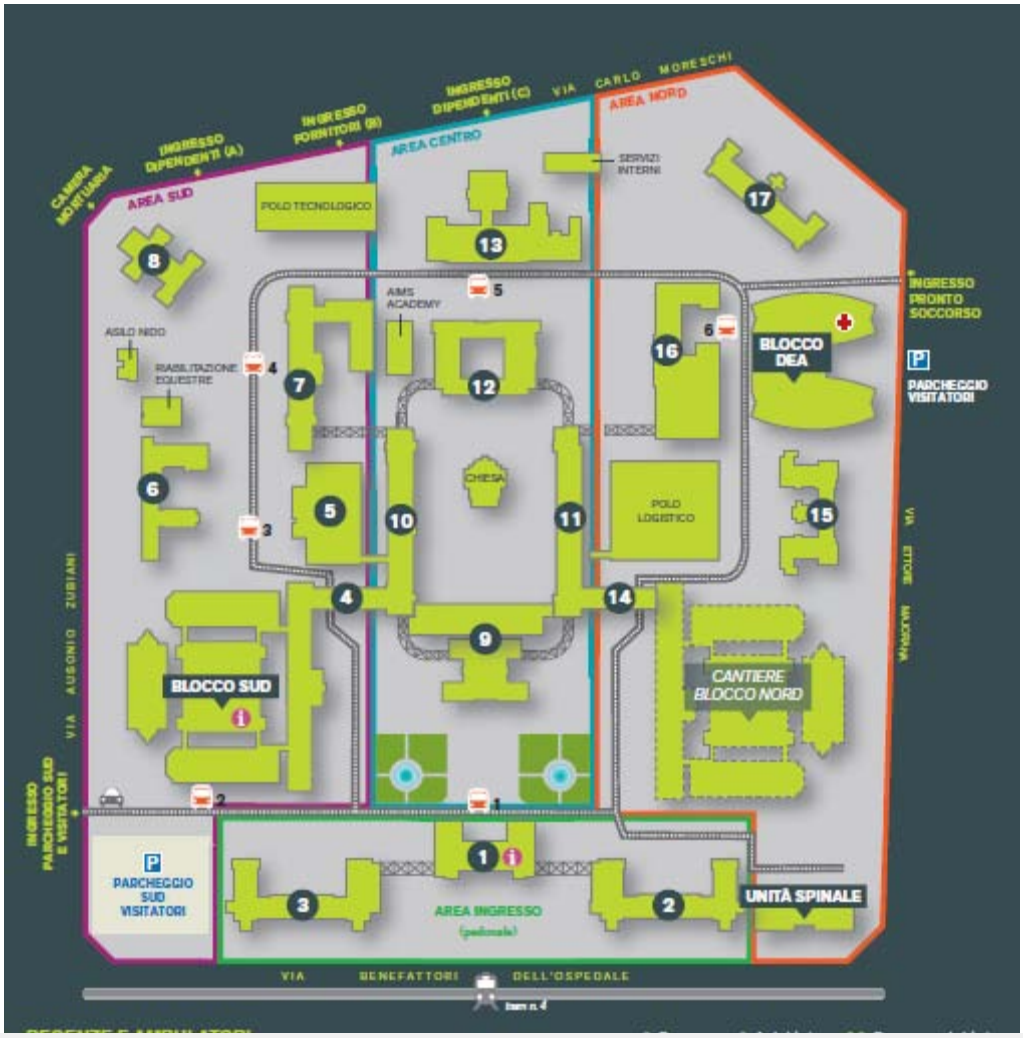
Azienda Ospedaliera
Ospedale Niguarda Ca' Granda

Allegato 1A - Allegato Tecnico NIG

1. DESCRIZIONE GENERALE

L'Azienda Ospedaliera Ospedale Niguarda Cà Granda (di seguto indicata come Ente) e' costituita da un Campus il cui ingresso principale e' in Piazza dell'Ospedale Maggiore 3, e da 12 Sedi Remote il cui dettagli e0 riportato nella sezione 1.3.

Ai fini di una piu' corretta comprensione della struttura del Campus Niguarda, si allega qui di seguito la mappa dei padiglioni con l'indicazione dei due nuovi Blocchi Ospedalieri: Blocco Nord e Blocco Sud:



1.1. SCHEMA GENERALE DELLA RETE

Lo Schema generale della rete Niguarda e' riportato in Fig. 1; i0 blocchi logici rappresentano quanto segue:

- **Inside** area degli utenti interni del comprensorio Niguarda (INSIDE Campus Niguarda) e delle sedi remote (INSIDE Sedi Remote). L'INSIDE Campus Niguarda e' collegata alle Sedi Remote via WAN MPLS Fastweb tramite Router dedicati.
- **Server Farm** area dei server ad uso interno
- **Imalan**: area dei Server delle immagini radiografiche, in gestione a AGFA (fornitore dell'area imaging),
- **Server (nuova DMZ)** area dei server accessibili da Internet (Web server, e altri server)
- **DMZ**: appliance con necessità di IP Pubblico diretto (Es.Appliance SSL di acceso remoto alle risorse interne per i fornitori o medici)
- **Remoteria**:
  - Area di accesso dei fornitori e manutentori tramite router dedicati
  - Area di accesso da e per alcuni servizi esterni specializzati.

  SISS: rete esterna, in gestione a Lombardia Informatica per il servizio SISS
- **Outside**: accesso Internet

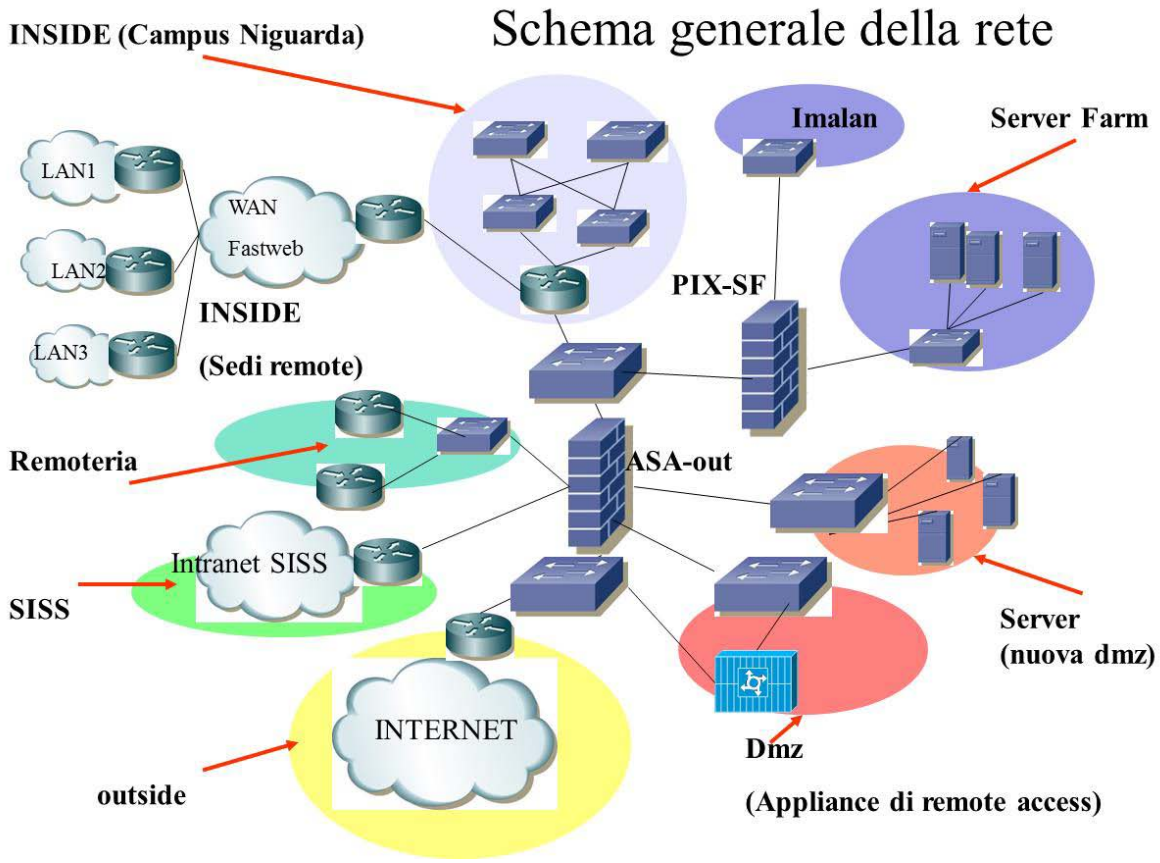


Fig. 1 - Schema Generale della Rete A.O. Niguarda

1.2. ARCHITETTURA DELLA RETE INSIDE

La rete di distribuzione Inside del Campus e' costituita da 8 Switch Cisco WS-C6509 con collegamenti ridondati tra di loro in Fibra Ottica a 1Gb, come da figura seguente:

