V Incontro del GARR
Roma, 24-26 Novembre 2003

Istituto Nazionale di Fisica Nucleare
Laboratori Nazionali di Frascati

Angelo Veloce
Via E. Fermi,40
00044 Frascati (RM) Italy
angelo.veloce@lnf.infn.it

Il Campus dei LNF

- Il territorio e gli edifici serviti
- Il cablaggio
- Gli apparati attivi
- Le soluzioni tecniche adottate a livello 2
- Le soluzioni tecniche adottate a livello 3
- L’interconnessione con la WAN
- Il POP del GARR

LNF: il territorio

- Directorate, Administration
- Accelerator Division
- Bar
- ARES L
- Accelerator Division
- LISA
- Technology Building
- Gran Sasso
- DAPHNE Building
- Cryogenic Plant
- Experimental Hall
- KLOE Experimental Hall
- FINUDA Experimental Hall
- Computing Service
- Health Physics Office
- LADON VIRGO Building
- LADON VIRGO Workshop
- Machine Hall
- Experimental Hall
- Modulators Hall
- LINAC
- Nuclear Physics Building
- Accumulator Building
- High Energy Auxil. Offices
- HTSC Processing Laboratory
- Guesthouse A
- KLOE Tacking Laboratory
- SAC-INFN Store
- Detector Test Laboratory
- Central Administration

- Guard Door (Main Entrance)
- Guard Door
- Guesthouse B
- baracche

- ENEA Guard Door
- High Energy Building
- ENEA Computing Center
- Electric Power Station

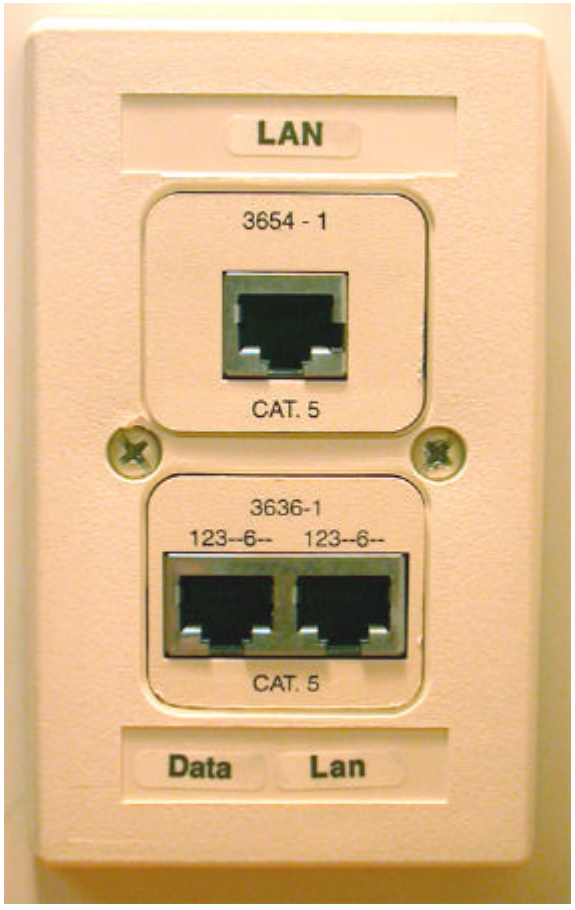
Il cablaggio edificio-edificio

- Interconnessione tra edifici in FO multimodale 62.5/125 μm a topologia stellare
  - Centro stella nell'edificio Calcolo
  - Tratte in fibra ottica realizzate con cavi a 12 fibre
  - Tutte di lunghezza inferiore a 400m
  - Connettorizzazione ST sui Patch Panel ottici
  - Protocollo trasportato Gigabit Ethernet
    - 1000BaseSX prima finestra
    - 1000BaseLX seconda finestra

Il cablaggio interno agli edifici

- Edifici in cablaggio strutturato STP (Foiled):
  - Edifici cablati in classe D (100MHz):
    - Calcolo PT, Alte Energie, Laboratori Adone, Kloe
  - Tutti gli altri edifici cablati in classe E (~300MHz)
  - Sistema utilizzato marca AMP modello ACO
    - Sfrutta tutti i doppini del singolo cavo trasportando 2 connessioni Ethernet
    - Prevede frutti binati (dual ethernet) facilmente intercambiabili
    - Garanzia 15 anni on-site
  - Protocollo trasportato Ethernet 10/100/1000 BaseTX

Il cablaggio interno agli edifici



- Esempio di presa utente (2 cavi STP):
  - Connettori schermati
  - Singolo per tutte le funzionalita’ (4 coppie)
  - Duale per funzionalita’ Ethernet 10/100/1000 Mb/s (2 + 2 coppie)

