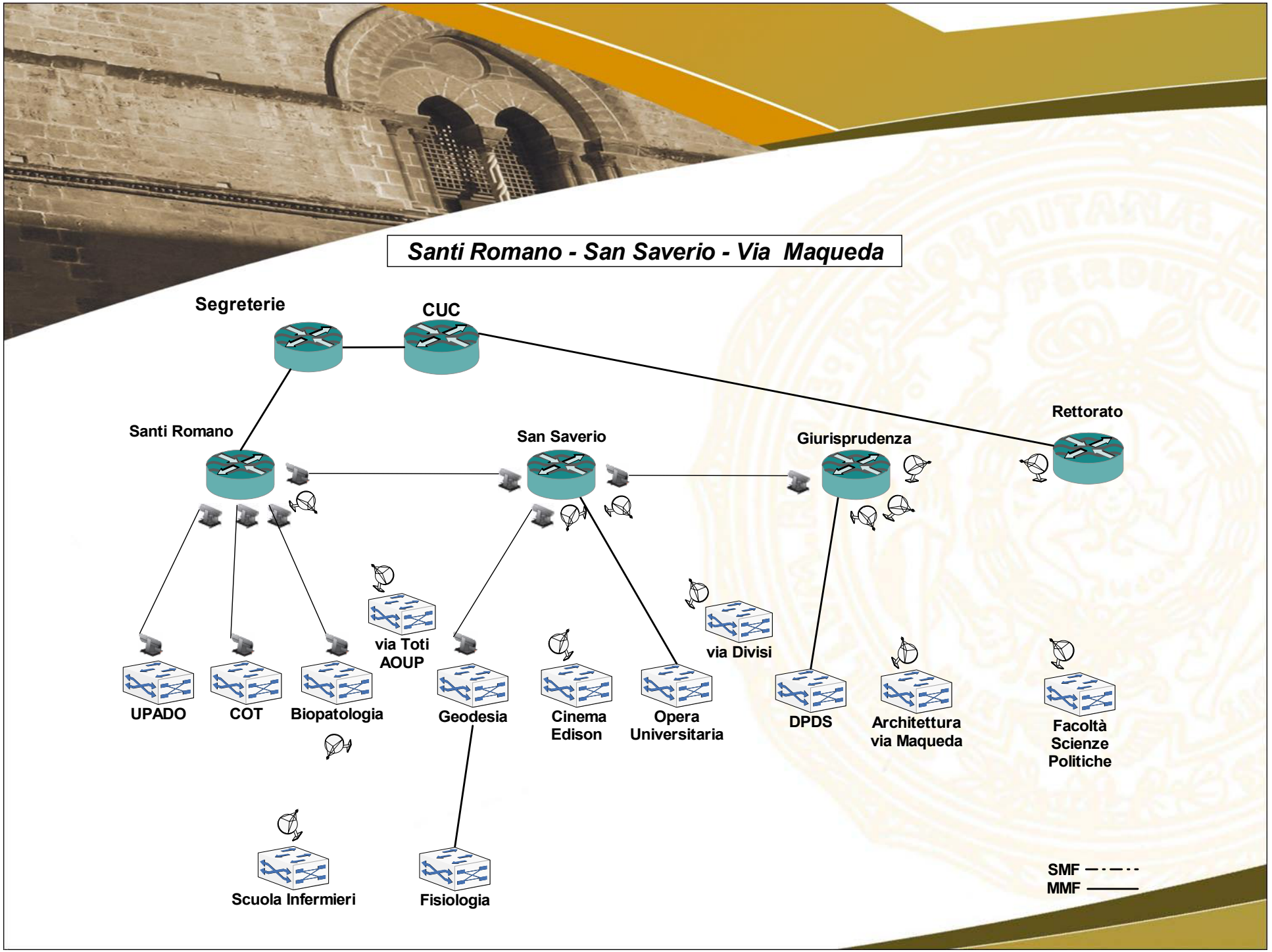


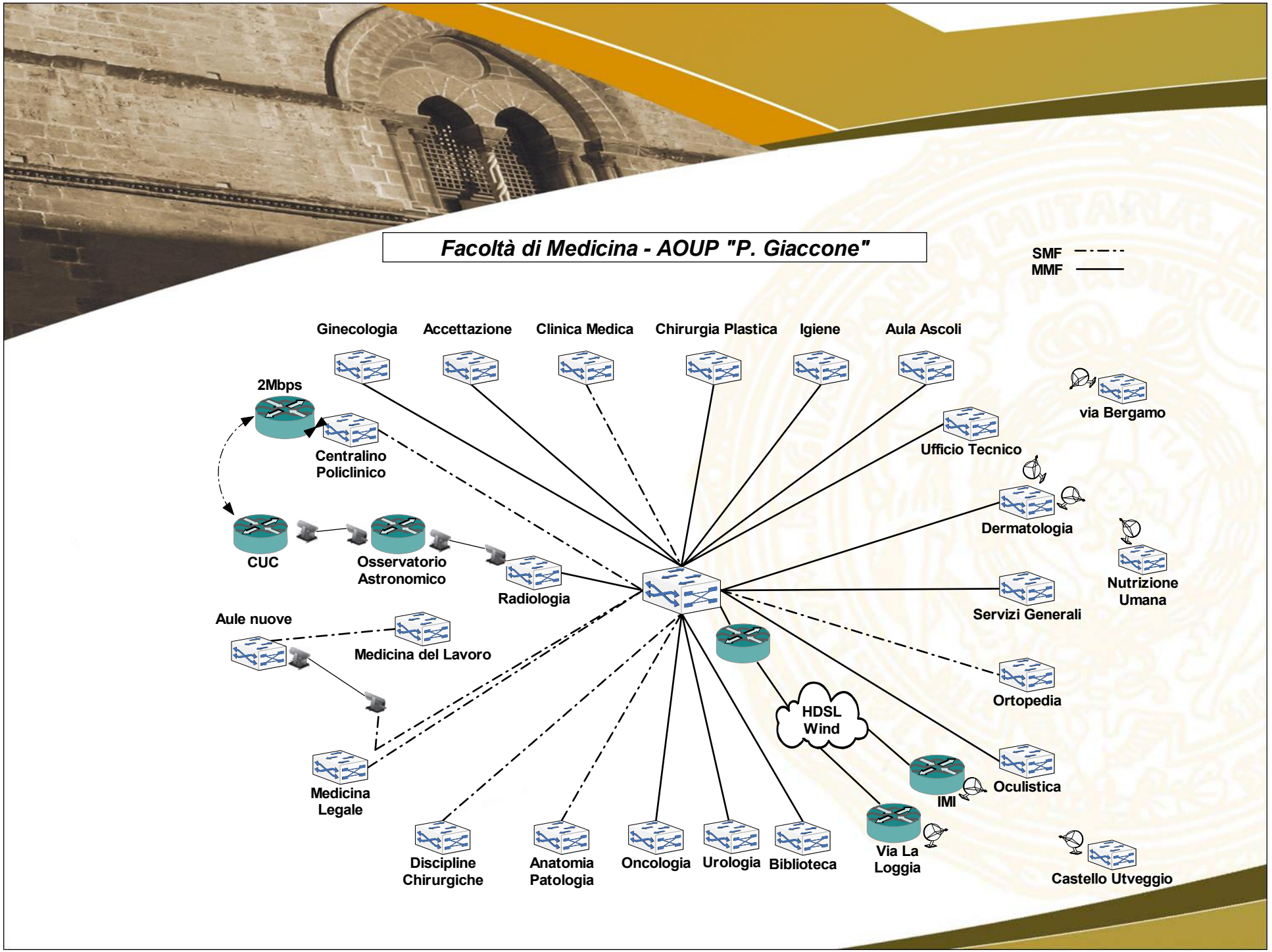
Rete wireless di Parco d'Orleans

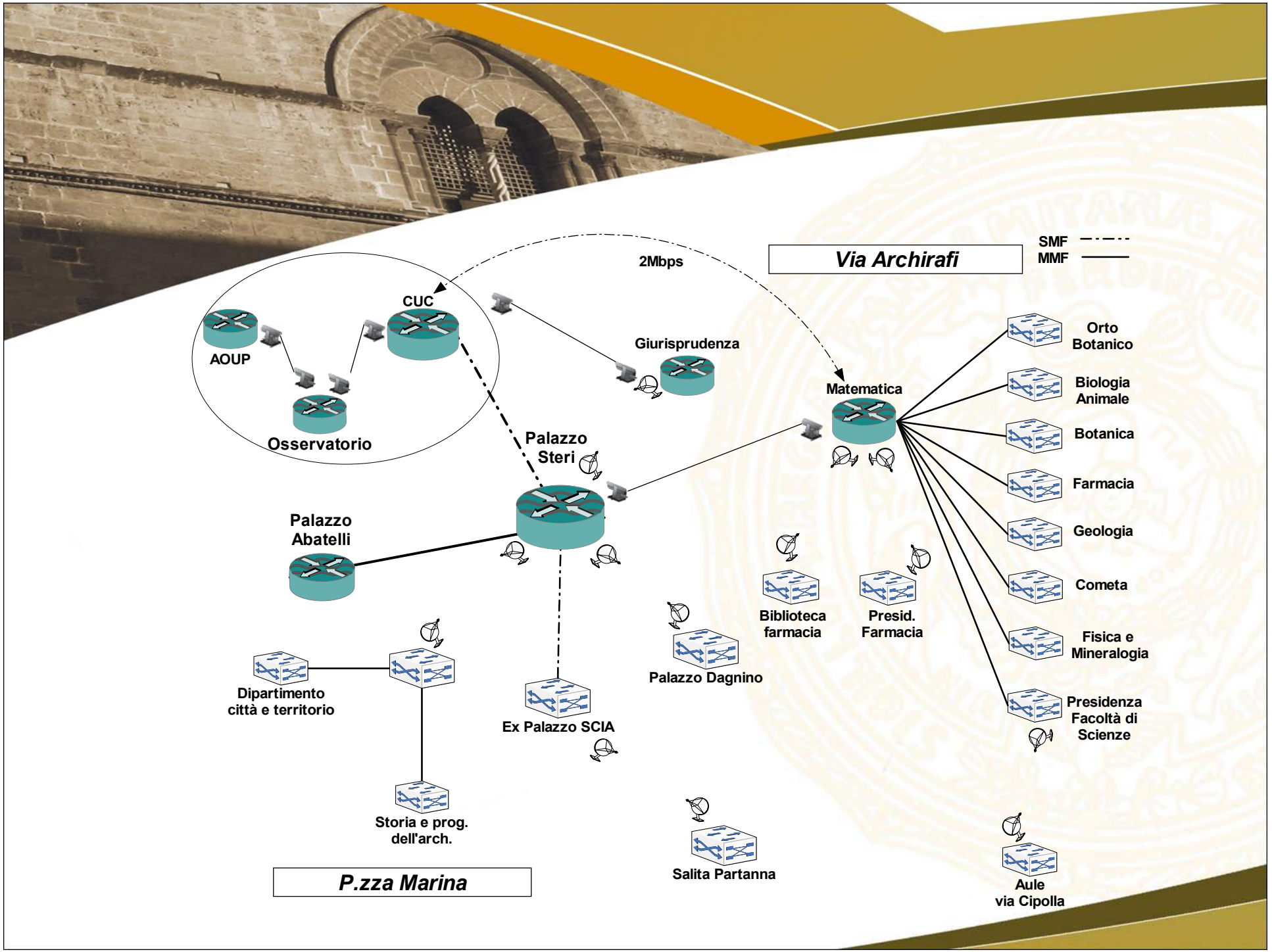
- 18 server Linux
- 29 switch HP e 13 switch Cisco
- Oltre Access Point
- Consente l'accesso contemporaneo di oltre 1022 utenti (personale universitario, studenti e ospiti); quotidianamente è utilizzata da oltre 400 utenze diverse
- Tutti i sistemi sono collegati in VLAN con indirizzamento privato (rete 192.168.4.0/22)

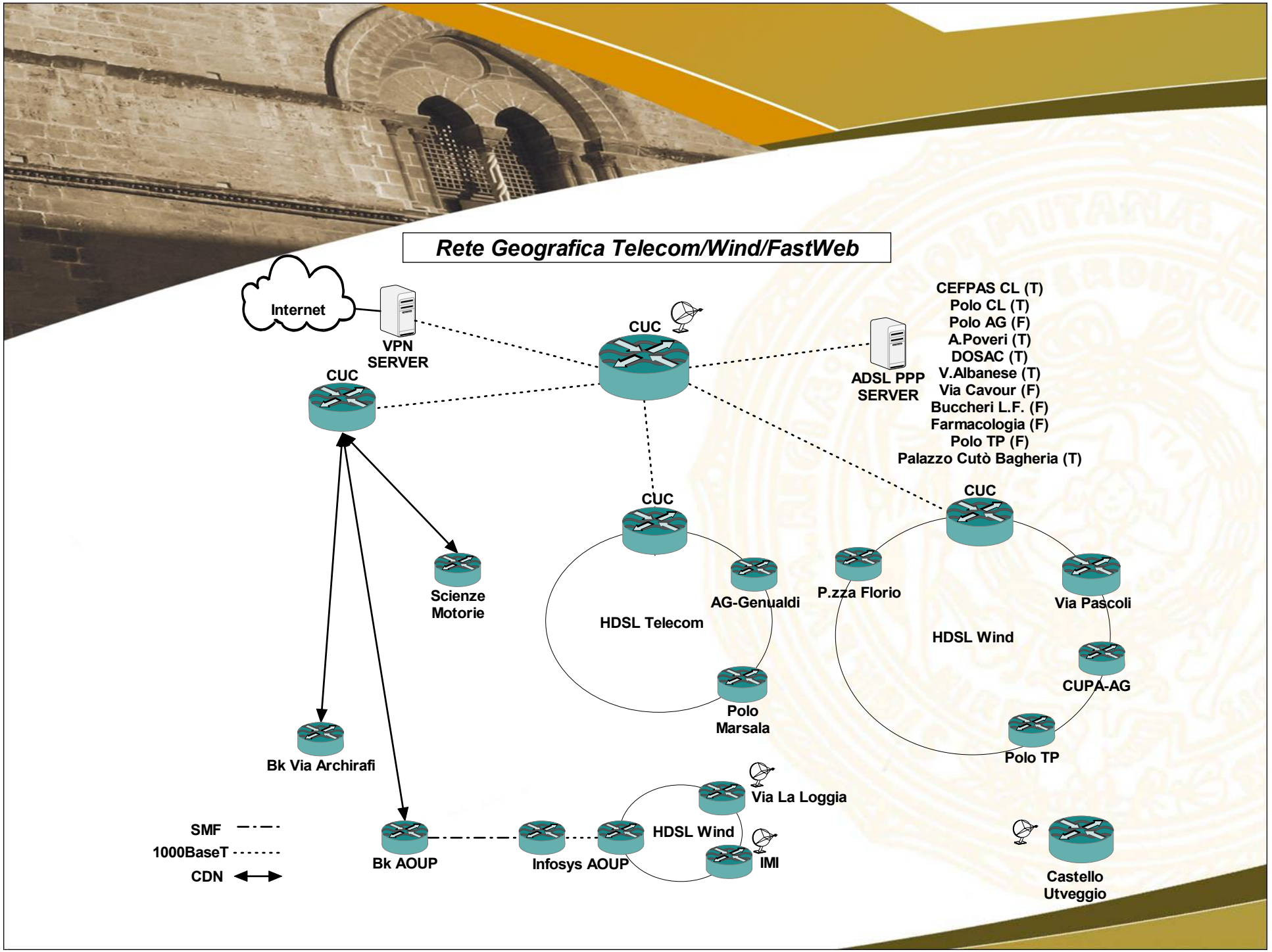
Rete wireless all'interno del singolo edificio




