

G. CANNATARO, G. CARETTO

Dipartimento Tecnologie Energetiche
Divisione per lo Sviluppo Sistemi per l'Informatica e l'ICT
Laboratorio Infrastrutture e Servizi di Rete
Centro Ricerche Brindisi

REALIZZAZIONE DELL' INFRASTRUTTURA DI RETE DEL CENTRO ENEA DI BRINDISI

RT/2020/6/ENEA



AGENZIA NAZIONALE PER LE NUOVE TECNOLOGIE,
L'ENERGIA E LO SVILUPPO ECONOMICO SOSTENIBILE

G. CANNATARO, G. CARETTO

Dipartimento Tecnologie Energetiche
Divisione per lo Sviluppo Sistemi per l'Informatica e l'ICT
Laboratorio Infrastrutture e Servizi di Rete
Centro Ricerche Brindisi

REALIZZAZIONE DELL' INFRASTRUTTURA DI RETE DEL CENTRO ENEA DI BRINDISI

RT/2020/6/ENEA



AGENZIA NAZIONALE PER LE NUOVE TECNOLOGIE,
L'ENERGIA E LO SVILUPPO ECONOMICO SOSTENIBILE

I rapporti tecnici sono scaricabili in formato pdf dal sito web ENEA alla pagina www.enea.it

I contenuti tecnico-scientifici dei rapporti tecnici dell'ENEA rispecchiano l'opinione degli autori e non necessariamente quella dell'Agenzia

The technical and scientific contents of these reports express the opinion of the authors but not necessarily the opinion of ENEA.

REALIZZAZIONE DELL' INFRASTRUTTURA DI RETE DEL CENTRO ENEA DI BRINDISI

G. Cannataro, G. Caretto

Riassunto

La realizzazione di un'infrastruttura di rete è complessa e riguarda molteplici aspetti tecnici e tecnologici.

Il primo aspetto riguarda l'infrastruttura fisica, in particolare la distribuzione della rete telematica passiva e la cablatura degli edifici, mediante un progetto ben strutturato con l'obiettivo di realizzare una rete che abbia connettività fisica omogenea, prestazioni in termini di velocità adeguate alle esigenze attuali e future, essere dunque scalabile, con possibili evoluzioni tecnologiche e con possibilità di espansioni future, infine supportare i protocolli standard di comunicazione;

Il secondo aspetto riguarda la distribuzione della rete telematica attiva ovvero la distribuzione degli apparati telematici quali router, switch, firewall e la corretta gestione e mantenimento degli armadi telematici.

Il terzo aspetto riguarda l'implementazione della rete dal punto di vista logico. Lo schema logico di una rete è una astrazione dal livello fisico e strutturale e ne permette l'implementazione secondo una idea di sicurezza, affidabilità, resilienza e accessibilità, mediante l'utilizzo di politiche di sicurezza, segmentazione della rete, regole di accessibilità ecc.

Un ulteriore aspetto riguarda l'infrastruttura fisica del Data Center, la corretta realizzazione dello stesso, l'installazione e implementazione di Server e Storage per la distribuzione dei servizi, la climatizzazione degli ambienti, la continuità elettrica, la tolleranza ai guasti e altro ancora.

Parole chiave: infrastruttura fisica, rete, server, data center, networking, routing, firewall

Abstract

The creation of a network infrastructure is complex and involves multiple technical and technological aspects.

The first aspect concerns the physical infrastructure, in particular the distribution of the passive telematic network and the cabling of the buildings, through a well-structured project with the aim of creating a network that has homogeneous physical connectivity, performance in terms of speed adapted to the needs current and future, therefore to be scalable, with possible technological evolutions and with the possibility of future expansions, and finally to support the standard communication protocols;

The second aspect concerns the distribution of the active telematic network or the distribution of telematic devices such as routers, switches, firewalls and the correct management and maintenance of telematic cabinets.

The third aspect concerns the implementation of the network from a logical point of view. The logical scheme of a network is an abstraction from the physical and structural level and allows its implementation according to an idea of security, reliability, resilience and accessibility, through the use of security policies, network segmentation, accessibility rules etc.

A further aspect concerns the physical infrastructure of the Data Center, the correct implementation of the same, the installation and implementation of Servers and Storage for the distribution of services, air conditioning of the environments, electrical continuity, fault tolerance and more.

Keywords: physical infrastructure, network, server, data center, networking, routing, firewall

INDICE

PREMESSA	6
INTRODUZIONE	7
INFRASTRUTTURA DI RETE	8
1 RETE PASSIVA	8
1.1 Introduzione	8
1.2 Realizzazione del 2004	9
1.3 Adeguamento del 2006	11
1.4 Ampliamento del 2012	12
2 RETE ATTIVA	16
2.1 Realizzazione 2004	16
2.2 Ampliamento 2012	17
2.3 Ampliamento 2018	18
2.4 Ampliamento 2019-20	19
APPARATI ATTIVI	21
1 IL POP GARR	21
2 APPARATI LAYER 3	24
2.1 Router (GARR)	24
2.2 Router (ENEA)	25
2.3 Centro Stella (Huawei P6720)	29
2.4 Centro Stella Calcolo (Huawei P6810)	32
2.5 Centro Stella (Cisco 4900M)	33
3 APPARATI LAYER 2	34
3.1 Cisco WS-C2960, WS-C3750	34
3.2 Huawei S5700, S5720	35
3.3 Enterasys C1, A2, B5, N7	37
3.4 Enterasys VH2402S	38
4 CONTROLLER WI-FI	39
4.1 Alcatel-Lucent	39
4.2 WatchGuard	40
4.3 Huawei	40
4.4 Access Point	41
5 FIREWALL	42
SCHEMA LOGICO	45
1 INDIRIZZAMENTO IP	47
1.1 IP Privati	47
1.2 IP Pubblici	48
2 VLAN	49
2.1 Introduzione	49
2.2 VLAN Interface	50
2.3 Interfacce terminate sul firewall	51
2.4 Interfacce terminate sul centro stella	54
2.1 Interfacce terminate su Packet Fence	59
2.2 Interfacce interne	62
2.3 Evoluzioni future	63
PARCO MACCHINE	64
1 INFRASTRUTTURA FISICA	64
2 INFRASTRUTTURA VIRTUALE	65
2.1 Networking in vSphere	66
CONCLUSIONI	70
SITOGRAFIA	71
INDICE DELLE FIGURE	71
INDICE DELLE TABELLE	72
APPENDICE	72

Premessa

Le attività scientifiche e di sviluppo tecnologico dell'ENEA vengono svolte nei Centri di Ricerca dislocati sul territorio nazionale ai quali si aggiungono i laboratori, la sede legale di Roma, una rete di uffici regionali e l'Ufficio di collegamento di Bruxelles per la partecipazione a progetti di ricerca europei e internazionali. Tutte le sedi sono dotate di connettività con altissima capacità di banda, in particolar modo i centri di ricerca più importanti quali Casaccia, Frascati, Portici, Brindisi ecc. Tutti i centri sono dotati di una rete ad altissima efficienza e sono interconnesse tra loro mediante reti intranet creando di fatto una macro rete a livello nazionale. Il Laboratorio RETE svolge le proprie attività nell'ambito delle tecnologie di rete, della sicurezza informatica e dei servizi ICT. In tale ambito definisce l'architettura generale di rete finalizzata alle applicazioni tecnico-scientifiche ed ai servizi informativi dell'ENEA, sviluppa e gestisce le infrastrutture della rete locale e geografica garantendo la connettività fra tutte le sedi ed il circuito internazionale della ricerca, curando i rapporti con il Consortium GARR e partecipando alle relative evoluzioni tecnologiche.