Apparati Attivi

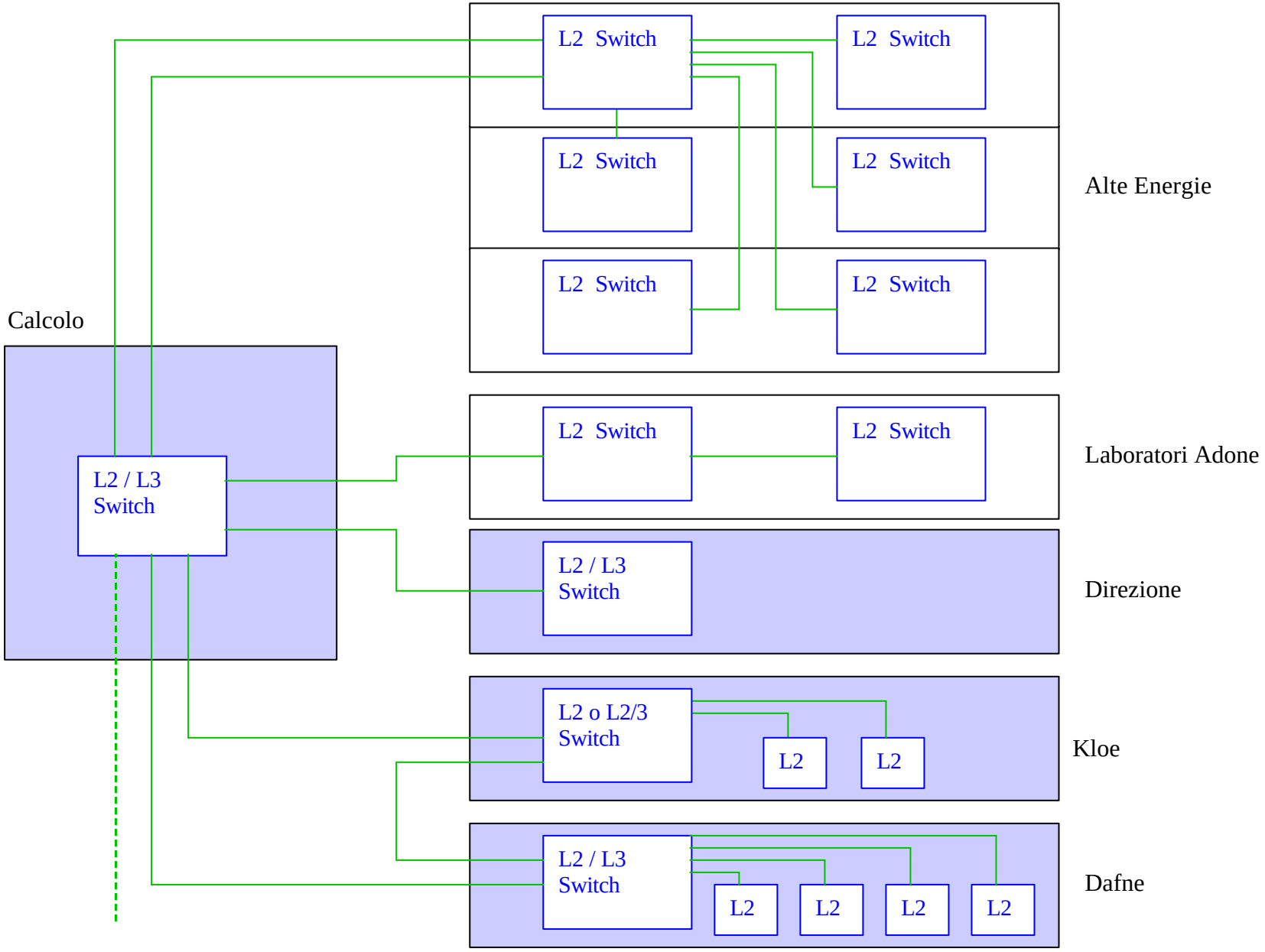
- Scelta monolitica dettata dall'esigenza di minimizzare le difficolta' di gestione
- Soluzione vincente anche per implementare soluzioni non ancora previste dagli standard ma gia' implementate in modalita' proprietaria
- Una grossa gara iniziale ha determinato il vincitore tra i vari competitor: Cisco, Enterasys e Nortel

Soluzione Cisco

- Router di accesso alla WAN 7507 RSP II
  - Interfacce FastEthernet e ATM OC3 155Mb/s
- 5 Core switch (layer 2, 3 e superiore):
  - Catalyst 6509 Sup II MSFC II completamente ridondato in sala calcolo
  - Catalyst 6509 Sup II MSFC II completamente ridondato in sala KLOE (HSRP)
  - 2 Catalyst 6506 Sup II MSFC II in sala controllo Dafne e Direzione
  - Catalyst 4006 Layer 3 in edificio Master

Soluzione Cisco

- Edge switch (layer 2):
  - Catalyst 6506
  - Catalyst 4006
  - Catalyst 3550
  - Catalyst 3524
- Soluzione wireless implementata nelle aule destinate alle riunioni, conferenze e seminari
  - Cisco aironet 350 e 1200


L2 Switch
L2 Switch
L2 Switch
L2 Switch
L2 Switch
L2 Switch
Alte Energie
Calcolo
L2 / L3
Switch
L2 Switch
L2 Switch
Laboratori Adone
L2 / L3
Switch
Direzione
L2 o L2/3
Switch
L2
L2
Kloe
L2 / L3
Switch
L2
L2
L2
L2
Dafne

Componenti attivi della LAN

- Nuovi apparati installati nei seguenti edifici:

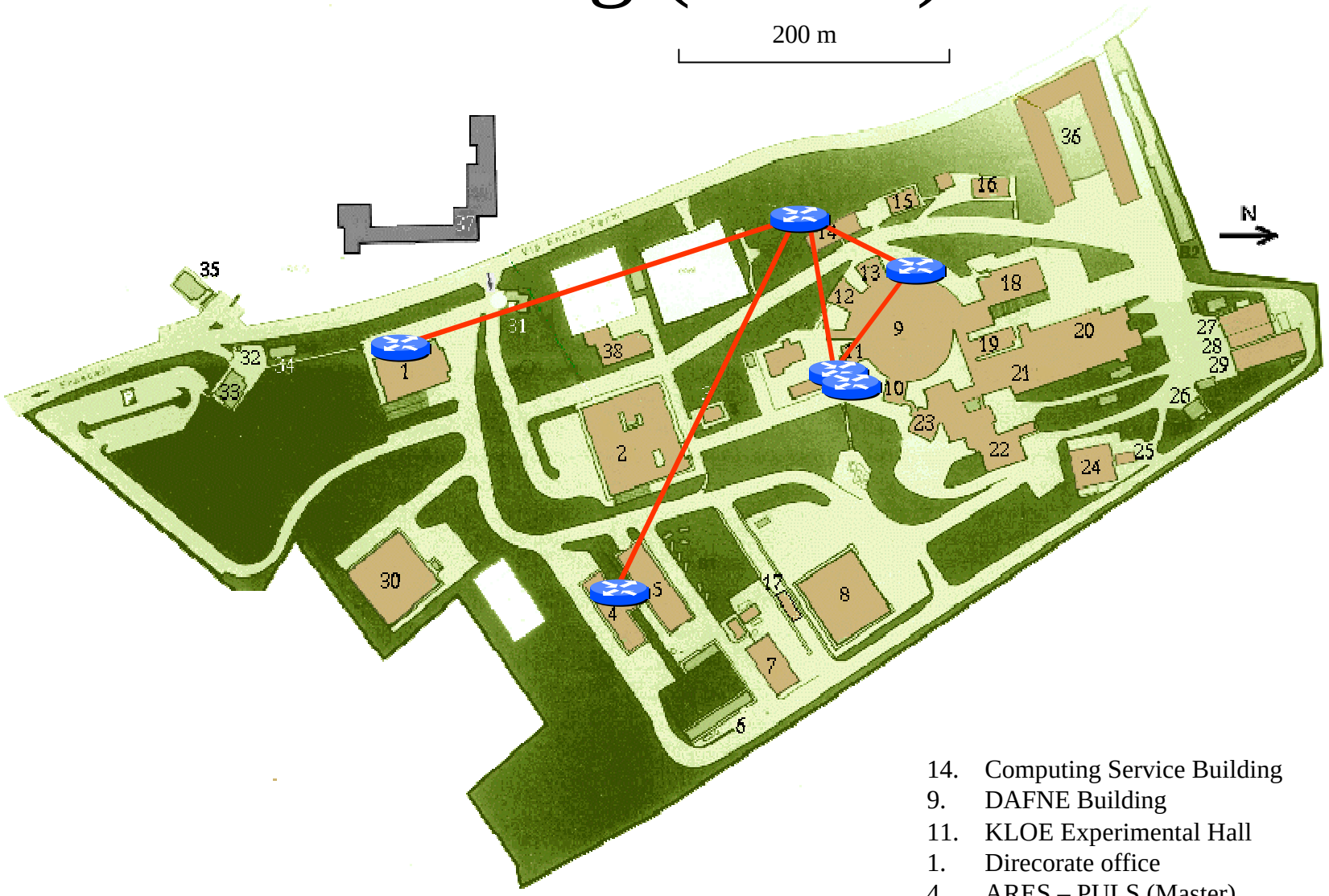
Edificio	Switch Layer 2/3	Switch Layer 2	Porte (2220)
Calcolo	1	2 + 2	150
Dafne	1	6	220
Direzione	1		100
Ares	1	1	150
Kloe	1	2	150
Leale		3	150
Alte Energie		6 + 3	500
Div. Acceleratori		2	200
Rivelatore Finuda		1	30
Amm Centrale		2	450
Luce di Sincrotrone		1	30
SMI		1	30
Finuda		2	60

Componenti attivi della LAN (2)

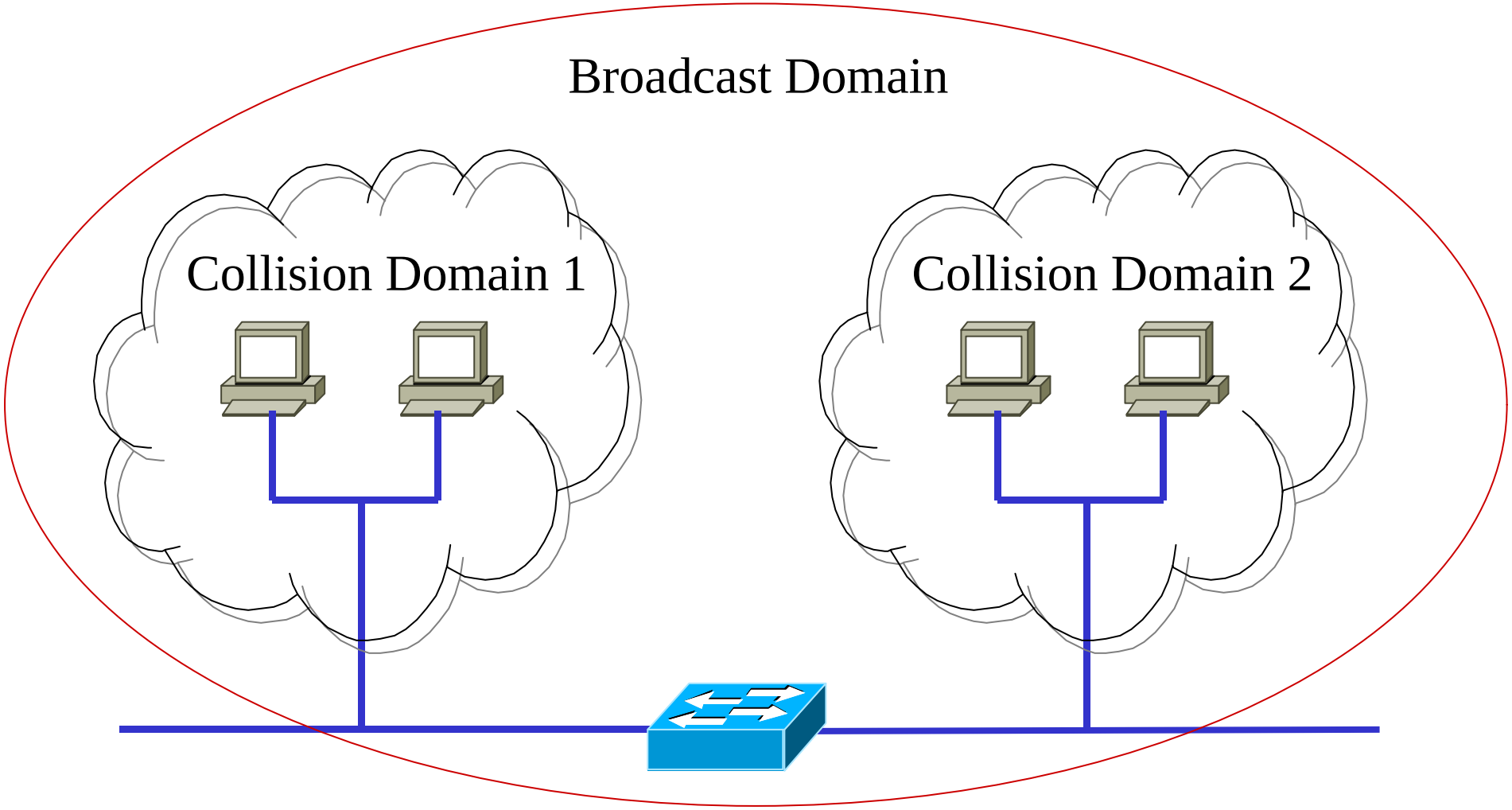
- Nuovi apparati installati nei seguenti edifici:

Edificio	Switch Layer 2	Porte (340)
Cabina elettrica	1	30
Linac	1	30
Gran Sasso	1	50
Tubificio	1	50
Camera a Bolle	1	50
Guardiania	1	20
Misure Magnetiche	1	20
Fisica Sanitaria	1	30
Officina Virgo	1	20
Lab Crio ROG	1	20
Sala controllo Lisa	1	20
TOTALI	45	2560

LNF: IP routing (OSPF)



Il layer 2 switch termina domini di collisione, ma non di broadcast



Partizionamento della LAN

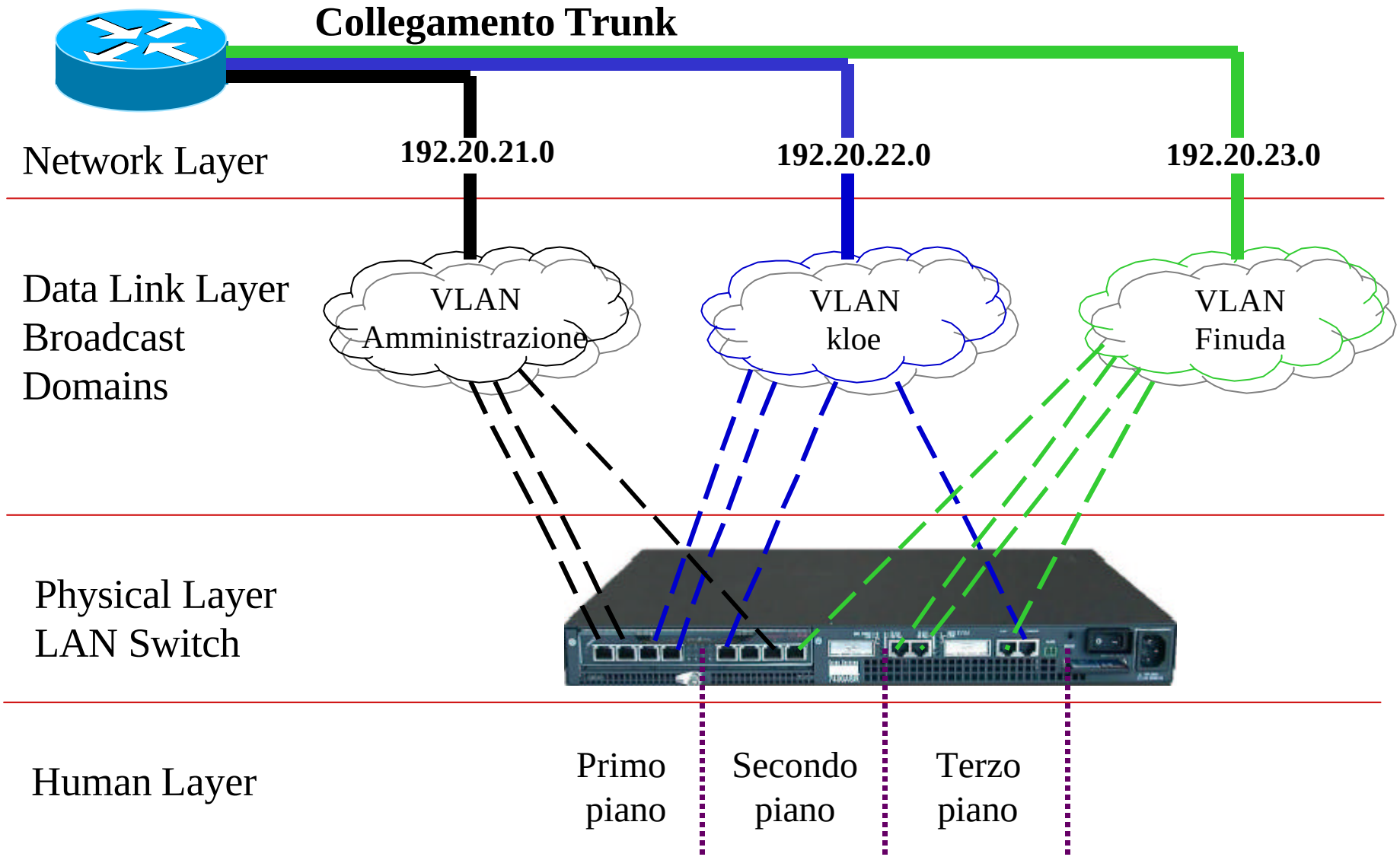
- I broadcasts possono consumare tutta la banda disponibile (Broadcast storm)
- Ciascun device che riceve un broadcast frame e' "costretto" ad analizzarlo
  - Questo comporta degli interrupts alla CPU con degrado delle performance
- La soluzione adottata e' il partizionamento del traffico tramite VLAN

Partecipazione ad una VLAN

- VLAN statiche
  - Vengono assegnati manualmente gruppi di porte sullo switch a specifiche VLAN. L'utente partecipa alla VLAN mappata sulla porta dello switch a lui assegnata