Santi Romano - San Saverio - Via Maqueda
Segreterie
CUC
Rettorato
Santi Romano
San Saverio
Giurisprudenza
via Toti
AOUP
via Divisi
UPADO
COT
Biopatologia
Geodesia
Cinema
Edison
Opera
Universitaria
DPDS
Architettura
via Maqueda
Facoltà
Scienze
Politiche
Scuola Infermieri
Fisiologia
SMF
MMF


Facoltà di Medicina - AOUP "P. Giaccone"
SMF
MMF
Ginecologia
Accettazione
Clinica Medica
Chirurgia Plastica
Igiene
Aula Ascoli
2Mbps
Centralino Policlinico
via Bergamo
Ufficio Tecnico
Dermatologia
Nutrizione Umana
CUC
Osservatorio Astronomico
Radiologia
Servizi Generali
Aule nuove
Medicina del Lavoro
Ortopedia
HDSL Wind
Oculistica
IMI
Medicina Legale
Via La Loggia
Discipline Chirurgiche
Anatomia Patologia
Oncologia
Urologia
Biblioteca
Castello Utveggio


SMF
MMF
2Mbps
Via Archirafi
CUC
AOUP
Osservatorio
Giurisprudenza
Matematica
Orto Botanico
Biologia Animale
Botanica
Farmacia
Geologia
Cometa
Fisica e Mineralogia
Presidenza Facoltà di Scienze
Palazzo Steri
Palazzo Abatelli
Biblioteca farmacia
Presid. Farmacia
Palazzo Dagnino
Dipartimento città e territorio
Ex Palazzo SCIA
Storia e prog. dell'arch.
Salita Partanna
Aule via Cipolla
P.zza Marina


Rete Geografica Telecom/Wind/FastWeb
Internet
VPN SERVER
CUC
CUC
ADSL PPP SERVER
CEFPAS CL (T)
Polo CL (T)
Polo AG (F)
A.Poveri (T)
DOSAC (T)
V.Albanese (T)
Via Cavour (F)
Buccheri L.F. (F)
Farmacologia (F)
Polo TP (F)
Palazzo Cutò Bagheria (T)
CUC
CUC
Scienze Motorie
HDSL Telecom
AG-Genualdi
Polo Marsala
P.zza Florio
Via Pascoli
HDSL Wind
CUPA-AG
Polo TP
Bk Via Archirafi
Via La Loggia
HDSL Wind
IMI
Bk AOUP
Infosys AOUP
Castello Utveggio
SMF
1000BaseT
CDN

Sicurezza

- La sicurezza è demandata ad un doppio firewall (Linux in bridge con iptables) interposto tra il router cisco collegato direttamente a quello del GARR e il centro stella universitario
- Il controllo del traffico viene effettuato tramite server Linux con SNORT che riceve il mirroring del traffico complessivo prima e dopo il firewall

L'Università degli Studi di Palermo va in "onda"

UNIPA Wireless Campus

- **01 IDEA PROGETTUALE**
- **02 FORNITURA**
- **03 IMPLEMENTAZIONE DEL SISTEMA**

01 – Cronologia

L'Università di Palermo presenta al MIUR una proposta di finanziamento per la realizzazione di una rete wireless nel campus di Parco d'Orleans

La proposta di finanziamento denominata "UNIPA Wireless Campus" viene finanziata dal MIUR sull'avviso 901 del PON per 635.234,00 €

Il Prof. Mario Enea, responsabile del procedimento, coinvolge il Centro Universitario di Calcolo per l'ideazione della soluzione progettuale.

Il 7/3/2006 viene bandito il capitolato speciale di appalto a cura del settore PROvveditorato D'Ateneo

Nel luglio 2006 viene aggiudicata la gara d'appalto alla RTI costituita da EDA, FinSol e OrCom per 590.068,86€

01 – Obiettivi

Realizzazione di una rete wireless, nell'area di Parco d'Orleans, per l'accesso ai servizi di rete da parte di studenti, personale universitario e "ospiti"

Realizzazione di un sistema di Identity Management centralizzato per studenti, docenti, personale universitario

Accesso ai servizi di rete globali (Internet) e locali (Intranet universitaria e dipartimentale)

Adesione agli standard IEEE 802.11 a/b/g/ per la trasmissione dati e WPA e WPA2 (IEEE 802.11i) per la sicurezza

01 – Idea progettuale

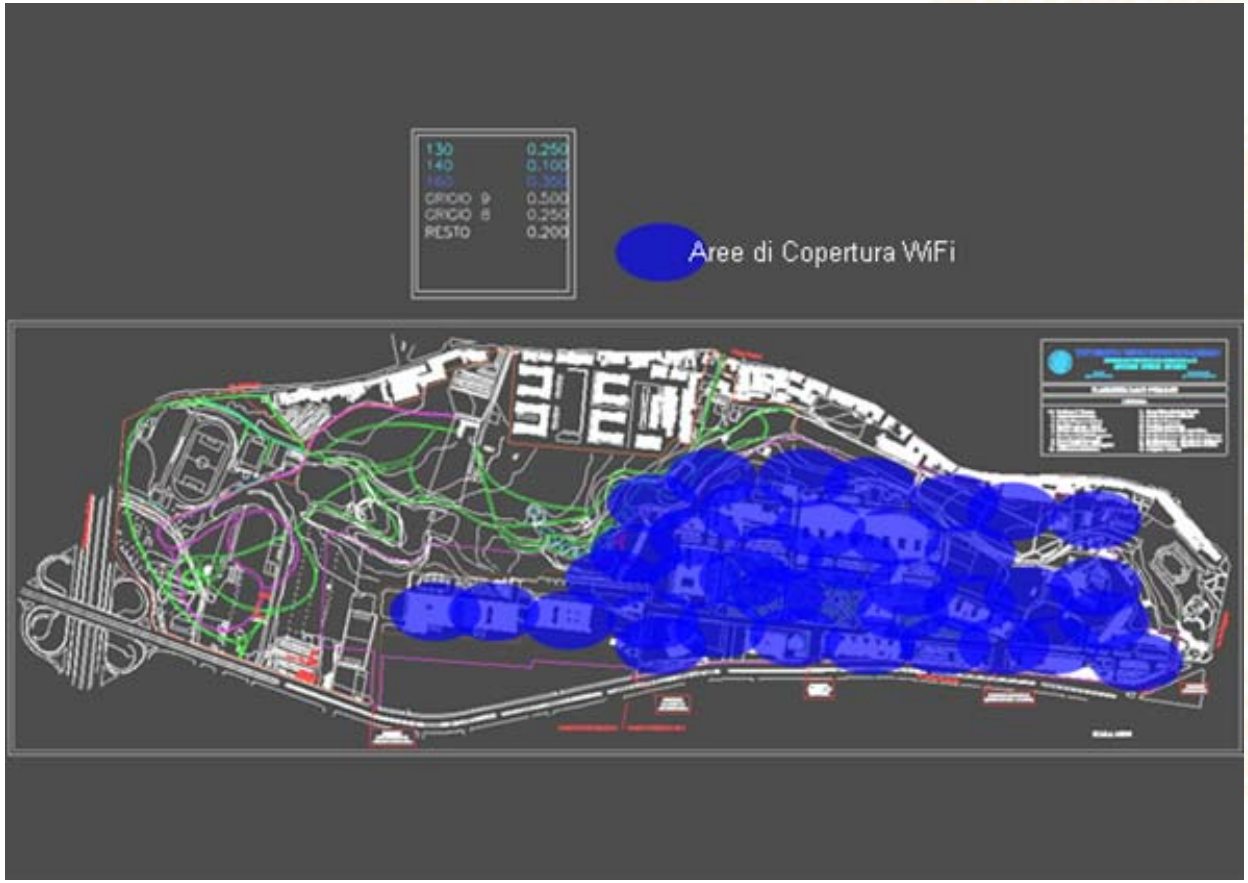
Utilizzo di server Linux multihomed nei vari plessi di Parco d'Orleans per la raccolta del traffico wireless e per la implementazione delle policy di sicurezza

Realizzazione di un cablaggio separato da quello preesistente per la connessione dei vari Access Point