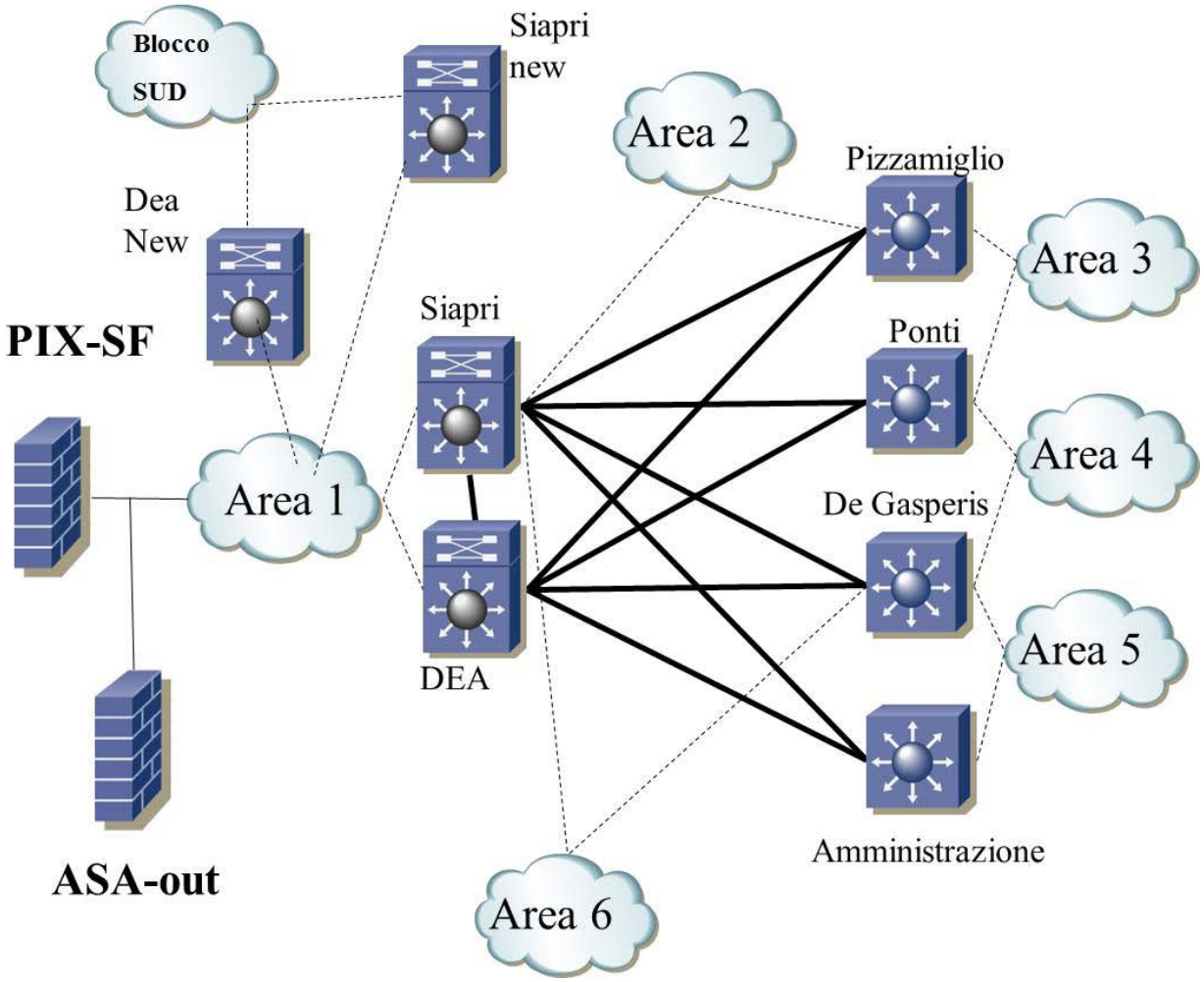


Fig. 2 Schema Layer 2 della rete Inside Campus

1.2.1. Architettura Blocco SUD

L'architettura di distribuzione della rete del Blocco SUD e' autonoma e costituita da 10 Switch Cisco WS-C6509 interconnessi al resto della rete Campus tramite protocollo OSPF.

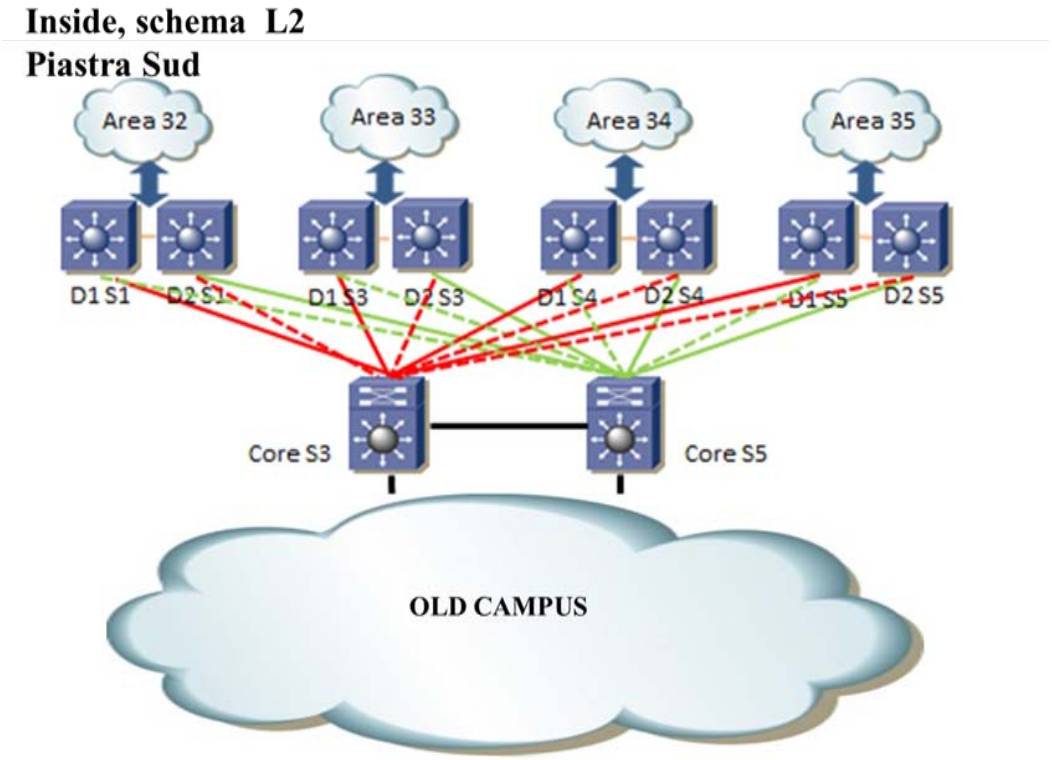


Fig. 3 – Schema Layer 2 Piastra Sud.

1.2.2. Collegamenti di Area (livello di accesso)

Gli utenti accedono alla rete tramite collegamenti a Switch (Cisco 3750, 3650, etc.) interni alle singole Aree; ogni switch ha collegamenti ridondati ad una coppia di switch 6509 di riferimento.

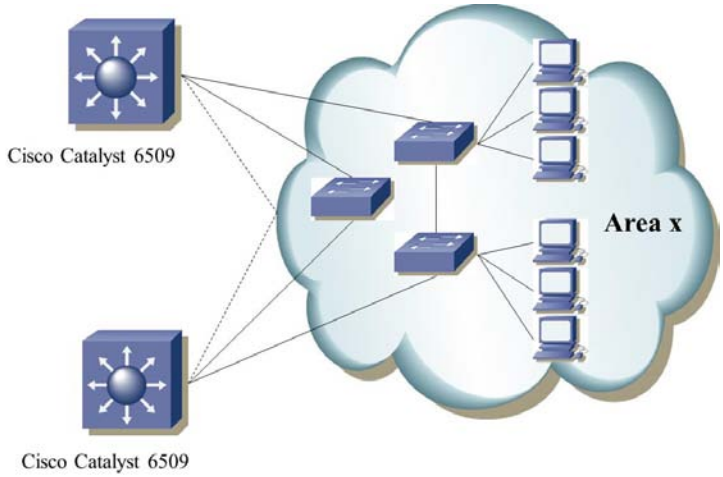


Fig. 4 Schema di dettaglio dei collegamenti interni di Area

1.2.3. Ridondanza di Area

Le coppie di router denominate:

- Siapri e DEA,
- D1S1 e D2S1,
- D1S3 e D2S3,
- D1S4 e D2S4,
- D1S5 e D2S5

sono configurati in modalità ridondata tramite protocollo HSRP per la gestione delle vlan ad essi afferenti, come da schema di seguito riportato:

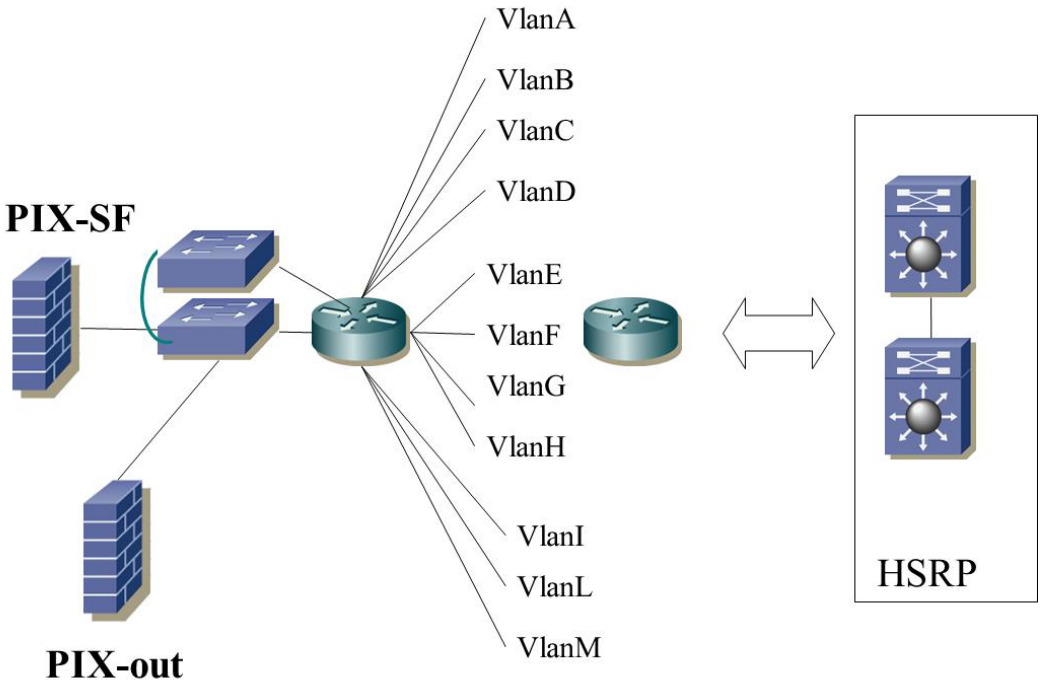


Fig. 5 Schema Layer 3 di Campus

1.3. SEDI SEDI REMOTE:

I distaccamenti Niguarda sono collegati alla rete Campus tramite MPLS fornita da Fastweb; nella tabelal seguente l'elenco delle sedi remote e la tipologia di collegamento:

