



*Consiglio Nazionale delle Ricerche
Istituto di Calcolo e Reti ad Alte Prestazioni*

Infrastruttura di Rete dell'ICAR-CNR Sede di Napoli

Angelo Esposito, Gennaro Oliva

Istituto di Calcolo e Reti ad Alte Prestazioni del Consiglio
Nazionale delle Ricerche (ICAR-CNR)
Via Pietro Castellino, 111 – 80131 Napoli

angelo.esposito@icar.cnr.it
gennaro.oliva@icar.cnr.it

Versione 4.0

RT-ICAR-NA-2020-05

Dicembre 2020



Consiglio Nazionale delle Ricerche, Istituto di Calcolo e Reti ad Alte Prestazioni (ICAR) Sede di Napoli, Via P. Castellino 111, I-80131 Napoli, Tel: +39-0816139508, Fax: +39-0816139531, e-mail: napoli@icar.cnr.it, URL: www.icar.cnr.it



Consiglio Nazionale delle Ricerche
Istituto di Calcolo e Reti ad Alte Prestazioni

Infrastruttura di Rete dell'ICAR-CNR Sede di Napoli

Angelo Esposito, Gennaro Oliva

Istituto di Calcolo e Reti ad Alte Prestazioni del Consiglio
Nazionale delle Ricerche (ICAR-CNR)
Via Pietro Castellino, 111 – 80131 Napoli

angelo.esposito@icar.cnr.it
gennaro.oliva@icar.cnr.it

Versione 4.0

RT-ICAR-NA-2020-05

Dicembre 2020

I rapporti tecnici dell'ICAR-CNR sono pubblicati dall'Istituto di Calcolo e Reti ad Alte Prestazioni del Consiglio Nazionale delle Ricerche. Tali rapporti, approntati sotto l'esclusiva responsabilità degli autori, descrivono l'attività del personale e dei collaboratori dell'ICAR, in alcuni casi in un formato preliminare prima della pubblicazione definitiva in altra sede.

Infrastruttura di Rete dell'ICAR-CNR Sede di Napoli

Angelo Esposito, Gennaro Oliva

Istituto di Calcolo e Reti ad Alte Prestazioni del Consiglio Nazionale delle Ricerche (ICAR-CNR) Via Pietro Castellino, 111 – 80131 Napoli

angelo.esposito@icar.cnr.it, gennaro.oliva@icar.cnr.it,

Abstract

Questo lavoro descrive l'infrastruttura di rete della sede di Napoli dell'Istituto di Calcolo e Reti ad Alte prestazioni (ICAR) e la sua collocazione all'interno della rete dell'area della ricerca Napoli I del Consiglio Nazionale delle Ricerche (CNR). La descrizione riguarda le caratteristiche delle apparecchiature di rete, la loro configurazione e il loro dispiegamento presso la sede dell'Istituto.

Keywords: Infrastruttura di Rete, Topologia della Rete, Attrezzature di Rete, Dispiegamento dell'infrastruttura della rete, configurazione degli apparati di rete






1. Introduzione


L'Istituto di Calcolo e Reti ad Alte Prestazioni (ICAR) [1], è un Istituto del Consiglio Nazionale delle Ricerche (CNR) [2] che afferisce al Dipartimento di Ingegneria, ICT e Tecnologie per l'Energia e i Trasporti (DIITET) [3]. L'Istituto è presente sul territorio nazionale con tre sedi, Rende, Napoli e Palermo. La sua missione è quella di sviluppare ricerca, trasferimento tecnologico e alta formazione nell'area dei sistemi intelligenti a funzionalità complessa. L'Istituto sviluppa applicazioni significative nel campo dell'e-health, energia, sicurezza, bioinformatica, beni culturali, High Performance Computing e città intelligenti.

In questo lavoro si propone a valle dall'attività di ricognizione degli apparati di rete dell'Istituto, svolta dagli autori, la descrizione dell'infrastruttura di Rete dell'ICAR. La descrizione riguarda le caratteristiche delle apparecchiature di rete, la loro configurazione e il loro dispiegamento presso la sede di Napoli dell'Istituto.

2. Attrezzature di Rete

In questa sezione sono riportate le attrezzature di rete dispiegate presso l'Istituto di Calcolo e Reti ad Alte prestazioni della sede di Napoli. In tabella sono schematicamente riportati i modelli e la quantità delle apparecchiature di rete dispiegate.

Modello	Quantità
Switch Juniper Networks EX 2200 24 Port Gig Switch 10/100/1000 Base with 4x SFP Ports [4]	11
	
Cisco - ASA5520-BUN-K9 - ASA 5520 Appliance with SW, HA, 4GE+1FE, 3DES/AES [5]	1
	
Catalyst Series 3500 XL 48 Port Switch [6]	1
	
Bay Networks - Nortel Networks BayStack 350-24T Switch [7]	1
	
Juniper Networks EX4200-24F 24SFP 24 Port 100/1000Base-X SFP Switch [8]	4
	

Ubiquiti Networks UAP-AC-PRO WLAN access point - WLAN access points (1300 Mbit/s, 10,100,1000 Mbit/s, 1300 Mbit/s, 122 m, CE, FCC, IC, AES, TKIP, WEP, WPA, WPA2) [9]	4
	

Le attrezzature di rete dispiegate presso la sede dell'ICAR di Napoli sono riportate graficamente in questo lavoro. In particolare, per ogni switch sono indicate le seguenti informazioni: nome dello switch *switch name*, *parte host del suo indirizzo IP di gestione*, *produttore e modello dello switch*, *rack di posizionamento*.

La rete dell'ICAR (ICAR-LAN) è parte della rete dell'area della ricerca NA 1 del CNR (AREA-NA1- LAN) che collega tutti gli istituti presenti nei diversi edifici della sede di via Pietro Castellino 111 del CNR. L'ICAR in particolare occupa parte dell'edificio 4.

La rete AREA-NA1-LAN ha una topologia a stella per cui ogni switch della rete è collegato direttamente in fibra multimodale ad uno di 4 switch Juniper EX 4200 da 24 porte presenti nel centro stella configurati in stack (Figura 1).

```
> show virtual-chassis

Virtual Chassis ID: 6af7.6ee9.27ac
Virtual Chassis Mode: Enabled

Member ID  Status  Serial No  Model  Mstr  Role  Mixed Neighbor List
0 (FPC 0)  Prsnt   BR0212503851  ex4200-24f  128  Master*  N  1 vcp-0
           3 vcp-1
1 (FPC 1)  Prsnt   BR0213033910  ex4200-24f  128  Linecard  N  2 vcp-0
           0 vcp-1
2 (FPC 2)  Prsnt   BR0213033903  ex4200-24f  128  Linecard  N  3 vcp-0
           1 vcp-1
3 (FPC 3)  Prsnt   BR0216060225  ex4200-24f  128  Backup   N  0 vcp-0
           2 vcp-1

Member ID for next new member: 4 (FPC 4)
```

Figura 1: Configurazione stack centro stella AREA-NA1-LAN

Le interfacce di management degli switch sono tutte raggiungibili sulla subnet di management della rete AREA-NA1-LAN, la cui parte network degli indirizzi IP verrà di seguito indicata con la stringa XXX.XXX.XXX.

