8° Workshop tecnico GARR - GARR-X, Il futuro della Rete
1-4 Aprile 2008
Università Statale di Milano

Infrastruttura e politiche di accesso della MAN dell'Università di Milano Bicocca

Stefano Moroni

Sistemi Informativi
Università degli studi di Milano Bicocca

stefano.moroni@unimib.it

Università degli Studi Milano Bicocca

Presentazione dell'Ateneo

Studenti iscritti: 40.000 (7.000 matricole)

Personale strutturato (docenti e personale t/a): 1.500 unità

21 dipartimenti 8 facoltà

22 sedi in Lombardia distribuite nelle province di Milano, Monza-Brianza, Lecco e Sondrio

Università degli Studi Milano Bicocca

Presentazione rete di Ateneo

La rete dati/fonia dell'Università di Milano Bicocca è interamente amministrata dall'Area Sistemi Informativi che, oltre a gestire rete, server farm e relativi servizi, ne garantiscono il funzionamento fino alle prese di rete utente.

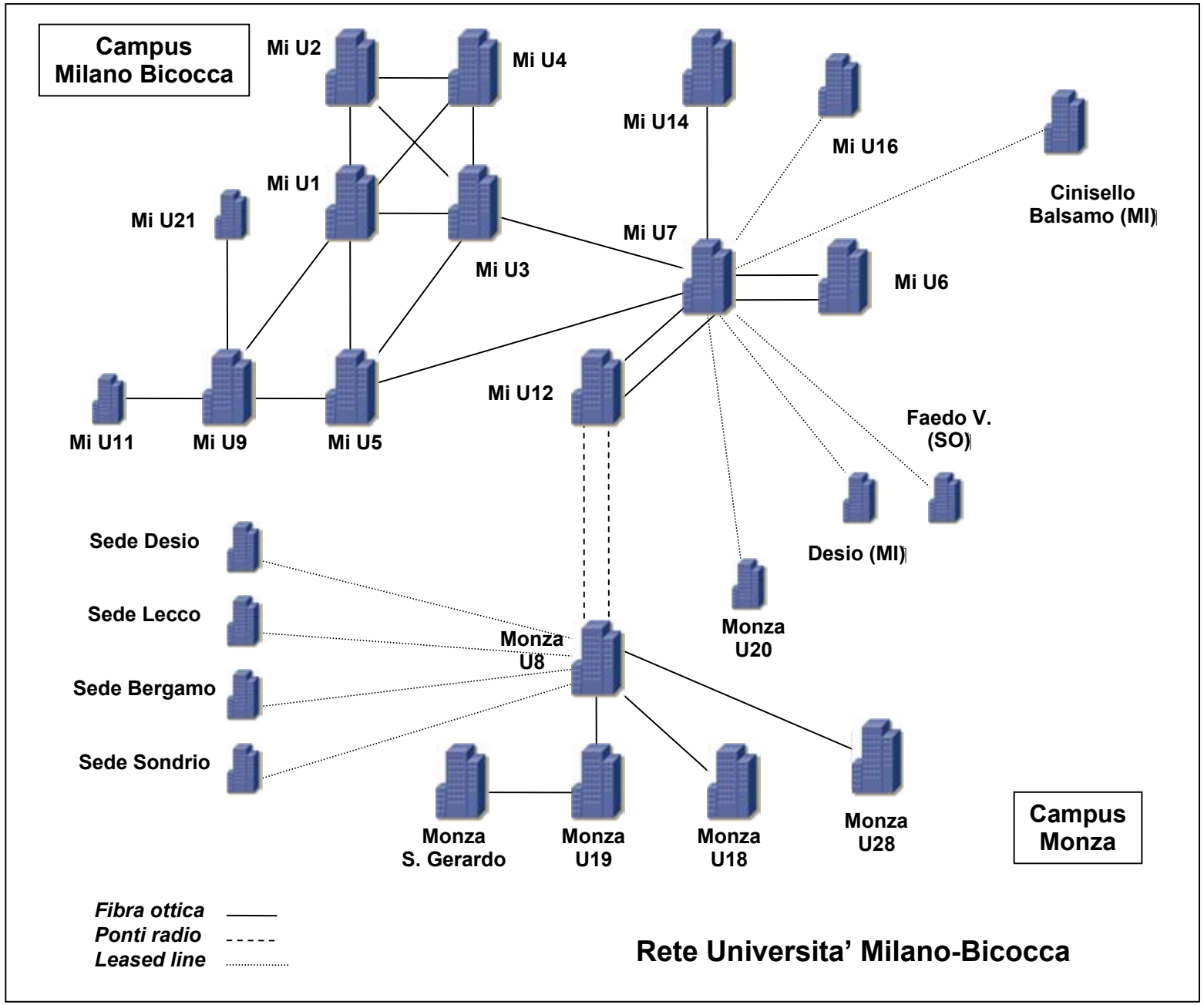
Non esiste alcuna forma di esternalizzazione e/o outsourcing e, dove possibile, tutti i servizi e gli applicativi di rete sono realizzati con software open source dal personale interno.

149.132.0.0/16
unimib.it / unimib.eu

La distribuzione delle sedi universitarie è su scala regionale con i campus di Milano Bicocca e di Monza che ne rappresentano il centro nevralgico.

I collegamenti geografici delle sedi periferiche convergono nel centro stella del campus di Milano Bicocca che ospita anche l'accesso alla rete GARR.

Sedi connesse alla rete di Ateneo



I numeri della rete Milano Bicocca

Infrastruttura passiva di proprietà

90 locali tecnici trasmissione dati

Dorsali di backbone:	- 8.500 m di cavidotti - 500 km fibre ottiche (smf e mmf)
Dorsali di edificio:	- 3.500 m di cavidotti - 125 km fibre ottiche (smf e mmf)
Cablaggio orizzontale in rame:	- 1.000 km cavi FTP (cat. 5, 5e, 6) - **21.000 punti rete**

I numeri della rete Milano Bicocca

Infrastruttura attiva e utenza di rete

Apparati	Multilayer switch di core:		9 (fully redundant)
	Switch di Accesso:		400
	Router veloci:		2 (fully redundant)
	Apparati WAN/RAS/VPN:		30
	Appliance Server Farm:		10
	Server (Server Farm):		70
	Wireless Access Point:		300
	PABX:		11
Interfacce fisiche	Porte apparati 10Gb/s FX:		12
	Porte apparati Gb/s FX:	1250	
	Porte apparati 10/100TX:		12.000
	Porte apparati 10/100/1000TX:	1.000	
Utenza	Rete dati:		10.000
	(40 Laboratori Informatici:)		(2.000)
	Fonia (utenza digitale, VoIP, dect, ISDN):		3.000
	Wireless (studenti, personale,ospiti) 32K Certs		

Caratteristiche progettuali

L'intero progetto della rete dell'Università di Milano Bicocca è basato sugli **standard** internazionali delle organizzazioni che definiscono le tecnologie ed i protocolli per le infrastrutture IT ed è, quindi, una **rete multivendor**.

Infrastruttura passiva:	Standard per Cablaggio Strutturato TIA/EIA e ISO/IEC
Infrastruttura attiva:	Standard della suite TCP/IP e relativi Internet Standard IETF *In particolare per i livelli Physical e Data Link del modello OSI:* Standard IEEE 802.1 e 802.2 Standard IEEE 802.3 e annessi (wired) Standard IEEE 802.11 e annessi (wireless)

Caratteristiche progettuali

Fault Tolerance & High Availability

Architettura "no single point of failure".
L'intero progetto della rete è basato sull'ottenimento del massimo grado di alta disponibilità e tolleranza ai guasti sia per la parte passiva che per la parte attiva

Locali tecnici sotto continuità elettrica (UPS) e condizionati *(si sta procedendo ad ultimare gli impianti dei locali tecnici non ancora a norma che rappresentano circa il 30%).*
Percorsi ridondati per le dorsali di backbone e di edificio.
Ridondanza parti funzionali 1:1: l'intera infrastruttura attiva del backbone, server farm compresa, è ridondata 1:1 in ogni sua parte funzionale (dalle alimentazioni alle interfacce sugli apparati).
Ogni collegamento tra gli apparati di tutti e tre i livelli del backbone utilizza due coppie di fibre ottiche connesse a interfacce appartenenti a moduli di I/O diversi.

Per I nodi di backbone si è optato per hardware modulare a chassis completamente passivo, in luogo a coppie di apparati in HA, onde evitare gli svantaggi dell'uso di protocolli di ridondanza (un esempio su tutti: rotte asimmetriche nelle architetture VRRP).

Caratteristiche progettuali

Architettura & Performance

Tipologia di **rete a commutazione di pacchetto** su protocolli **IP/MPLS.**
Topologia secondo il **modello gerarchico a tre livelli (Core/Distribution/Access).**

Il backbone è **"*routed*"** (layer 3 OSI) con VLAN e domini di broadcast (layer 2 OSI) confinati al livello di accesso che è esclusivamente **"*switched*"** (separazione dei domini di collisione); non sono utilizzati apparati di rete operanti esclusivamente al livello fisico del modello di riferimento OSI (Repeater/Hub).

Gli **apparati del backbone** IP/MPLS (core e distribution) sono dual stack IPv4 e Ipv6, ad architettura non bloccante, equipaggiati con ASICs programmabili e dimensionati per ottenere prestazioni a **"*wire speed*"** nelle varie operazioni di lookup e rule matching.
Non sono utilizzati protocolli tipo Spanning Tree (elevati tempi di convergenza) e si implementa H-VPLS con Fastreroute (FRR).

Sui collegamenti geografici a limitata larghezza di banda e nel caso di apparati del livello di accesso con una certa "*oversubscription rate*" è implementata la **QoS** con approccio DiffServ (DSCP e 802.1p mapping e rewriting).
Le classi di servizio che determinano il PHB sono quelle standard IETF.

Infrastruttura passiva: backbone

Nei campus di Milano Bicocca e Monza l'Università dispone di **cavidotti e fibre ottiche di proprietà**.

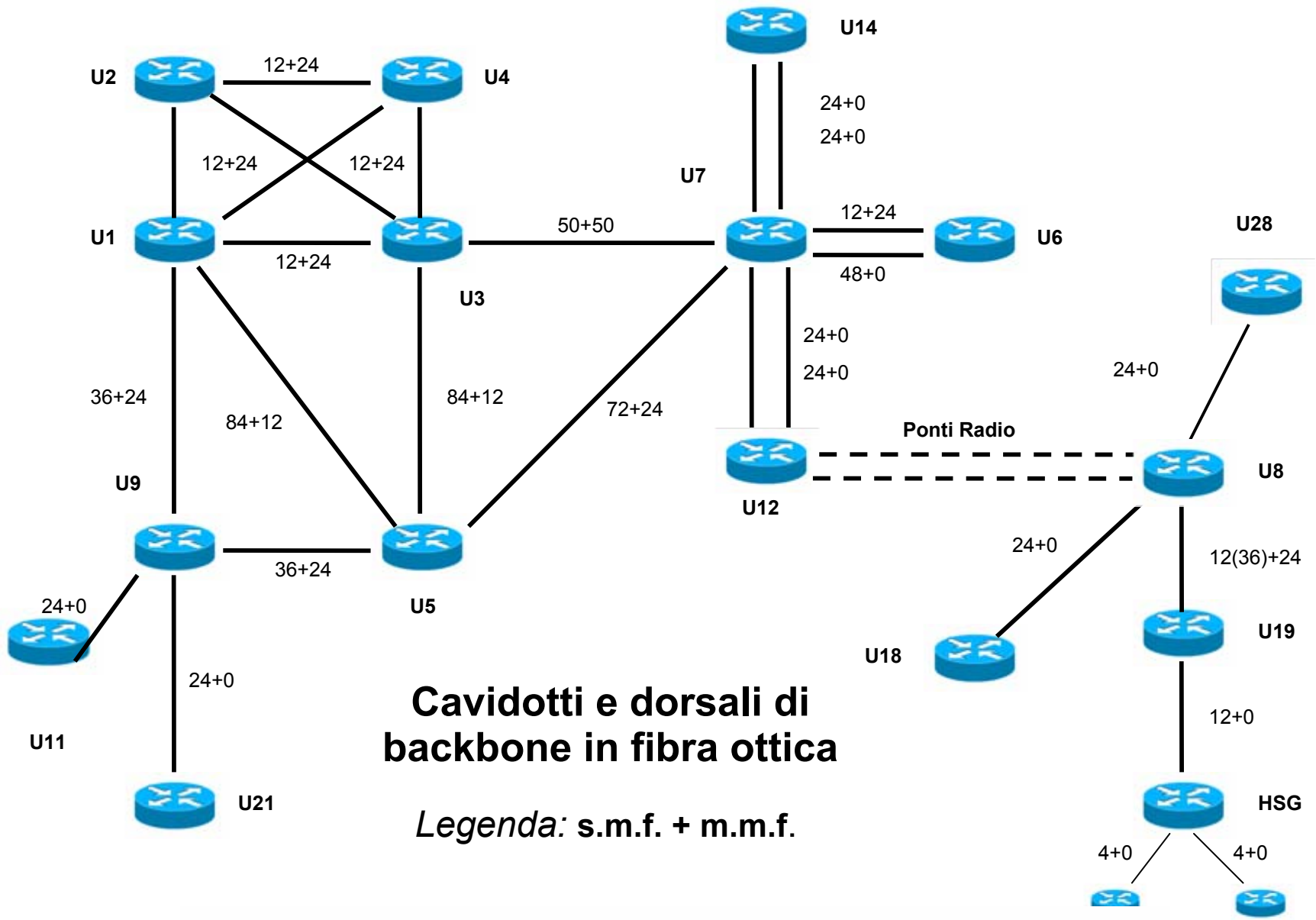
Magliatura completa dei cavidotti ospitanti le dorsali in fibra ottica tra gli edifici rappresentanti i nodi di Core backbone

Ogni edificio rappresentante un nodo del backbone di distribuzione è collegato da due dorsali in fibra ottica, su **percorsi fisicamente distinti**, ad almeno due nodi di core backbone.

Gli edifici non inclusi nel backbone di core e distribuzione sono collegati agli edifici del backbone da uno o due cavidotti per fibra ottica in funzione della dimensione e dell'importanza dell'edificio nell'economia di rete.