Sede Remota	Indirizzo	Città	Servizio	Tecnologia	Banda
CRA PLEBISCITI	C. PLEBISCITI 6	Milano	VPN	SHDSL	4.000
AVIS LAMBRATE	LARGO VOLONTARI DEL SANGUE 1	Milano	VPN	FO	4.000
	LARGO VOLONTARI DEL SANGUE 1	Milano	VPN BACKUP MA STANDARD	CVP	4.096
CPS LIVIGNO	V. LIVIGNO 3	Milano	VPN	SHDSL	4.000
CPS RUFO	V. PUBLIO RUTILIO RUFO 8	Milano	VPN	FO	10.000
	V. PUBLIO RUTILIO RUFO 8	Milano	VPN BACKUP MA STANDARD	FO	10.000
CORSICO	V. TRAVAGLIA 5	Corsico	VPN	CVP	4.000
CPS CHERASCO	VIA CHERASCO 7	Milano	VPN	FO	4.000
FARINI	VIA FARINI 9	Milano	VPN	FO	4.000
	VIA FARINI 9	Milano	VPN BACKUP MA STANDARD	SHDSL	4.000
IPPOCRATE	VIA IPPOCRATE 45	Milano	VPN	FO	10.000
	VIA IPPOCRATE 45	Milano	VPN BACKUP MA STANDARD	FO	10.000
CPS MARIO BIANCO	VIA MARIO BIANCO 12	Milano	VPN	SHDSL	4.000
CPS CINISELLO	VIA SALA 22	Cinisello	VPN	SHDSL	8.000
CPS ANGERA	VIA. ANGERA 3	Milano	VPN	FO	10.000
	VIA. ANGERA 3	Milano	VPN BACKUP MA STANDARD	FO	10.000
VILLA MARELLI	VIALE ZARA 81	Milano	VPN	FO	10.000
	VIALE ZARA 81	Milano	VPN BACKUP MA STANDARD	FO	10.000

2. INFRASTRUTTURA DI RETE

Di seguito sono descritte le componenti salienti dell'infrastruttura di rete.

2.1. CENTRO STELLA.

Il livello di core è gestito da 6 Cisco Catalyst 6509, configurati a livello HW in modi differenti:

1. Due Catalyst 6509 (Siapri e Dea), gestiscono il protocollo HSRP per la ridondanza delle reti di Campus, il protocollo NTP e la creazione di Vlan nel dominio VTP "Campus".
2. Quattro Cisco Catalyst 6509 (Siapri NEW, Dea NEW, Core S3, Core S5), gestiscono il protocollo di routing OSPF, il protocollo NTP.

La creazione delle VLAN nell'area Campus utilizza un VTP Domain, mentre nell'area Piastra Sud gli switch sono configurati in modalità Transparent e pertanto lla creazione di Vlan è a livello locale.

Si riporta qui di seguito il dettaglio delle configurazioni Hw dei Catalist:

6509_dea	6509_Siapri	NSUD-6509-03_1C
WS-X6K-SUP1A-2GE	WS-X6K-SUP1A-2GE	WS-X6708-10GE
WS-F6K-MSFC2	WS-F6K-MSFC2	WS-X6708-10GE
WS-X6K-SUP1A-2GE	WS-X6K-SUP1A-2GE	VS-S720-10G
WS-F6K-MSFC2	WS-F6K-MSFC2	WS-F6700-DFC3C
WS-X6324-100FX-MM	WS-X6324-100FX-MM	WS-F6700-DFC3C
WS-X6416-GBIC	WS-X6408-GBIC	VS-F6K-PFC3C
WS-X6416-GBIC	WS-X6416-GBIC	VS-F6K-MSFC3
WS-F6K-PFC	WS-X6416-GBIC	
WS-F6K-PFC	WS-F6K-PFC	
	WS-F6K-PFC	

NSUD-6509-05_1C	NSUD-6509-Siapri New	NSUD-6509-Dea New
WS-X6708-10GE	WS-X6708-10GE	WS-X6708-10GE
WS-X6708-10GE	WS-X6708-10GE	WS-X6708-10GE
VS-S720-10G	VS-S720-10G	VS-S720-10G
WS-F6700-DFC3C	WS-F6700-DFC3C	WS-F6700-DFC3C
WS-F6700-DFC3C	WS-F6700-DFC3C	WS-F6700-DFC3C
VS-F6K-PFC3C	VS-F6K-PFC3C	VS-F6K-PFC3C
VS-F6K-MSFC3	VS-F6K-MSFC3	VS-F6K-MSFC3

2.2. LIVELLO DI DISTRIBUZIONE.

Al livello di distribuzione lavorano 12 Cisco Catalyst 6509, configurati a coppie in ridondanza. I Catalyst 6509 di Piastra Sud gestiscono il protocollo HSRP per ogni singola area.

Si riporta qui di seguito al configurazione Hw di ogni Catalist:

6509_Amministrazione	6509_Degasperis	6509_Pizzamiglio	6509_Ponti
WS-X6K-SUP1A-2GE	WS-X6K-SUP1A-2GE	WS-X6K-SUP1A-2GE	WS-X6K-SUP1A-2GE
WS-F6K-MSFC2	WS-F6K-MSFC2	WS-X6324-100FX-MM	WS-F6K-MSFC2
WS-X6416-GBIC	WS-X6416-GBIC	WS-X6408A-GBIC	WS-X6408A-GBIC
WS-F6K-PFC	WS-X6416-GBIC	WS-X6416-GBIC	WS-X6416-GBIC
	WS-X6324-100FX-MM	WS-F6K-PFC	WS-F6K-PFC
	WS-F6K-PFC		

NSUD-6509-01_1D	NSUD-6509-01_2D	NSUD-6509-03_1D	NSUD-6509-03_2D
WS-X6708-10GE	WS-X6708-10GE	WS-X6708-10GE	WS-X6708-10GE
WS-X6708-10GE	WS-X6708-10GE	WS-X6708-10GE	WS-X6708-10GE
WS-X6708-10GE	WS-X6708-10GE	WS-X6708-10GE	WS-X6708-10GE
VS-S720-10G	VS-S720-10G	WS-X6716-10GE	WS-X6716-10GE
WS-F6700-DFC3C	WS-F6700-DFC3C	VS-S720-10G	VS-S720-10G
WS-F6700-DFC3C	WS-F6700-DFC3C	WS-F6700-DFC3C	WS-F6700-DFC3C
WS-F6700-DFC3C	WS-F6700-DFC3C	WS-F6700-DFC3C	WS-F6700-DFC3C
VS-F6K-PFC3C	VS-F6K-PFC3C	WS-F6700-DFC3C	WS-F6700-DFC3C
VS-F6K-MSFC3	VS-F6K-MSFC3	WS-F6700-DFC3C	WS-F6700-DFC3C
		VS-F6K-PFC3C	VS-F6K-PFC3C
		VS-F6K-MSFC3	VS-F6K-MSFC3

NSUD-6509-04_1D	NSUD-6509-04_2D	NSUD-6509-05_1D	NSUD-6509-05_2D
WS-X6708-10GE	WS-X6708-10GE	WS-X6708-10GE	WS-X6708-10GE
WS-X6708-10GE	WS-X6708-10GE	WS-X6708-10GE	WS-X6708-10GE
WS-X6708-10GE	WS-X6708-10GE	WS-X6708-10GE	WS-X6708-10GE
VS-S720-10G	VS-S720-10G	VS-S720-10G	VS-S720-10G
WS-F6700-DFC3C	WS-F6700-DFC3C	WS-F6700-DFC3C	WS-F6700-DFC3C
WS-F6700-DFC3C	WS-F6700-DFC3C	WS-F6700-DFC3C	WS-F6700-DFC3C
WS-F6700-DFC3C	WS-F6700-DFC3C	WS-F6700-DFC3C	WS-F6700-DFC3C
VS-F6K-PFC3C	VS-F6K-PFC3C	VS-F6K-PFC3C	VS-F6K-PFC3C
VS-F6K-MSFC3	VS-F6K-MSFC3	VS-F6K-MSFC3	VS-F6K-MSFC3

Si riporta qui di seguito la tabella con il livello di maintenance Cisco smartnet per i catalyst di cui sopra.
Si precisa che e' in previsione di acquisire nel 2014 un lotto di 6 catalyst in sostituzione dei vecchi apparati non piu' coperti da smartnet. **Si precisa altresi' che i nuovi apparati verranno acquisiti con servizio Smartnet della durata di 5 anni.**

Apparato	Smartnet
6509_Amministrazione	NO
6509_Degasperis	NO
6509_Pizzamiglio	NO
6509_Ponti	NO
6509_dea	NO
6509_Siapri	NO
NSUD-6509-01_1D	14/01/2015
NSUD-6509-01_2D	14/01/2015
NSUD-6509-03_1D	14/01/2015
NSUD-6509-03_2D	14/01/2015
NSUD-6509-04_1D	14/01/2015
NSUD-6509-04_2D	14/01/2015
NSUD-6509-05_1D	14/01/2015
NSUD-6509-05_2D	14/01/2015
NSUD-6509-03_1C	14/01/2015
NSUD-6509-05_1C	14/01/2015
NSUD-6509-Siapri New	14/01/2015
NSUD-6509-Dea New	14/01/2015

2.3. LIVELLO DI ACCESSO.

L'accesso degli utenti finali alla rete avviene attraverso Cisco Catalyst di varia tipologia secondo la seguente tabella, che comprende anche gli switch delle sedi remote.