3. Dispiegamento delle Attrezzature di Rete

Il lavoro di ricognizione delle apparecchiature di rete dell'ICAR ha previsto la localizzazione fisica di ogni dispositivo. In questa sezione è presentato graficamente il dispiegamento delle attrezzature di rete di competenza dell'ICAR. La rappresentazione grafica è stata scelta in quanto consente in maniera semplice e veloce l'individuazione e la localizzazione di ogni dispositivo di rete.

Di seguito sono riportate sulle planimetrie dell'edificio 4 le collocazioni dei dispositivi di rete dell'ICAR.

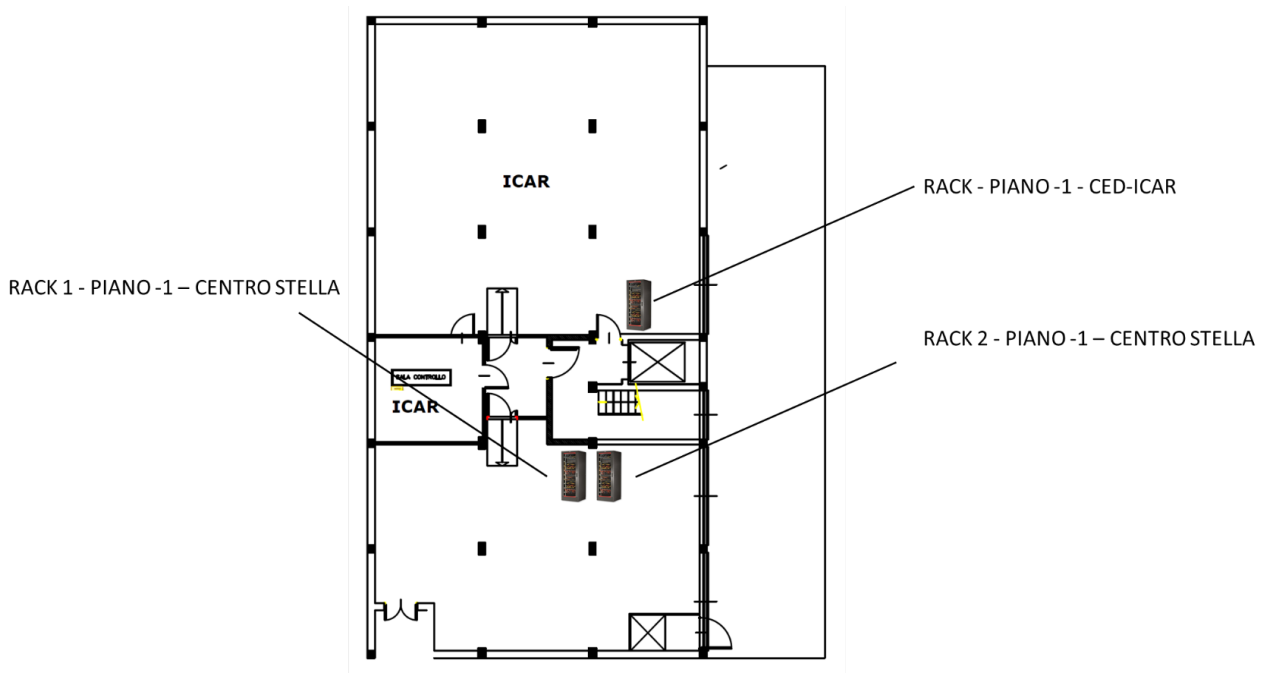


Figura 2 - Planimetria Edificio 4 - Piano -1

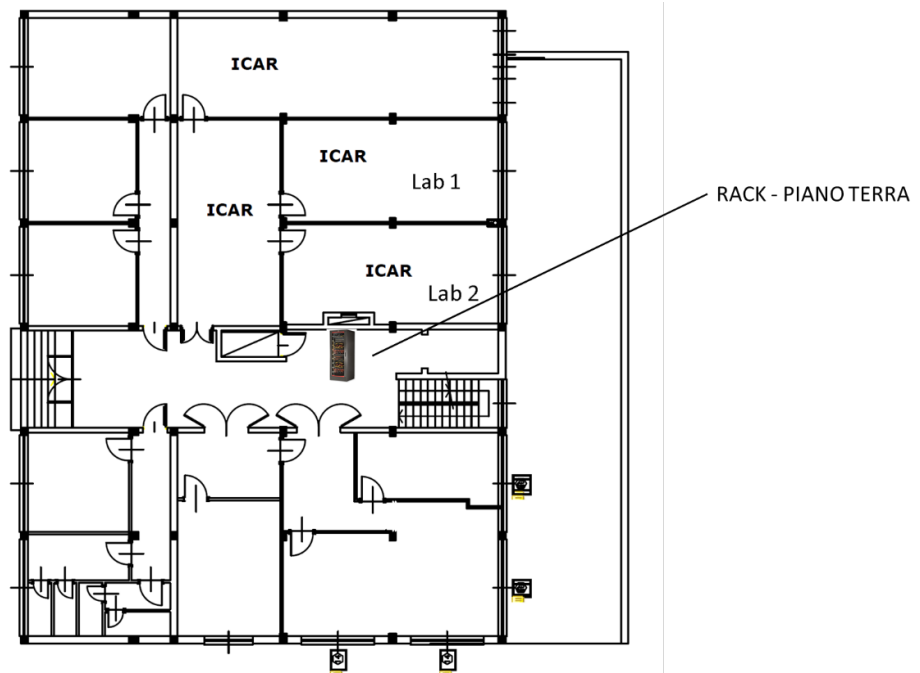
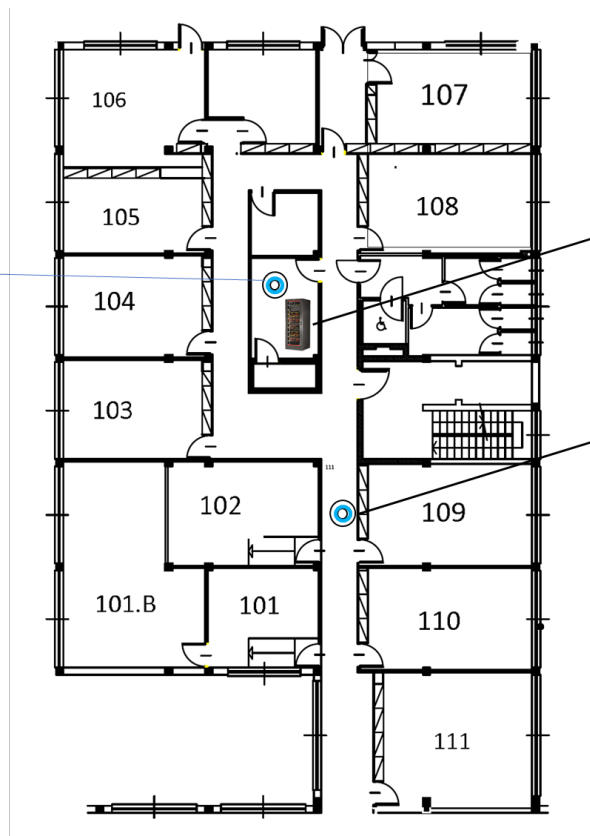