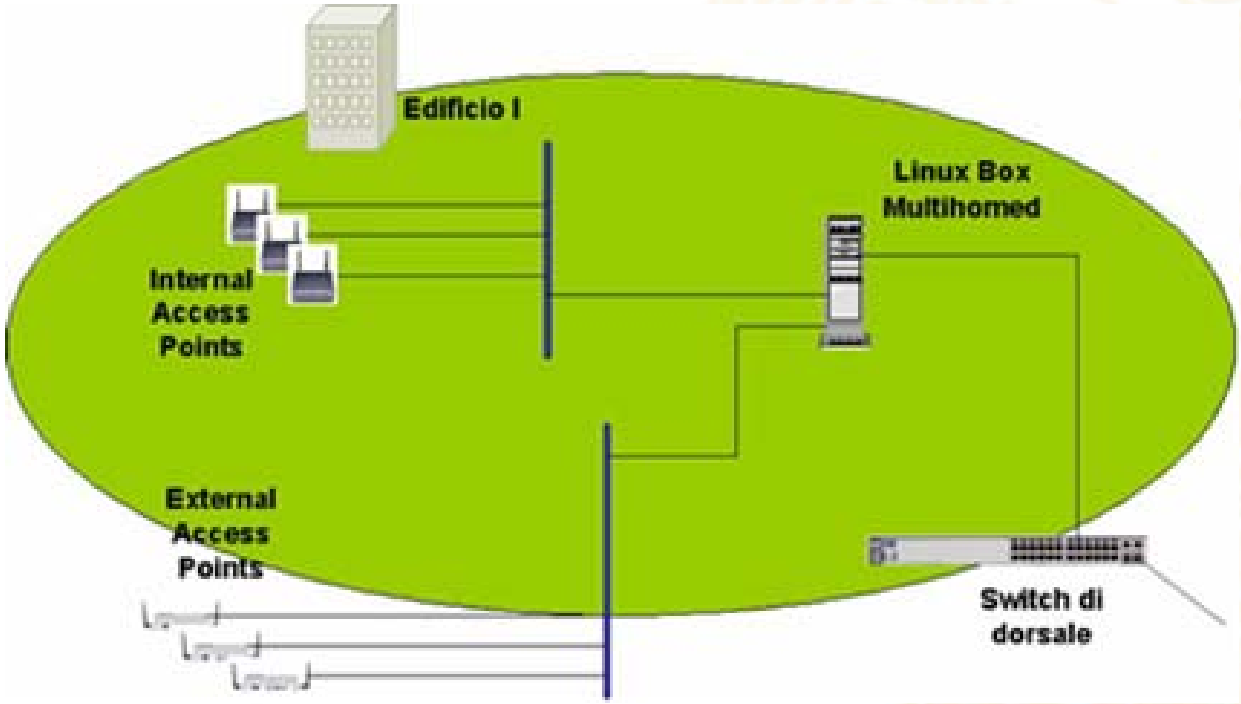
Server centralizzati presso il Centro Universitario di Calcolo per i servizi di identity management, proxy, DHCP server, log server e network management

Roaming nell'area del parco d'Orleans

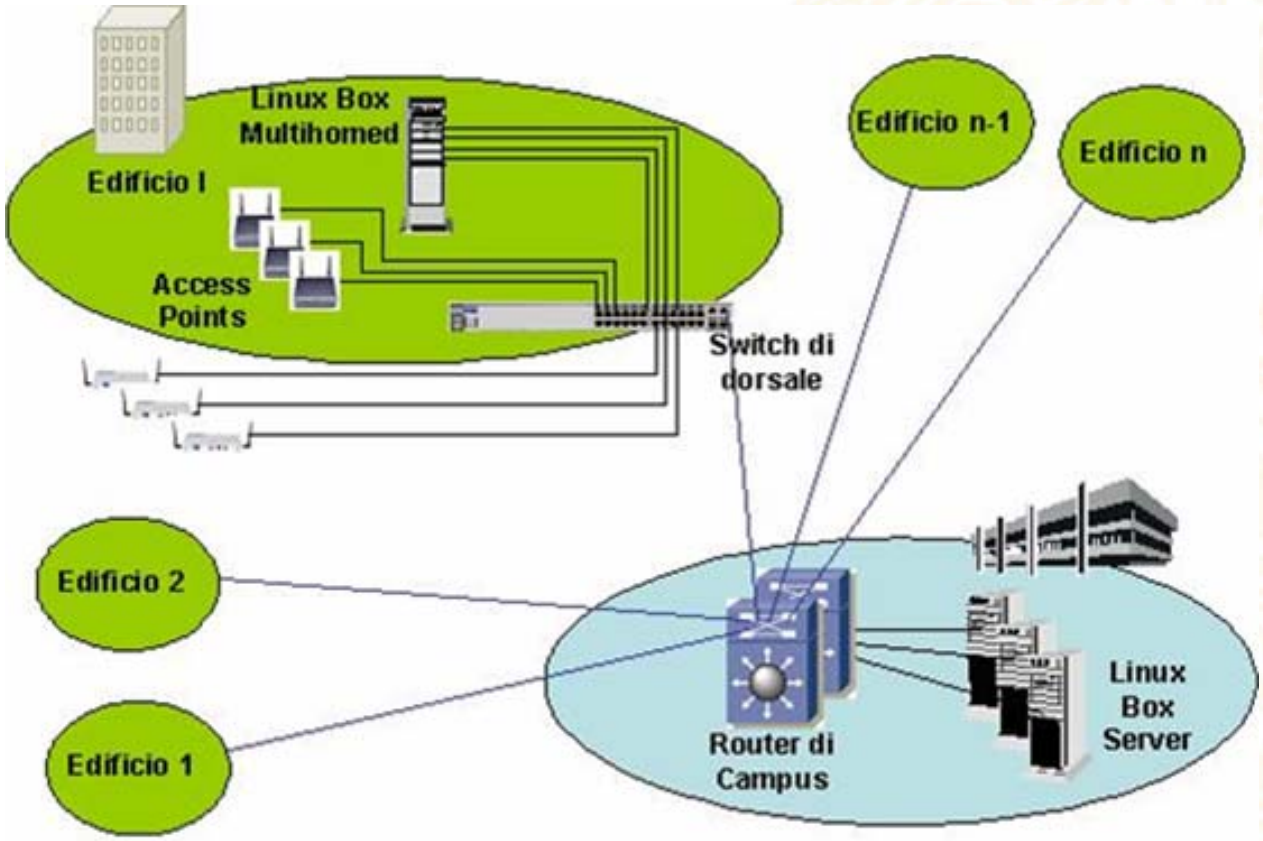
01 – Copertura Wi-Fi nel P.d'O.



01 – Edificio I-esimo



01 – Connessione al CUC



01 – Credenziali per l'utilizzo della rete

- server LDAP (OpenLDAP) ridondato: dedicato agli studenti; tramite portale *studenti.unipa.it*, lo studente inserisce i propri dati, convalidati da GEDAS, e crea le proprie credenziali per l'accesso ai servizi di rete universitari, per esempio username *stud_x@studenti.unipa.it e* relativa *password;*

- server LDAP (OpenLDAP) ridondato: dedicato al personale docente e tecnico/amministrativo; è necessario avere/richiedere un account di posta elettronica, per es. *docen_y@unipa.it e* relativa *password* ;

- server RADIUS (FreeRadius) distribuiti: per la registrazione degli accessi e per l'accesso via proxy radius alle credenziali disponibili e nei domini universitari registrati come *utentex@dicpm.unipa.it, utentey@economia.unipa.it*, etc.

- server PPTP (PopTop) distribuiti: per l'accesso alle risorse dipartimentali (stampanti, mail relay, etc.)