Il laboratorio garantisce la crescita infrastrutturale dei centri in modo trasversale mediante l'upgrade della rete sia dal punto di vista fisico, sia dal punto di vista logico. Esso fa parte della divisione ICT insieme ad altri due laboratori fondamentali per lo sviluppo e il funzionamento di tutta l'infrastruttura, ovvero il laboratorio HPC – per gli aspetti legati al calcolo scientifico ad alte prestazioni, lo sviluppo di soluzioni per la gestione e la visualizzazione di grandi moli di dati ottenuti sia dalle attività di modellistica e simulazione che da impianti sperimentali complessi e la gestione dei super calcolatori, ed il laboratorio IGEST – per tutte le attività necessarie ad assicurare la funzionalità e la gestione del sistema informativo, le esigenze amministrative, contabili e gestionali, provvedendo ad adeguare e promuovere costantemente le performance e le risposte del sistema agli output richiesti. Questi laboratori sono tra i primissimi “clienti” ed interlocutori del laboratorio RETE in quanto, buona parte delle scelte implementative e infrastrutturali ed iniziative, sono frutto di richieste da parte di queste utenze “privilegiate” per le quali il laboratorio fa il massimo sforzo per garantire massime performance, massima sicurezza ed affidabilità, ecc.

Nel lavoro presentato si descrive la LAN di Brindisi, tuttavia, ci sono tantissimi aspetti che procedono in “armonia” con gli altri Centri e vengono di fatto elaborati, concertati, organizzati a tavolino, con l'ausilio oltre che dei responsabili dei laboratori, con i colleghi delle altre sedi. Le scelte fatte per organizzare la rete in un certo modo, sia fisico, ma soprattutto logico, sono frutto di scelte condivise a seguito di incontri, discussioni e riunioni tra il personale ICT delle varie sedi. Obiettivo comune di tutti i colleghi del laboratorio di rete è quello di centralizzare scelte e metodologie per un funzionamento ottimale ed una esperienza di lavoro sempre migliore.

Introduzione

Il Centro Ricerche ENEA di Brindisi è dotato di una infrastruttura hardware e software tecnologicamente avanzata. Il centro è dotato di una rete lan di ultima generazione con capacità massima di 10 Gbps. Il centro ospita nei suoi locali il POP¹ del GARR² – service provider della rete ENEA – al quale è collegata con 2 link con capacità trasmissive di 1 Gbps cadauno. Questa capacità imposta dal provider, in base ad un contratto tra le parti, non rappresenta un limite tecnico ed è configurabile, con i dovuti upgrade degli apparati e previ accordi tra le parti, per ottenere velocità di trasmissione di oltre i 40 Gbps.

La rete si estende su una vasta superficie comprendenti cinque edifici e molteplici armadi che ospitano gli apparati di rete attivi e passivi. La rete del centro di Brindisi è stata realizzata originariamente nel 2004, con un cablaggio strutturato che contava n. 252 punti presa doppi in Categoria 6 e più di 25 chilometri di cavo steso per tutto il campus. Nel 2012 ha avuto un considerevole ampliamento nell'ambito di un progetto infrastrutturale per la realizzazione di reti di collegamento tra apparecchiature di laboratorio e reti di collegamento tra diverse strutture scientifiche e di alta formazione. **Ad oggi la rete realizzata è di altissimo profilo tecnologico, si estende in diversi edifici e si configura come una Campus Area Network** e al momento il cablaggio strutturato conta circa 450 postazioni di lavoro doppie. Nel 2018 la rete ha avuto un ulteriore upgrade fisico con l'acquisto di apparati di networking di ultima generazione, tra i quali spiccano due centro stella con interfacce di uplink con capacità di 40 Gbps.

Negli ultimi anni la rete ha avuto un upgrade ed è stata ristrutturata anche dal punto di vista logico. La buona riuscita della implementazione di una rete necessita, di fatto, dello studio e realizzazione di un buon schema logico. Lo schema logico di rete rappresenta un'astrazione dal livello fisico della rete e permette al gestore di implementarla secondo una sua idea di sicurezza, affidabilità, resilienza e accessibilità. Una rete organizzata in un certo modo e con una certa resilienza e affidabilità a livello logico, non può prescindere dall'utilizzo di determinate applicazioni e metodologie di implementazione, senza le quali, altrimenti, la rete non avrebbe le suddette caratteristiche. Nel corso del documento vedremo come questi strumenti, uno su tutti le vlan, sono stati utilizzati e implementati per la realizzazione della rete, aumentandone la sicurezza e l'affidabilità.

¹ Point of presence

² La rete GARR è ideata e gestita dal Consortium GARR, un'associazione senza fini di lucro fondata sotto l'egida del Ministero dell'Istruzione, dell'Università e della Ricerca. I soci fondatori sono CNR, ENEA, INFN e Fondazione CRUI, in rappresentanza di tutte le università italiane.

Infrastruttura di Rete

La realizzazione di una Infrastruttura di Rete avanzata e veloce ha molteplici vantaggi. Lo scambio di informazioni è un elemento fondamentale nella vita di ogni persona e azienda e/o ente. Elemento chiave nel raggiungimento di tali obiettivi è una unica infrastruttura di comunicazione, che consenta di integrare qualsiasi flusso informativo. L'infrastruttura di comunicazione consente lo scambio di informazioni all'interno del singolo edificio, del comprensorio, dell'intero ambito cittadino o geografico. Con tali presupposti, l'infrastruttura di comunicazione multimediale all'interno dell'edificio, rappresenta il punto di integrazione delle varie strutture ambientali, una solida base su cui poi costruire e far evolvere l'intera area degli impianti nell'edificio. Da questo aspetto consegue che il ciclo di vita dell'infrastruttura di comunicazione è sicuramente superiore a quello dei singoli apparati/impianti presenti nella sede. Simili realizzazioni devono garantire mediamente un investimento per la durata di oltre quindici anni. La soluzione è quella di creare una rete di trasmissione, capillarmente diffusa, messa in opera indipendentemente dall'ubicazione, numero o tipo di postazioni ad essa collegati rispondente ai principi del Cablaggio Strutturato. Tale sistema consente il soddisfacimento delle esigenze di comunicazione, flessibilità di utilizzo, modularità di crescita, secondo le moderne tecnologie dettate dagli standard di riferimento, onde avere la possibilità di realizzare sotto reti logicamente e/o fisicamente distinte all'interno dell'unica struttura fisica di cablaggio, dotata di adeguati raccordi con i Server e gli altri soggetti di comunicazione.