Infrastruttura passiva: backbone

Modello parzialmente magliato



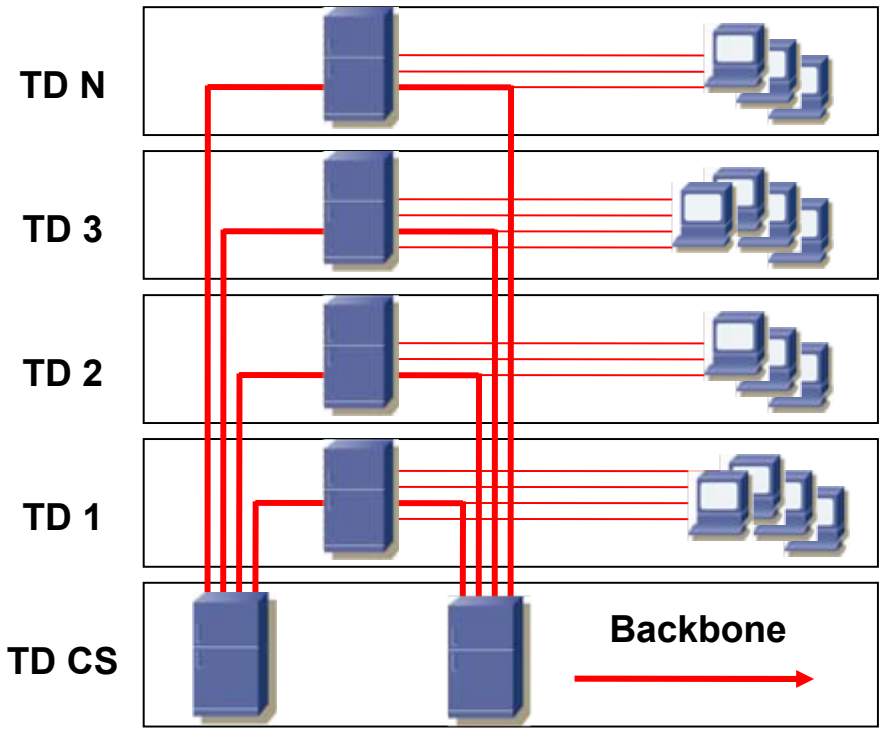
Cavidotti e dorsali di backbone in fibra ottica

Legenda: **s.m.f. + m.m.f.**

Infrastruttura passiva: building

Modello a stella

Ogni edificio universitario è provvisto di un certo numero di locali tecnici per trasmissione dati con collegamenti in fibra ottica punto-punto (dorsali verticali) verso un particolare locale tecnico detto “centro stella” di edificio.



Da ogni locale tecnico si diramano i cavi in rame (L_{max} 90 m) costituenti il cablaggio orizzontale.

Dorsali verticali

Cavo 24 m.m.f.
Cavo 12 s.m.f.

Alta disponibilità: continuità elettrica

UPS (Uninterruptible Power Supply) centralizzati per ogni edificio con autonomia di 2/4 h in funzione dell'importanza del nodo sotto continuità nell'economia della rete.
Per i tre edifici costituenti i nodi di core backbone e ospitanti il “Centro Stella” di Ateneo con i collegamenti geografici e la Server Farm si è optato per due UPS ridondati in bilanciamento di carico.

Nei sette edifici principali del campus di Milano Bicocca (U1-U7) e nell'edificio U8 del campus di Monza è presente un **gruppo elettrogeno**.

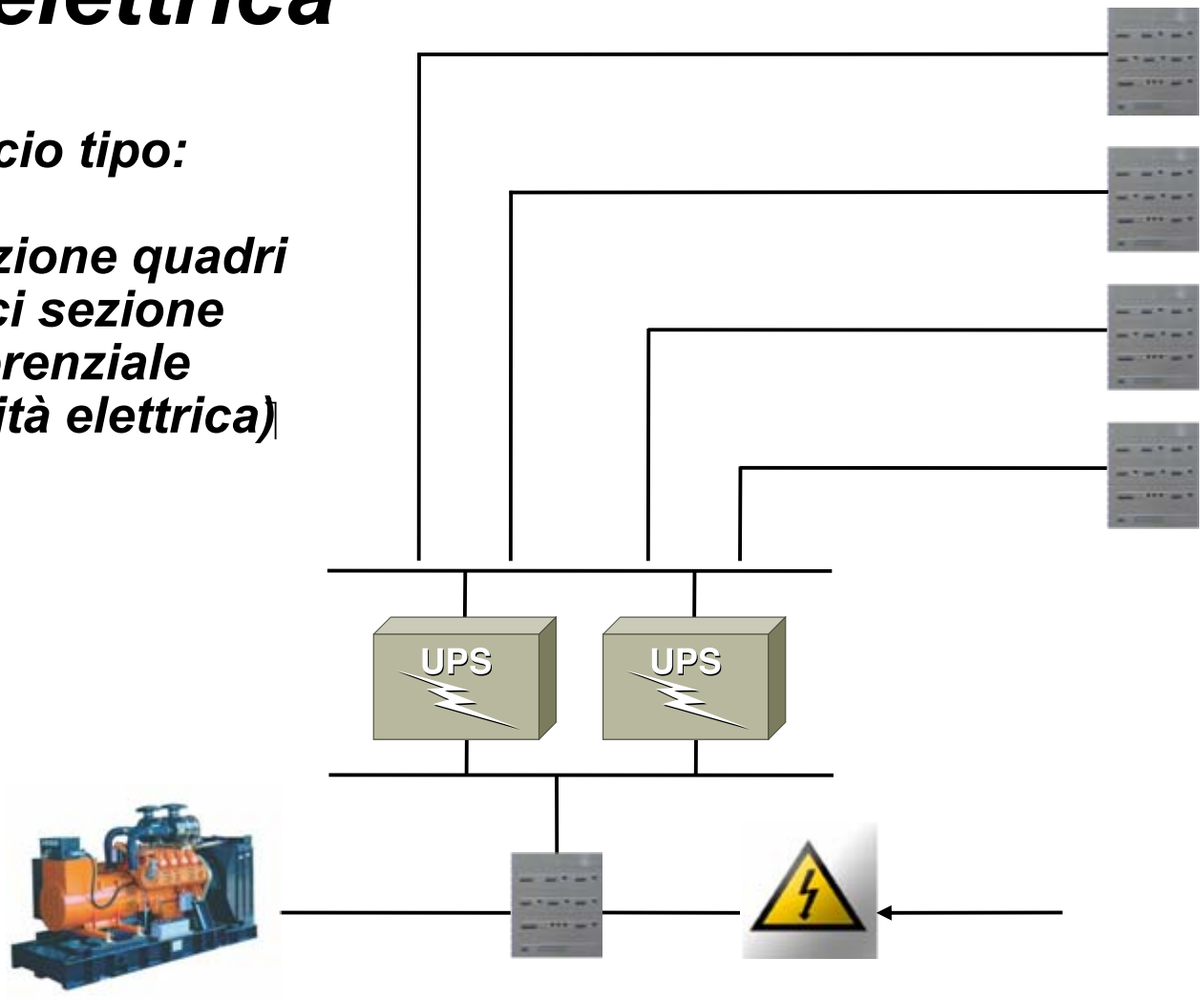
La tecnologia scelta per gli UPS è quella **on-line con bypass statico**.
I gruppi di continuità on-line al momento del black-out smettono di prelevare energia dalla rete elettrica e iniziano a prelevarla dagli accumulatori, continuando a fornire tensione in uscita in modo assolutamente continuativo e trasparente al carico.

Ogni UPS è dotato di scheda SNMP per monitoraggio e malfunzionamenti.
Il server di gestione è centralizzato ed è interfacciato con un combinatore telefonico per l'inoltro degli allarmi.

Alta disponibilità: continuità elettrica

Edificio tipo:

alimentazione quadri elettrici sezione preferenziale (continuità elettrica)



Quadri elettrici locali tecnici

Linea alta/media tensione

Gruppo elettrogeno

Quadro elettrico generale

Cabina elettrica

Architettura di rete: backbone

Rete IP/MPLS con topologia del backbone a tre livelli

Core layer: anello su tecnologia 10 Gigabit Ethernet

Distribution layer: ogni nodo di distribuzione è collegato a due nodi di core tramite link a 2 Gbps (802.3ad). Sulla tratta che collega il campus di Milano Bicocca con il campus di Monza (10.8 km in linea d'aria) sono attivi due ponti radio (HiperLan: 5.470 – 5.725 GHz OFDM) in bilanciamento di carico e un collegamento di ulteriore backup.

Access layer: ogni nodo di accesso è collegato al relativo blocco di distribuzione tramite link ridondati di 2 Gbps (802.3ad).
Del livello di accesso fanno parte anche gli apparati che concentrano i tunnel con gli AP wireless che sono in HA semplice.

WAN link: ogni sede remota è collegata al backbone del campus tramite collegamenti geografici punto-punto.

Architettura di rete: protocolli

Protocolli della suite TCP/IP

Protocolli di routing unicast

IGP **OSPFv2**

Protocolli di routing multicast

PIM SM con IGMP e IGMP snooping

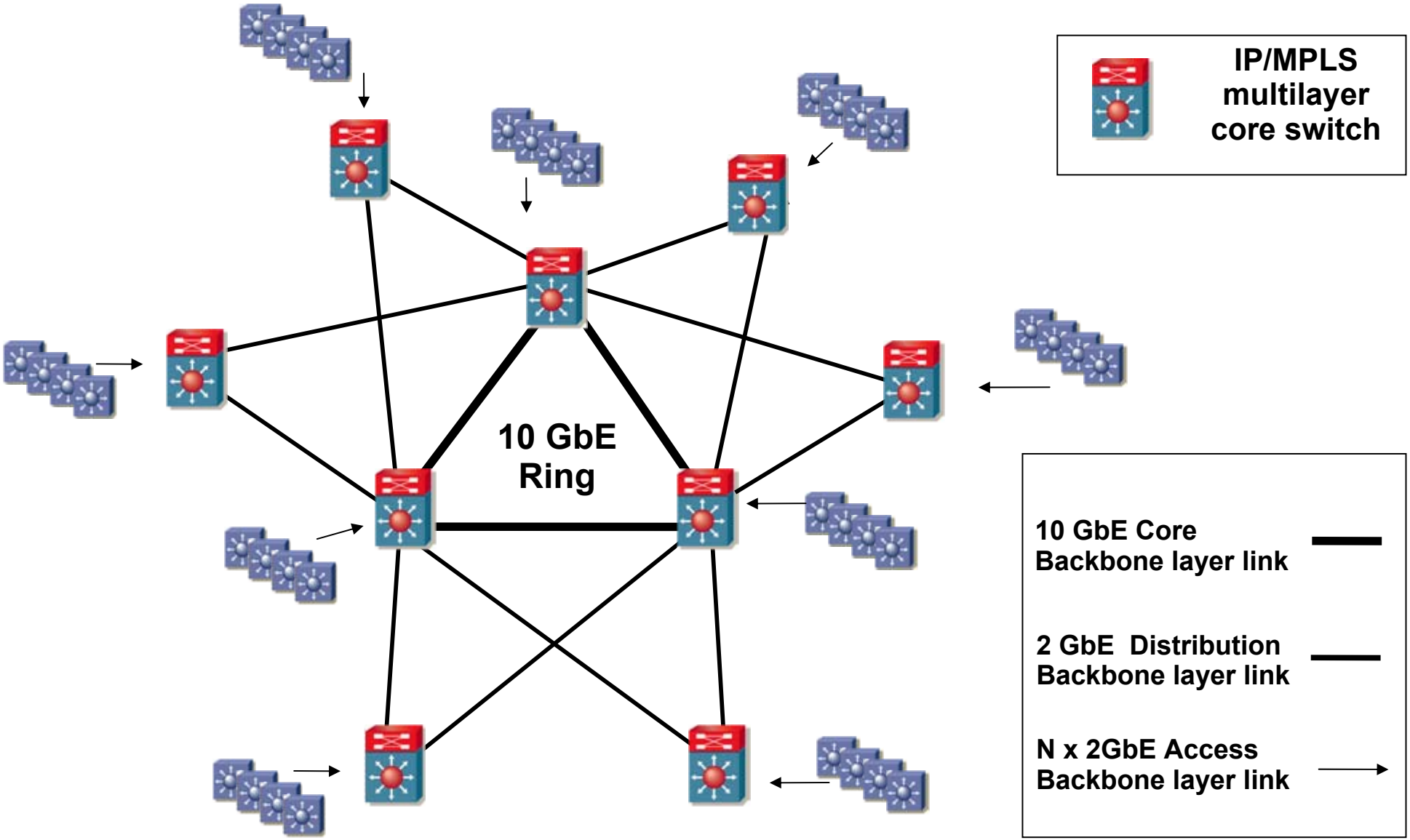
Protocolli di traffic engineering

MPLS; in particolare **H-VPLS** con **LDP** signaling (RFC 4762)

Protocolli layer 1 e layer 2

IEEE 802 working group (**802.3**, 802.2, 802.1)
in particolare: 802.3ad, 802.3af, 802.1Q, 802.1X, 802.11i

Unimib Hierarchical Backbone



Architettura di rete: fonia

Sistema misto PABX tradizionali e VoIP

Premessa:
dalla sua fondazione l'Università è proprietaria di PBX e di fibre ottiche di collegamento. Il costo dell'intero sistema di fonia, essendo esclusivamente quello di manutenzione degli apparati, è molto basso. Fermo restando che ogni espansione della rete fonia utilizza VoIP da due anni, per ora è economicamente conveniente una architettura mista.