UNIPA Wireless Campus

- 01 IDEA PROGETTUALE
- 02 FORNITURA
- 03 IMPLEMENTAZIONE DEL SISTEMA

02 – PROPOSTA

RTI aggiudicataria: Enterprise Digital Architects (EDA), Fin.Sol. e Or.Com

EDA: con compiti di installazione e testing infrastruttura wireless

Fin.Sol: con compiti di fornitura hardware (AP, switch e gruppi di continuità)

Or.Com.: con compiti di supporto sistemistico, cablaggio strutturato e di education

02 – Precisamente EDA …

Enterprise Digital Architects ha fornito apparecchiature e precisamente si è occupato di:

- Fornire gli apparati di rete (switch hp, access point hp e antenne varie per la rete wireless e router Cisco 6500 di backup in fault-tolerant al centro stella di campus)

Installare il router Cisco 6500 con funzioni di backup all'attuale centro stella di campus dotato di 50 porte RJ45 10/100/1000 Mbps e 32 porte in fibra a 1000 Mbps

Installare la piattaforma per il management (windows 2003 + HP Procurve Management + hw di base)

02 – Precisamente Fin.Sol. ....

Fin.Sol ha fornito apparecchiature e precisamente:

3 Linux Box Server installate presso il Centro Universitario di Calcolo

15 Linux Box Multihomed

15 armadi rack da 24 unità

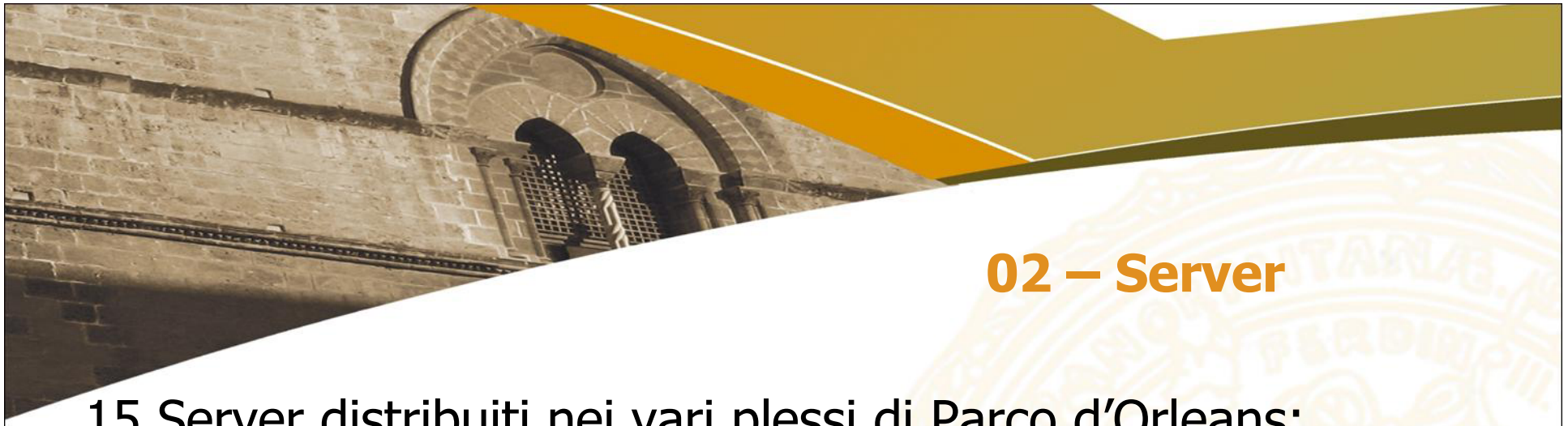
15 gruppi di continuità

6 portatili (HP TC4400 Tablet) e 6 telefoni palmari (3 Nokia 9500 e 3 JasJar)

02 – Precisamente Or.Com. …

Or.Com. ha realizzato cablaggi e fornito servizi e precisamente si occupato di:

- Erogare i corsi di formazione per il personale universitario coinvolto nel progetto (27 gg.) con certificazione Red Hat per 6 unità
- Costituire, per due anni, il presidio on site con due unità di personale dipendente
- Realizzare il cablaggio necessario in tutti gli edifici coinvolti
  Offrire supporto sistemistico
  Fornire un software aggiuntivo commerciale per l'identity management (non richiesto in gara) e precisamente il SUN Java System Access Manager



02 – Server

15 Server distribuiti nei vari plessi di Parco d'Orleans:

Marca : HP (Hewlett Packard)
Modello : Proliant DL 380 G4 da rack
CPU: 2 Intel Xeon 3.6 Ghz – 2MB L2
RAM: 2GB
Schede Ethernet: 4 10/100/1000 Mbps
S.O.: CentOS 4.4

3 Server centralizzati presso il centro Universitario di Calcolo:

Marca : HP (Hewlett Packard)
Modello : Proliant DL 370 G4 tower
CPU: 2 Intel Xeon 3.6 Ghz – 2MB L2
RAM: 4GB
Schede Ethernet: 2 10/100/1000 Mbps
S.O.: CentOS 4.4

02 – Switch e Access Point

178 Access Point:
Marca : HP
Modello : Procurve 530
Radio: supporto simultaneo di IEEE 802.11a e 802.11b/g
Caratteristiche:
Supporto IEEE 802.1h
Supporto IEEE 802.11i
possibile alimentazione tramite PoE
- supporto WMM (Wireless MultiMedia) per la gestione del QOS
- rilevamenti di access point non autorizzati e di rete wireless ad hoc
- doppia antenna diversity per una robusta copertura radio
- selezione automatica del canale (ACS) per ridurre l'interferenza

39 switch a 24 porte
Marca : HP
Modello : Procurve 2626-PWR
Caratteristiche:
- crittografia SSHv2 e SSL per una gestione sicura
- supporto e tagging VLAN (802.1Q e 253 VLAN)
- protocollo di convergenza rapida dello spanning tree 802.1w
- gestione della priorità a livello 4 basata sul port number TCP/IP
- classificazione delle priorità di traffico (802.1p)

13 canali IEEE 802.11b/g disponibili sull'access point

- C01 a 2,412 MHz, C02 a 2,417 MHz, C03 a 2,422 MHz, C04 a 2,427MHz, C05 a 2,432MHz
- C06 a 2,437MHz, C07 a 2,442MHz, C08 a 2,447MHz, C09 a 2,452MHz, C10 a 2,457 MHz,
- C11 a 2,462MHz, 12 a 2,467MHz e 13 a 2,472MHz

19 canali IEEE 802.11a disponibili sull'access point

- **8 canali tra 5,180 e 5,320 GHz**

- Canale 36 a 5,180 GHz
- Canale 40 a 5,200 GHz
- Canale 44 a 5,220 GHz
- Canale 48 a 5,240 GHz
- Canale 52 a 5,260 GHz
- Canale 56 a 5,280 GHz
- Canale 60 a 5,300 GHz
- Canale 64 a 5,320 GHz

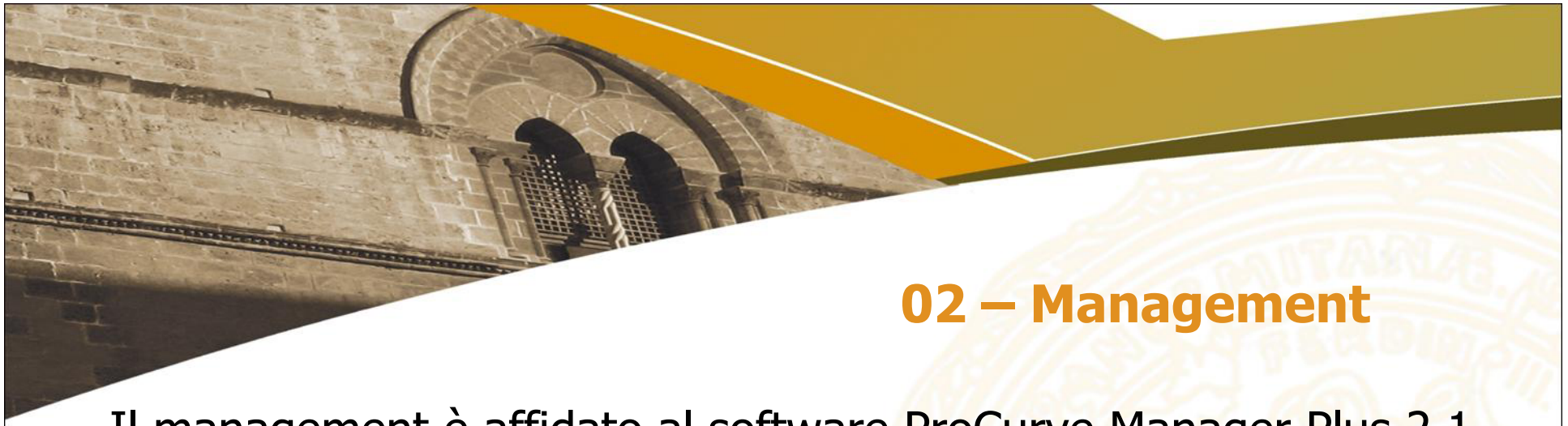
19 canali IEEE 802.11a disponibili sull'access point