Gli obiettivi che il progetto si pone sono i seguenti:

- connettività fisica omogenea per tutta la rete;
- prestazioni in termini di velocità adeguata alle esigenze attuali e future;
- possibilità di seguire le evoluzioni tecnologiche;
- facilità di gestione e di espansione della rete, sia in caso di spostamenti, che di interruzioni e/o malfunzionamenti;
- supporto di protocolli standard di comunicazione;

1 Rete Passiva

1.1 Introduzione

Il centro di Brindisi, attivo fin dagli anni '90 con uno sportello tecnologico e altre iniziative volte a promuovere le attività di ricerca e sviluppo e a trasferirne i risultati verso il mondo produttivo e imprenditoriale, consolida la sua presenza sul territorio nel 2001, quando nasce un vero e proprio centro di ricerca all'interno dell'area denominata "Cittadella della Ricerca". Da allora, quello di Brindisi, è divenuto un centro di eccellenza nei settori dei Materiali e delle relative tecnologie per applicazioni in

più ambiti: Trasporti (Aerospaziale), Energia (Fonti Rinnovabili), Ambiente (Sistemi di monitoraggio e diagnostica). Uno dei primi obiettivi del Servizio Centralizzato Informatica e Reti³, affinché il centro potesse crescere ed essere competitivo, al pari degli altri centri ENEA, è stato quello di rendere il centro tecnologicamente avanzato e di conseguenza modernizzare l'infrastruttura di rete ereditata del precedente conduttore e diventata nel tempo obsoleta, attraverso un progetto per il rinnovamento della rete dati e fonia.

1.2 Realizzazione del 2004

Il cablaggio di rete del centro di Brindisi è stato realizzato nell'ambito della convenzione Consip⁴ – Rete dati-fonia. Il progetto è stato sviluppato nel contesto delle attività della Convenzione stipulata con la ditta aggiudicataria della gara per la fornitura apparecchiatura di vario genere quali apparati passivi e attivi per le reti locali e fornitura dei servizi connessi.

Il progetto prevedeva la realizzazione di un cablaggio strutturato per un totale di n. 252 postazioni telematiche doppie in Cat. 6. Per una tabella più dettagliata si veda in appendice.

Q.tà	Elemento	Ubicazione
1	Centro Stella Building/campus distributor (BD CD)	Edificio A2 PT
8	Armadi periferici o di Piano Floor distributor (FO)	Edifici C,AE,9,6
9	Dorsali in fibra ottica 9/125 monomodale a 8 fibre ottiche	Campus
7	Dorsali di cavo 50 cp cat. 3 per dorsali fonia	Campus
1	Dorsale di cavo 100 cp cat. 3 per dorsali fonia	Campus
252	Punti doppi di cablaggio ovvero in rame Cat.6	Campus
75	Scavo per collegamento palazzina A2 con la palazzina 9 (mt.)	Edifici AE, 9
25000	Cavo UTP cat 6, 100Ohm, rivestito con guaina esterna (mt.)	Campus

Tabella 1: Cablaggio strutturato: tabella riassuntiva

³ Successivamente UTICT e ICT-RETE

⁴ Consip è la centrale acquisti della pubblica amministrazione italiana; è una società per azioni il cui unico azionista è il Ministero dell'economia e delle finanze del governo italiano ed opera nell'esclusivo interesse dello Stato.

Armadio	Ubicazione	Funzione	Link FO	GB	MB
1	ED. A2 PT 4° blocco CED	centro stella	10	30	
2	ED. A2 PT 4° blocco CED	dati-fonia ED. A2 PT 3° 4° blocco	1		90
3	ED. A2 P1 1° blocco	dati-fonia ED. A2 PT 1° blocco	1		36
4	ED. A2 P1 4° blocco	dati-fonia ED. A2 P1 4° blocco	1		29
5	ED. A2 P1 3° blocco	dati-fonia ED. A2 P1 3° blocco	1		20
6	ED. C P1	dati-fonia ED. C	1		12
7	ED. AE PT	dati-fonia ED. AE	1		33
8	ED. 9 PT	dati-fonia ED. 9	1		32
9	ED. 6 P1	dati-fonia ED. 6 P1	1		0

Tabella 2: Cablaggio strutturato: distribuzione

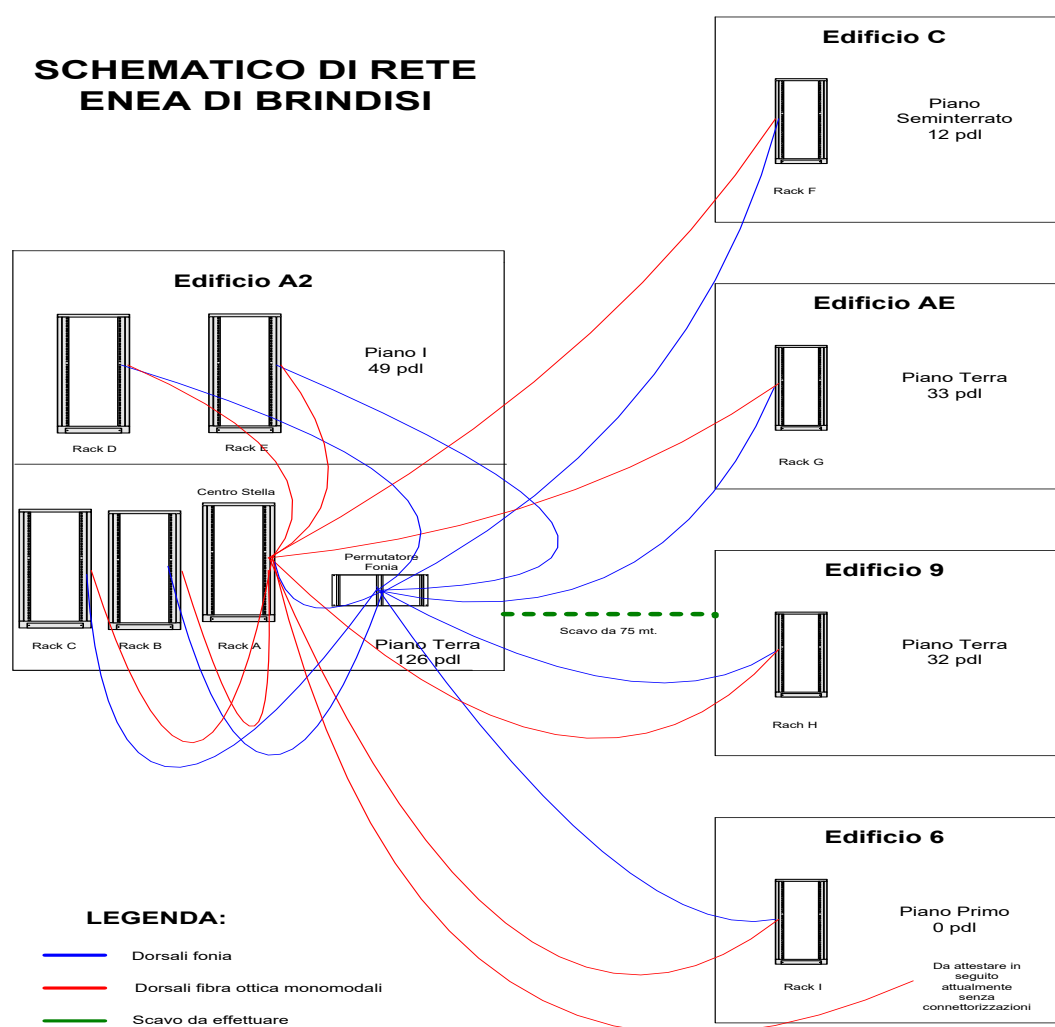


Figura 1: Schema di rete del cablaggio strutturato

Da progetto è stata prevista anche l'installazione di elementi accessori alla rete, quali canalizzazioni sospese, canalizzazioni di raccordo a battiscopa, canalina di alimentazione ed interruttore magnetotermico, prese elettriche da armadio, apparati UPS, ecc. Sono state inoltre previste opere infrastrutturali per la realizzazione dei nuovi punti rete, passaggi delle canalizzazioni e opere murarie eseguite secondo le esigenze specifiche. Per maggiori info si veda in Appendice.