Figura 3 - Planimetria Edificio 4 - Piano Terra

YYY.YYY.YYY.18
f0:9f:c2:fc:40:23

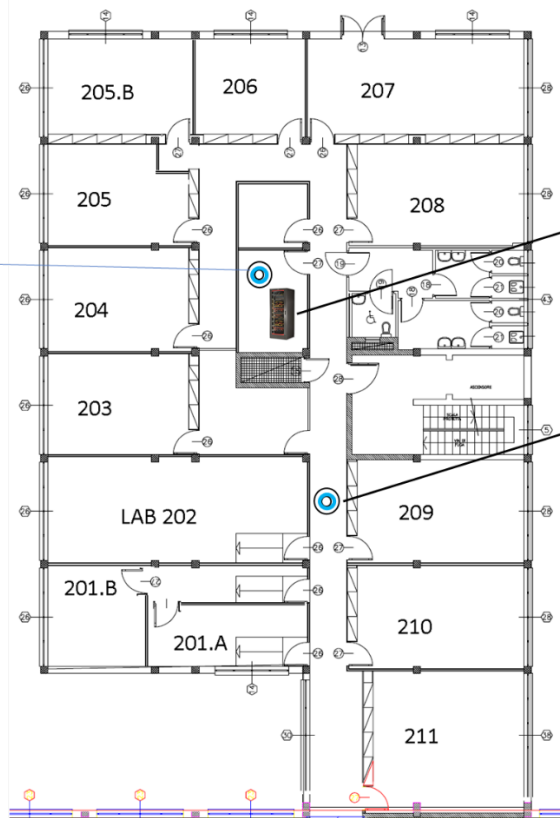


RACK - PIANO 1 - ICAR

YYY.YYY.YYY.14
f0:9f:c2:fc:0d:78

Figura 4 - Planimetria Edificio 4 - Piano 1

YYY.YYY.YYY.12
f0:9f:c2:fc:0d:b1



RACK - PIANO 2 - ICAR

YYY.YYY.YYY.5
f0:9f:c2:fc:40:1e

Figura 5 - Planimetria Edificio 4 - Piano 2

4. Composizione dei Rack della rete ICAR-LAN

Il Rack rappresentato graficamente in Figura 1 è localizzato presso l'edificio numero 4 dell'Area di Ricerca NA1 piano -1 stanza CED-ICAR ed è costituito dagli apparati di rete specificati in figura. In particolare il rack è costituito da uno switch Bay Stack modello 350-24T, da due switch Juniper modello EX2200 con 24 porte e con ottetti host 216 e 36. Completa il RACK un Firewall modello Cisco ASA 5520 dotato di 4 interfacce di rete di cui una avente ottetto host 12 sulla rete di management, e 3 interfacce con i seguenti indirizzi IP privati assegnati: 172.16.1.1, 172.16.2.1, 172.16.3.1.

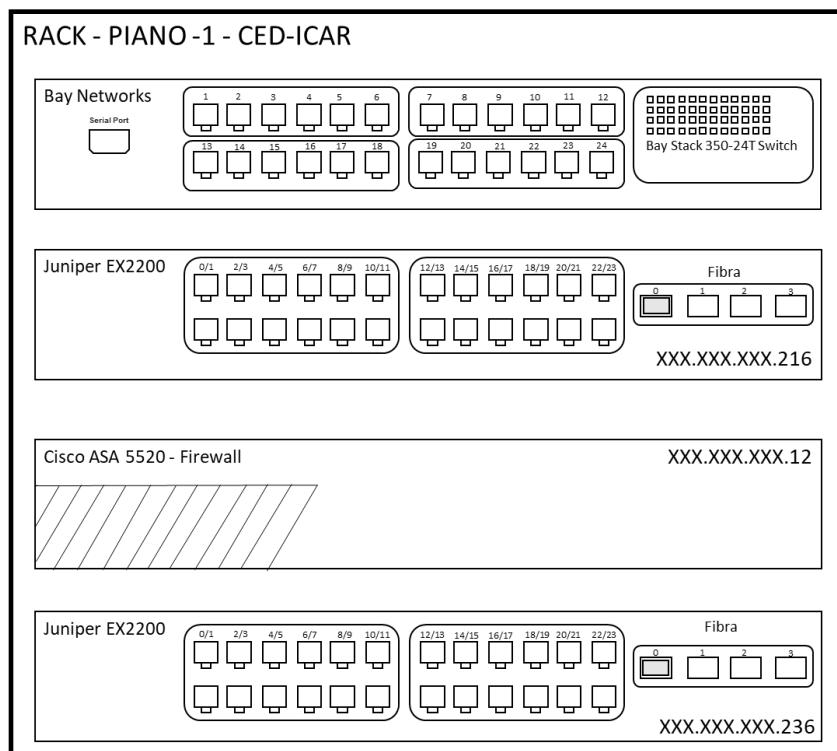


Figura 6 - Rack Piano -1 - CED – ICAR

Il Rack rappresentato graficamente in Figura 7 è localizzato presso l'edificio numero 4 dell'Area di Ricerca NA1 piano terra ed è costituito dagli apparati di rete specificati in figura. In particolare, il rack è costituito da due switch Juniper modello EX2200 a 24 porte con ottetti host 247 e 192 sulla rete di management.

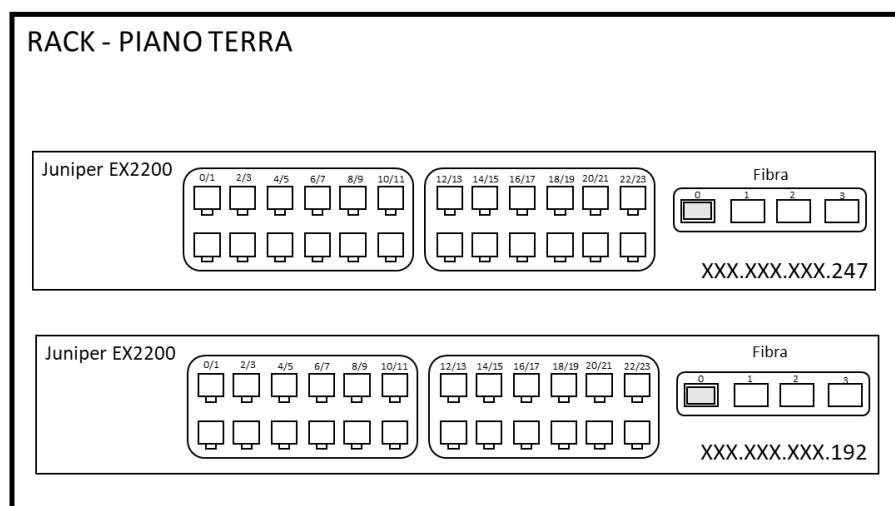


Figura 7 – Rack Piano Terra

Il Rack rappresentato graficamente in Figura 8 è localizzato presso l'edificio numero 4 dell'Area di Ricerca NA1 piano 1 stanza ICAR ed è costituito dagli apparati di rete specificati in figura. In particolare il rack è costituito da due switch Juniper modello EX2200 a 24 porte con ottetti host 233 e 237 e uno switch Cisco modello Catalyst 3500 XL a 24 porte con ottetto host 21 sulla rete di management.