Tipologia	Modello	QTY	Manutenzione attiva
Switch Accesso	WS-C1924	1	NO
Switch Accesso	WS-C2924MXL	7	NO
Switch Accesso	WS-C2924XL-LRE	2	NO
Switch Accesso	WS-C2950-24	9	NO
Switch Accesso	WS-C2950-24SX	4	NO
Switch Accesso	WS-C2960G-24TC-L	2	NO
Switch Accesso	WS-C3524XL	8	NO
Switch Accesso	WS-C3548XL	2	NO
Switch Accesso	WS-C3550-24	13	NO
Switch Accesso	WS-C3550-48	3	NO
Switch Accesso	WS-C3560-24PS	4	NO
Switch Accesso	WS-C3560-24TS	12	NO
Switch Accesso	WS-C3560-48PS	4	NO
Switch Accesso	WS-C3560-48TS	6	NO

Switch Accesso	WS-C3750G-48PS	1	NO
Switch Accesso	WS-C3750G-48TS	1	NO
Switch Accesso	WS-C3750G-24TS	4	NO
Switch Accesso	WS-C3750G-12S	8	NO
Switch Accesso	WS-C3750G-24TS-1U	2	NO
Switch Accesso	WS-C3750X-24P	58	09-giu-17
Switch Accesso	WS-C3750E-24PD	251	14-dic-15

Si precisa che e' in corso un piano di dismissione degli switch fuori garanzia entro il primo anno di vigenza contrattuale.

Cio' avverrà sia tramite lo spostamento di interi reparti verso il nuovo Blocco Nord (vedi cap. 7.5), sia tramite sostituzione dei vecchi switch con nuovi apparati.

Tutti i nuovi apparati sarano acquisiti con servizio Smartnet per la durata di 5 anni.

2.4. LIVELLO DI ACCESSO WIRELESS.

E' presente presso l'Ente una copertura wireless realizzata mediante 3 WLC Cisco 5500 e circa 450 Access Point modello Cisco AIR-LAP/AIR-CAP distribuiti in tra tutto il campus e la piastra sud
Tale infrastruttura permette l' accesso a terminali aziendali e dispositivi di personale esterno (fornitori, consulenti)

Tipologia	Modello	QTY	Manutenzione attiva
Access Point	AIR-LAP /AIR-CAP	450	14-gen-15
Wireless Controller	WLC-5500	3	14-gen-15

2.5. COLLEGAMENTO AD INTERNET.

La rete interna si connette ad Internet tramite un collegamento dedicato da 60 Mbps, realizzato attraverso l'utilizzo di una linea in fibra ridondata ed attestata su una coppia di Cisco 3845, in gestione al fornitore della connettività (attualmente Fastweb)

2.6. POP EXTRANET.

Il "pop extranet" è una parte dell'infrastruttura che offre la possibilità di connettersi da remoto ai Fornitori e ai dipendenti mediante connessione Virtual Private Network (**VPN**).

Sostanzialmente le modalità di connessione sono due:

1) **VPN Fornitori (SSL anche in NetworkConnect, Router dedicati (area remoteria) o VPN LAN-to_LAN)**
2) **VPN Dipendenti (SSL anche in NetworkConnect)**

La prima modalità consiste in un sistema di accesso remoto tramite protocollo SSL con un doppio grado di autenticazione, il primo livello autentica il client vpn direttamente su una coppia di firewall Juniper, dedicati a questo servizio, che funge da vpn concentrator, il secondo livello utilizza un' autenticazione mediante Username e password di AD.
Questi apparati di sicurezza hanno il compito di indirizzare i fornitori esclusivamente verso il sistema su cui deve essere eseguita manutenzione e solo per i servizi precedentemente concordati.

Qualora il fornitore necessiti di collegamenti più veloci per il trasferimento di grosse quantità di dati, l'Ente mette a disposizione un'area dedicata del firewall aziendale (Remoteria) su cui attestare le linee/apparati messe a disposizione del fornitore.

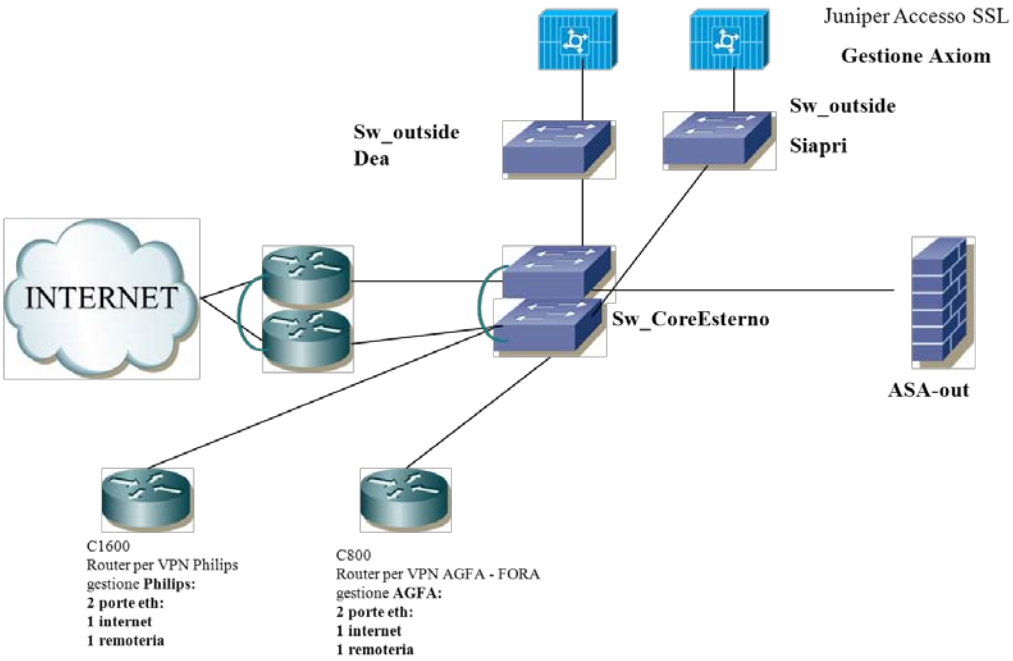
L'ente consente anche la possibilità di accesso tramite la creazione di una VPN LAN_to_LAN tramite i firewall aziendali, configurando precise policy che consentono l'accesso a specifici indirizzi e servizi concordati tra le parti.

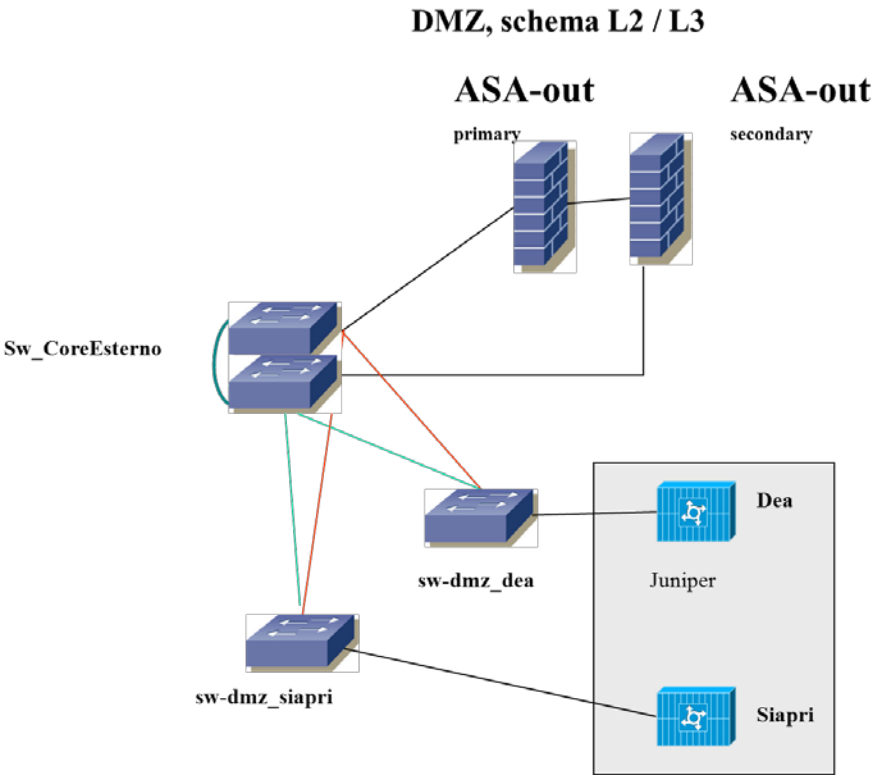
Analogamente la VPN Dipendenti consente ai dipendenti l'accesso alla rete aziendale da remoto tramite protocollo SSL con un doppio grado di autenticazione: il primo livello autentica il client vpn direttamente su una coppia di firewall Juniper, dedicati a questo servizio che funge da vpn concentrator, il secondo livello utilizza un' autenticazione mediante Username e password di AD.

.

Si riportano di seguito due schemi esemplificativi di struttura delle aree Outside e DMZ.