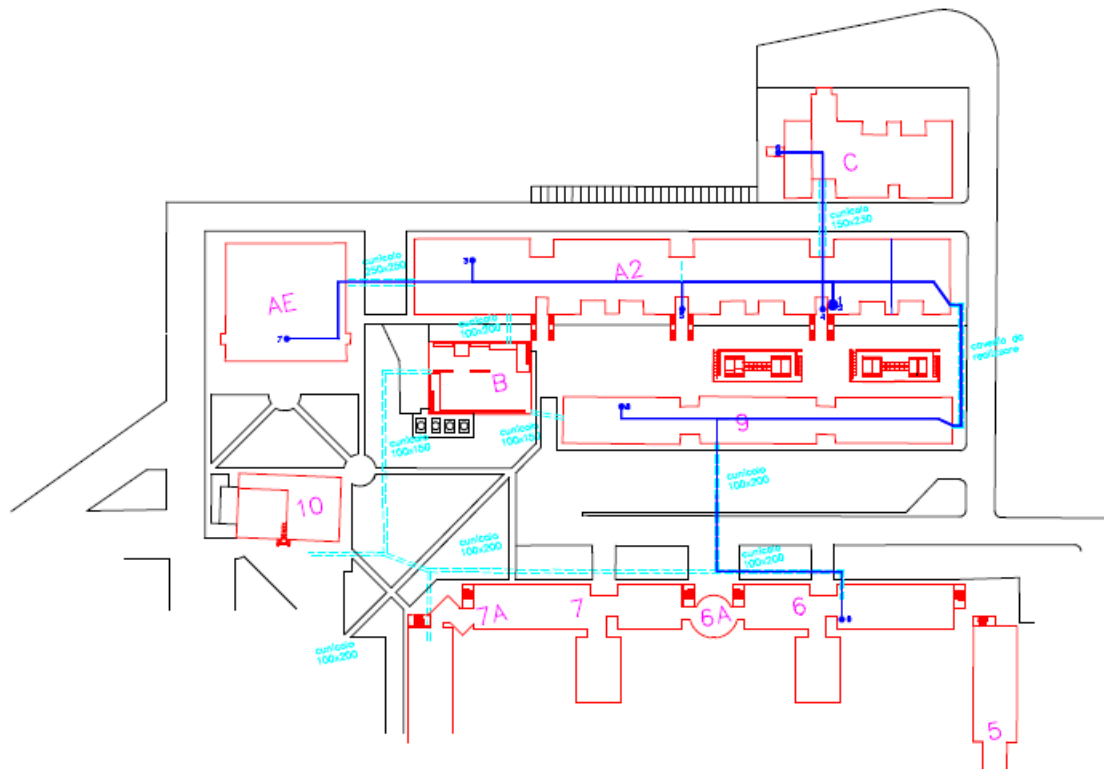


Figura 2: Stralcio della planimetria generale Cittadella della Ricerca con riferimento agli spazi ENEA

1.3 Adeguamento del 2006

Nel corso del 2006 il CR Brindisi ha richiesto e ottenuto dalla proprietà degli immobili l'autorizzazione all'utilizzo di rimanenti 12 studi posti al primo piano dell'edificio A2. Per garantire a questi nuovi spazi la massima funzionalità si è proceduto all'ampliamento della rete dati esistente, realizzata nel 2004, installando in questi uffici nuovi punti presa dati doppi e collegarli agli armadi telematici già presenti nelle vicinanze.

Il cablaggio dei 12 uffici ha visto la fornitura di 2 punti presa doppi per ogni ambiente, conformemente a quanto già realizzato negli altri uffici, per un totale di 24 punti.

La fornitura è stata realizzata all'interno della convenzione “reti fonia/dati” già utilizzata per la realizzazione della rete dati.

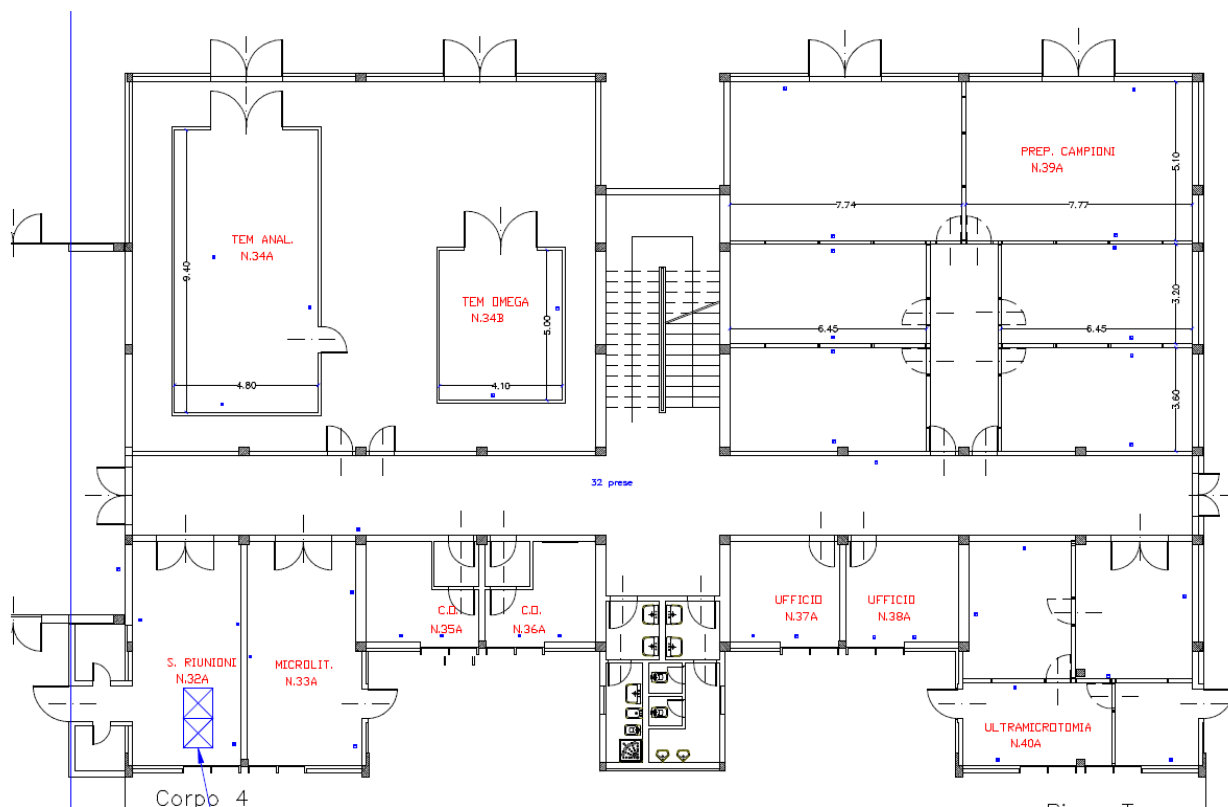


Figura 3: Planimetria Edificio A2 PT Blocco 4

1.4 Ampliamento del 2012

La rete lan del centro ENEA di Brindisi, nell'anno 2012, ha avuto un considerevole ampliamento nell'ambito della convenzione Consip – reti locali 4 e del progetto infrastrutturale TEDAT⁵ per la realizzazione di reti di collegamento tra apparecchiature di laboratorio e reti di collegamento tra diverse strutture scientifiche e di alta formazione.