- **11 canali tra 5,500 e 5,700 GHz:**

- Canale 100 a 5,500 GHz
- Canale 104 a 5,520 GHz
- Canale 108 a 5,540 GHz
- Canale 112 a 5,560 GHz
- Canale 116 a 5,580 GHz
- Canale 120 a 5,600 GHz
- Canale 124 a 5,620 GHz
- Canale 128 a 5,640 GHz
- Canale 132 a 5,660 GHz
- Canale 136 a 5,680 GHz
- Canale 140 a 5,700 GHz

- La lunghezza d'onda relativa allo standard IEEE 802.11b/g è circa 12,50 cm

- La lunghezza d'onda relativa allo standard IEEE 802.11a è circa 6,25 cm



02 – Management

Il management è affidato al software ProCurve Manager Plus 2.1 che consente:

- un'analisi approfondita del traffico: tramite protocolli come XRMON e sFlow si controllano i livelli di traffico generale e i segmenti con traffico più elevato;
- la gestione di gruppi e policy: si possono creare raggruppamenti di dispositivi e gestirli con policy di gruppo;
- una gestione delle VLAN avanzata: un'interfaccia di gestione VLAN consente di creare e assegnare le VLAN all'intera rete in modo abbastanza semplice;
- l'aggiornamento software dei dispositivi;
- l'utilizzo di SNMPv3: questo protocollo di gestione garantisce la privacy dei dati scambiati tra server e dispositivi gestiti.

02 – Antenne

Tipi di antenne:

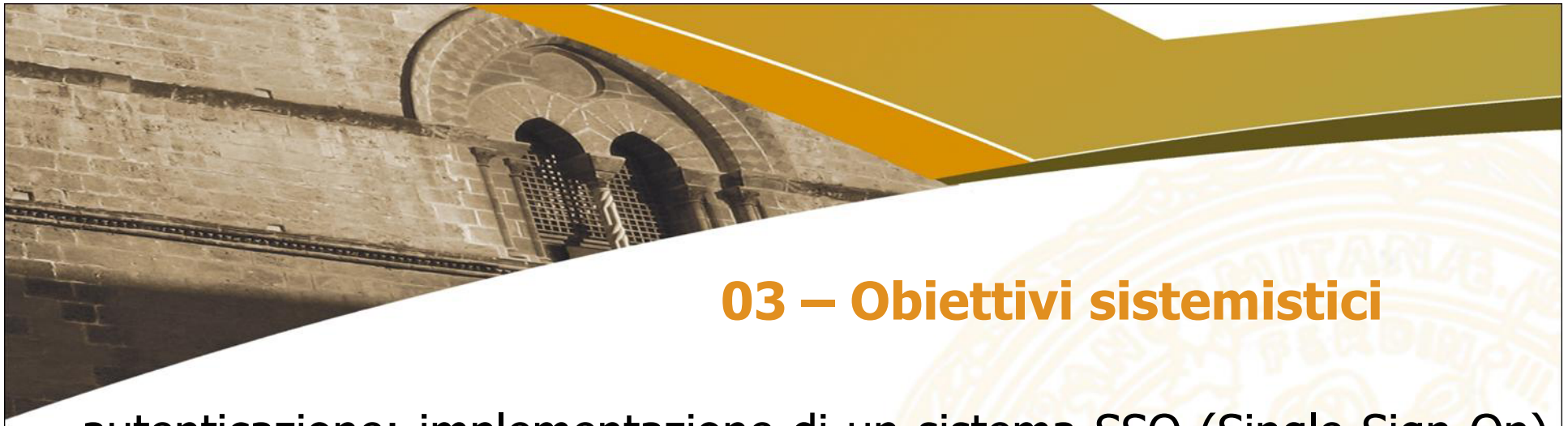
- n. 16 Antenne tipo Yagi 2,4 Ghz
- n. 30 Antenne a pannello 2,4 Ghz
- n. 4 Antenne Settoriali 2,4 Ghz
- n. 2 Antenne omnidirezionali 2,4 Ghz

02 – Luoghi in cui sono stati posizionati i server

1. DREAM (19.254)
2. Ingegneria Idraulica (48.254)
3. DTPM (18.254)
4. Presidenza Ingegneria / Matematica (24.254)
5. DICPM-DINFO-DIN (37.254)
6. Facoltà di Economia (25.254)
7. Facoltà di Lettere e Filosofia (23.254)
8. DFT (52.254)
9. Facoltà di Architettura (121.254)
10. Biologia (17.254)
11. Dipartimenti Chimici (14.254)
12. Facoltà di Agraria (39.254)