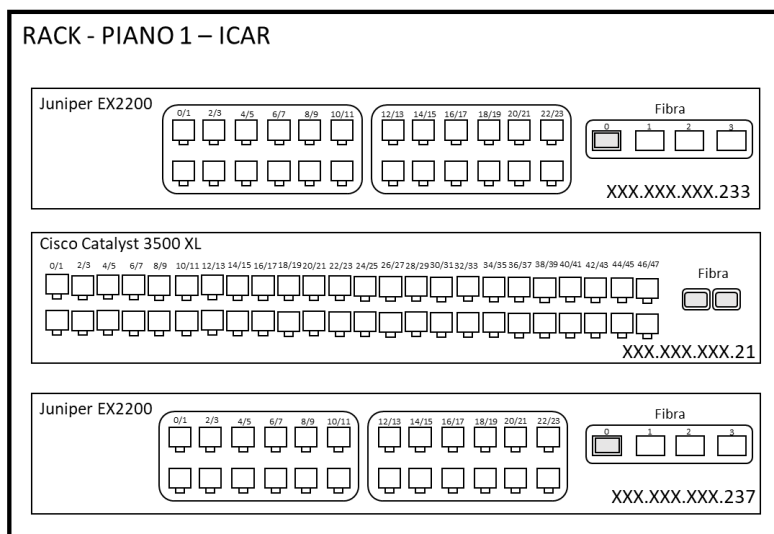


Figura 8 - Rack - Piano 1 - ICAR

Il Rack rappresentato graficamente in Figura 9 è localizzato presso l'edificio numero 4 dell'Area di Ricerca NA1 piano 2 stanza ICAR ed è costituito dagli apparati di rete specificati in figura. In particolare il rack è costituito da quattro switch Juniper modello EX2200 con i seguenti ottetti host 17, 234, 250, 238.

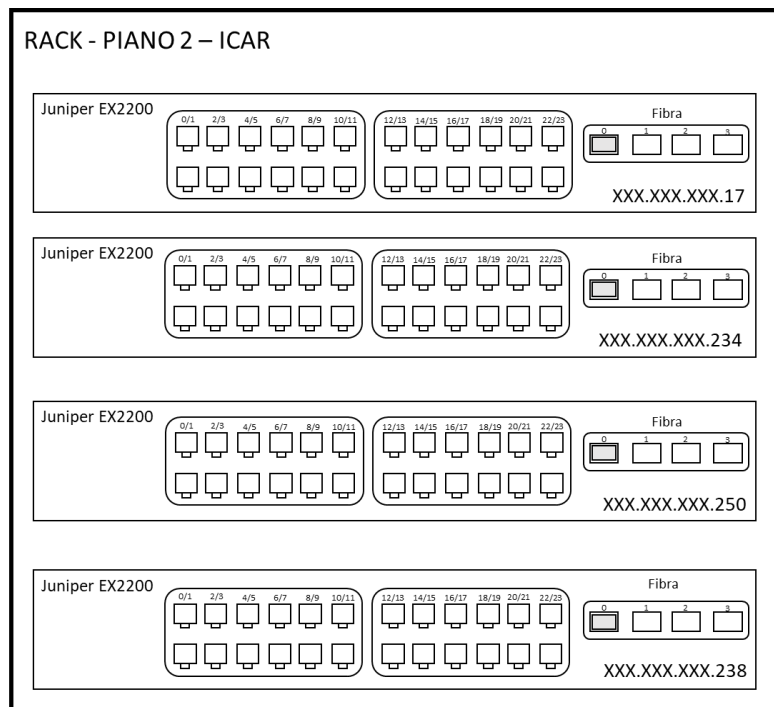


Figura 9 - Piano 2 - ICAR

I Rack che sono rappresentati graficamente in Figura 10 sono localizzati presso l'edificio numero 4 dell'Area di Ricerca NA1, piano -1 stanza centro stella e sono costituiti dagli apparati di rete specificati in figura. Gli switch presenti nei due Rack sono condivisi tra gli istituti che fanno parte

dell'Area di ricerca NA1. Inoltre, in figura sono evidenziati anche i collegamenti tra gli switch del centro stella e quelli di frontiera della rete GARR.

In particolare i 4 switch Juniper modello EX 4200 sono configurati in trunk mode e rispondono all'indirizzo IP `YYY.YYY.YYY.1` (dove con `YYY.YYY.YYY` indichiamo la subnet associata ai servizi di rete dell'Area della ricerca NA1), mentre lo switch Juniper modello EX2200 con ottetto host 195.