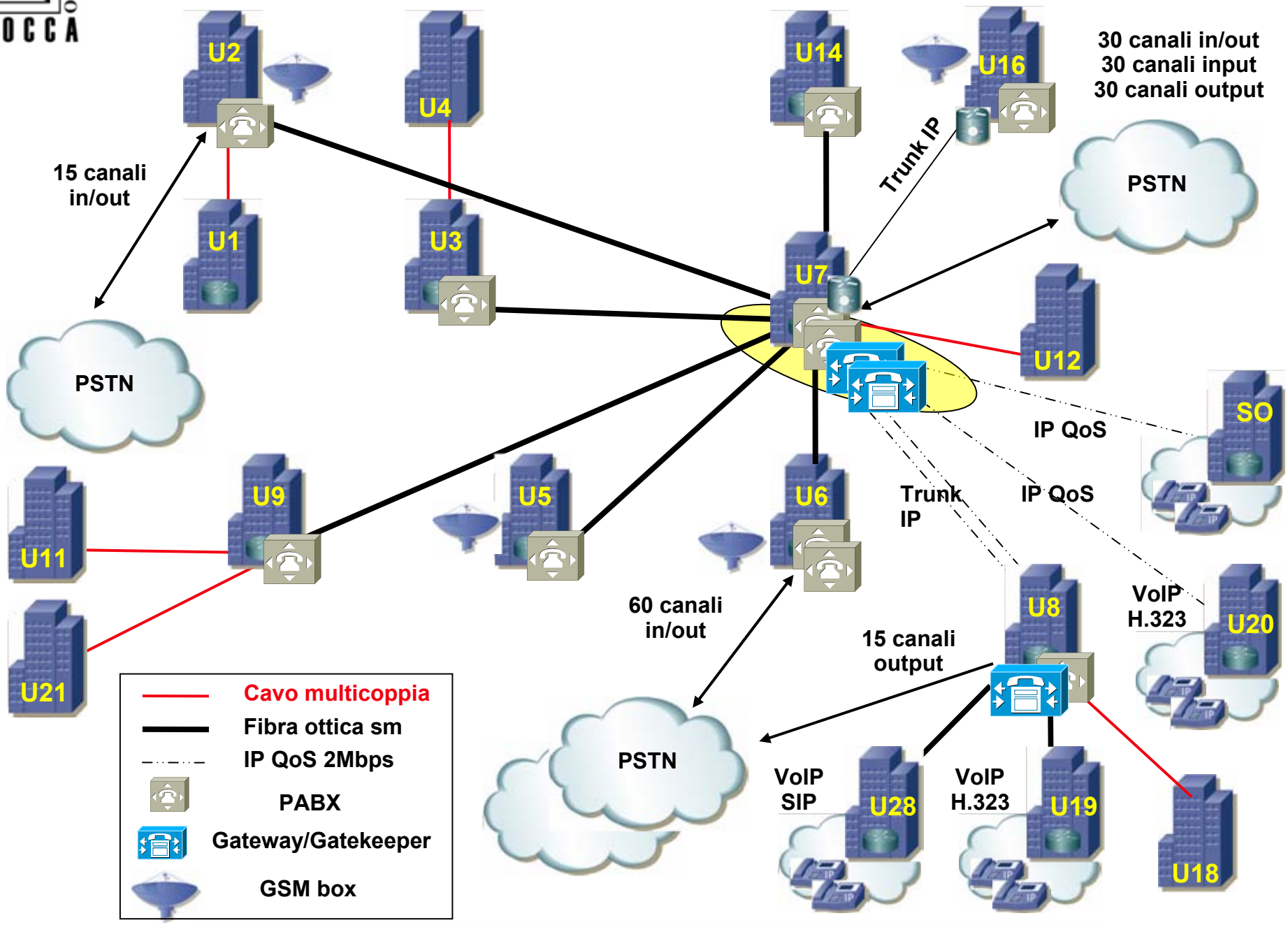
La rete fonia utilizza lo stesso cablaggio strutturato della rete dati.

In tutte le sedi remote, dove si avrebbe un costo per un collegamento geografico dedicato, si utilizza VoIP. In ogni sedi di nuova attivazione si utilizza VoIP.

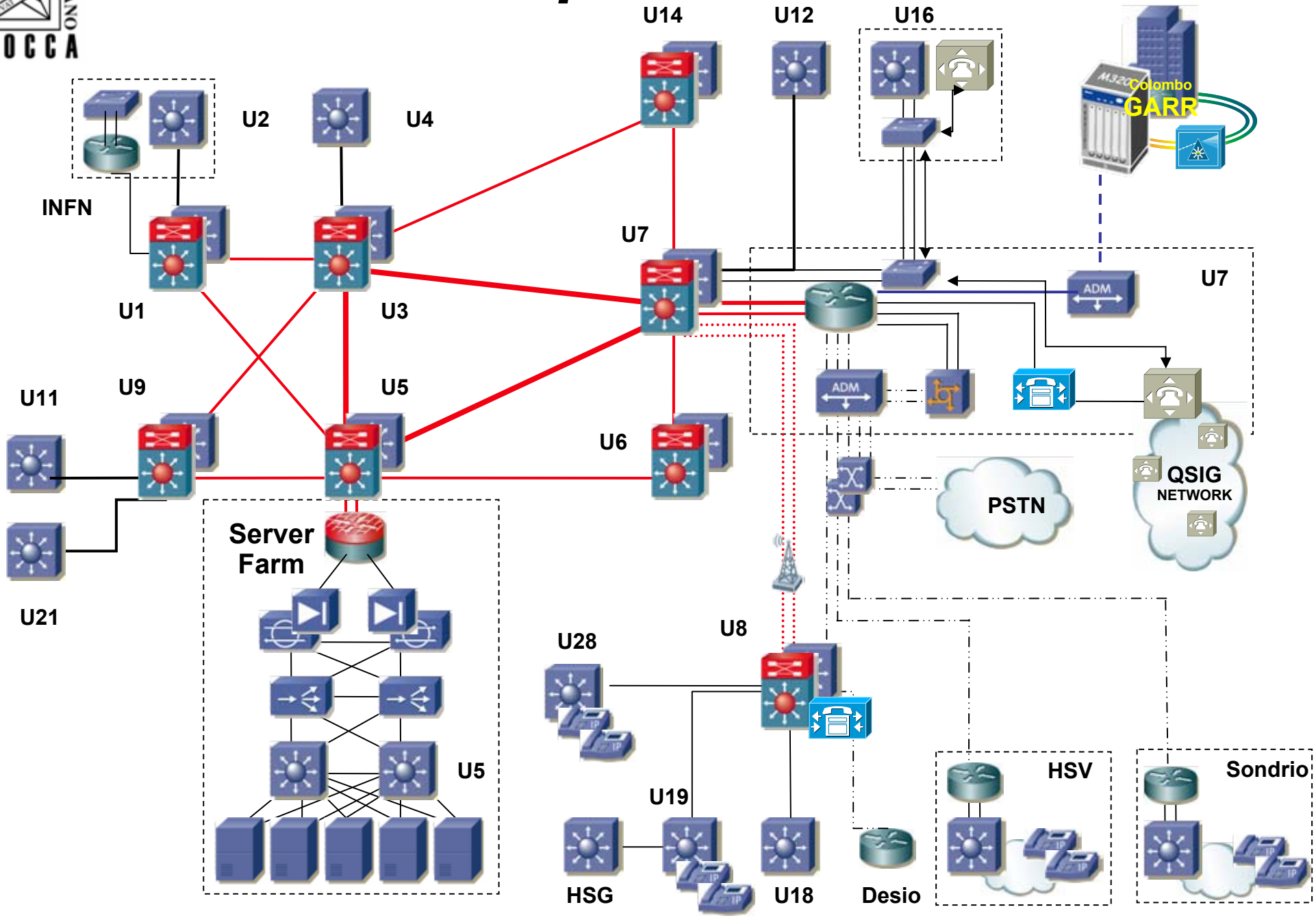
Ogni sede a tecnologia VoIP è collegata a gatekeeper e gateway tramite collegamenti IP con QoS attivata.

Sono in fase di test diverse soluzioni su protocollo SIP con implementazione di MPLS con Local Protection (FRR) sul backbone per il passaggio completo a fonia su IP.

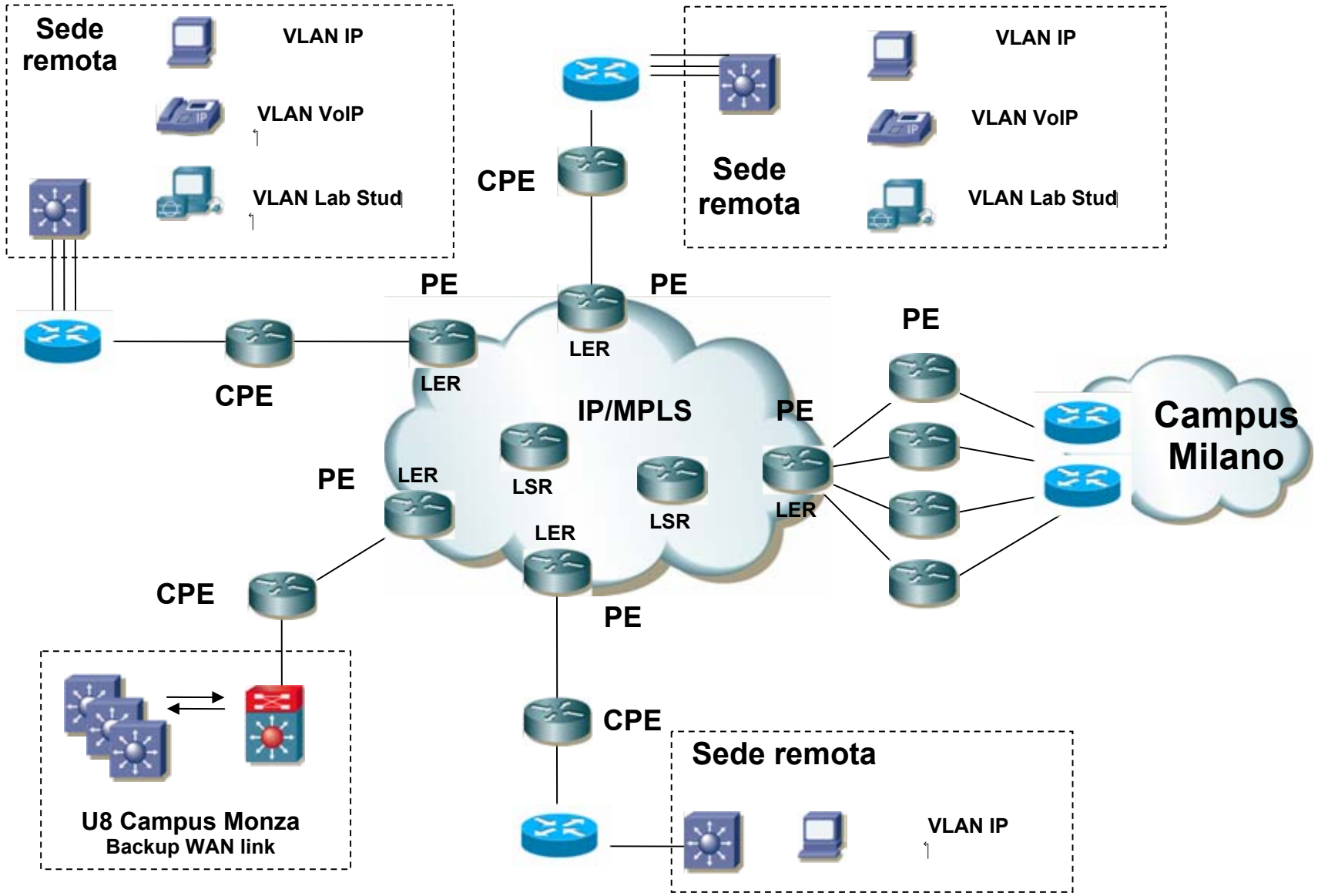
Unimib QSIG/VoIP network



Unimib metropolitan area network



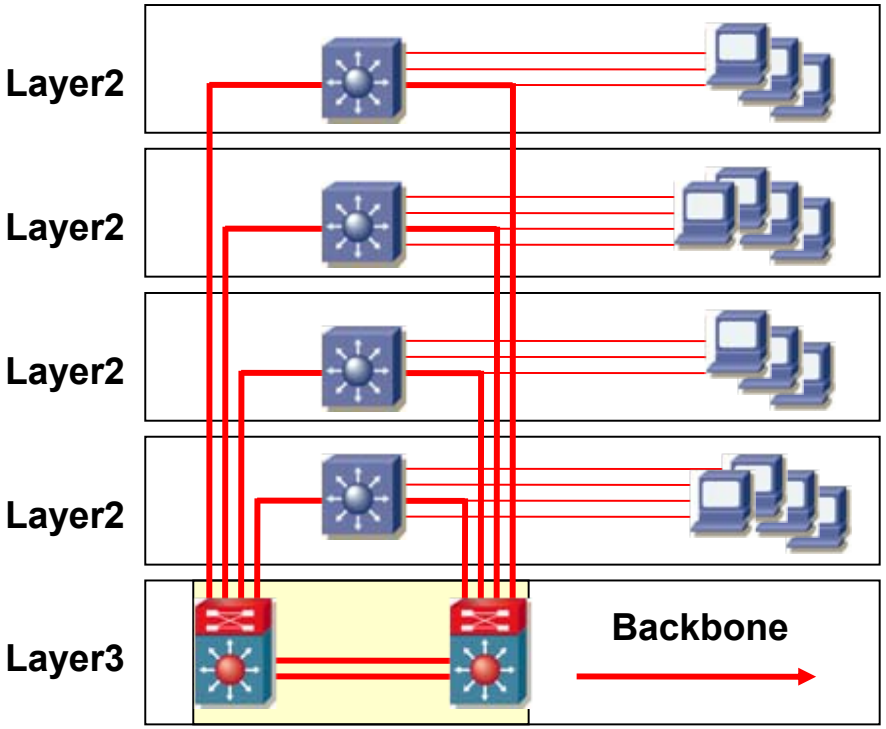
Unimib Wide Area Network



CPE: Customer Premise Edge PE: Provider Edge (LER: Label Edge Router) LSR: Label Switch Router

Building Access Layer

Modello a stella



Ogni nodo di accesso è collegato al rispettivo nodo di distribuzione tramite due uplink 1000Base SX o LX su moduli di I/O diversi (HA). Per utilizzare l'intera larghezza di banda si implementa 802.3ad

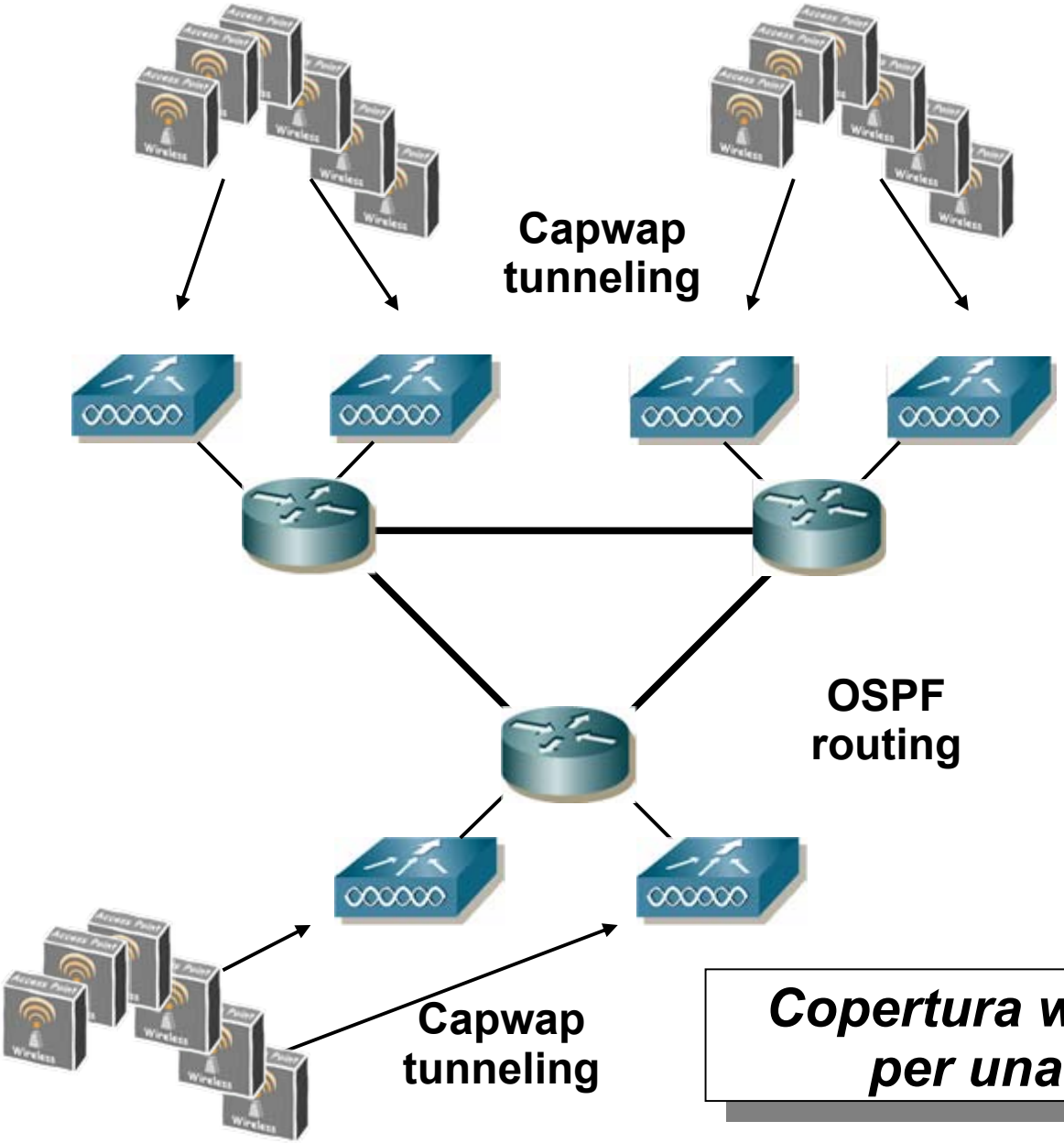
La topologia stellare permette di evitare l'utilizzo di Spanning Tree che sarebbe un limite per applicazioni “real time”.