⁵ Progetto di potenziamento e formazione, **TE**cnologie e la **Di**agnostica **Av**anzata nel settore dei **Tr**asporti, con gli obiettivi di rafforzare e consolidare infrastrutture esistenti per ricerca e sviluppo promuovere il potenziamento di tecnologie e strumentazione per i processi, le analisi e la diagnostica avanzata nel settore trasporti (aerospaziale, automotive, ferroviario, navale).

Nel centro è già presente un cablaggio strutturato, dati-fonia, realizzato nel 2004 usufruendo di una convenzione CONSIP. Questo cablaggio copre completamente quattro edifici su cinque; infatti nel primo piano dell'edificio 6, che ospita gli uffici della Direzione Centro, le sale riunioni ed alcuni uffici utilizzati dalle unità scientifiche, è stato installato esclusivamente un armadio di piano, mentre per la distribuzione sono stati utilizzati due cablaggi (Token Ring ed Ethernet) ereditati da precedenti conduttori dell'immobile.

Il progetto TEDAT ha previsto, nelle zone di pertinenza dello stesso progetto, un ampliamento/adeguamento della rete dati presente nel centro. Per quattro edifici su cinque (edifici AE, A2, C, 9) si è proceduto con un potenziamento dell'esistente, mentre per il quinto (primo piano edificio 6) si è realizzato un rifacimento totale della distribuzione di piano, partendo dall'armadio già presente, per le specifiche esigenze del progetto. Complessivamente è stata prevista la realizzazione di nr. 177 postazioni di lavoro doppie cat. 6A, distribuite all'interno del Campus come di seguito indicato in tabella.

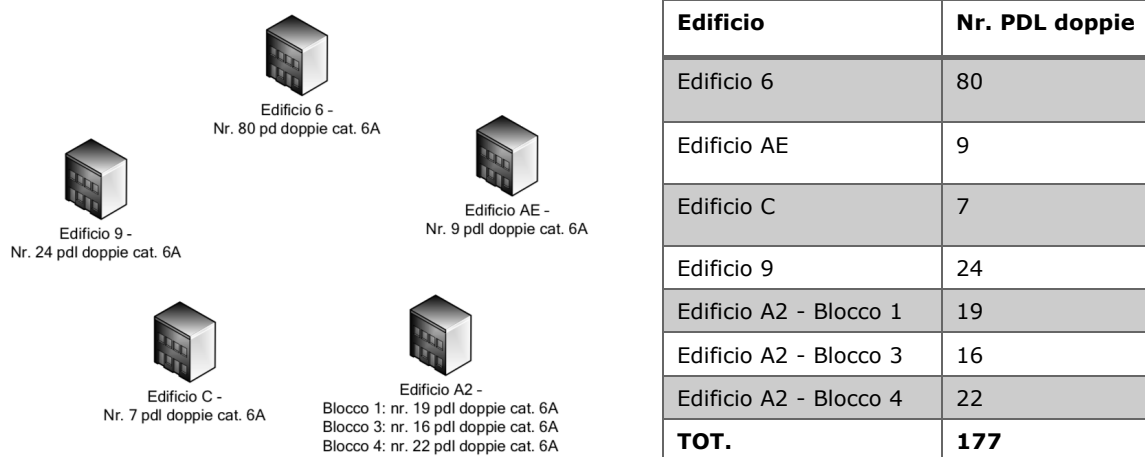


Figura 4: Distribuzione delle postazioni di lavoro doppie cat. 6° all'interno del Campus

Le fasi operative sono state le seguenti:

- **Analisi dei requisiti:** che ha portato a individuare le sedi di interesse, il numero e la dislocazione delle PDL, le tecnologie impiegabili, la configurazione delle utenze in termini di capacità di banda, protocolli e servizi, qualità di servizio, logiche di ripartizione di classi di utenze, esigenze di connettività intranet/extranet; verifica dello stato dell'infrastruttura esistente al fine di potere valutare l'impatto tecnico/economico per la scelta della migliore soluzione tecnologica per l'integrazione della nuova rete;

- **Sopralluogo e Progetto Preliminare:** l'analisi dei requisiti effettuata dall'Amministrazione Contraente e le possibili integrazioni derivanti dal sopralluogo; il dimensionamento del Progetto in termini di sistemi e servizi (per consentire all'Amministrazione Contraente una corretta valutazione dell'offerta); i tempi di realizzazione proposti; il Preventivo economico preliminare ovvero la valorizzazione economica dei sistemi e dei servizi richiesti sulla base del Listino di Fornitura di Convenzione;
- **Valutazione del Progetto Preliminare:** chiarimenti, modifiche, integrazioni;
- **Valutazione del Progetto esecutivo e dell'offerta economica e sua approvazione;**
- **Realizzazione e messa in opera del Progetto.**

La rete realizzata è di altissimo profilo tecnologico. Essa si estende in diversi edifici e si configura come una Campus Area Network.

La realizzazione ha richiesto attività presso 5 edifici o porzioni degli stessi, la realizzazione di un cablaggio in categoria 6A presso gli edifici del Campus, in ampliamento e/o sostituzione del cablaggio esistente. Il progetto ha visto la realizzazione di un cablaggio strutturato per un totale di n. 177 postazioni di lavoro doppie cat. 6A, distribuite all'interno del Campus. Per una tabella più dettagliata si veda in appendice.