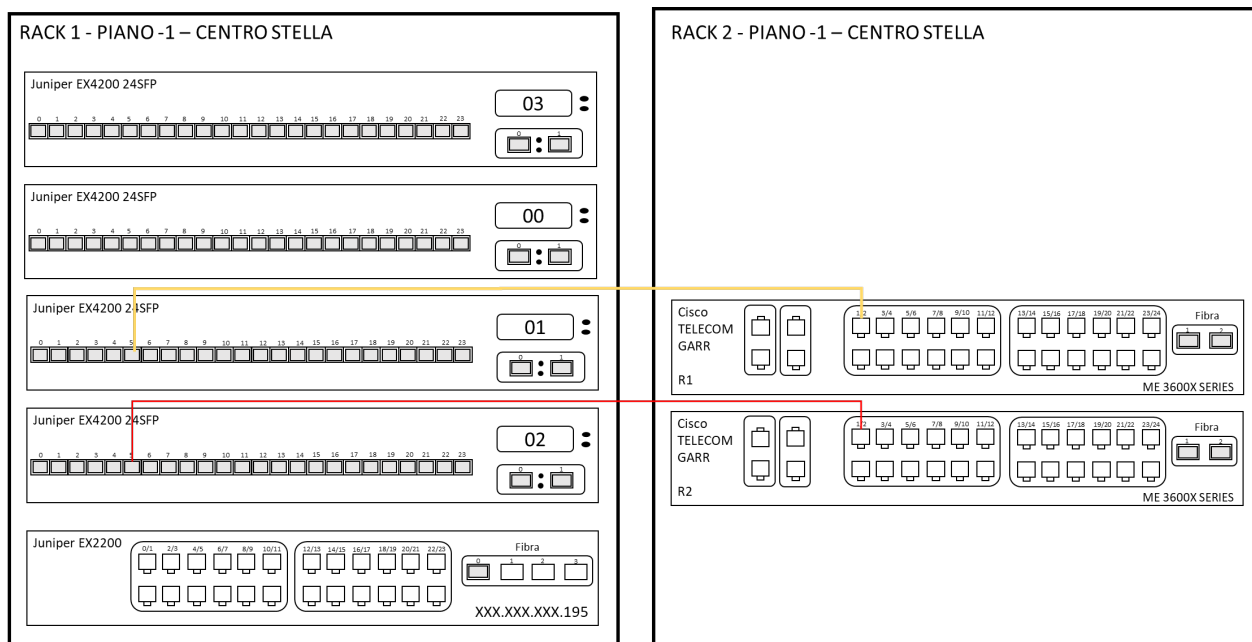


Figura 10 - Rack 1 e 2 - Piano -1 - Centro Stella

5. Topologia della rete

In questa sezione è descritta la topologia della rete dell'Istituto. Ogni switch della rete è collegato direttamente ad uno degli switch presenti nel centro stella collegati a loro volta agli switch di frontiera della rete GARR. Tale configurazione determina una rete con topologia a stella dove tutti i nodi (switch della rete) sono collegati ad un nodo centrale che in questo caso è rappresentato da uno dei quattro switch Juniper EX 4200 da 24 porte (che rappresentano logicamente un unico nodo, in quanto configurati in trunk mode con indirizzo ip `YYY.YYY.YYY.1`).

Inoltre, dalla attività di ricognizione effettuata sono stati determinati i collegamenti tra i vari nodi della rete. Tali collegamenti sono riportati graficamente in Figura 11.

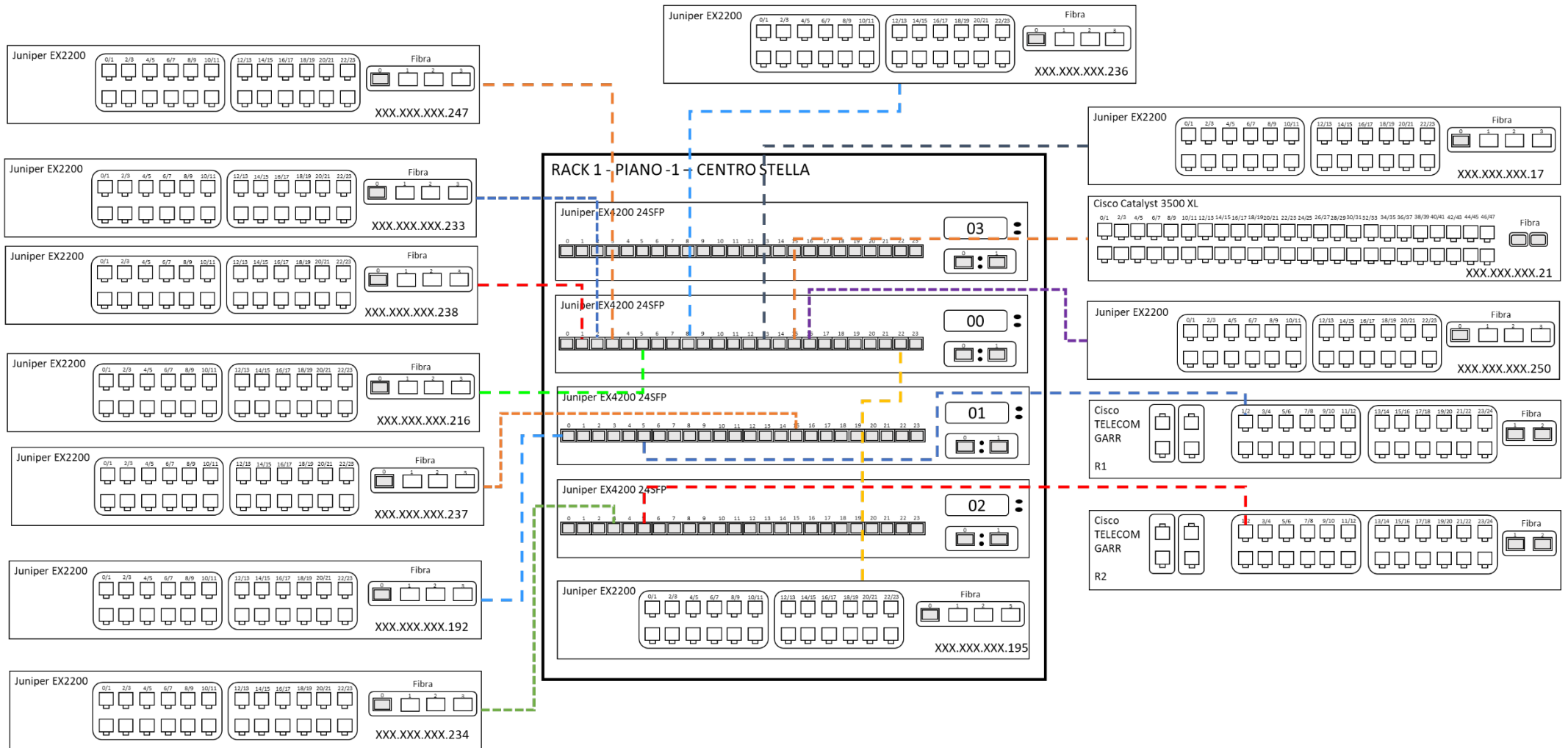


Figura 11 - Configurazione Tipologia Rete ICAR

6. Configurazione delle apparecchiature di rete

In questa sezione sono riportate le configurazioni delle apparecchiature che costituiscono l'infrastruttura di rete dell'Istituto di Calcolo e Reti ad Alte prestazioni della sede di Napoli. L'analisi delle apparecchiature di rete ha consentito la definizione di una serie di schede tecniche dettagliate delle informazioni di interesse per ogni switch. In particolare, le informazioni raccolte riguardano le Virtual Local Area Network (Vlan), le Subnet, gli Indirizzi IP e i nomi logici degli switch. Prima di riportare le schede tecniche di dettaglio di ogni switch, di seguito sono descritte le Vlan definite per la rete ICAR:

- **AREA-NEW:** è la Vlan dedicata all'Area di Ricerca NA 1. Su questa rete sono presenti diversi host e macchine server che hanno un indirizzo IP che appartiene alla subnet `YYY.YYY.YYY.0/24`. Questa Vlan è condivisa dagli istituti che fanno parte dell'area di ricerca. Il Tag Id della Vlan "Area New" è 112.
- **ICAR-INSIDE:** è la Vlan dedicata alle postazioni di lavoro presenti negli uffici del personale dell'istituto. Su questa rete sono presenti gli host che hanno un indirizzo IP che appartiene alla subnet `172.16.1.0/24`. Questa rete è protetta da un dispositivo Firewall con valore di sicurezza assegnato uguale a 100. Il Tag Id della vlan "ICAR-INSIDE" è 50.
- **ICAR-LAB:** è la Vlan dedicata alle postazioni di lavoro presenti nei laboratori. Su questa rete sono presenti dispositivi che hanno indirizzo IP che appartiene alla della subnet `172.16.3.0/24`. Questa rete è protetta da un dispositivo Firewall con valore di sicurezza assegnato uguale a 75. Il Tag Id della vlan "ICAR-LAB" è 52.
- **ICAR-DMZ:** è la Vlan definita e utilizzata per le apparecchiature e server di front-end. Su questa rete sono presenti macchine che hanno indirizzo IP che appartiene alla subnet `172.16.2.0/24`. Questa rete è protetta da un dispositivo Firewall con valore di sicurezza assegnato uguale a 25. Il Tag Id della vlan "ICAR-DMZ" è uguale a 51.
- **ICAR-NA:** è la Vlan dedicata agli host che necessitano di essere esposti su internet con indirizzo IP pubblico. Su questa rete sono presenti macchine server che offrono servizi al personale dell'Istituto e che hanno indirizzo IP che appartiene alla subnet `140.164.14.0/24`. Il Tag Id della vlan "ICAR-NA" è 11.
- **Oliva:** è la Vlan dedicata alle interfacce di management dei server in dotazione all'ICAR che non è instradata su internet. Le apparecchiature su questa rete hanno indirizzi ip che appartengono alla subnet `140.164.78.0/24`. Il Tag Id della vlan "Oliva" è 78.

Altre Vlan presenti nelle configurazioni degli switch ma non di competenza dell'ICAR sono descritte di seguito:

- **IAC-NA:** è la Vlan definita e dedicata alle apparecchiature dell'Istituto per le Applicazioni del Calcolo "Mauro Picone" (IAC). Su questa rete sono presenti dispositivi e macchine server che hanno indirizzo ip che appartiene alla subnet `140.164.12.0/24`. Questa Vlan è utilizzata esclusivamente dall'Istituto IAC e non di competenza ICAR. Il Tag Id della Vlan "IAC-NA" è 113.
- **imm-na:** è la Vlan definita e dedicata alle apparecchiature dell'Istituto per la microelettronica e microsistemi (IMM sede di Napoli). Su questa rete sono presenti dispositivi e macchine server che hanno indirizzo ip che appartiene alla subnet

140.164.38.0/24. Questa Vlan è utilizzata esclusivamente dall'Istituto IMM e non di competenza ICAR. Il Tag Id della Vlan "imm-na" è 21.

- **igb:** è la Vlan definita e dedicata alle apparecchiature dell'Istituto di genetica e biofisica "Adriano Buzzati Traverso" (IGB). Su questa rete sono presenti dispositivi e macchine server che hanno indirizzo ip che appartiene alla subnet 140.164.60.0/24. Questa Vlan è utilizzata esclusivamente dall'Istituto IGB e non di competenza ICAR. Il Tag Id della Vlan "igb" è 2.

L'analisi relativa alla configurazione degli switch è riportata in forma tabellare, per ogni switch è presente una tabella dove sono specificate le seguenti informazioni: modello dello switch, rack di riferimento, l'ottetto host e il nome logico dello switch. Inoltre, per ogni vlan è specificato il tag id, la subnet e le interfacce di rete collegate alla vlan.

Modello	Rack	Ottetto Host	Nome
Juniper EX2200	RACK - PIANO 2 – ICAR	17	ji.17Ed4_p2
Vlan	Tag id	Subnet	Interfaces
area-new	112	xxx.xxx.7.0/24	0/1/0
iac-na	113	xxx.xxx.12.0/24	0/1/0
icar-inside	50	172.16.1.0/24	0/0/11-23; 0/1/0
icar-lab	52	172.16.3.0/24	0/1/0
icar-na	11	xxx.xxx.14.0/24	0/0/0, 0/0/1-10

Modello	Rack	Ottetto Host	Nome
Juniper EX2200	RACK - PIANO 2 – ICAR	234	ji.234Ed4_p2
Vlan	Tag id	Subnet	Interfaces
area-new	112	xxx.xxx.7.0/24	0/0/10, 0/1/0
c3p-new	115	xxx.xxx.58.0/24	-----
icar-inside	50	xxx.xxx.1.0/24	0/0/1-5,7,9,12,15-17,19-23; 0/1/0
icar-na	11	xxx.xxx.14.0/24	0/0/0,6,8,11,13,14,18; 0/1/0

Modello	Rack	Ottetto Host	Nome
Juniper EX2200	RACK - PIANO 2 – ICAR	250	ji.250Ed4_p2
Vlan	Tag id	Subnet	Interfaces
area-new	112	xxx.xxx.7.0/24	0/1/0.0
c3p-new	115	xxx.xxx.58.0/24	0/1/0.0
icar-inside	50	172.16.1.0/24	0/0/4-23; 0/1/0
icar-na	11	xxx.xxx.14.0/24	0/0/0-3; 0/1/0
icar-lab	52	172.16.3.0/24	0/1/0

Modello	Rack	Ottetto Host	Nome
Juniper EX2200	RACK - PIANO 2 – ICAR	238	ji.238Ed4_p2
Vlan	Tag id	Subnet	Interfaces
area-new	112	xxx.xxx.7.0/24	0/0/4,20; 0/1/0
c3p-new	115	xxx.xxx.58.0/24	0/0/1,16,18; 0/1/0

icar-inside	50	172.16.1.0/24	0/0/2,3,12,14,15,19,22; 0/1/0
icar-na	11	xxx.xxx.14.0/24	0/0/0,6-9
icar-lab	52	172.16.3.0/24	0/0/10,11,13; 0/1/0

Modello	Rack	Ottetto Host	Nome
Juniper EX2200	RACK - PIANO 1 – ICAR	233	ji.233Ed4_p1
Vlan	Tag id	Subnet	Interfaces
area-new	112	xxx.xxx.7.0/24	0/0/16,17,20; 0/1/0
c3p-new	115	xxx.xxx.58.0/24	-----
icar-inside	50	172.16.1.0/24	0/0/1-13,15,19,21,22; 0/1/0
icar-na	11	xxx.xxx.14.0/24	0/0/0,14,18,23; 0/1/0
no-route	81	xxx.xxx.81.0/24	0/1/0
vlan_1	1	xxx.xxx.40.0/24 xxx.xxx.59.0/24	-----

Modello	Rack	Ottetto Host	Nome
Juniper EX2200	RACK - PIANO 1 – ICAR	237	ji.237Ed4_p1
Vlan	Tag id	Subnet	Interfaces
area-new	112	xxx.xxx.7.0/24	0/0/1, 0/1/0
iac-na	113	xxx.xxx.12.0/24	0/0/13, 0/1/0
icar-inside	50	172.16.1.0/24	0/0/0, 0/0/2-12,14-16,18-23; 0/1/0
icar-na	11	xxx.xxx.14.0/24	0/0/17, 0/1/0
vlan_1	1	xxx.xxx.40.0/24 xxx.xxx.59.0/24	-----