UNIPA Wireless Campus

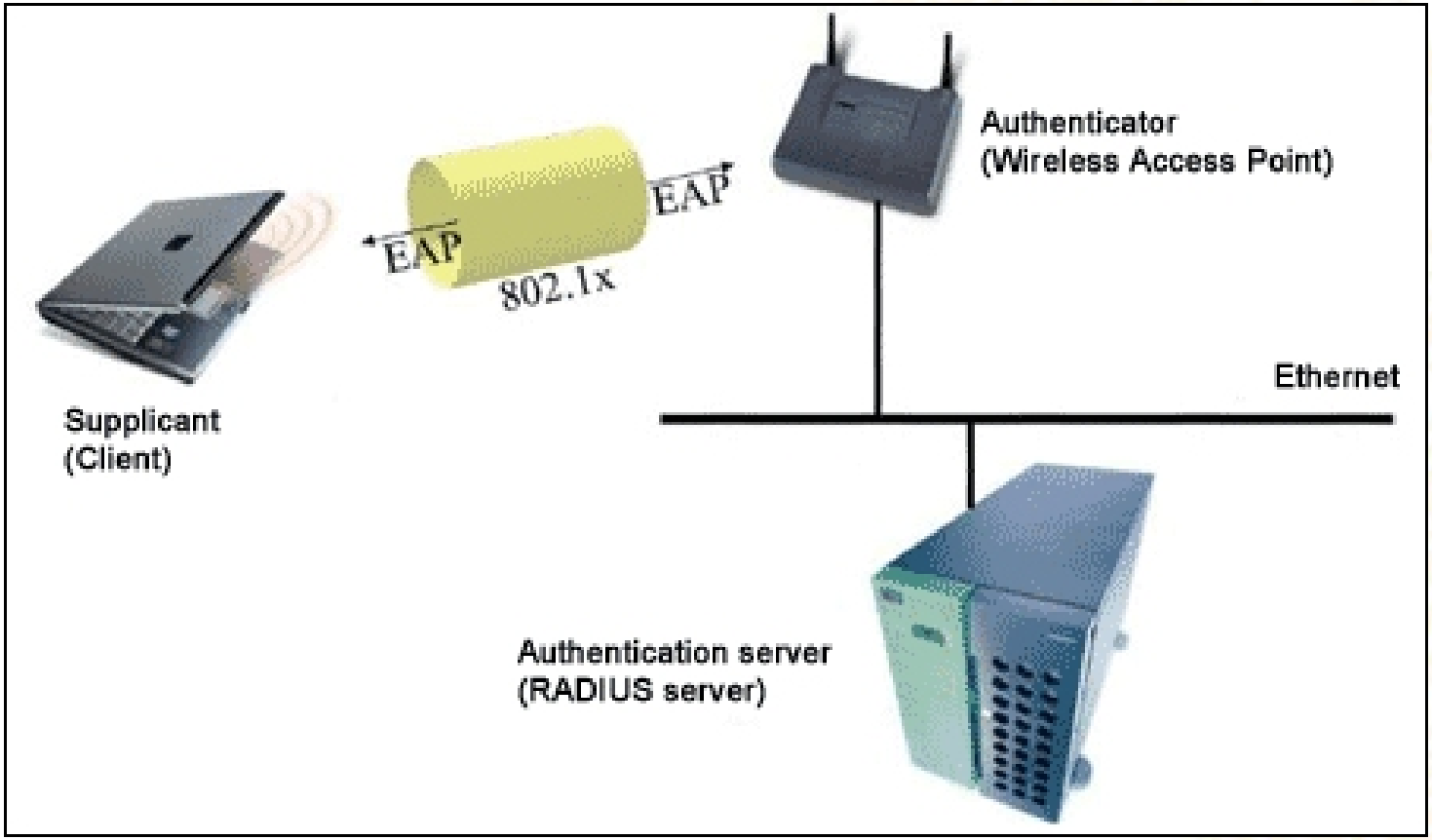
- 01 IDEA PROGETTUALE
- 02 FORNITURA
- 03 IMPLEMENTAZIONE DEL SISTEMA



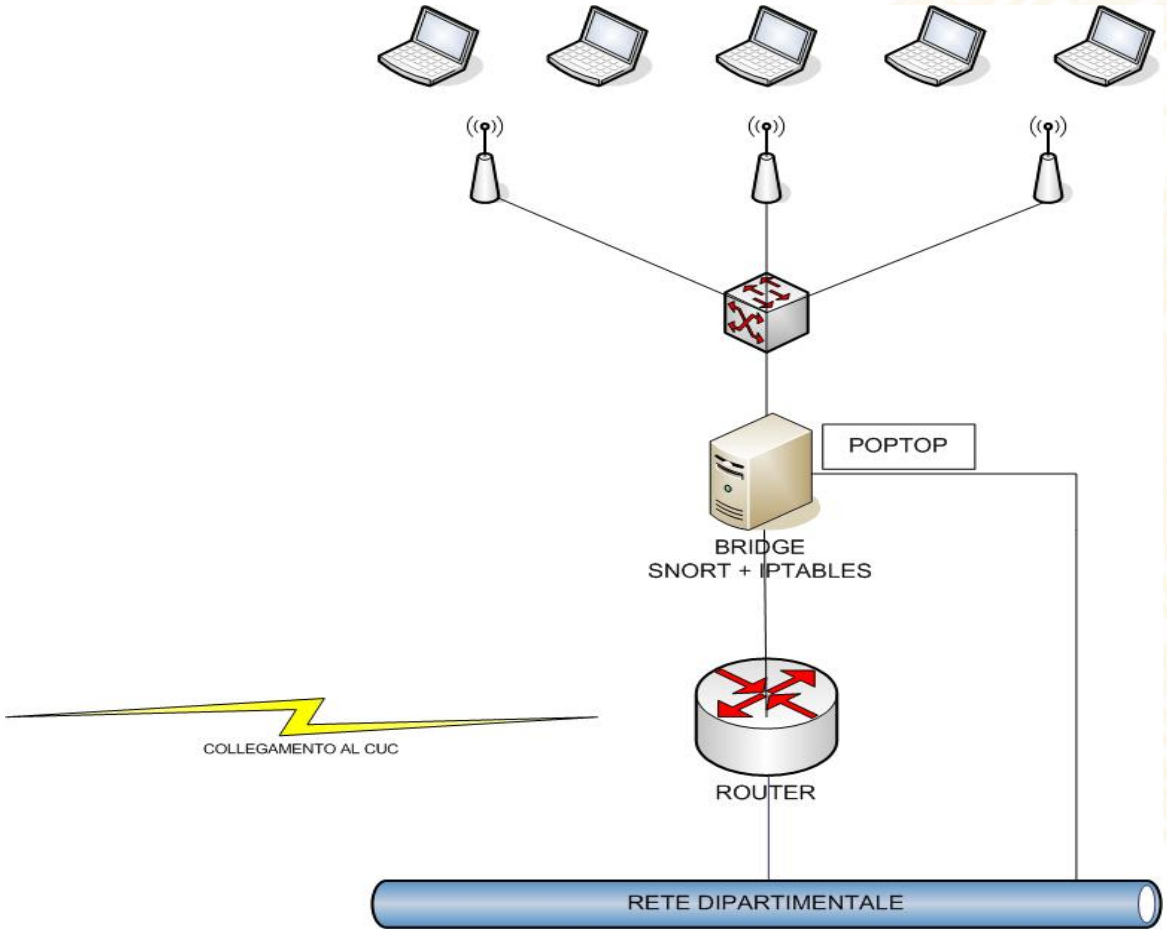
03 – Obiettivi sistemistici

- autenticazione: implementazione di un sistema SSO (Single Sign On) utile a più servizi (accesso ai sistemi di mail, PDC, ..) tramite RADIUS e LDAP
- VLAN: creazione di almeno 2 VLAN wireless, con rispettivi SSID distinti (wifi-unipa e wifi-unipa-wpa), tali da consentire l'accesso alla maggior parte dei dispositivi in commercio, via PEAP
- Accesso alla rete dipartimentale: una volta autenticati dal SSO centralizzato, tramite la creazione di una VPN con il server multihomed dipartimentale, si potrà accedere alle risorse del dipartimento e/o della Facoltà per stampare, inviare e-mail con il relay dipartimentale, etc.
- Accesso alla Rete solo per determinati servizi tramite iptables