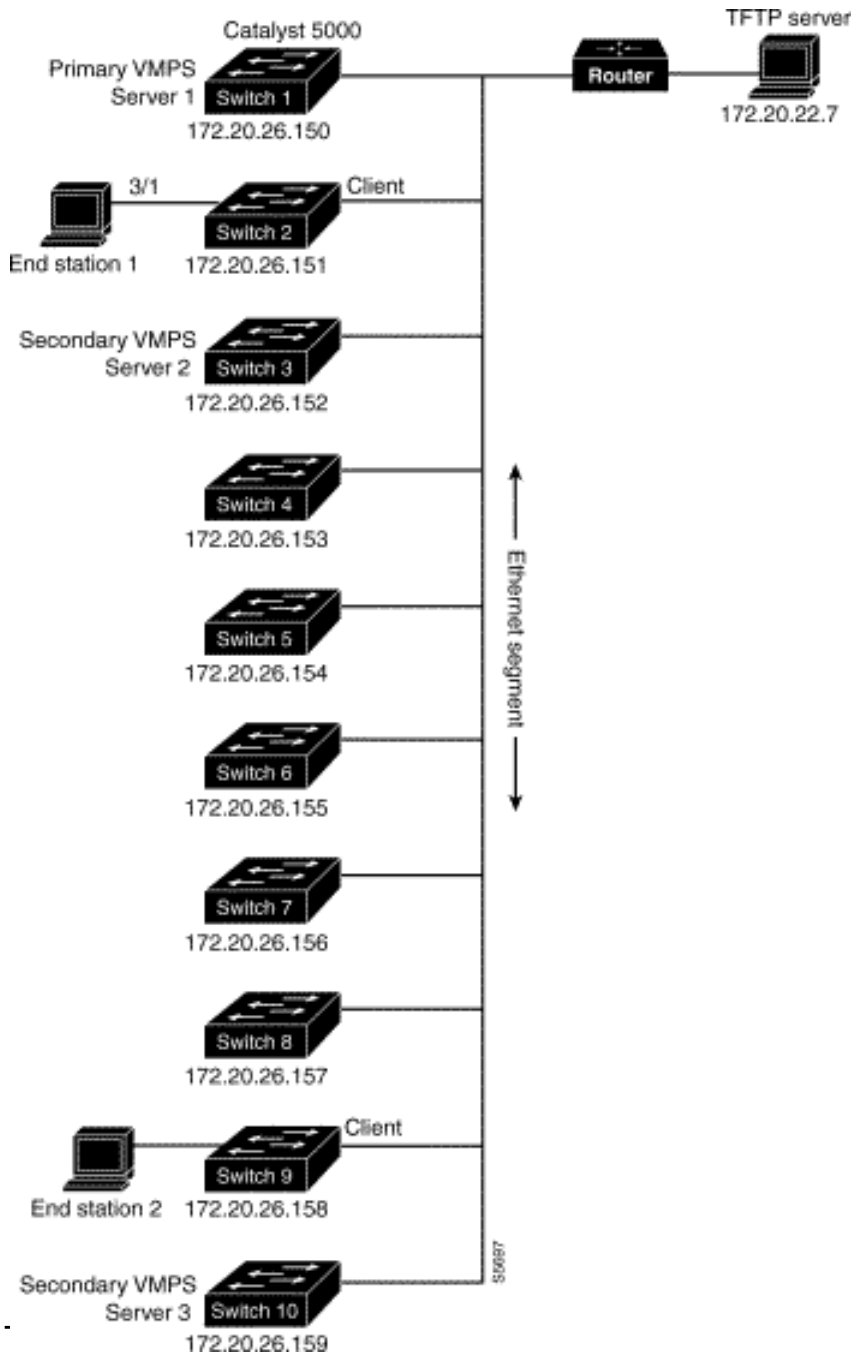
- VLAN dinamiche
  - L'utente partecipa alla VLAN in base al proprio MAC Address. **In questo modo si garantisce la mobilita' dell'utente in tutto il campus**.
  - Soluzione proprietaria Cisco VMPS (VLAN Membership Policy Server)

Configurazione delle VLAN statiche



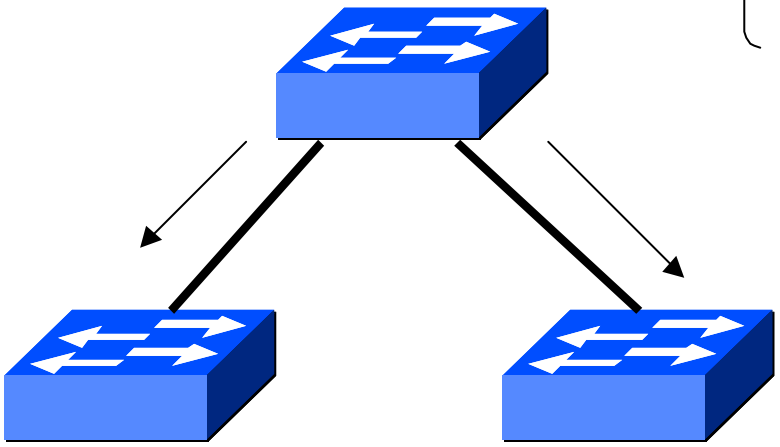
VLAN dinamiche

- In questo esempio il VMPS server e il VMPS client sono su switch separati
- Switch 1 e' il primary VMPS server
- Switch 3 e 10 sono secondary VMPS servers
- Gli host sono connessi sui due Switch client 2 e 9
- Il database di configurazione e' memorizzato sul TFTP Server con IP 172.20.22.7 e scaricato sui VMPS server
- Ogni Mac address noto viene mappato sulla VLAN ad esso assegnata nel file di configurazione
- Per tutti i Mac address sconosciuti:
  - Porta in shutdown oppure
  - Assegnati a fall-back VLAN



VLAN Trunk Protocol (VTP)

- Grazie a questo protocollo proprietario e' possibile definire, su uno Switch VTP Server, il database delle VLAN, che sara' visibile su tutti gli Switch VTP Client