Livello di accesso “***switched***” (separazione domini di collisione)

Poichè gli apparati del livello di accesso lavorano con un certo rapporto di “oversubscription”, in funzione del tipo di traffico, per l'inoltro dei frame è utilizzato 802.1p, poi mappato, dal nodo di distribuzione, su classi di servizio DiffServ per il PHB su backone.

Layer 2: LAN e VLAN rimangono confinate all'interno del relativo blocco di **accesso**.
I relativi default gateway sono configurati sulle interfacce del nodo di distribuzione.

Unimib Wireless network



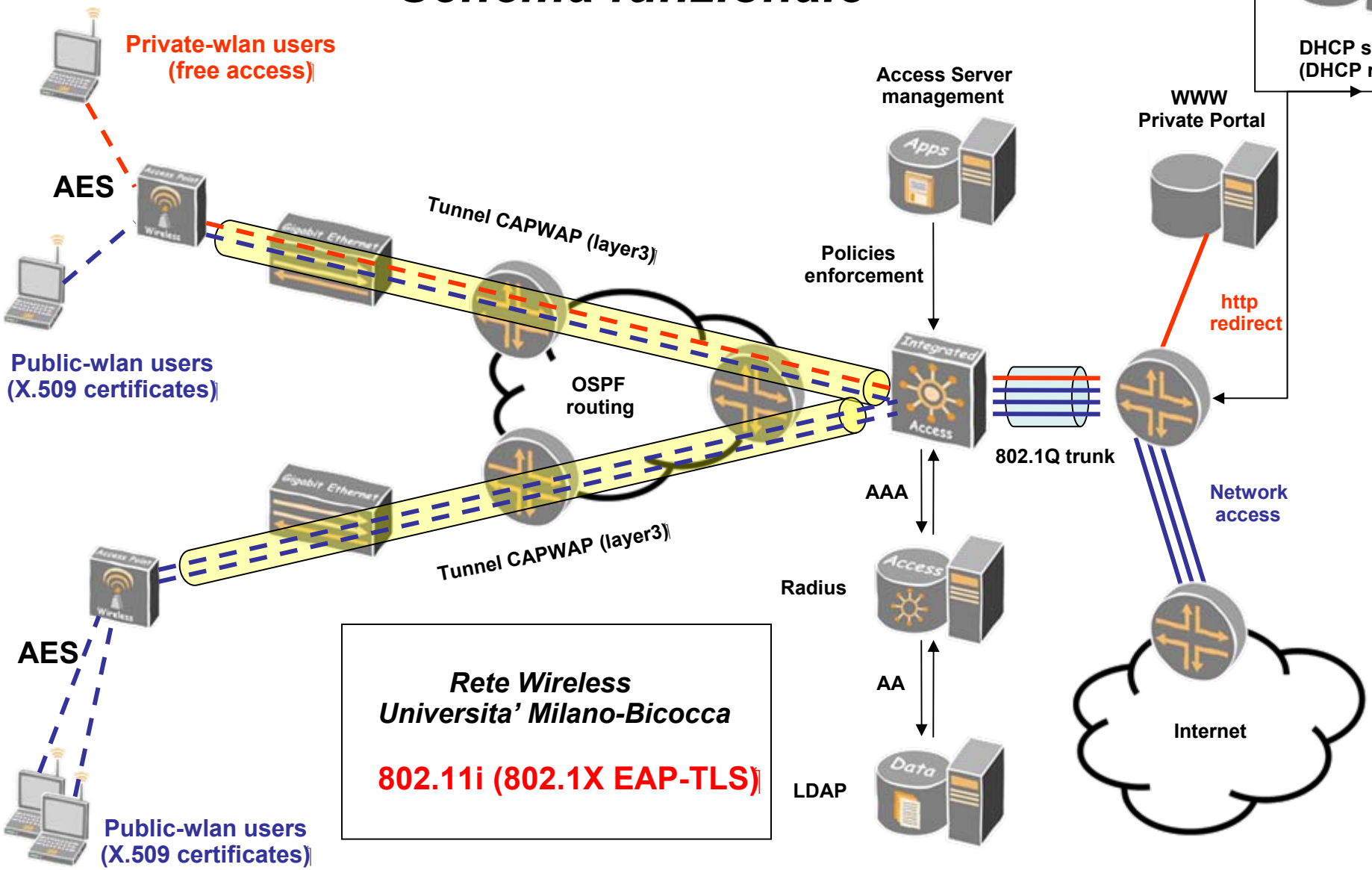
Ogni coppia di WLAN Access Server è collegata ad uno dei tre nodi di core backbone.

Gli Access Point Wireless sono concentrati sugli apparati di accesso tramite tunnel capwap a layer 3

Copertura wireless completa dell'Ateneo per una superficie di 230.000 mq

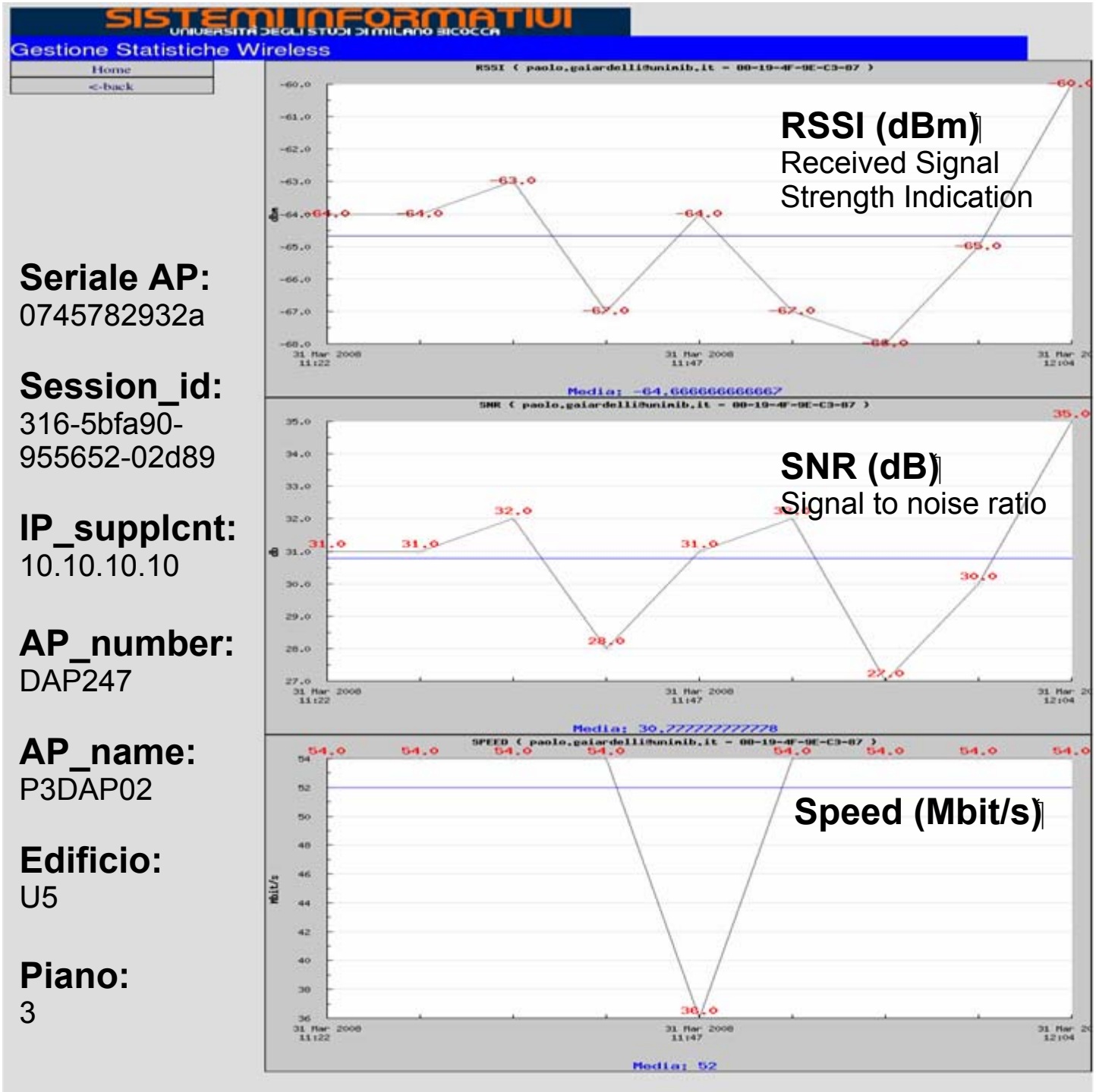
Unimib Wireless network

Schema funzionale

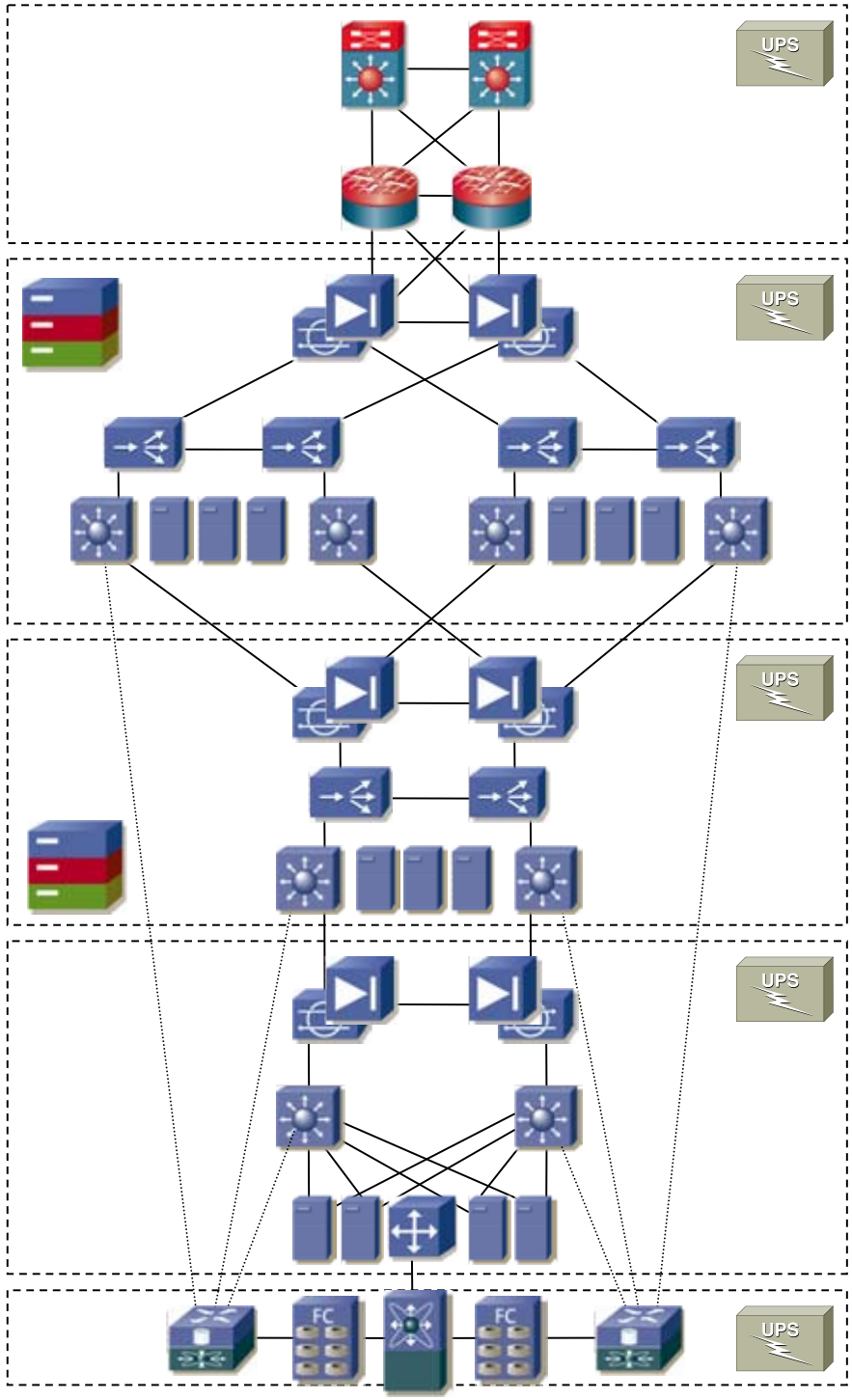


Screenshot qualità connessione per Supplicant

Raccolta valori effettuata con SNMP polling su vendor specific *MIB*



Server Farm



Aggregation layer

Front-end layer

Application layer

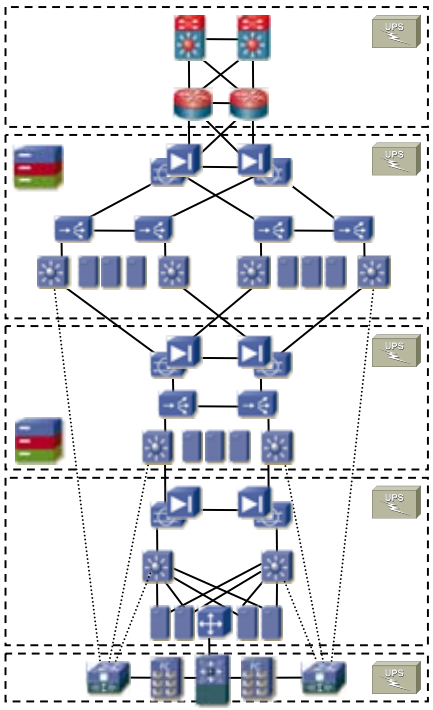
Back-end layer

Storage layer

Server Farm: Alta Disponibilità

Architettura "no single point of failure":

Come nella progettazione del backbone, per l'alta disponibilità si è optato per apparati modulari a chassis e backplane passivi onde evitare le complessità architetturali e di gestione derivanti da l'utilizzo di protocolli di ridondanza come il VRRP. Nel caso di *appliance* operanti ai livelli superiori della pila OSI, per la ridondanza tra i nodi, si utilizza clustering.