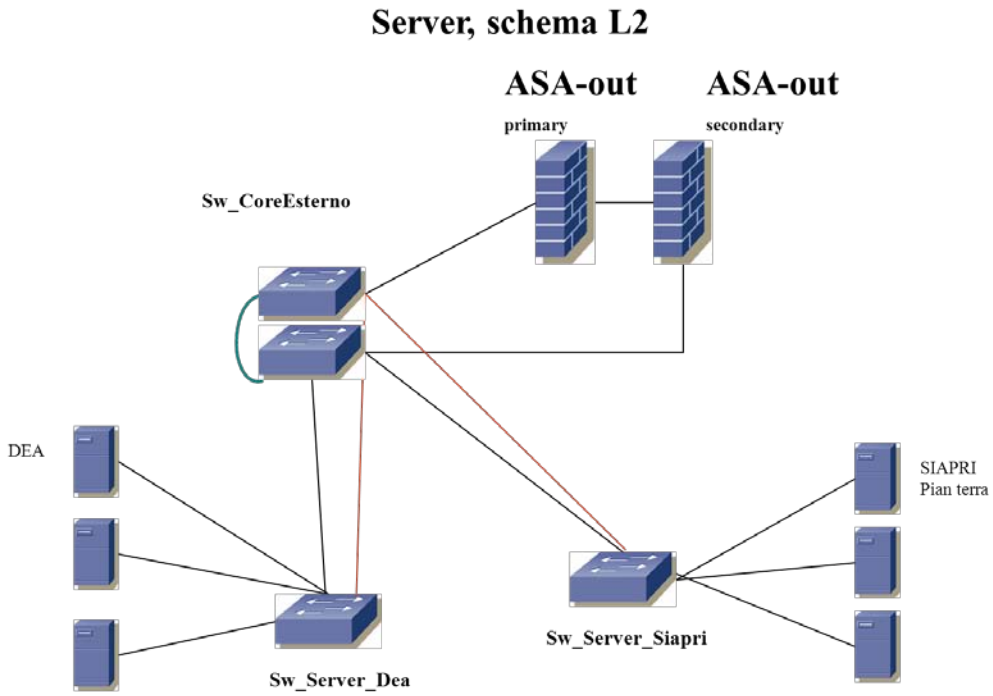
Outside, schema L2 / L3





2.7. AREA SERVER

In questa area vi sono i server con servizi aziendali pubblicati in Internet:



2.8. BROWSING INTERNET

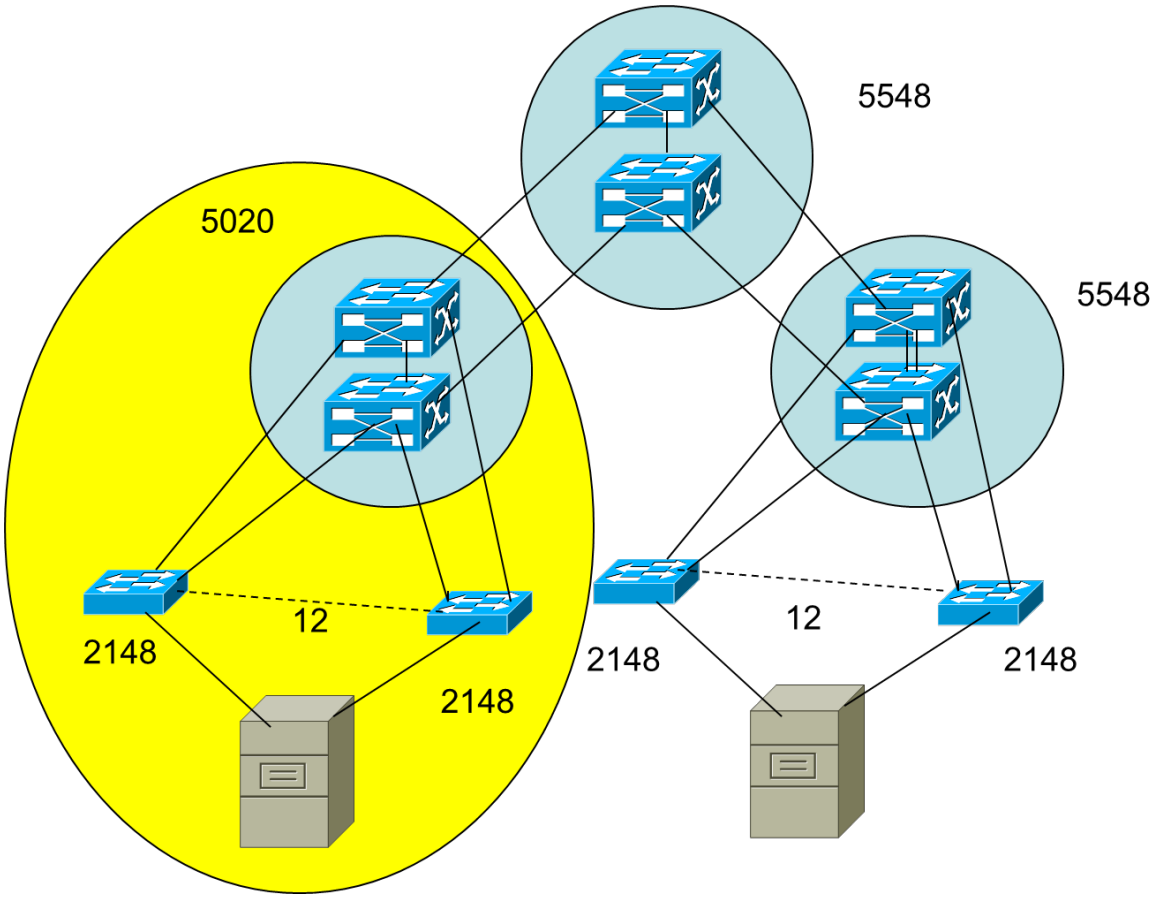
Le richieste HTTP e HTTPS degli utenti sono indirizzate su un' infrastruttura Proxy Microsoft ed un Web-Filter McAfee. Oltre a velocizzare l'accesso ai vari siti Internet, questi apparati svolgono un' azione di filtering per tutti quei siti di carattere non "istituzionale". I filtri sono applicati utilizzando data base aggiornati automaticamente dal sistema.

Si veda il capitolo sui sistemi di Infrastruttura per maggiori dettagli.

2.9. SERVER FARM

La server Farm è costituita da apparati Nexus della Cisco con collegamenti a 10G e configurati in full redundancy tra di loro:

Tipologia	Modello	QTY	Manutenzione attiva
Switch di Server Farm	Nexus-5020	2	14-gen-15
Switch di Server Farm	Nexus-5548	4	09-giu-17
Switch di Server Farm	Nexus-2148	12	14-gen-15
Switch di Server Farm	Nexus-2248	12	09-giu-17



2.10. SICUREZZA

L'infrastruttura di rete è protetta da intrusioni e violazioni della riservatezza dei dati da apparati specificamente preposti. Si è optato per una soluzione di tipo hardware con l'adozione di Cisco ASA nei punti di maggior criticità.
Il traffico da e per il mondo esterno (Internet,Remoteria,SISS,DMZ,Server) è filtrato da due Cisco ASA 5550 connessi in failover, assicurando così la continuità del servizio in caso di fault di una delle macchine. Sono dotati di tre schede di rete 8 Gbps full-duplex che consentono all'apparato di gestire più zone con differenti livelli di sicurezza.
Il traffico verso la Server Farm e verso la rete Imalan (servizi di Radiolofgia) è separata dai client mediante una coppia di ASA 5580 in high availability con interfacce a 10G:

Tipologia	Modello	QTY	Manutenzione attiva
Firewall	ASA-5550	2	14-gen-15
Firewall	ASA-5580	2	14-gen-15

3. SISTEMA FONIA

La rete fonia di Niguarda è in fase di migrazione da un servizio tradizionale costituito da 4 Centrali Alcatel 4400 presenti nel campus e da satelliti collegati presso 3 sedi remote (Villa Marelli, Cherasco e Ippocrate) ad una tecnologia IP attualmente costituita da 3 Cisco CUCM installati su MCS-7835 in cluster tra di loro. I flussi Primari della PSTN sono attestati sulla centrale Alcatel e gestiti da N°7 Posti Operatore , di cui 2 installati su PC) : la migrazione attuale è a circa il 50% dei telefoni.
Sulla centrale Alcatel vi è installato un servizio ACD (Automatic Call Distribution) licenziato per 15 agenti di cui 8 in uso.

I 2 sistemi sono collegati tramite un Trunk QSIG ridondato ed attestato su 2 Router Cisco WS-C3825 configurati in MGCP sul Cluster di CUCM;

Internamente è inoltre presente un secondo cluster di N°2 CUCM e N° 2 UCCX (installati rispettivamente su MCS-7825 e MCS-7835) che svolge la gestione del servizio CAV (centro.antiveleni) di Niguarda che ha un suo flusso Primario separato e gestiti tramite N°2 MGCP Gateway WS-C2901: il sistema CAV e completamente integrato con il sitema Niguarda tramite un TRUNK Cisco tra i 2 cluster.