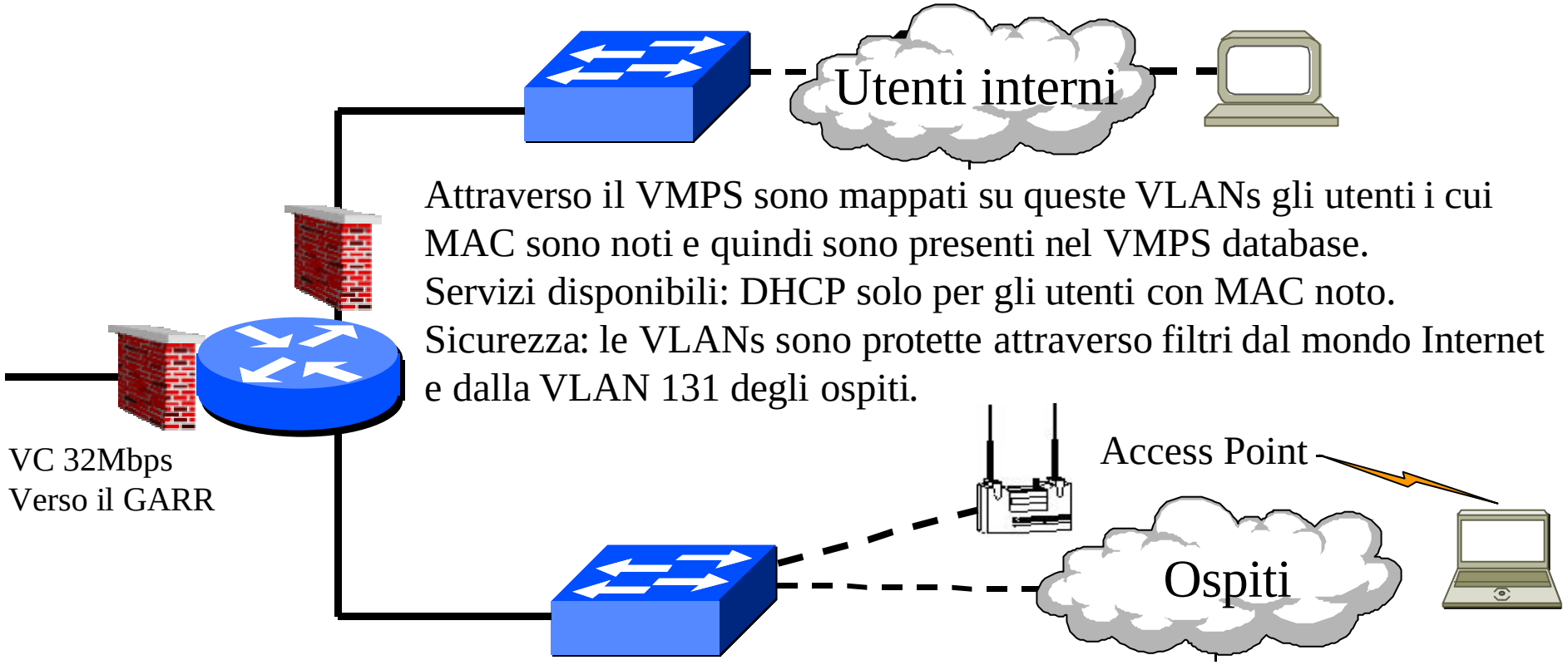
Su questo switch e' possibile definire e cancellare VLANs

Su questi switch non sono possibili cambiamenti sul Database delle VLANs

Impostazione del VTP

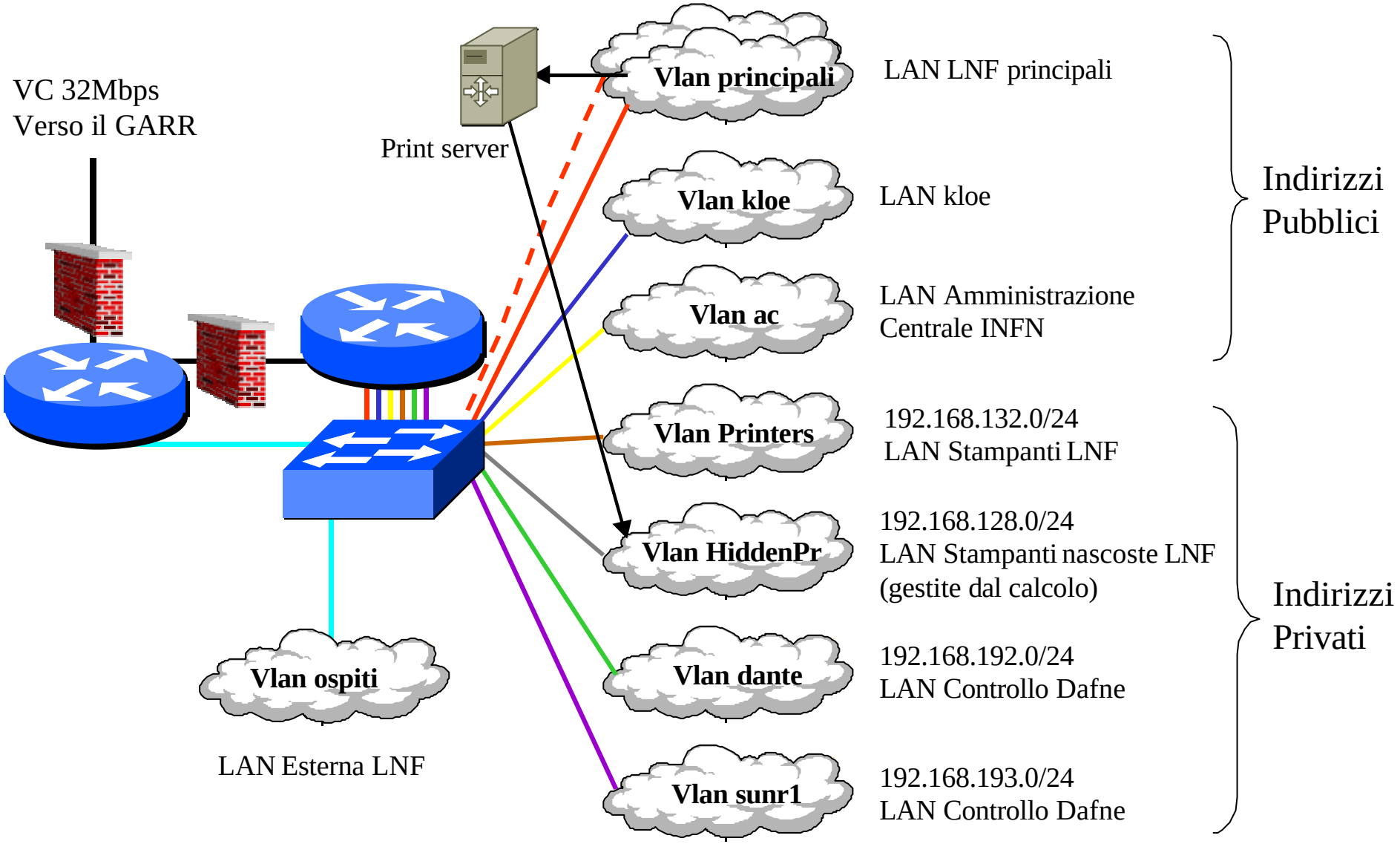
- Il database delle VLAN viene comunque propagato sugli switch che partecipano al dominio VTP attraverso la definizione dei vari trunk di collegamento
- VTP Pruning:
  - Grazie a questa funzionalita' e' possibile ottimizzare il traffico sui trunk.
  - Verra' inoltrato sui trunk, il traffico delle VLANs effettivamente utilizzate dagli switch.