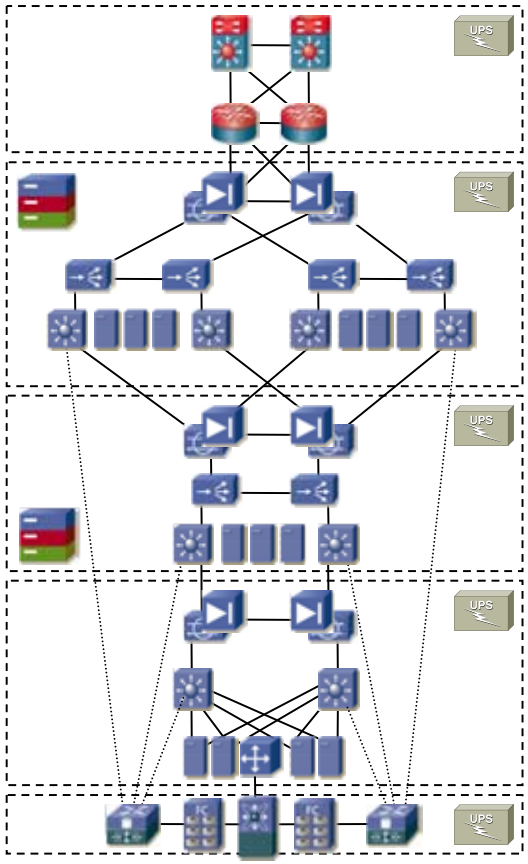


Locale compartimentato secondo standard REI.
Impianto anti incendio a gas estinguente (N).

L'impianto di alimentazione della sala macchine ha due distinti quadri elettrici sotto continuità fornita da due UPS in bilanciamento di carico e un generatore diesel per i black out di lunga durata. Ogni rack della server farm è dotato di almeno due linee di alimentazione, di adeguato amperaggio, derivate da sezionatori su quadri elettrici differenti.

L'impianto di condizionamento è costituito da tre condizionatori in bilanciamento di carico.

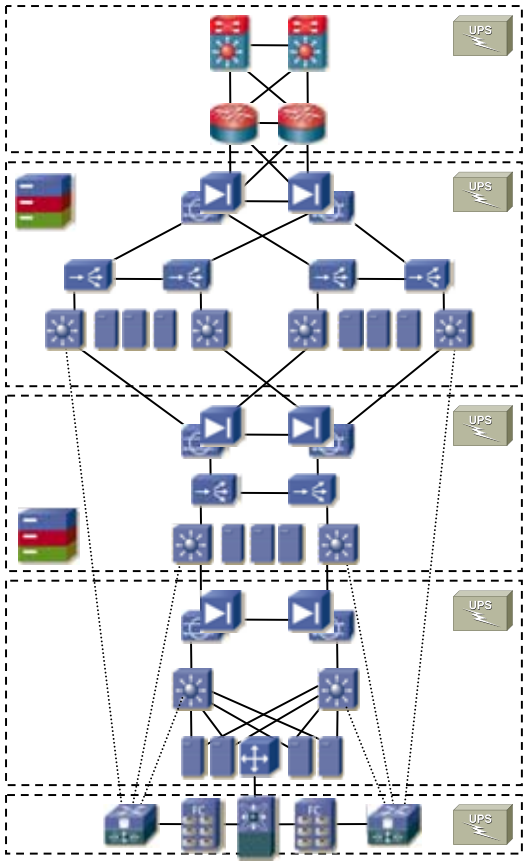
Server Farm:
Alta Disponibilità e Prestazioni



Aggregation Layer:
Apparati modulari a chassis e backplane passivi e completamente ridondati in ogni parte attiva.
Interconnessioni Gigabit Ethernet full-mesh.
Wire speed switching/routing (ASICs).

Front End & Application Layer:
Cluster di Firewall/IDP ad alte prestazioni.
Cluster di bilanciatori di carico ad alte prestazioni.
Server cosolidation/virtualization.
Switch modulari a backplane passivo e completamente ridondati in ogni parte attiva.
Interconnessioni Gigabit Ethernet full-mesh.

Server Farm: Alta Disponibilità e Prestazioni

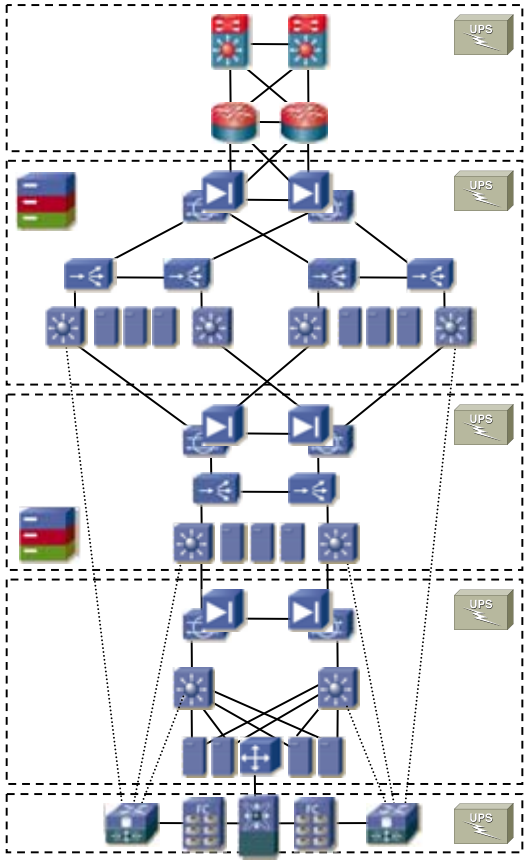


Back End Layer:
Cluster di Firewall/IDP ad alte prestazioni.
Switch modulari a backplane passivo e completamente ridondati in ogni parte attiva.
Interconnessioni Gigabit Ethernet full-mesh.
Interconnessioni Fibre Channel 4 Gbps full-mesh.

Storage Layer:
Switch Fibre Channel in HA.
Cluster SAN con doppio storage FC disk.
Interconnessioni Fibre Channel 4 Gbps full-mesh.

Server Farm: Politiche di Sicurezza

Accesso fisico: Porta blindata con ingresso tramite badge personale.



Aggregation Layer:
Layer ¾ packet filtering in hardware (ASICs).

Front End Layer:
Stateful Inspection &
Layer 7 Intrusion Prevention (IDP)
(ASICs & dedicated high-speed microprocessor).

Application Layer:
Stateful Inspection &
Layer 7 Intrusion Prevention (IDP)
(ASICs & dedicated high-speed microprocessor).

Back End Layer:
Stateful Inspection &
Layer 7 Intrusion Prevention (IDP)
(ASICs & dedicated high-speed microprocessor).

Infrastruttura di accesso

GARR Acceptable Use Policy

*"Tutti gli **utenti** a cui vengono forniti accessi alla rete Garr devono essere **riconosciuti ed identificabili**. Devono perciò essere attuate tutte le misure che impediscano l'accesso a utenti non identificati. Di norma gli utenti devono essere dipendenti del soggetto autorizzato, anche temporaneamente, all'accesso alla Rete GARR.*
Per quanto riguarda I soggetti autorizzati all'accesso alla Rete GARR (S.A.) gli utenti possono essere anche persone temporaneamente autorizzate da questi in virtù di un rapporto di lavoro a fini istituzionali. Sono utenti ammessi gli studenti regolarmente iscritti ad un corso presso un soggetto autorizzato con accesso alla Rete GARR."

Infrastruttura di accesso

Politiche di accesso

In funzione dell'utilizzo dei luoghi (sale riunioni, aule, uffici, spazi comuni...) e di fattori quali, per esempio, mobilità e nomadismo, viene fornito il tipo di connettività ritenuto più adatto allo scopo.

All'interno del tipo di connettività offerto le modalità di accesso alla rete, con l'eventuale necessità di autenticazione, e le relative autorizzazioni sono in funzione della categoria di appartenenza dell'utente.

Sistema di autenticazione centralizzato

La gestione del tipo di accesso,della identificabilità e della categoria dell'utente avviene tramite un'infrastruttura di **Autenticazione, Autorizzazione e Accounting (AAA)** con un directory server **LDAP** e una **infrastruttura a chiave pubblica (PKI)** per la generazione dei certificati personali X.509.

Infrastruttura di accesso

Politiche di Accesso: terminali fissi in rete

Terminali in rete personale strutturato o convenzionato
Indirizzo IP pubblico statico e accesso al terminale in locale tramite username e password personali *(fermo restando l'accettazione del regolamento di rete http://web1.si.unimib.it/regolamenti/).*

Terminali VoIP in rete personale strutturato o convenzionato
Indirizzo IP privato statico, VLAN "voice" e accesso al terminale in locale tramite username e password personali *(fermo restando l'accettazione del regolamento di rete http://web1.si.unimib.it/regolamenti/).*

Terminali Laboratori Didattici
Indirizzo IP privato, VLAN "LabX" e accesso al terminale tramite autenticazione su server LDAP di Ateneo o del laboratorio stesso (in funzione del roaming richiesto).

Telecamere e sistemi di allarme sistema di sicurezza di Ateneo
Indirizzo IP privato, VLAN "sicurezza", autenticazione con certificato su server dedicato con tunnelling VPLS crittografato.

Infrastruttura di accesso

Politiche di accesso: mobilità e nomadismo

Terminali mobili su rete cablata (aule, sale riunione, spazi comuni)
Accesso tramite protocollo 802.1X EAP-TLS con mutua autenticazione
tra X-supplicant e Authentication Server con certificati X.509.
Per gli utenti ***EduRoam*** il tipo di EAP dipende dall'organizzazione di origine dell'utente.

Terminali mobili su rete wireless (copertura totale dell'Ateneo)
Accesso tramite standard 802.11i; AES ed EAP-TLS con mutua autenticazione
tra X-supplicant e Authentication Server con certificati X.509.
Per gli utenti ***EduRoam*** il tipo di EAP dipende dall'organizzazione di origine dell'utente.

Terminali remoti con accesso da rete PSTN
Accesso al NAS tramite protocollo CHAP, autenticazione su protocollo Radius.

Terminali remoti con accesso da rete IP
Accesso ai concentratori VPN, TLS tunneling e autenticazione su protocollo Radius.

Infrastruttura di accesso

Tipologie di utenza e flussi di registrazione

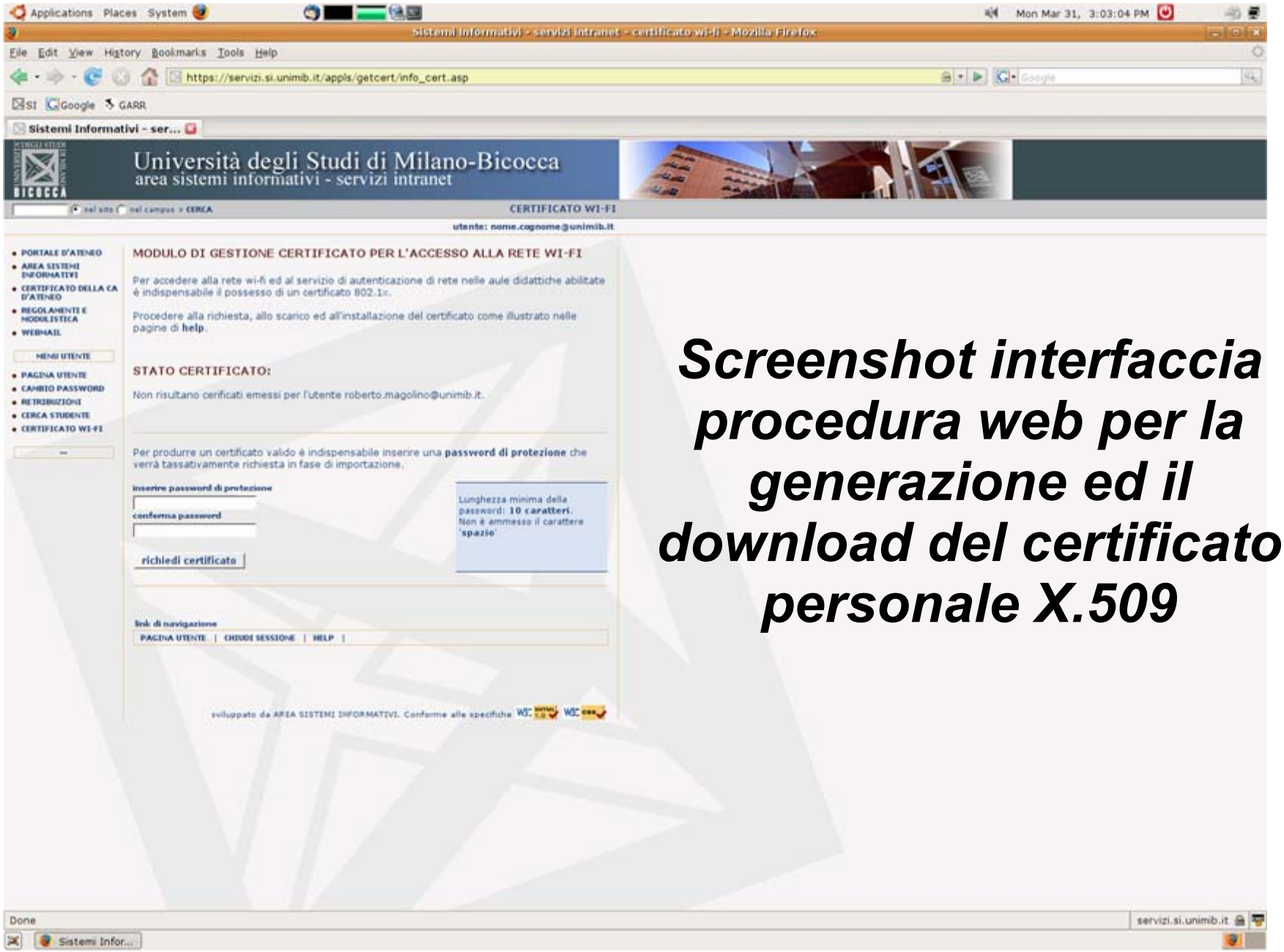
Studenti e personale strutturato: registrazione automatica (con username e password) nel sistema centralizzato di autenticazione di Ateneo al momento della immatricolazione o della presa in servizio.