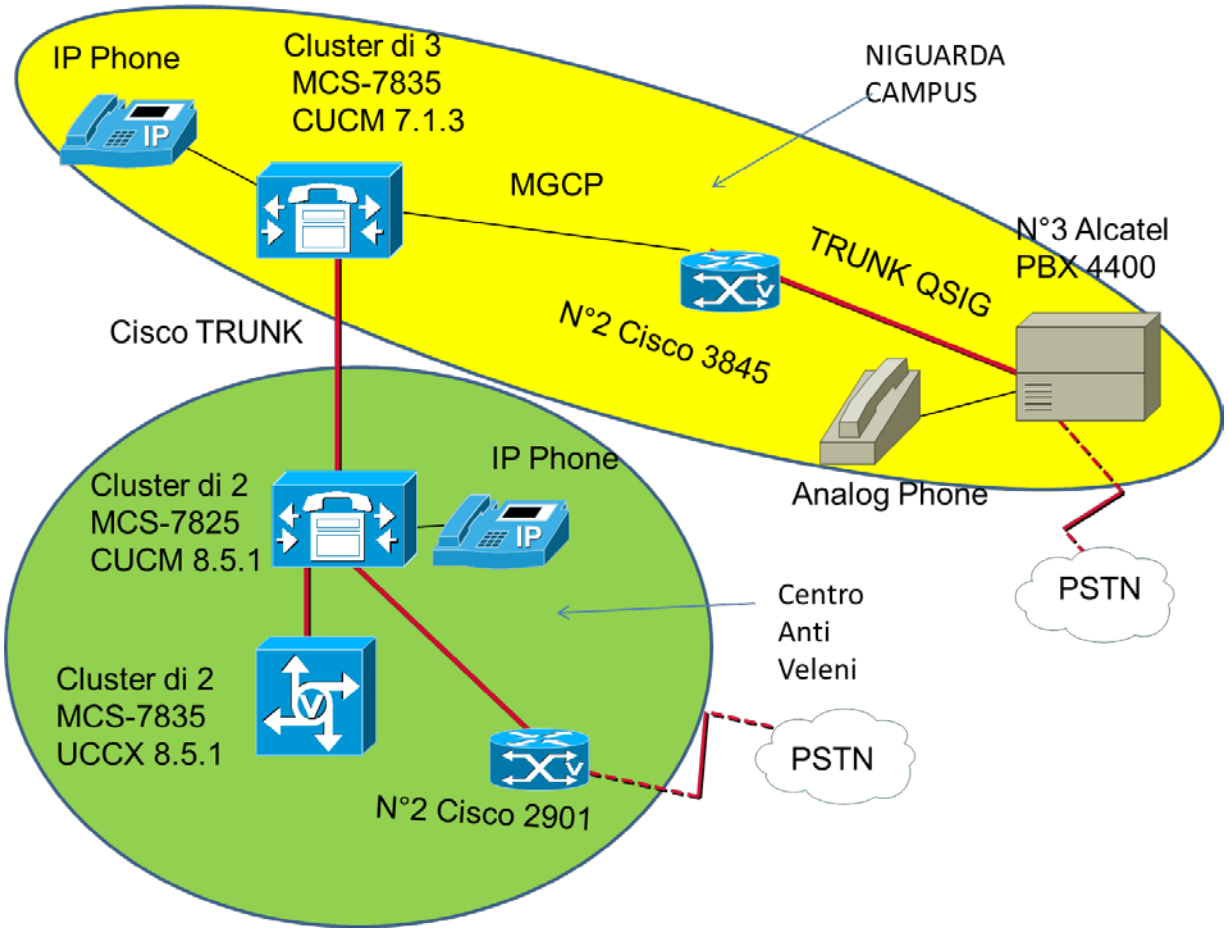


Fig xx – Telefonia IP

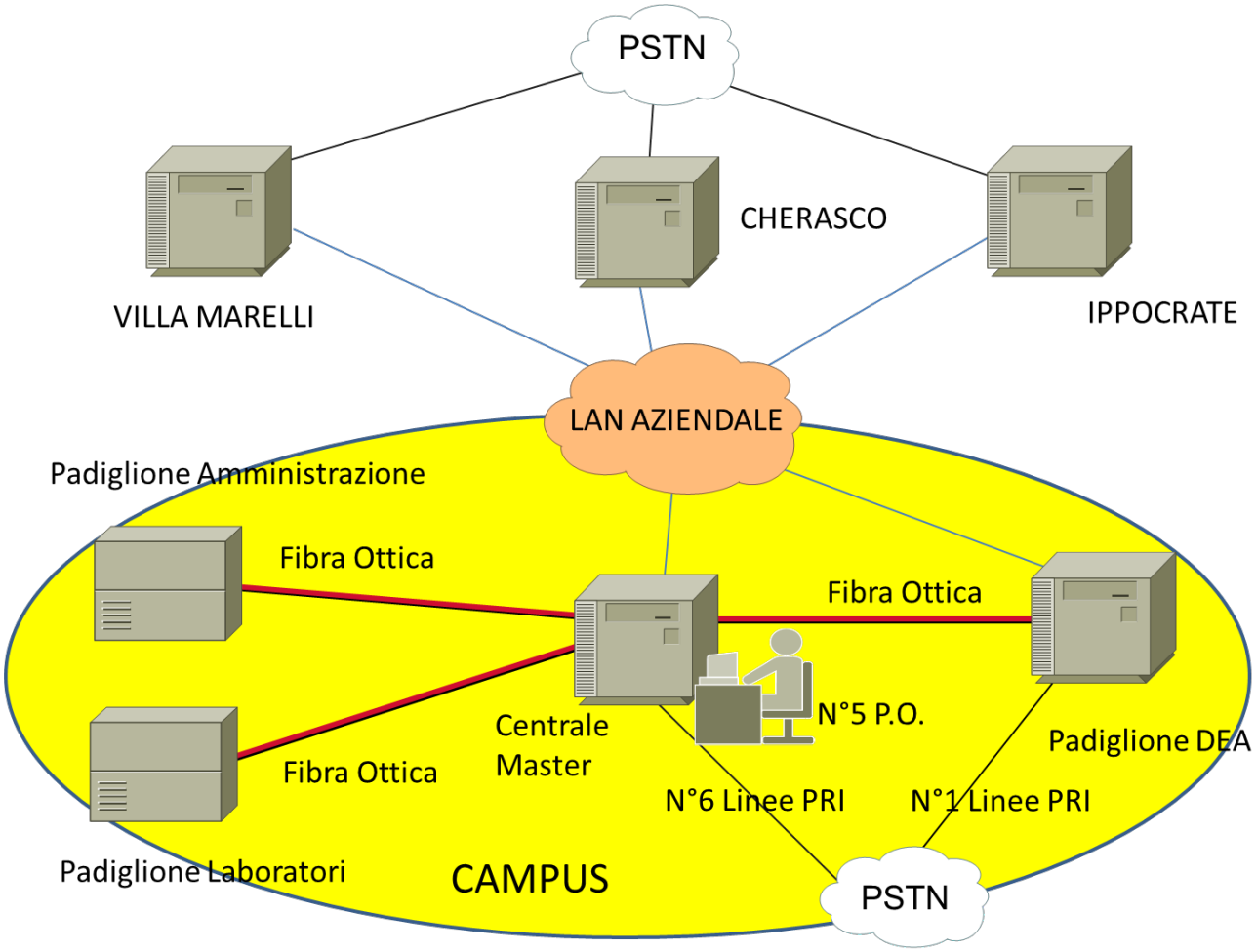


Fig. 6 - Telefonia Tradizionale

L'elenco di tutti i dispositivi telefonici installati presso Niguarda e' riportato nella tabella seguente:

Tipologia	Modello	QTY	Manutenzione attiva
Telefono	analogici	1500	NO
Telefono Digitale	4035 (24 tasti)	112	NO
Telefono Digitale	4020(12 tasti)	65	NO
Telefono Digitale	4010(8 tasti)	65	NO
Telefono IP	CP-G7911	1125	14-gen-15
Telefono IP	CP-G7962	118	14-gen-15
Telefono IP	CP-G7942	58	14-gen-15
Telefono IP	CP-G7975	12	14-gen-15
Telefono IP	CP-G7965	3	14-gen-15
Telefono IP	CP-G6921	63	09-giu-17
Telefono IP	CP-G6961	14	09-giu-17
Telefono IP	CP-G7925	68	14-gen-15
Gateway Analogico	VG202	90	14-gen-15
Voice Server	MCS7835	4	14-gen-15

La tabella seguente riporta il dettaglio degli apparati costituenti il CAV (Centro Anti Veleni):

Tipologia	Modello	QTY	Manutenzione attiva
Telefoni	CP-G7962	10	14-gen-15
Telefoni	CP-G7942	4	14-gen-15
Telefoni	CP-G7975	2	14-gen-15
Voice Gateway	CISCO2901	2	14-gen-15
Voice Server	MCS7835	2	14-gen-15
Voice Server	MCS7825	1	14-gen-15
Voice Server	MCS7825	1	NO

Si riporta qui di seguito la configurazione Hw delle centrali Alcatel:

NODO 1 Master							
Tipo scheda	QTY						
CS (cpu) appliance	2						
RMA a rack	1						
Tipo scheda	EX PS: N° 2 CABINET modello M3					LABORATORI: N° 1 CABINET modello MW1	AMMINISTRAZIONE: N° 1 CABINET modello M2
	Qty su Magazzino 0:	Qty su Magazzino 1:	Qty su Magazzino 2:	Qty su Magazzino 3:	Qty su Magazzino 4:	Qty su Magazzino 5:	Qty su Magazzino 6:
CPU (CS)	2						
Z24		13	14	2		6	15
Z24_2			1				4
UA32			2	2	1	1	3
INTOF_B		2	2	2		1	1
NPRAE				4			
PRA2				2	1		
GPA				1			
NDDI				4			
EMTL				1			
INTOF_A					8		
BPRA2					6		
IOIP					2		
INTIPA					1		
SPA3					2		
VPCPU/VPM35					1		
VG					1	1	
Z32							1