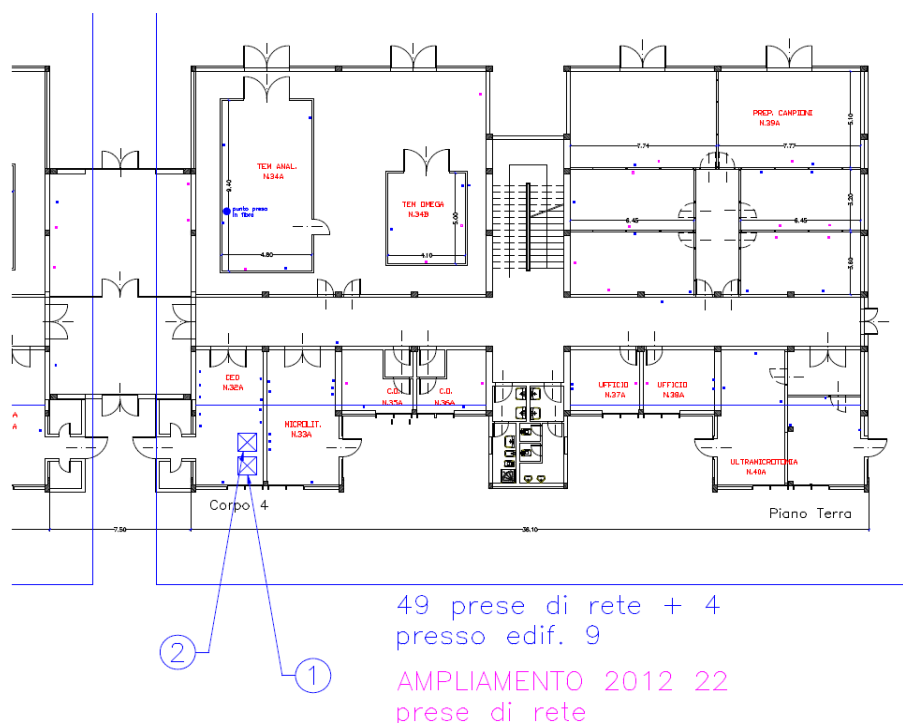


Figura 5: Planimetria Edificio a2_PT Blocco 4

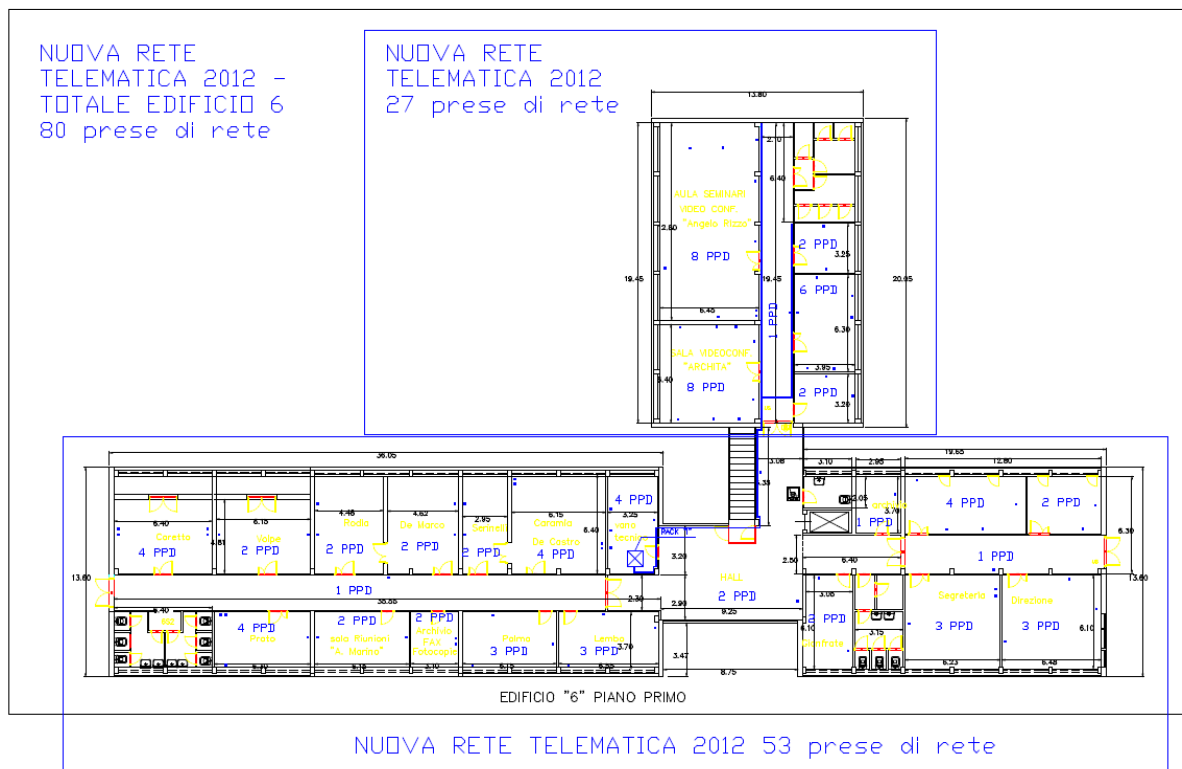


Figura 6: Planimetria Edificio 6_P1

Nel 2013, oltretutto, sono stati installati quattro Access Point WIFI marca Alcatel-Lucent modello AP-68 acquistati dalla Divisione ICT. Tramite questi AP, controllati da un apparato centrale installato nella sede di Casaccia, si è iniziato ad avere la disponibilità di connessione WIFI in due dei cinque edifici di pertinenza ENEA. In particolare con l'utilizzo di due AP si sono coperti due blocchi su quattro dell'edificio A2 e con gli altri due si sono coperti due corridoi su tre dell'edificio 6. Successivamente, per rendere disponibile la connettività WIFI in tutte le zone di pertinenza ENEA si è proceduto con l'acquisto di ulteriori apparati AP dello stesso modello e famiglia. Tutti gli apparati sono stati corredati di specifici alimentatori PoE (Power over Ethernet) che consentono di alimentare elettricamente gli AP tramite il cavo Ethernet che connette gli stessi alla LAN.

2 Rete Attiva

2.1 Realizzazione 2004

Nell'ambito della convenzione CONSIP, nell'anno 2004, è stata realizzata l'infrastruttura di rete attiva del centro. Il progetto ha riguardato, tra le altre cose, l'installazione e messa in opera del centro stella di Campus e degli Switch periferici. Il brand utilizzato è stato Enterasys, all'epoca uno di marchi più prestigiosi e validi nel mondo del networking.

L'installazione ha riguardato per il centro stella, lo Switch Layer 3 modello Matrix N7 – 1000 Base-TX mini GBIC, per gli Switch di piano i modelli Matrix V2 – 100 Base-TX mini GBIC, e per lo Switch destinato al CED il modello Matrix C1 – 1000 Base-TX mini GBIC.

Le attività lavorative hanno visto il personale impegnato nelle diverse fasi di installazione, configurazione, test e collaudo. In appendice è possibile vedere la tabella con il dettaglio degli acquisti.