Collaboratori esterni e ospiti: registrazione previa autorizzazione online del responsabile.

Ogni utente registrato nel sistema di autenticazione di Ateneo può generare e scaricare il certificato X.509 personale online, tramite procedura web su canale sicuro (https), previa autenticazione con le proprie credenziali LDAP (username e password).

Accesso per convegni e ospiti occasionali: generazione di certificati X.509, a durata limitata, tramite stessa procedura web su canale sicuro (https) da parte di utenti autorizzati.

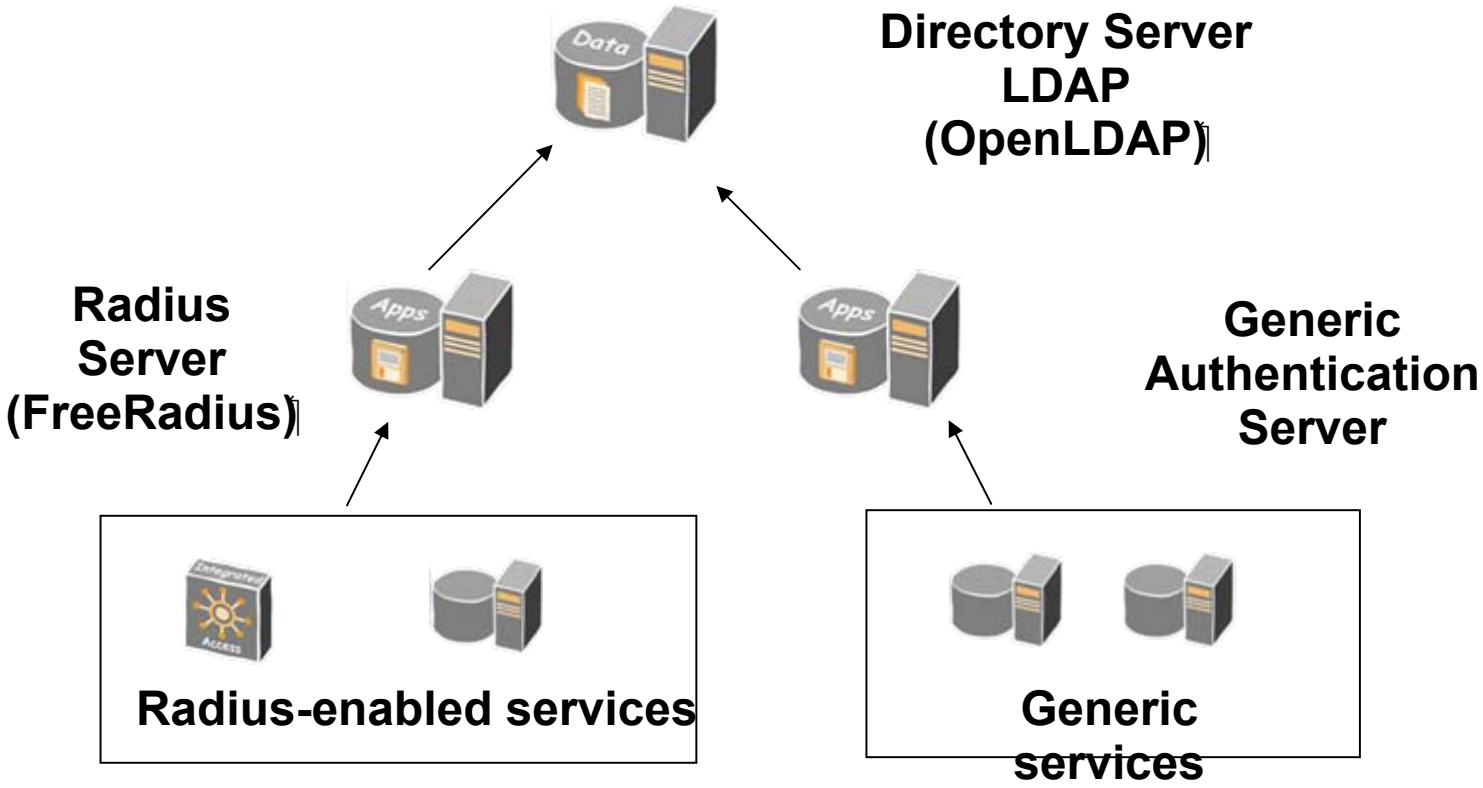
Infrastruttura di accesso



Screenshot interfaccia procedura web per la generazione ed il download del certificato personale X.509

Infrastruttura di accesso

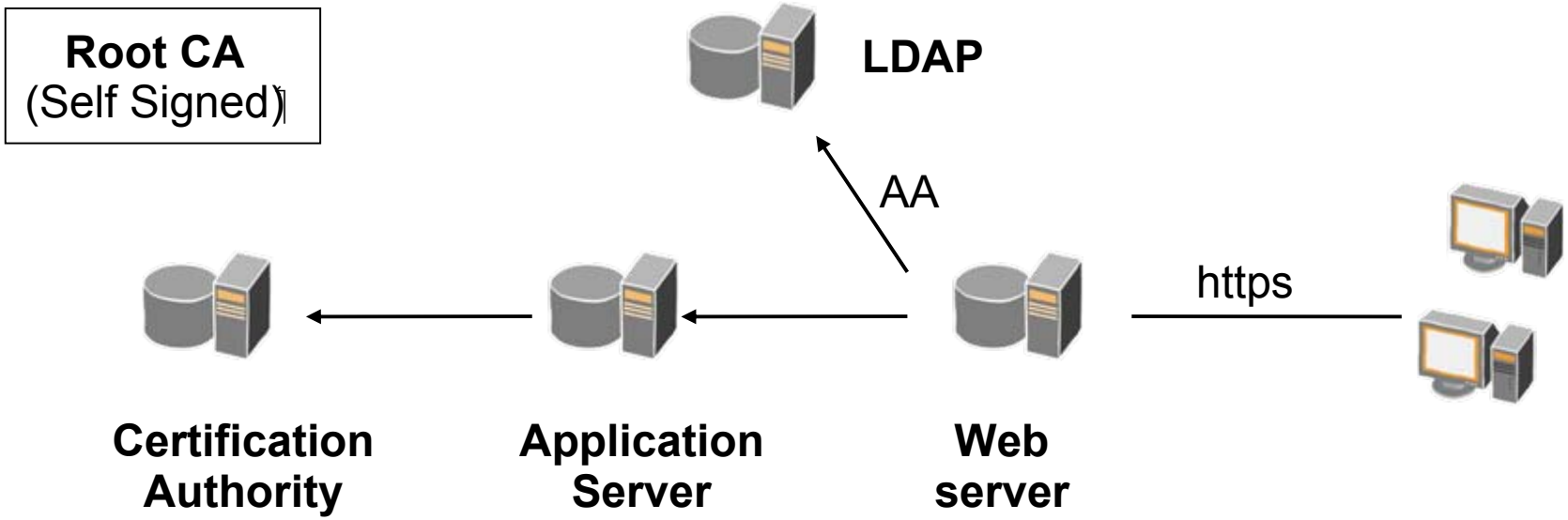
Sistema di autenticazione centralizzato di Ateneo



Le credenziali di personale, collaboratori e studenti sono immagazzinate nel "Directory Server" LDAP. Queste credenziali, sottoforma di username e password, consentono l'accesso a tutti i servizi offerti dall'Ateneo che sono LDAP-enabled.

Infrastruttura di accesso

Infrastruttura a chiave pubblica (PKI)



Generazione certificato X.509 utente registrato nel direttorio LDAP tramite procedura web su canale sicuro (https) e sotto autenticazione