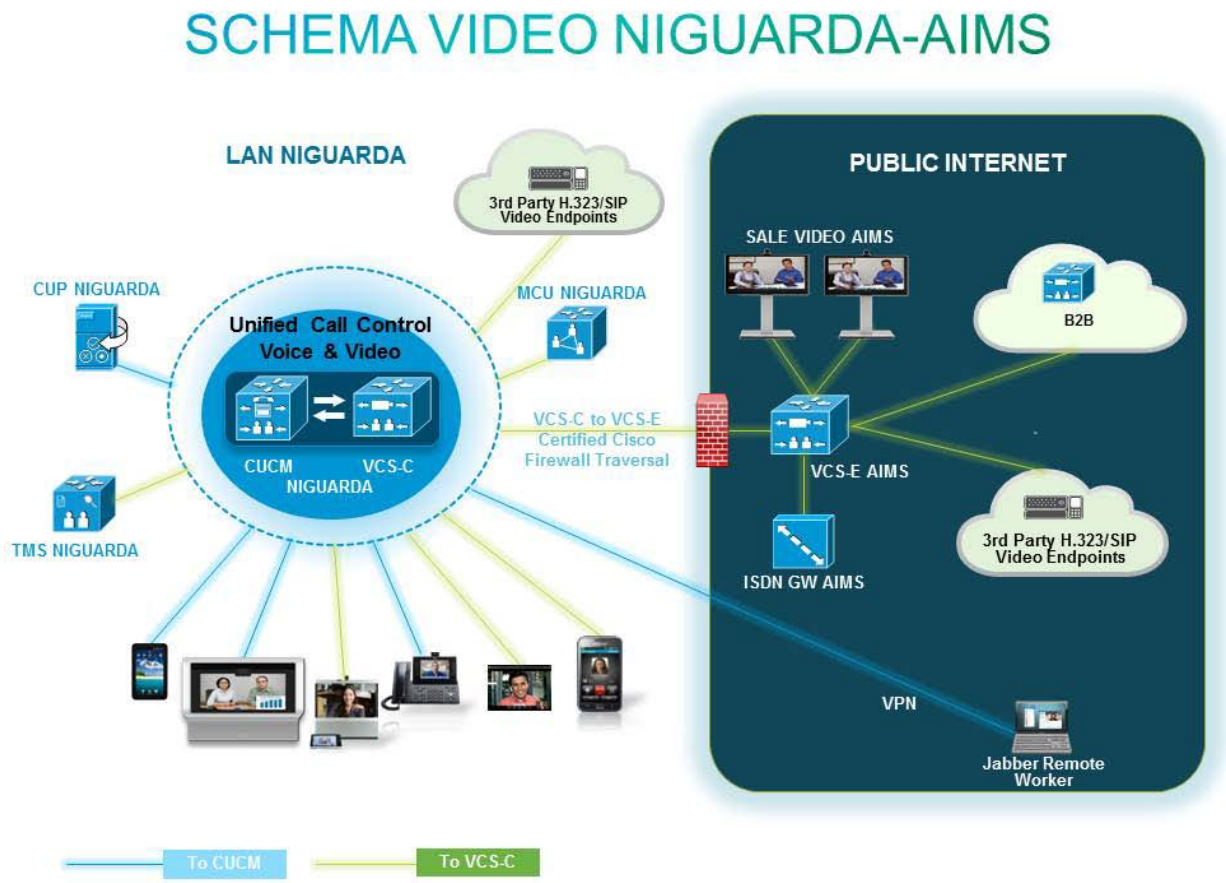
Si precisa che e' in corso la sostituzione della telefonica analogica verso al telefonia VOIP, il cui completamento sara' a carico dell'aggiudicatario (vedi cap. 7.1).

NODO 7 DEA			NODO 2 V.MARELLI	NODO 4 IPPOCRATE	NODO 5 CHERASCO
Tipo scheda	QTY		QTY	QTY	QTY
RMA	1		1	1	1
N° 1 CABINET modello M3			Cabinet : M2(1)	Cabinet : M2(1)	Cabinet : WM1(1)
Tipo scheda	Qty su Magazzino 0:	Qty su Magazzino 1:	Qty su Magazzino 0:	Qty su Magazzino 0:	Qty su Magazzino 0:
Z24	6	5	3	7	1
Z24_2	4		1		1
UA32	3	1	1	1	1
INTOF_B		2			
USCVG				1	1
PRA2	2		1		
GPA	1		1	1	
NDDI			1		
CPU6			2	2	1
INTOF_A	2				
BPRA2	1		2	1	
VG	1		1		
Z32		2			
DSI	1				
CPU7	2				
BRA2	2				1

Il

4. SISTEMA DI VIDEOCONFERENZA

Presso l'Ospedale è presente un sistema di VideoConferenza (VDC) basato su tecnologia Cisco costituito da N° 2 Telepresence 1100, N°1 MCU-4501 , N°1 VCS-Control, N°1 VCS Expressway e N°2 C20 UNIT, N°1 ISDN PRI Gateway, N°1 Server TMS; questo sistema è completamente integrato con il cluster di CUCM a cui afferisce il servizio CAV secondo lo schema qui di seguito riportato:.



5. SISTEMI DI INFRASTRUTTURA

I sistemi di Infrastruttura gestiscono i seguenti servizi:

- Active Directory, DNS, DHCP
- Proxy, Web Filter
- VPN

Nelle sezioni seguenti si da' una descrizione della situazione AS_IS dei sistemi Hw, precisando che e' intenzione dell'Ente provvedere all'aggiornamento tecnologico dei server, sia con sostituzione dell'attuale Hw, che tramite virtualizzazione dei server.

All'aggiudicatario dei servizi e' richiesto la stesura di un piano di aggiornamento Hw/Sw da sottoporre all'Ente, e la sua implementazione. All'Ente compete l'acquisto dei materiali Hw/Sw.

5.1. ACTIVE DIRECORY

I sistemi d'infrastruttura (Active Directory, DNS, Dhcp…) sono strutturati con sette Domain Controller che gestiscono l'Active Directory: due gestiscono il dominio Schema, e gli altri 5 gestiscono dominio ospedaleniguarda.it. Sono tutte macchine Windows Server 2003.

Tre domain controller svolgono anche la funzione di DNS interno.

Il DNS pubblici sono invece server linux.

La gestione del DHCP avviene attraverso 3 server (2 domain controller oltre un istanza virtuale di un cluster)

Tipo Apparato	Servizio/Funzione	Marca Apparato	Modello Apparato	S.O.
Server Fisico	DNS Server Pubblico (Niguardaonline.it)	IBM	XSeries 306	Linux Slackware 12.0
Server Fisico	DNS Server Pubblico (Niguardaonline.it)	IBM	XSeries 306	Linux Slackware 12.0
Server Fisico	Domain Controller - Ospedale Niguarda.schema	IBM	XSeries 335	Microsoft Windows Server 2003 Standard Edition
Server Virtuale	Domain Controller - Ospedale Niguarda.schema			Microsoft Windows Server 2003 Standard Edition
Server Virtuale	Domain Controller - Ospedaleniguarda.it			Microsoft Windows Server 2003 Standard Edition
Server Virtuale	Domain Controller - Ospedaleniguarda.it			Microsoft Windows Server 2003 Standard Edition
Server Fisico	Domain Controller - Ospedaleniguarda.it	IBM	XSeries 335	Microsoft Windows Server 2003 Standard Edition
Server Fisico	Domain Controller - Ospedaleniguarda.it	IBM	XSeries 3550 M2	Microsoft Windows Server 2003 Standard Edition
Server Fisico	Domain Controller - Ospedaleniguarda.it	IBM	XSeries 3550 M2	Microsoft Windows Server 2003 Standard Edition

5.2. PROXY

Il servizio proxy viene erogato attraverso Microsoft ISA Server su due server il cui carico viene bilanciato da uno switch Nortel.

Il Webfilter è costituito da due appliance McAfee configurati in modo da garantire la continuità di servizio.

Servizio/Funzione	Marca Apparato	Modello Apparato	***Type***	S.O.
Nodo Proxy	IBM	Blade HS20	8843-41Y	Microsoft Windows Server 2003 R2 Standard Edition
Nodo Proxy	IBM	Blade HS20	8843-41Y	Microsoft Windows Server 2003 R2 Standard Edition
Reverse Proxy Cluster	IBM	XSeries 3250 M2	4194-K2G	Linux Debian Lenny 5.0.6
Reverse Proxy Cluster	IBM	XSeries 3250 M2	4194-K2G	Linux Debian Lenny 5.0.6
Servizio FTP Pubblico	IBM	XSeries 335	8676-61X	Microsoft Windows Server 2003 R2 Standard Edition
Web filter	McAfee	SIG 3300	BJSPL3J	Email and Web Security Appliance (3300) v5.5
Web filter	McAfee	SIG 3300	4JSPL3J	Email and Web Security Appliance (3300) v5.5

5.3. VPN

Il servizio VPN viene erogato attraverso due server Juniper a cui sono collegati dati altri quattro server (due per il cluster radius e due per il cluster RSA).

Servizio/Funzione	Marca Apparato	Modello Apparato	***Type***	S.O.
Servizio VPN	Juniper	SA-4000	SA-4000	IVE 6.5R8
Servizio VPN	Juniper	SA-4000	SA-4000	IVE 6.5R8
RSA - Accesso Web Autenticazone RSA Server	IBM	XSeries 3550	797871G	Microsoft Windows Server 2003 R2 Standard Edition
RSA - Accesso Web Autenticazone RSA Server	IBM	xSeries 3550	797871G	Microsoft Windows Server 2003 R2 Standard Edition

La gestione dei token SMS avviene tramite un cluster di server virtualizzati:

Servizio/Funzione	S.O.
Autenticazione SMS	Microsoft Windows Server 2003 R2 Standard Edition
Autenticazione SMS	Microsoft Windows Server 2003 R2 Standard Edition

6. SISTEMA DI POSTA ELETTRONICA

La gestione del sistema di Posta Elettronica non rientra nei servizi che A.O. Niguarda richiede all'aggiudicatario del bando di gara, in quanto e' in corso l'esternalizzazione del servizio su altro fornitore.