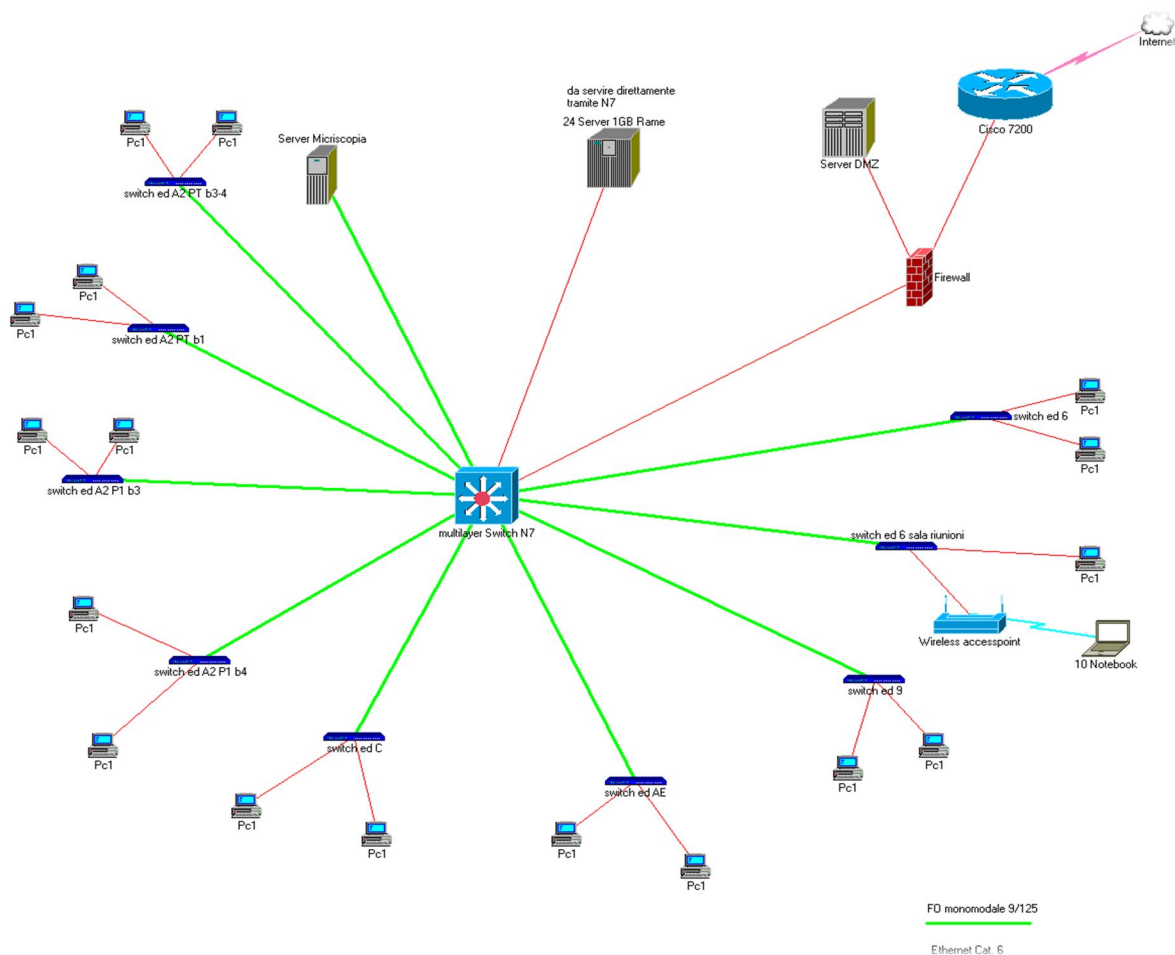


Figura 7: Schema fisico, apparati attivi 2004

2.2 Ampliamento 2012

Nell'ambito del Progetto infrastrutturale TEDAT⁶ – per la realizzazione di reti di collegamento tra apparecchiature di laboratorio e reti di collegamento tra diverse strutture scientifiche e di alta formazione, l'infrastruttura di rete attiva del centro è stata ampliata in modo considerevole. Tra i vari aspetti che il progetto ha riguardato, vi è infatti la rete con l'installazione e messa in opera di apparati di networking attivi quali router, switch, dispositivi wireless, appliance per la sicurezza, installazione di nodi di calcolo CRESCO⁷ (224 nodi di calcolo su Portici per 5.376 cores, 10 nodi su Brindisi per 240 cores), installazione di storage, installazione di sistemi front end e visualizzazione 3D, virtualizzazione laboratori, ecc. Il brand scelto⁸ per gli apparati di networking è stato Cisco.

Le attività di installazione, configurazione, test e collaudo sono state espletate con l'ausilio del personale del laboratorio UTICT⁹ e della ditta aggiudicataria del bando¹⁰. Tutta l'infrastruttura è stata interamente connessa e tutti i device sono stati configurati e testati all'interno del ced prima di essere installati fisicamente presso l'armadio indicato. In un report dettagliato sono state descritte tutte le attività e salvate tutte le configurazioni degli switch e del centro stella.

Gli apparati installati con successo per la sede di Brindisi sono stati i seguenti:

Quantità	Tipologia Dispositivo	Marca e Modello	Capacità Host/Uplink
1	Router	Cisco Catalyst 3925	1GB
1	Switch layer 3	Cisco Catalyst 4900	1GB/10GB
3	Switch layer 2	Cisco Catalyst 3750/48	1GB/4-10GB
9	Switch layer 2	Catalyst 2960/48	1GB/1-1GB/1-10GB

⁶ Il progetto è stato importantissimo per il rafforzamento infrastrutturale e ha avuto come partner di progetto le unità tecniche presenti a Brindisi, quali UTTMATB come capofila, ma anche altre unità importanti quali UTP-NANO e UTP-MDB, nonché l'unità UTICT per la parte ICT. La sinergia e collaborazione tra i vari partner progettuali ha permesso che tutte le attività venissero portate a termine con successo e che l'infrastruttura presente a Brindisi e in altri siti venisse potenziata adeguatamente.

⁷ Centro Computazionale di RicErca sui Sistemi Complessi, presso il Centro Ricerche ENEA di Portici, è la più importante infrastruttura di calcolo ad alte prestazioni ("HPC- High Performance Computing") del Sud Italia, oltre che fra le più importanti del paese.

⁸ Il brand Cisco è quello in vendita dall'aggiudicatario della convenzione in corso.

⁹ Remotamente da Matteo De Rosa (Portici) che ha curato l'implementazione iniziale delle configurazioni e Giacinto Caretto e Giovanni Cannataro (Brindisi) per le implementazioni personalizzate in loco.

¹⁰ R1 S.p.A.

Il Router Cisco Catalyst 3925 chiamato P_CIS3925BRI, è il router di frontiera ENEA attualmente in produzione, mentre l'apparato di nome B_CIS3925BRI è il router di backup. Il centro stella, apparato Cisco Catalyst 4900 chiamato CODI_4900M (Core Distribution) è l'apparato che fa da router interno, più comunemente definito centro stella, raggiunge le foglie e gli altri apparati in fibra 10GB, fibra 1GB e rame 1GB. Gli switch, apparati WS-C2960X-48 sono le foglie e sono installate presso i cinque edifici che la rete raggiunge. Essi hanno porte uplink verso il centro stella a 1 Gbps con nomenclatura di tipo mnemonico per indicarne con puntualità l'ubicazione, (EdA2Arm4_P1b4), come Edificio, Armadio, Piano, Blocco. Gli switch, apparati WS-C3750X-48 sono le foglie, installati presso i locali che ospitano i nodi di calcolo, l'infrastruttura virtuale e lo storage, e per i servizi per i quali necessità maggiore banda disponibile. Essi, infatti, hanno uplink verso il centro stella a 10GB per le sale calcolo e server del progetto TEDAT.