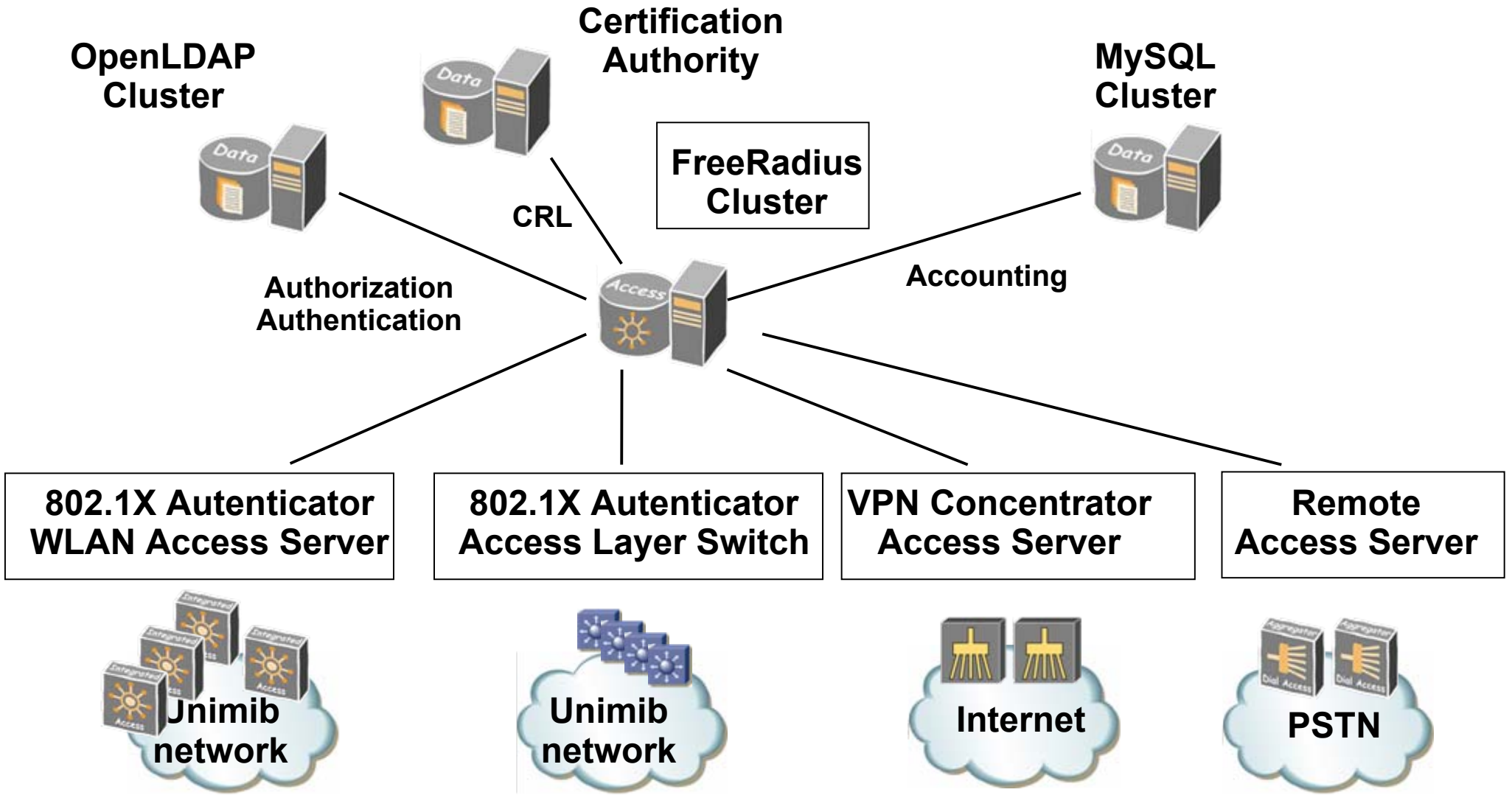
Dimensionamento CA: 32.000 Certs

Messa in produzione della PKI per l'accesso alla rete: settembre 2007

Certificati generati al 30 marzo 2008: 4.000

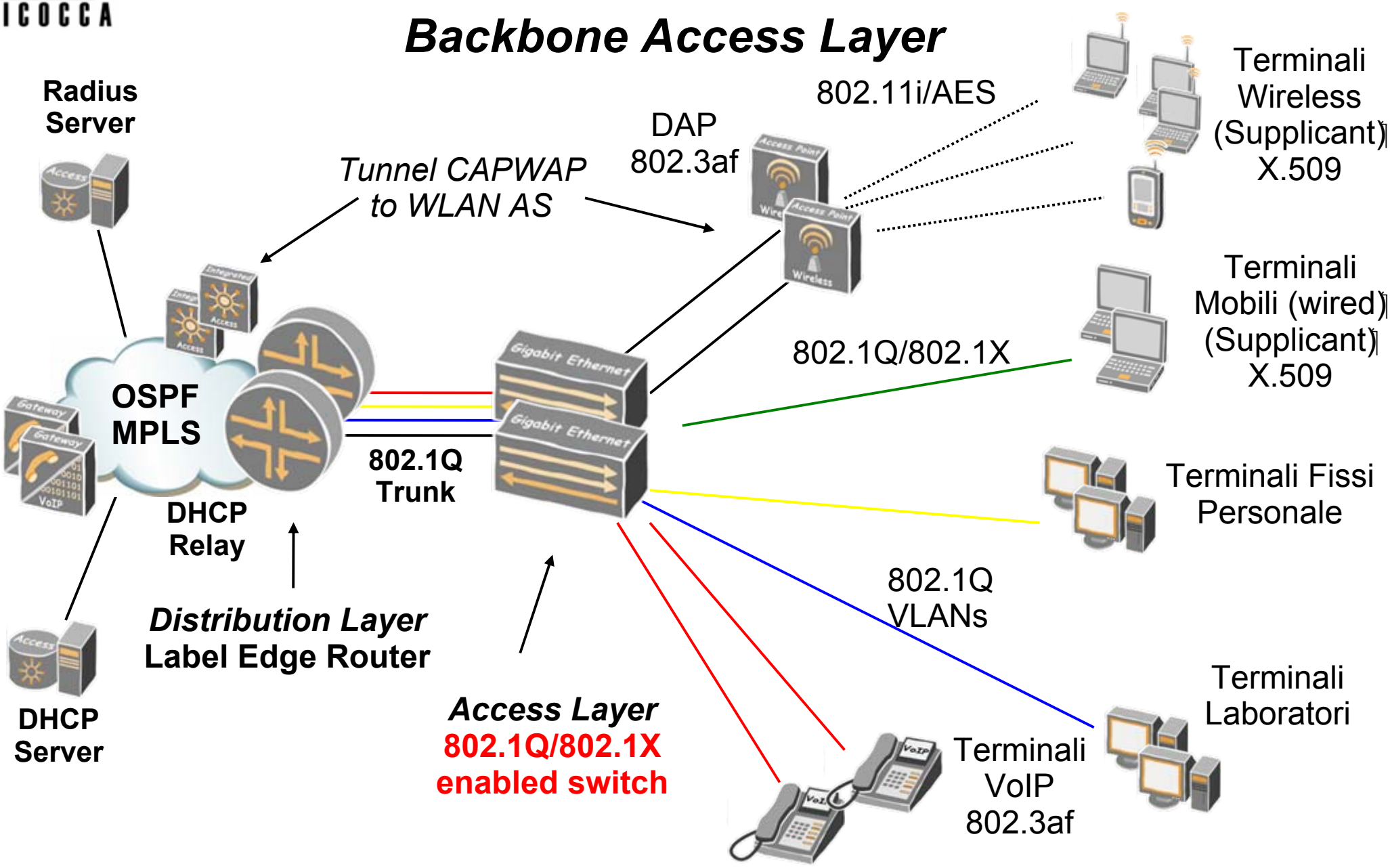
Infrastruttura di accesso

Infrastruttura AAA



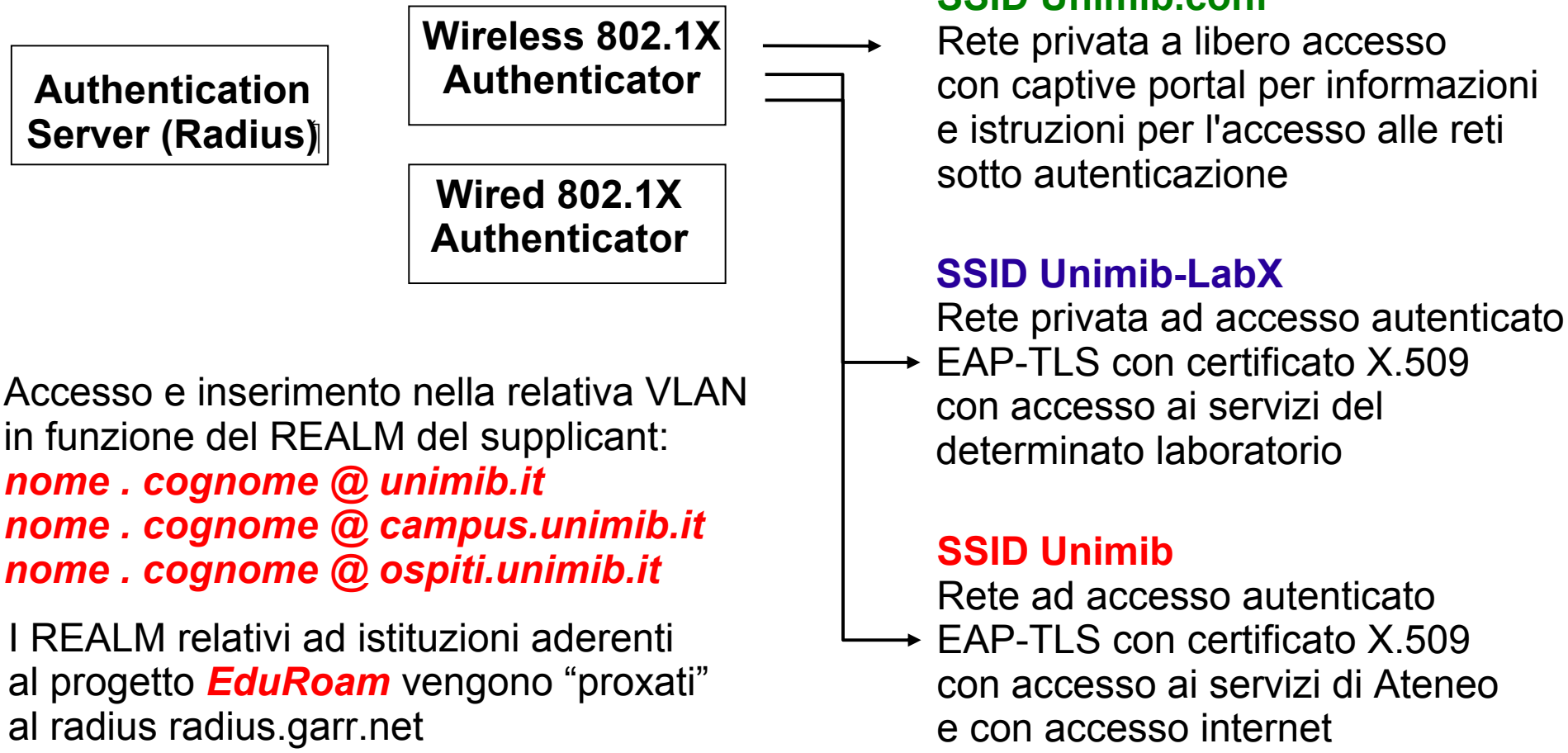
Infrastruttura di accesso

Backbone Access Layer



Infrastruttura di accesso

Logica accesso 802.1X



Accesso e inserimento nella relativa VLAN in funzione del REALM del supplicant:
nome . cognome @ unimib.it
nome . cognome @ campus.unimib.it
nome . cognome @ ospiti.unimib.it

I REALM relativi ad istituzioni aderenti al progetto ***EduRoam*** vengono “proxati” al radius radius.garr.net

Assegnata la VLAN il supplicant emette una DHCP request che viene raccolta ed inoltrata al server DHCP dal Relay Agent della VLAN

Infrastruttura di accesso

Autentication Server: Radius

 # FreeRadius users file (page 1)
Accesso wifi
Nella fase di autorizzazione viene verificato, in sequenza, che:
1) la modalita' di autenticazione del supplicant sia EAP (Default = TLS)
2) il NAS di provenienza appartenga allo huntgroup WirelessNAS relativo ai NAS WiFI.
3) il Realm estratto dal nome utente sia autorizzato
4) l'utente appartenga al gruppo degli utenti autorizzati ad utilizzare il servizio (verifica affettuata via LDAPS)
5) l'utente non sia gia' collegato con un'altra macchina

Passata la fase di autorizzazione inizia la fase di autenticazione via EAP-TLS, durante la quale viene
innanzitutto verificata la validita' del certificato contro la CRL piu' recente, aggiornata a intervalli di 1 ora.
Se l'autenticazione e' terminata con successo si passa alla fase di accounting che va a scrivere sul database
MySQL i dati salienti relativi alla connessione, incluso l'ID dell'access point (e la relativa porta logica)
sul quale e' attestato il supplicant
Infine viene inviato il pacchetto EAP Access Accept che tra i Reply-Items contiene Trapeze-VLAN-Name,
l'attributo che determina la VLAN di destinazione del Supplicant.
L'elemento discriminante per la VLAN di destinazione e' il Realm.

DEFAULT Auth-Type := Eap, Service-Type == Framed-User, Huntgroup-Name == "WirelessNAS", Realm == "**campus.unimib.it**",Ldap-Group == "wifi", Simultaneous-Use := 1, Trapeze-VLAN-Name = **Student-vlan**
DEFAULT Auth-Type := Eap, Service-Type == Framed-User, Huntgroup-Name == "WirelessNAS", Realm == "unimib.it",Ldap-Group == "wifi", Simultaneous-Use := 1,Trapeze-VLAN-Name = **Personnel-vlan**
DEFAULT Auth-Type := Eap, Service-Type == Framed-User, Huntgroup-Name == "WirelessNAS", Realm == "ospiti.unimib.it",Simultaneous-Use := 1, Ldap-Group == "wifi", Trapeze-VLAN-Name = **Guest-vlan**

Infrastruttura di accesso

Autentication Server: Radius

```
# FreeRadius users file (page 2)
# Accesso 802.1X Wired
# L'accesso 802.1X Wired effettua la fase di autorizzazione verificando gli stessi parametri del accesso
# wireless, con le ovvie differenze relative agli huntgroups.
# In questo caso viene controllata l'appartenenza al gruppo LDAP 802.1xwired. Anche in questo caso
# l'autenticazione e' EAP-TLs con verifica della validita' dei certificati contro la CRL aggiornata.
# I NAS wired consentono di specificare tra i Reply-Items l'attributo Framed-Filter-Id relativo
# alla porta fisica dello switch sulla quale e' attestato il supplicant. Questo attributo indica quale policy e quindi
# quali ACL verranno applicate al supplicant  per la durata della sessione.

DEFAULT Auth-Type := Eap, Huntgroup-Name == "Wired", Realm == "unimib.it", Ldap-Group ==
"802.1xwired", Simultaneous-Use := 1, Framed-Filter-Id = "Vendor:version=1:policy=xwired"
DEFAULT Auth-Type := Eap, Huntgroup-Name == "Wired", Realm == "ospiti.unimib.it", Simultaneous-Use :=
1,Ldap-Group == "802.1xwired", Framed-Filter-Id = "Vendor:version=1:policy=xwired"

# Autorizzazione e autenticazione degli utenti Dialup (normali e callback) contro LDAP (protocollo CHAP)
DEFAULT Autz-Type := LDAP
        Fall-Through = yes
DEFAULT Huntgroup-Name == "RAS", Ldap-Group == "callback",
User-Profile := "cn=pppcb,ou=profili,dc=unimib,dc=it", Simultaneous-Use := 2
DEFAULT Huntgroup-Name == "RAS", Ldap-Group == "ras", ser-Profile := "cn=ppp,ou=profili,dc=unimib,dc=it"

# Autorizzazione e autenticazione degli utenti VPN concentrator contro LDAP
DEFAULT Huntgroup-Name == "VPN", Realm == "unimib.it", Ldap-Group == "vpn", Simultaneous-Use := 1
```

Infrastruttura di accesso

Autentication Server: Radius

 # FreeRadius users file (page 3)
 # EDUROAM

```
# Nel caso di Eduroam il realm non e' noto a priori, quindi viene matchato il valore di DEFAULT:
# tutto cio' che non e' altrimenti definito.
# In questo caso, il dialogo EAP viene proxato verso radius.garr.net (come specificato su proxy.conf)
# dopo la prima breve fase di autorizzazione locale che consiste nella verifica degli huntgroups
# e del tipo di autenticazione (EAP).
# Sussiste tuttavia una differenza fondamentale:
# non viene specificata a priori la VLAN di destinazione: questa verra' forzata a piu' alto livello dai NAS.
# Nel caso Wired viene comunque specificata la policy da applicare al Supplicant.

DEFAULT Auth-Type := Eap, Realm == DEFAULT, Huntgroup-Name == "WirelessNAS", Simultaneous-Use :=
1
DEFAULT Auth-Type := Eap, Realm == DEFAULT, Huntgroup-Name == "Wired", Simultaneous-Use := 1
      Framed-Filter-Id = "Enterasys:version=1:policy=xwired"

DEFAULT Auth-Type := Reject
       Reply-Message = "Access Denied"
```

Infrastruttura di accesso

Autentication Server: Radius

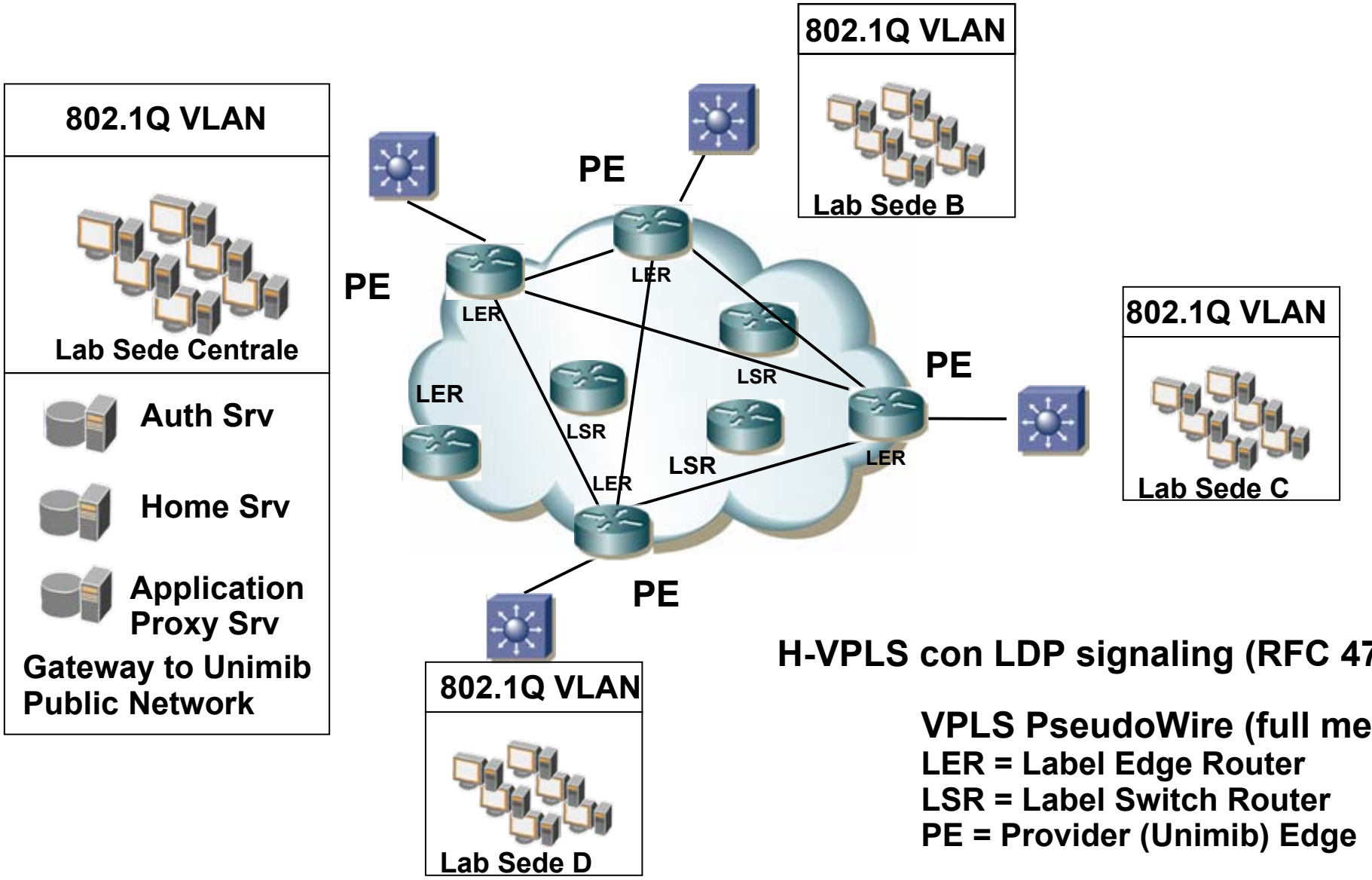
 # FreeRadius huntgroups file

VPN	NAS-IP-Address == 10.100.0.1
RAS	NAS-IP-Address == 10.0.0.1
RAS	NAS-IP-Address == 10.0.0.2
Wired	NAS-IP-Address == 10.10.1.200
Wired	NAS-IP-Address == 10.10.2.200
.....	.....
Wired	NAS-IP-Address == 10.10.250.200
Wired	NAS-IP-Address == 10.10.251.200
WirelessNAS	**NAS-IP-Address == radius.garr.net**
WirelessNAS	NAS-IP-Address == 10.20.0.200
.....	.....
WirelessNAS	NAS-IP-Address == 10.20.1.200
WirelessNAS	NAS-IP-Address == 10.20.2.200