Configurazione delle VLANs ai LNF



VLAN 131 o LANesterna mappata su network IP pubblica.
Su questa VLAN vengono proiettati gli utenti ospiti i cui MAC sono sconosciuti al VMPS.
Inoltre sono collegati a questa VLAN tutti gli access point del wireless.
Servizi disponibili: DHCP aperto senza che sia conosciuto il MAC, libero accesso ad Internet.
Limiti: gli utenti su questa VLAN sono a tutti gli effetti utenti esterni e sono sottoposti alle stesse politiche dei filtri (access-list) di un qualsiasi utente del mondo Internet.

Suddivisione utenti interni



Gestione degli utenti sul Primary VMPS Server

```
swlnf1> (enable) show vmps mac
00-00-39-db-60-eb default   172.16.36.101   4/26    367,08:16:27   Success
08-00-20-b0-fc-5d sunr1     172.16.9.1      6/34    367,08:13:27   Success
08-00-20-c3-fe-a4 dante     172.16.9.1      6/1     367,09:13:28   Success
08-00-20-fd-99-04 sunr2     0.0.0.0                   0,00:00:00   Success
08-00-20-f8-8c-6c sunr2     172.16.9.1      6/35    367,09:13:28   Success
00-c0-85-2a-ef-bb HiddenPri 172.16.36.2     6/42    367,08:21:23   Success
00-c0-85-2b-9f-da HiddenPri 172.16.36.201   6/31    367,10:17:03   Success
00-80-ad-07-77-1e ac        0.0.0.0                   0,00:00:00   Success
00-01-02-f5-ca-ec default   172.16.36.101   4/15    367,10:16:27   Success
00-01-02-f5-ca-ef default   172.16.36.201   4/28    367,08:17:00   Success
```

Vantaggi delle soluzioni L2 adottate

- Minimizzazione del carico amministrativo per il network manager o per l'utente:
  - Garanzia di mobilita' per gli host interni
  - Possibilita' di connessione degli utenti occasionali
- Sicurezza:
  - Controllo su base MAC degli host
  - Abilitazione sicura di prese non presidiate

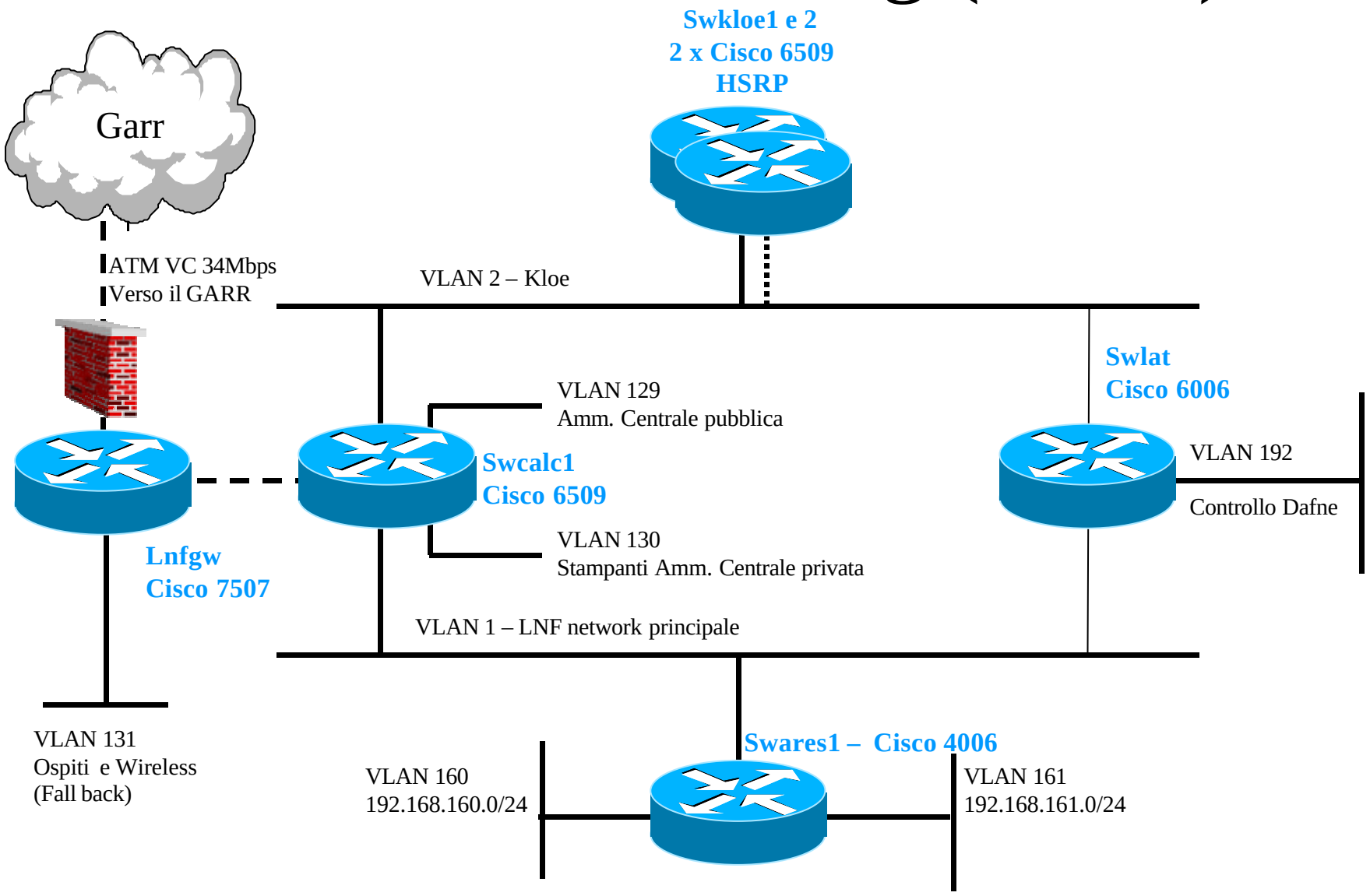
Svantaggi

- VMPS e VTP soluzioni proprietarie
  - Costringono ad avere una rete omogenea e monolitica
- Startup difficoltoso per il censimento dei MAC Address
  - Da noi realizzato con script automatici di interrogazione dell'ARP cache del router