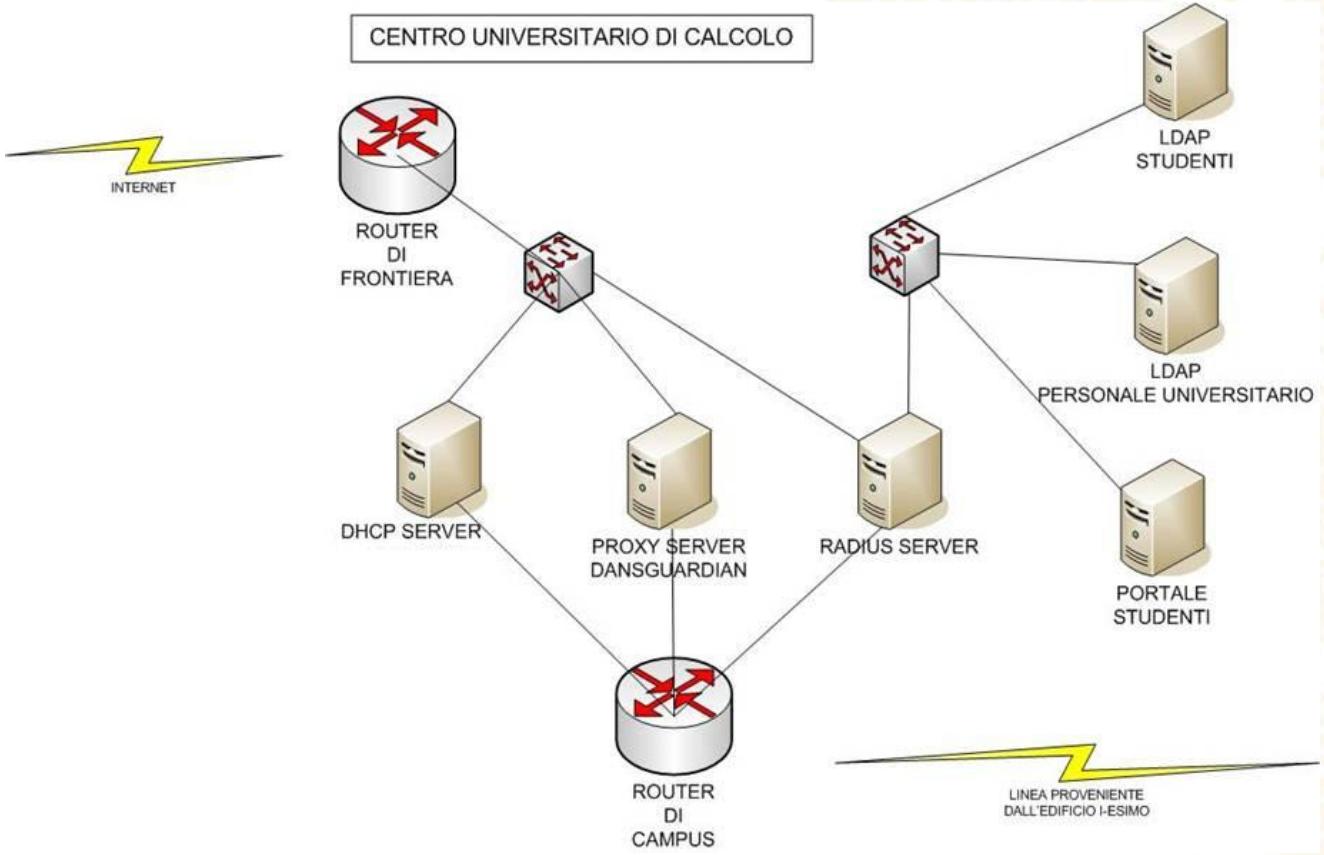
03 – Connessione via EAP



03 – Connettività presso l'edificio i-esimo



03 – Connettività al Centro Universitario di Calcolo



03 – Funzioni sistemistiche in gioco

- Server LDAP
- Server AAA con RADIUS
- Server DHCP, per il provisioning degli indirizzi IP ai supplicant wireless
- Server PopTop con radiusclient
- Server Proxy trasparente
- Server Proxy con Dansguardian e Clamav
- Server dei log
- Firewall con Iptables
- Analisi del traffico anomalo con SNORT
- VLAN con Cisco IOS

03 – Server LDAP

- Server LDAP studenti.unipa.it
- Server LDAP unipa.it
- Server LDAP cuc.unipa.it (per gli ospiti)
- Il ruolo di Samba

03 – Server AAA con RADIUS

- Nel processo di autenticazione AAA (Authentication, Authorization, Accounting) entrano in gioco:
  - Autenticazione (disporre di credenziali)
  - Autorizzazione (il sistema verifica le credenziali)
  - Accounting (registrazione degli eventi relativi alle autenticazioni e autorizzazioni)
- Le metodologie che vengono utilizzate sono:
  - Il metodo 802.1x denominato PEAP (Protected Extendable Authentication Protocol) e precisamente l'EAP type 25
  - MS-CHAP v2 (Challenge Response Handshake Authentication Protocol)
  - Crittografia di tipo WPA2/AES (IEEE 802.11i) e PEAP MS-CHAP v2
  - Crittografia di tipo WPA/TKIP e PEAP MS-CHAP v2

- WEP (Wired Equivalent Privacy) - Solo crittografia debole (RC4-56) - Autenticazione basata su chiave condivisa
- WPA (Wi-Fi Protected Access) - Subset di 802.11i HW compatibile con WEP - Autenticazione forte (802.1x/EAP) - RC4-128 con TKIP
- 802.11i (WPA2) [2004] - Sostituzione RC4 con AES - Key caching e pre-authentication (roaming)
- 802.11w WG istituito nel 2005 per ulteriori estensioni

03 – Server RADIUS decentralizzati

Accesso alla rete con domini personalizzati
@sottodominio.unipa.it

03 – Dettagli sulla crittografia

- **WPA. Un consorzio di aziende leader del settore, tra cui fanno parte Microsoft e il Wi-Fi Institute, ha creato lo standard WPA (Wi-Fi Protected Access) come implementazione parziale dello standard 802.11i che era ancora in fase di sviluppo. Questo standard offre un potente livello di crittografia che utilizza il protocollo TKIP (Temporal Key Integrity Protocol) per la crittografia dei dati. La maggior parte dei punti di accesso wireless (WAP) di oggi supporta lo standard WPA**
- **WPA2. Lo standard WPA2 (Wireless Protected Access 2) è stato creato nel settembre 2004 da Wi-Fi Alliance. È certificato come implementazione completa della specifica IEEE 802.11i, ratificata nel giugno 2004. Questo standard introduce un meccanismo di crittografia avanzato denominato AES (Advanced Encryption Standard), che utilizza il protocollo CCMP (Counter-Mode/CBC-MAC Protocol). Questa implementazione della crittografia wireless è estremamente sicura.**

03 – Server DHCP

192.168.4.3 → 192.168.7.254

03 – Server POPTOP con radiusclient

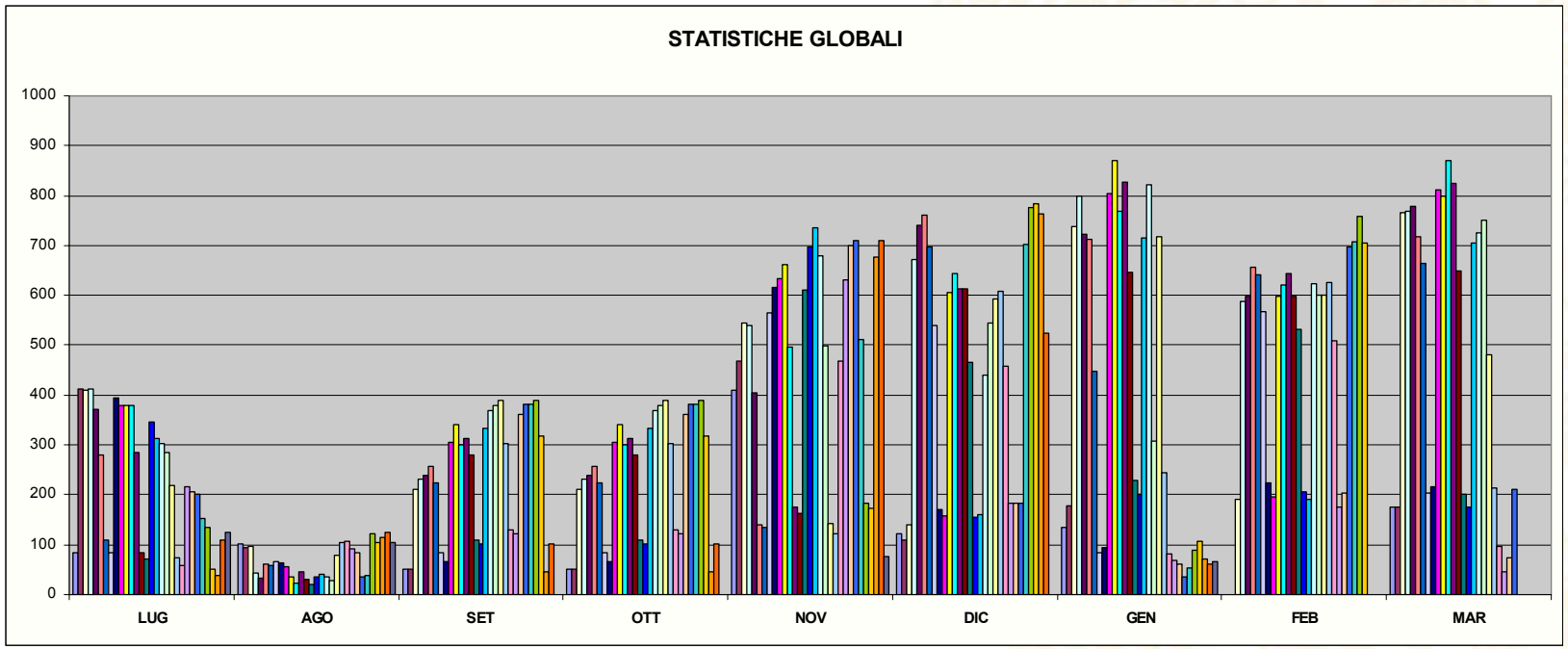
- Configurazioni
- Microsoft.dictionary

03 – Server Proxy trasparente

- Configurazioni
- Regola iptables
- Report di navigazione

03 – Server Proxy con controllo del contenuto

- Configurazioni Dansguardian
- Configurazioni Clamav



Accessi univoci (singole utenze) per giorno, nel periodo Luglio 2007 – Marzo 2008