Modello	Rack	Ottetto Host	Nome
Juniper EX2200	RACK - PIANO TERRA	247	ji.247Ed4_p0
Vlan	Tag id	Subnet	Interfaces
area-new	112	xxx.xxx.7.0/24	0/0/19, 0/1/0
iac-na	113	xxx.xxx.12.0/24	0/1/0
icar-inside	50	172.16.1.0/24	0/1/0, 0/0/1-18; 0/0/20-23;
icar-lab	52	172.16.3.0/24	0/1/0
icar-na	11	xxx.xxx.14.0/24	0/1/0
vlan_1	1	xxx.xxx.40.0/24 xxx.xxx.59.0/24	-----

Modello	Rack	Ottetto Host	Nome
Juniper EX2200	RACK - PIANO TERRA	192	ji.192Ed4_p0
Vlan	Tag id	Subnet	Interfaces
area-new	112	xxx.xxx.7.0/24	0/0/0-7,9,11; 0/1/0
iac-na	113	xxx.xxx.12.0/24	0/0/10,12-23; 0/1/0
igb	2	xxx.xxx.60.0/24	0/0/8, 0/1/0
vlan_1	1	xxx.xxx.40.0/24 xxx.xxx.59.0/24	-----

Modello	Rack	Ottetto Host	Nome
Juniper EX2200	RACK - PIANO -1 - CED-ICAR	216	ji.216Ed4_p-1
Vlan	Tag id	Subnet	Interfaces
area-new	112	xxx.xxx.7.0/24	0/0/4, 0/1/0
icar-dmz	51	172.16.2.0/24	0/1/0
icar-inside	50	172.16.1.0/24	0/0/6, 0/1/0
icar-lab	52	172.16.3.0/24	0/1/0
icar-na	11	xxx.xxx.14.0/24	0/0/0-3,5,7-9; 0/1/0
vlan_1	1	xxx.xxx.40.0/24 xxx.xxx.59.0/24	-----

Modello	Rack	Ottetto Host	Nome
Juniper EX2200	RACK - PIANO -1 - CED-ICAR	236	ji.236Ed4_p-1
Vlan	Tag id	Subnet	Interfaces
icar-inside	50	172.16.1.0/24	0/0/0, 0/0/3, 0/0/6, 0/1/0
icar-lab	52	172.16.3.0/24	0/0/7, 0/1/0
icar-na	11	xxx.xxx.14.0/24	0/0/1,2,4,5,8-10,16-21; 0/1/0
oliva	78	xxx.xxx.78.0/24	0/0/12-15,22,23; 0/1/0
vlan_1	1	xxx.xxx.40.0/24 xxx.xxx.59.0/24	-----

Modello	Rack	Ottetto Host	Nome
Juniper EX2200	RACK 1 - PIANO -1 – CENTRO STELLA	195	j-centrostella
Vlan	Tag id	Subnet	Interfaces
area-new	112	xxx.xxx.7.0/24	0/0/0,1,8,10,13;
c3p-new	115	xxx.xxx.58.0/24	0/0/2,3,7; 0/1/0
dompel	76	xxx.xxx.76.0/24	-----
iac-na	113	xxx.xxx.12.0/24	0/0/9,11,12,16,22,23; 0/1/0
icar-inside	50	172.16.1.0/24	0/1/0
icar-lab	52	172.16.3.0/24	-----
icar-na	11	xxx.xxx.14.0/24	0/0/4,5,14; 0/1/0
imm-na	21	xxx.xxx.38.0/24	0/1/0
vlan_1	1	xxx.xxx.40.0/24 xxx.xxx.59.0/24	-----

Modello	Rack	Ottetto Host	Nome
Catalyst 3500 XL	RACK 1 - PIANO 1 - ICAR	21	N.D.
Vlan	Tag id	Subnet	Interfaces
dhcp	13	xxx.xxx.7.0/24	0/1
c3p-new	115	xxx.xxx.58.0/24	0/2
icar-inside	50	172.16.1.0/24	0/3,4,8,10,11,17-22,24-31,41,42,44,48
area-new	112	xxx.xxx.7.0/24	0/7,9,13,14,16,23,33-39,43,45,46
igb	2	xxx.xxx.60.0/24	0/5
icar-na	11	xxx.xxx.14.0/24	0/6
ipiget	14	n.d.	0/12
iac-na	113	xxx.xxx.12.0/24	0/40
c3p-new	115	xxx.xxx.58.0/24	0/32

7. Firewall

La configurazione della rete ICAR prevede l'uso di un Firewall interno per la protezione tra le reti Vlan ICAR. Il dispositivo utilizzato è un Cisco ASA 55, esso è ubicato nell'armadio di rete della Sala Calcolo ICAR (RACK PIANO -1 – CED-ICAR).

Il firewall possiede quattro interfacce Gigabit Ethernet, una Fast Ethernet ed una interfaccia seriale per la console. L'accesso tramite console è sempre garantito utilizzando l'apposito cavetto adattatore incluso nella confezione.

L'interfaccia Fast Ethernet è dedicata al management ed è separata fisicamente dal resto del gruppo delle interfacce. Essa è attualmente deputata esclusivamente alla configurazione, ma può essere in futuro utilizzata come porta per una rete aggiuntiva se necessario.

Le altre quattro porte ethernet sono configurate in questo modo:

Porta	Nome assegnato	Sottorete	Indirizzo del Firewall
GigabitEthernet0/0	ICAR-NA	xxx.xxx.14.0/24	xxx.xxx.14.12
GigabitEthernet0/1	ICAR-INSIDE	172.16.1.0/24	172.16.1.1
GigabitEthernet0/2	ICAR-DMZ	172.16.2.0/24	172.16.2.1
GigabitEthernet0/3	ICAR-LAB	172.16.3.0/24	172.16.3.1

La route statica del gateway predefinito è assegnata all'indirizzo xxx.xxx.14.1, mentre i server DNS sono indicati come xxx.xxx.14.3 e xxx.xxx.14.4. Gli indirizzi vengono distribuiti dal firewall quando viene richiesto un indirizzo al server DHCP (se ovviamente il server DHCP è disponibile nella specifica sottorete).

In figura 12 sono rappresentate graficamente le Vlan ICAR e il collegamento rispetto al dispositivo Firewall.