Evoluzione relativa alla mobilita’

- IEEE 802.1x autenticazione su base porta attraverso Server RADIUS
  - Assegnazione di VLAN in funzione della username
- Client integrato nel Sistema Operativo solo su Microsoft XP
  - Per ora impraticabile in ambienti con client eterogenei

LNF internal routing (OSPF)



Pop GARR LNF located

- Ai Laboratori Nazionali di Frascati e' localizzato il POP di accesso alla rete GARR per tutti gli enti della Area di Ricerca di Frascati
  - ASI SDC
  - ENEA
  - ESA-Esrin
  - INFN LNF
  - ISPESL
  - MIUR-MPC
  - Oss. Astronomico di Roma

Pop GARR LNF located

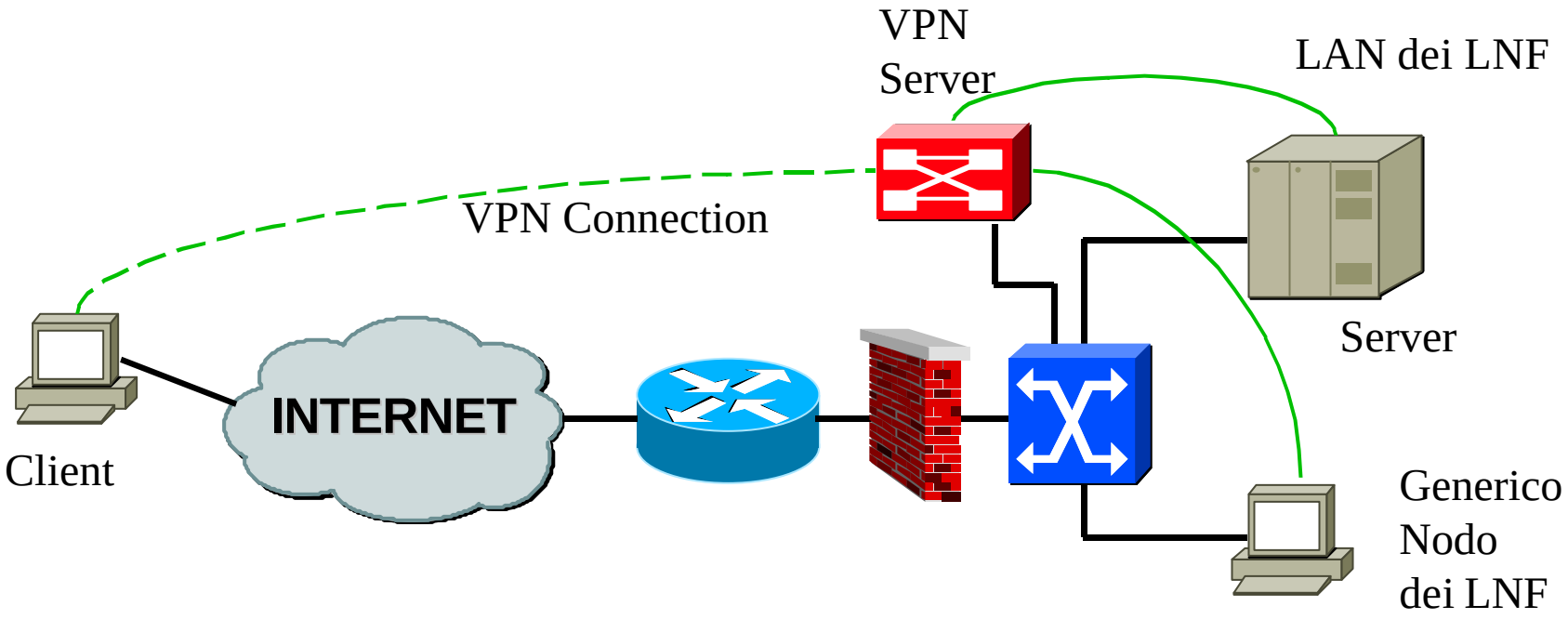
- La collocazione del POP e' nell'edificio Calcolo rispettando i migliori criteri di affidabilita'
  - Sicurezza dei locali (accesso controllato)
  - UPS e gruppo elettrogeno
  - Condizionamento
- Tale soluzione ha permesso fino ad ora di amministrare e di gestire tecnicamente il POP in modo molto piu' agile, superando i limiti derivanti dalla gestione di POP in casa dei Providers e minimizzando i tempi tecnici di intervento dovuti alla burocrazia.

Sicurezza della LAN

- La LAN e’ protetta da pseudoFirewall basato sulle ACL estese sul router di frontiera:
  - In: Accesso ad alcuni servizi gestiti dal calcolo
  - In: TCP-Established
  - Out: antispoofing, black list
- Mail check su SMTP relay:
  - Antivirus centralizzato (RAV)
  - AntiSPAM (SpamAssassin)

Sicurezza della LAN

- Le ACL sul router di frontiera, pur realizzando un sistema robusto ed affidabile, limita a volte le possibilita' di accesso da parte dell'utenza esterna
- L'acceso diventera' molto piu' semplice tramite l'uso di Virtual Private Network gia' sperimentate, ma non ancora in produzione



Domande?

angelo.veloce@lnf.infn.it