L'eventuale inclusione del servizio di gestione della Posta Elettronica sara' negoziato come estensione del contratto in essere.

7. PROGETTI IN CORSO

L'Ente ha in corso una serie di progetti di aggiornamento tecnologico e di implementazione di nuovi servizi che ricadono sotto la responsabilità del fornitore dei servizi NOC.

Al fornitore e' richiesto di garantire con il personale di presidio un'ampia competenza sulle tecnologie previste per progetti in corso, supportato quando necessario ulteriori tecnici specialisti di prodotto messi a disposizione del fornitore.

Di seguito si riportano i principali progetti in corso, fermo restando la facoltà dell'Ente di richiedere ulteriori implementazioni nel corso della vigenza contrattuale.

7.1. COMPLETAMENTO PIANO DI MIGRAZIONE FONIA SU IP

E' in corso il progetto di migrazione di tutta la telefonia su piattaforma IP, utilizzando l'infrastruttura descritta nelle sezioni precedenti.
La migrazione comporta una serie di attività, sinteticamente riportate di seguito:

- Supervisione presso reparto per rilevare le funzionalità telefoniche implementate sulla centrale analogica
- Studio per il porting delle stesse funzionalità su piattaforma IP
- Laddove necessario, la sostituzione di vecchi switch, per lo piu' per mancanza della funzionalità POE
- Migrazione del reparto su telefonia IP con sostituzione degli apparecchi telefonici

Alla data della stesura del presente documento, il numero di telefoni analogici e digitali attestati sulla centrale Alcatel ammonta a circa 1.750.

L'attuale dotazione di magazzino di telefoni IP e' riportata nella tabella seguente:

TIPOLOGIA	Modello	TOT	Manutenzione attiva
Telefono IP	CP-G7911	42	14-gen-15
Telefono IP	CP-G7942	45	14-gen-15
Telefono IP	CP-G7962	46	14-gen-15
Telefono IP	CP-G6921	331	09-giu-17
Telefono IP	CP-G6961	105	09-giu-17
Telefono IP	CP-G7965	2	14-gen-15
Telefono IP	CP-G7975	2	14-gen-15
Telefono IP	CP-G8961	5	09-giu-17
Telefono IP	CP-G7925	21	14-gen-15
Telefono IP	CP-G7925	10	14-gen-15
Telefono IP	CP-G7985	4	14-gen-15
Gateway Analogico	VG202	6	14-gen-15
Router	CISCO2851-V	1	14-gen-15
Switch Accesso	WS-C3750X-24P	41	09-giu-17

E' prevista l'acquisizione di ulteriori apparecchi telefonici IP per completare la sostituzione di tutta la telefonia analogica. I nuovi telefoni saranno acquisiti con servzio Smartnet per la durata di 5 anni.

7.2. POSTO OPERATORE DI CENTRALINO TELEFONICO.

Il progetto prevede al migrazione dell'infrastruttura di Posto Operatore su tecnologia IP.

Presso l'Ente ci sono attualmente nr.7 Posti Operatore (PO) attestati su centrale Alcatel, di cui 4 sono direttamente collegati alla centrale Alcatel, mentre i rimanenti 3 sono della tipologia PO-PC, ovvero attestati su Computer in rete.

Il fornitore e' chiamato ad implementare il Posto Operatore su tecnologia IP, individuando i prodotti necessari che saranno acquisiti dall'Ente.

7.3. INTEGRAZIONE SERVIZI DI FONIA IP

Al fornitore e' richiesto di sviluppare i progetti di integrazione della fonia IP con servizi diretti all'utenza, quali, ad esempio; gestione della rubrica telefonica condivisa, integrazione con AD, phone lock, etc., utilizzando l'infrastruttura attuale e/o proponendo prodotti integrativi che saranno acquisiti dall'Ente.

Al fornitore si chiede al minimo di implementare le funzioni ed i servizi gia' presenti sulla fonia analogica, in modo che la migrazione su tecnologia VOIP di interi reparti non comporti un downgrade di prestazioni.

7.4. SERVIZI AGGIUNTIVI DI SICUREZZA

Il progetto prevede l'analisi e l'implementazione di una soluzione integrativa di sicurezza sia sul fronte del controllo delle intrusioni , sia sul fronte dell'autenticazione.

L'Ente ha gia' acquisito i prodotti in tabella, ovvero 2 sonde IPS e due Server di controllo Accessi, su cui deve essere basato il progetto di sicurezza sviluppato dal fornitore.

TIPOLOGIA	Modello	TOT	Manutenzione attiva
Sonda IPS	IPS-4270	2	14-gen-15
Appliance Security Access	CSACS-1120	2	14-gen-15

7.5. PIASTRA NORD

L'Ospedale Niguarda sta completando un nuovo padiglione denominato BLOCCO NORD per il quale si rende necessario predisporre una rete LAN per abilitare i servizi evoluti di Unified Communication: VOIP, IPT, Video, Multicast, ecc.

Non fa' parte del presente capitolato tecnico il progetto e la fornitura di apparati per il Blocco Nord, che si prevede sarà gestito con un separato bando di gara.

Al fornitore dei servizi NOC, principalmente attraverso il presidio tecnico dedicato presso l'Ente, si richiede:

- Competenza tecnica per comprendere il progetto esecutivo di implementazione del Blocco Nord sviluppato dall'aggiudicatario del Bando di Gara
- Installazione, configurazione, collaudo e messa in produzione degli apparati attivi secondo il piano previsto nel progetto esecutivo predisposto dall'aggiudicatario del bando di gara.
- Integrazione con la rete Campus esistente

- Installazione, configurazione, collaudo e messa in produzione della infrastruttura wireless, integrandola con quella esistente.
- Attivazione Installazione, configurazione e messa in produzione della fonia VOIP e di tutti i servizi associati, integrandola con l'infrastruttura VOIP esistente.

Allo stato attuale del progetto, per l'attivazione del Blocco Nord si prevede di acquisire i seguenti apparati:

PRODOTTI	Quantità	Codice CISCO	Descrizione prodotto
Switch di Building	8	**WS-C6509-E**	Catalyst 6500 Enhanced 9-slot chassis 14RU no PS no Fan Tray
Switch di CORE	2	**WS-C6509-E**	Catalyst 6500 Enhanced 9-slot chassis 14RU no PS no Fan Tray
Switch di Piano	130	**WS-C3750X-24P-S**	Catalyst 3750X 24 Port PoE IP Base
Telefoni entry level b/n	500	**CP-6921-C-K9=**	Cisco UC Phone 6921 Charcoal Standard Handset
Telefoni medium level b/n	15	**CP-7942G=**	Cisco UC Phone 7942 spare
Telefoni High level b/n	45	**CP-7962G=**	Cisco UC Phone 7962 spare
Telefoni High level col.	5	**CP-7965G=**	Cisco UC Phone 7965 Gig Ethernet Color spare
Telefoni Professional col.	5	**CP-7975G=**	Cisco UC phone 7975 Gig Ethernet Color spare
Telefoni wireless	80	**CP-7925G-E-K9**	Cisco 7925G ETSI; CM/CME UL Reqd; Battery/PS Not Included
Voice Gateway analogici	100	**VG202**	Cisco VG202 Analog Voice Gateway
Switch Core di CAMPUS	4	**WS-C6509-E**	Catalyst 6500 Enhanced 9-slot chassis 14RU no PS no Fan Tray

Si precisa che nell'elenco di cui sopra compaiono 4 switch Core di Campus che sono previsti per l'aggiornamento tecnologico degli attuali Catalyst:

6509_Amministrazione
6509_Degasperis
6509_Pizzamiglio
6509_Ponti

L'installazione, configurazione e messa in produzione di tali Switch di Core sarà a completo carico del fornitore di servizi NOC.

8. PRESIDIO TECNICO

Con riferimento al Capitolato Tecnico, *sez. 8- Ruoli e Competenze del Presidio tecnico*, si precisa che il presidio tecnico presso la sede dell'Ente deve prevedere **composto come riportato in tabella** con i seguenti requisiti minimi di certificazione.

- **Nr.1 Sistemista di Rete Senior, con certificazione CCNP**
- **Nr.1 Sistemista Senior con competenze approfondite di gestione ed implementazione servizi di Infrastruttura su tecnologia Microsoft** (Active Directory, DHCP, DNS, etc.)
- **Nr.1 Sistemista di Rete con competenze di installazione configurazione apparati attivi e realizzazione cablaggio strutturato.**
- **Nr.1 Sistemista Fonia tradizionale** con comprovata competenza ed esperienza minimo triennale su centralini Alcatel.

Al termine del piano di migrazione su fonia IP, e conseguente dismissione della telefonia tradizionale, l'Ente si riserva la facoltà di richiedere la sostituzione del profilo di "Sistemista Fonia tradizionale" con un profilo tecnico aderente alle tecnologie installate.

L'Ente richiede la seguente copertura del servizio di presidio:

Servizio	Ente		
Orari	Lun - Ven	Sabato	Festivi
Presidio	7:30 - 18:00	8:00 – 12:00	no
Nr. Tecnici di Presidio	4 FTE	2 FTE	no
Reperibilità	24h		
Monitoraggio remoto	24h		

A fronte della copertura oraria giornaliera che eccede le 8 ore lavorative nei giorni infrasettimanali, si precisa che l'Ente comunicherà al fornitore la composizione del presidio nelle varie fasce orarie sulla base delle esigenze specifiche di periodo.

Per la giornata di Sabato, il presidio deve essere di almeno 2 tecnici per tutte le fasce orarie, comprendente un tecnico fonia ed uno per le reti.

Si precisa altresi' che il fornitore deve garantire la sostituzione con personale di equivalente skill in tutte le occasioni in cui uno o piu' tecnici di presidio non possano essere presenti (ferie, malattie, etc.),