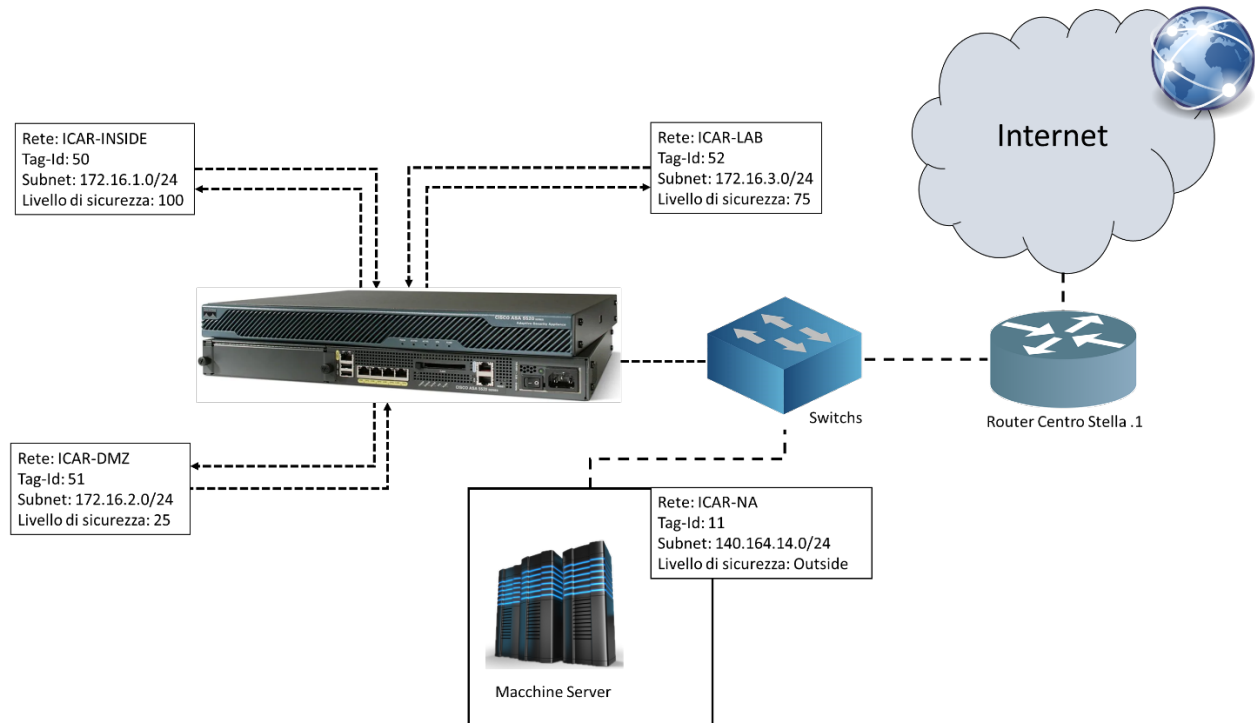


Figura 12 - Configurazione Firewall ICAR

8. Spanning Tree

Il protocollo Spanning tree sulla rete ICAR è configurato in modo da avere come root-Bridge lo switch modello Juniper EX4200 del centro stella con indirizzo ip YYY.YYY.YYY.1, tale configurazione è ottenuta impostando il valore Root ID Priority uguale a 7600 sullo switch. Tutti gli altri switch della rete sono collegati direttamente allo switch rootBridge configurando in questo modo un albero dei path con una topologia di rete a stella.

9. Rete eduroam

L'Area di Ricerca NA1 ha aderito all'iniziativa Education Roaming allo scopo di dotarsi di una rete wireless che permette agli utenti della comunità dell'Università e della ricerca in mobilità di fruire di una connessione internet.

Allo scopo di avere una copertura di rete sugli edifici dell'Area di Ricerca NA1, sono stati installati 11 dispositivi Access Point modello: Ubiquiti Networks UAP-AC-PRO WLAN.

Gli AP installati presso dell'edificio 4, dove sono presenti gli uffici e i laboratori afferenti all'istituto ICAR sono 4/11 controllati e configurati mediante il servizio Unifi installato su server dedicato e presente sulla subnet YYY.YYY.YYY.0/24.

L'autenticazione dei dipendenti ICAR sulla rete eduroam avviene grazie all'utilizzo delle credenziali SIPER, in dotazione ad ogni dipendente del CNR. Allo scopo di realizzare la summenzionata autenticazione, sulla subnet YYY.YYY.YYY.0/24 è configurato un client Radius (xxx.xxx.7.11) che comunica con il server Radius della sede centrale del CNR.

10. Conclusioni

L'attività svolta e descritta in questo RT ha riguardato l'individuazione degli apparati di rete da un punto di vista hardware, l'analisi delle configurazioni degli stessi, il loro dispiegamento e collegamento rispetto ad altri apparati di rete presenti nel centro stella e condivisi tra gli istituti che fanno parte dell'area di ricerca NA1.

Questo lavoro di ricognizione è stato di fondamentale importanza, in quanto ha consentito di fotografare l'attuale situazione di configurazione della rete e allo stesso tempo di individuare una serie di criticità presenti sull'infrastruttura.

Le criticità più rilevanti riguardano i seguenti aspetti:

1. Utilizzo di apparati di rete ben oltre la data di "fine vita" e quindi senza più alcun tipo di supporto hardware e software da parte del produttore, come ad esempio il "Firewall Cisco - ASA5520-BUN-K9", gli switch "Bay Networks - Nortel Networks BayStack 350-48T" e "Catalyst Series 3500 XL 48 Port".
2. Configurazioni degli apparati di rete inconsistenti, sono presenti sugli switch ICAR diverse Vlan non di pertinenza dell'Istituto, come ad esempio iac-na, imm-na, igb, c3p-new, no-route, SCASI, etc.
3. Tutti gli switch utilizzano firmware obsoleti.
4. Assenza di un sistema di monitoraggio.
5. Assenza di un sistema di archiviazione (syslog) degli eventi rilevati dalle apparecchiature.
6. Assenza di un sistema di archiviazione degli accessi alle apparecchiature di rete,
7. Assenza di accessi personalizzati ai dispositivi di rete.

8. Assenza di una politica di backup periodica degli apparati di rete.
9. Assenza di apparati di rete ridondanti.
10. Esposizione diretta su Internet dei server fisici e virtuali.
11. Assenza di un sistema di gestione delle reti wi-fi per l'accesso ad Internet da parte di personale ospite dell'ICAR.
12. Scarsa copertura della rete wi-fi per gli uffici e laboratori ICAR.

Le criticità portate alla luce dalla ricognizione saranno affrontate e risolte mediante una attività di riconfigurazione e ottimizzazione degli apparati di rete, sostituzione dei vecchi switch presenti sulla rete non più affidabili e performanti, acquisto di un nuovo dispositivo Firewall per aumentare il livello di sicurezza dell'intera rete ICAR.

Inoltre, allo scopo di aumentare il livello di sicurezza di accesso alle macchine server si intende configurare una Virtual Private Network per il collegamento da remoto con le macchine server.

11. Ringraziamenti

In questa sezione gli autori vogliono ringraziare l'Ing. Carmine Raimo per il supporto e le utili informazioni fornite, indispensabile per la realizzazione del presente lavoro.

12. Riferimenti

- [1] www.icar.cnr.it
- [2] www.cnr.it
- [3] www.diiit.cnr.it
- [4] https://www.juniper.net/documentation/en_US/release-independent/junos/topics/topic-map/ex2200-system-overview.html
- [5] https://www.cisco.com/c/en/us/products/security/asa-5500-series-next-generation-firewalls/data_sheet_c78-345385.html
- [6] <https://www.cisco.com/web/ANZ/cpp/refguide/hview/switch/3500xl.html>
- [7] <https://www.manualslib.com/manual/113182/Bay-Networks-Baystack-350.html>
- [8] https://www.juniper.net/documentation/en_US/release-independent/junos/topics/topic-map/ex4200-system-overview.html
- [9] <https://www.ui.com/unifi/unifi-ap-ac-pro/>