Il radius garr è **NAS per gli utenti Unimib-EduRoam**

Infrastruttura di accesso

Laboratori/Biblioteche/Enti convenzionati



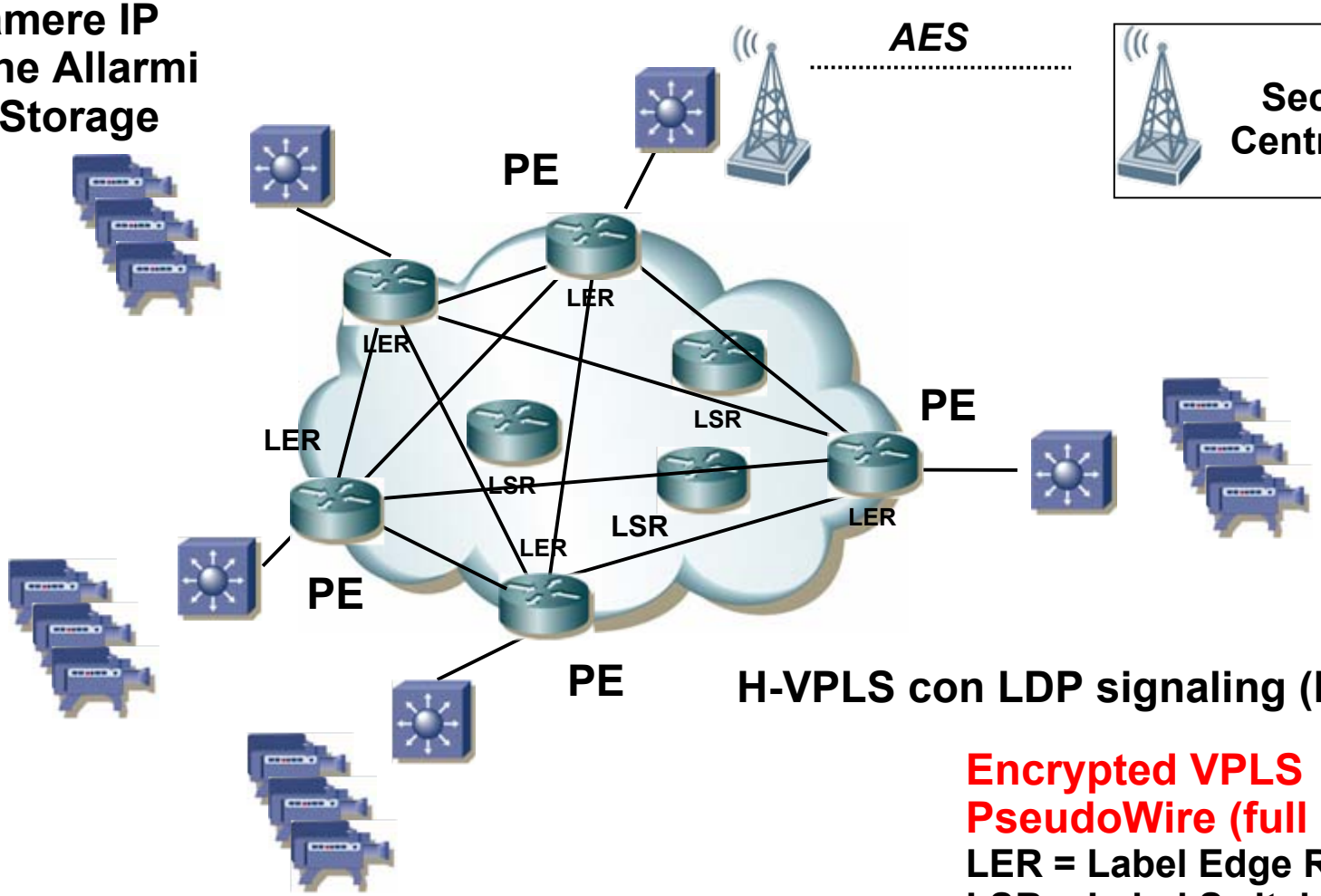
H-VPLS con LDP signaling (RFC 4762)

VPLS PseudoWire (full mesh)
LER = Label Edge Router
LSR = Label Switch Router
PE = Provider (Unimib) Edge

Infrastruttura di accesso

Rete Sistema di Sicurezza

Security:
Telecamere IP
Centraline Allarmi
Video Storage



H-VPLS con LDP signaling (RFC 4762)

Encrypted VPLS
PseudoWire (full mesh)
LER = Label Edge Router
LSR = Label Switch Router
PE = Provider (Unimib) Edge

Infrastruttura di monitoraggio

Schema flusso implementativo

Definizione di traffico permesso e di una politica di sicurezza

Analisi e definizione comportamenti anomali e/o sospetti nel traffico di rete

Assegnazione di pattern comportamentali a questi flussi anomali

Scrittura delle regole descriventi i pattern assegnati negli ASICs degli apparati.

Definizione delle azioni conseguenti al pattern matching:

- deny del traffico
- caricamento dinamico di ACL per il deny o il rate limiting
- mirroring verso rete di monitoraggio per analisi di livello superiore
- esportazione dei flussi sottoforma di “x”Flow.

Infrastruttura di monitoraggio

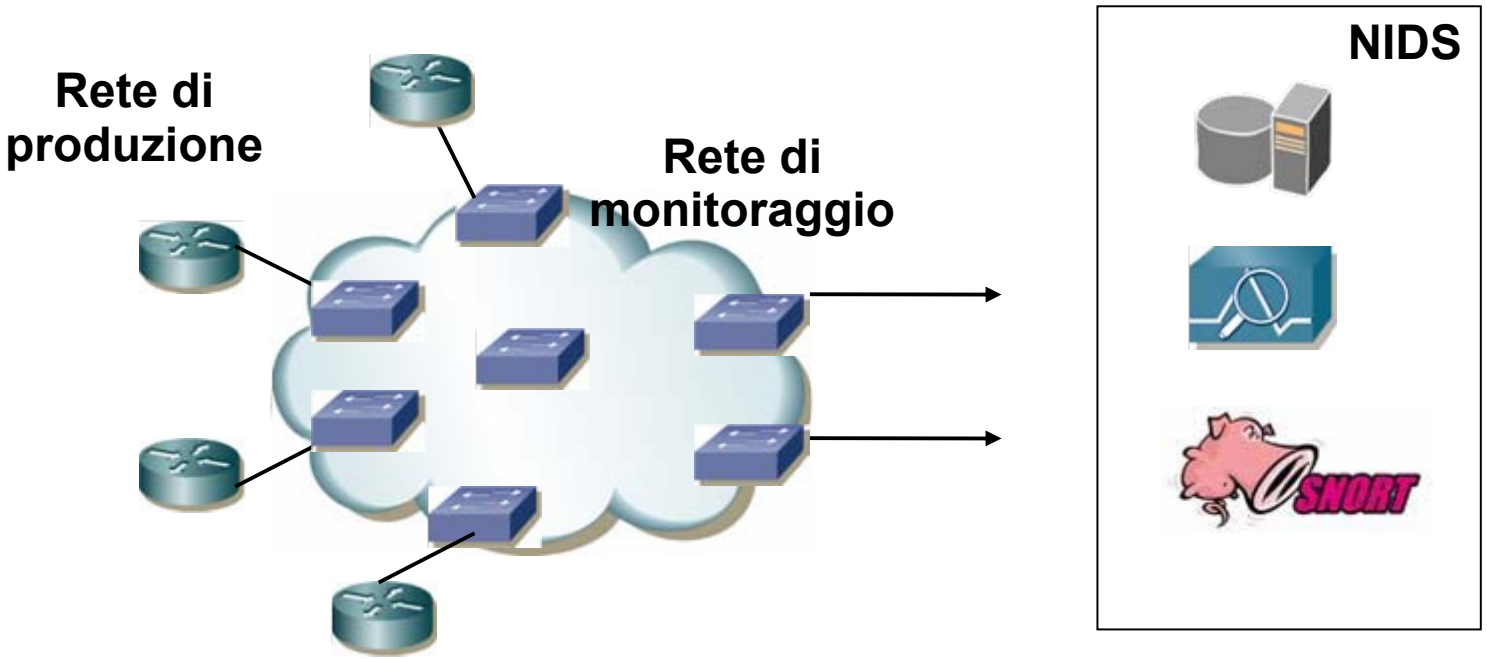
Tutte le **politiche** di traffic shaping, traffic filtering e traffic sampling/mirroring sono implementate negli ASICs dei nodi del **livello di distribuzione**.
Ogni azione è basata su una policy e la struttura del linguaggio, utilizzando **logica condizionale**, permette la configurazione di **politiche complesse**.
Il supporto del linguaggio condizionale e la dotazione di ASICs tali da permettere l'implementazione in hardware di policy complesse, rendono possibile lo spostamento di una parte della logica di monitoraggio sugli apparati di backbone.
Questo screening consente l'inoltro verso la rete di monitoraggio dei **soli flussi di traffico sospetti** rendendo più efficiente l'attività dei NIDS che possono focalizzare la loro analisi su dati già selezionati e a minore throughput.

Ogni apparato di backbone (apparati WAN compresi) è equipaggiato, oltre ai vari syslog, SNMP agent, RMON, con un sistema di collezione ed esportazione dei flussi di traffico (cFlow/IPFIX/jFlow/NetFlow/sFlow in funzione del vendor).

Ulteriore funzionalità implementata sugli apparati è la possibilità di definire dei **contatori a soglia** (trigger) scatenanti determinate azioni.

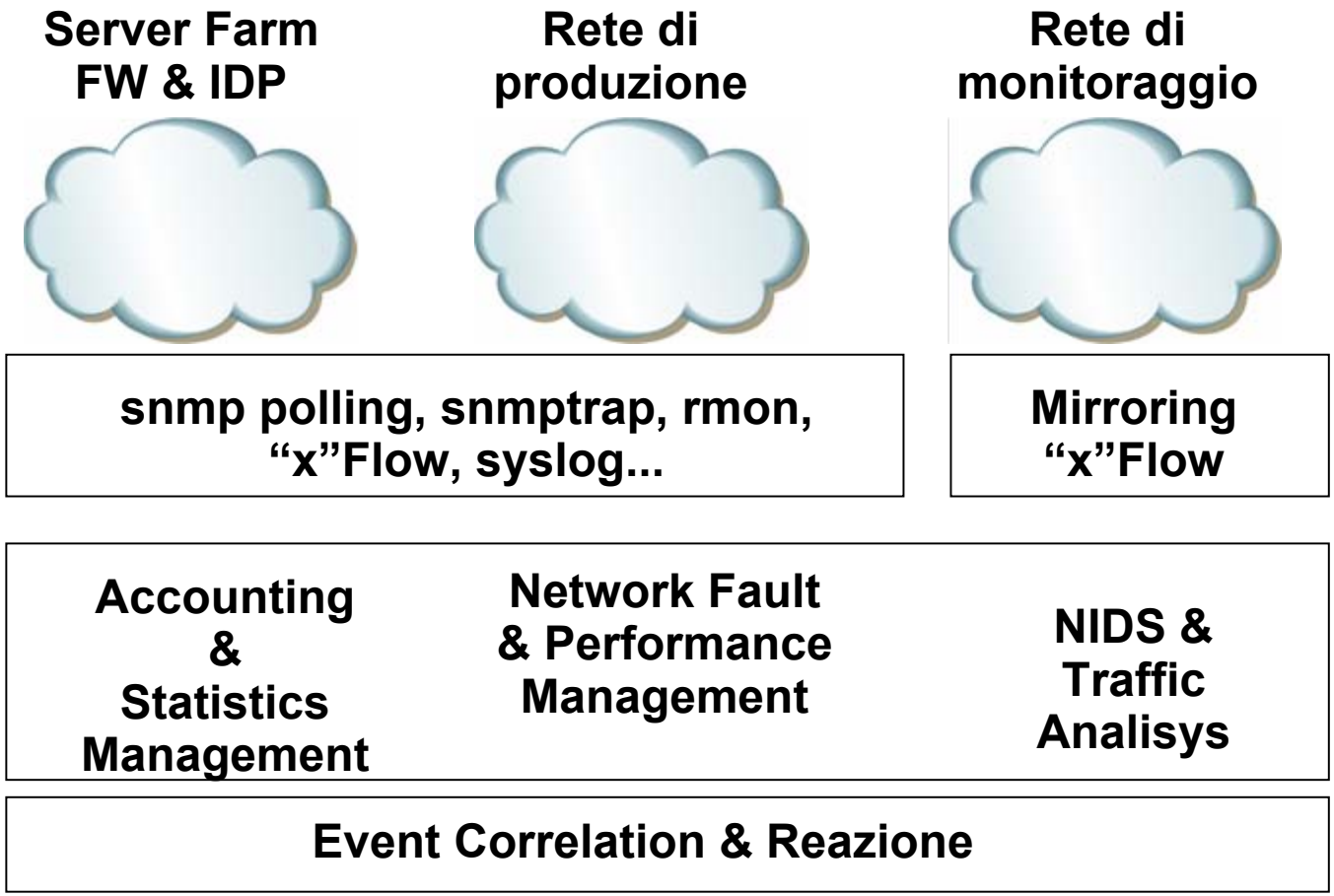
Infrastruttura di monitoraggio

Su ogni nodo di Core e Distribution backbone è configurata una interfaccia Gigabit Ethernet connessa ad uno switch facente parte della rete di monitoraggio parallela che utilizza **collegamenti dedicati**.



A questa rete sono collegati i vari sistemi NIDS che raccolgono i flussi di mirroring e sampling per l'analisi del traffico sospetto.

Infrastruttura di monitoraggio – a blocchi



Grazie dell'attenzione