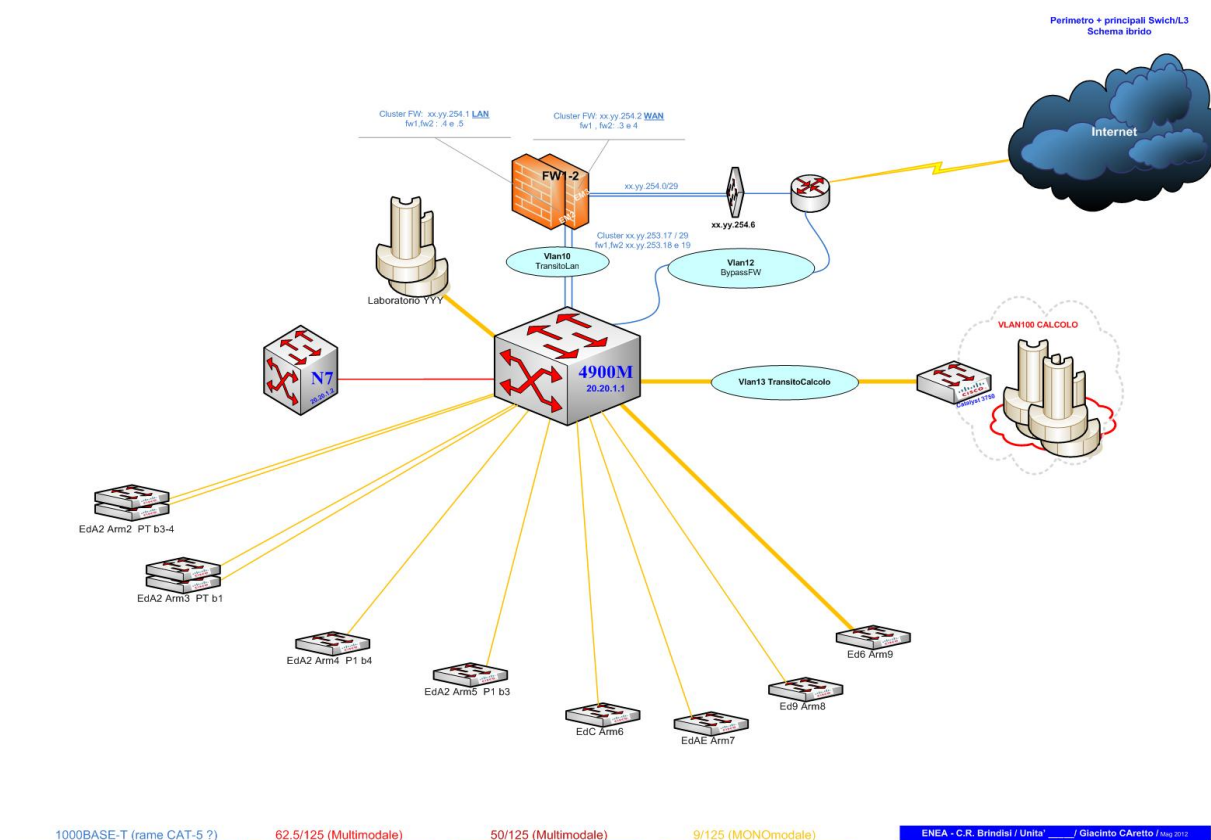


Figura 8: Schema fisico, apparati attivi 2012

2.3 Ampliamento 2018

Nel 2018 l'infrastruttura di rete è stata ampliata. Sono stati acquistati nuovi switch di piano marca Huawei modello S5700-52X. Gli stessi apparati sono stati acquistati, in minor numero, con modulo PoE (S5720-52X) e destinati agli armadi telematici che servono gli uffici, in modo da collegare i telefoni

VoIP in continuità elettrica. Sono stati acquistati anche numerosi transceiver SFP-10G per collegare la quasi totalità delle foglie in uplink verso il centro stella a 10 Gbps.

Tutte le configurazioni sono state implementate dal personale di ICT-RETE di Brindisi, con le dovute personalizzazioni rispetto al sito locale, ma nel pieno rispetto delle politiche di networking e di sicurezza in accordo con le altre sedi ENEA.

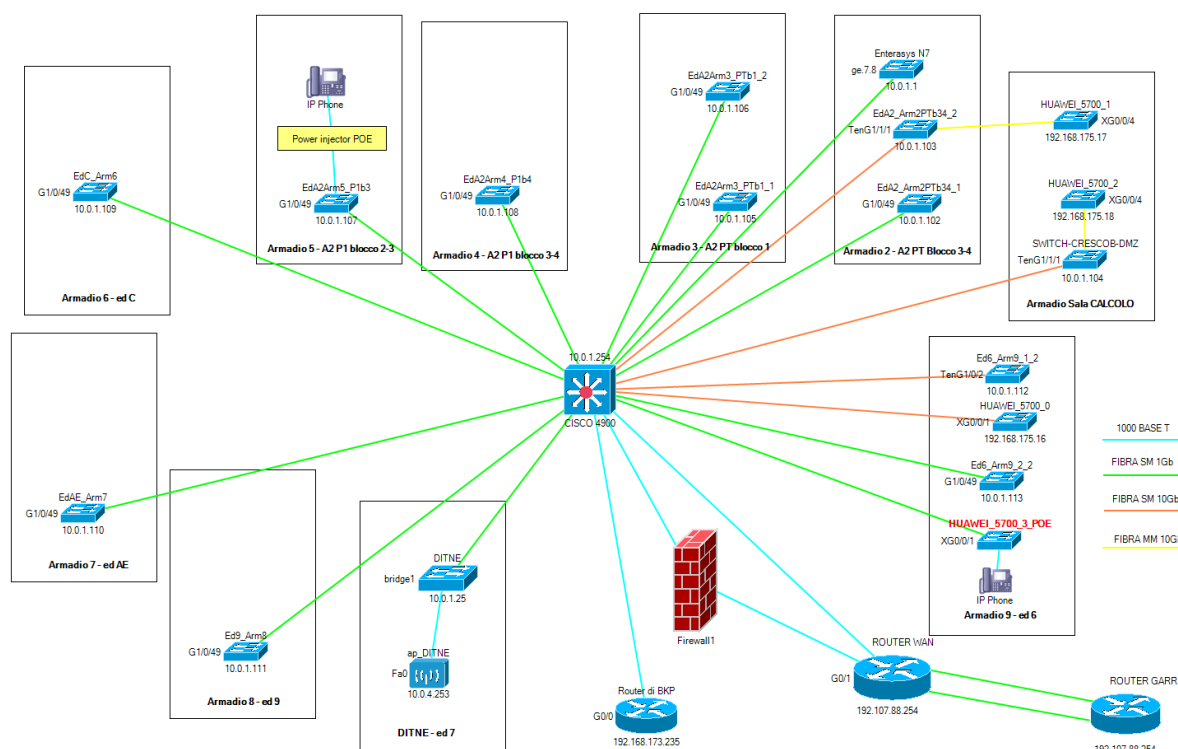


Figura 9: Schema fisico, apparati attivi 2018

2.4 Ampliamento 2019-20

Nel corso dell'anno 2019 il centro è stato dotato di nuovi apparati e la rete ristrutturata cospicuamente in termini di capacità di banda, resilienza, capacità di prese di rete e velocità in uplink. A tutto il 2020 il centro sarà dotato di un **nuovo centro stella**, uno switch multilayer marca Huawei modello 6720 configurato come router interno (centro stella) per sostituire l'attuale Cisco 4900 ed un **nuovo centro stella calcolo**, uno switch multilayer marca Huawei modello 6810 configurato come centro stella per il collegamento allo storage e all'infrastruttura virtuale e per il calcolo, entrambi con porte uplink a 40 GB. Oltretutto il centro sarà dotato di **ulteriori foglie**, switch con velocità nominale sulla porta host a 1/10 GB, e velocità nominale sulla porta uplink a 10/20/40 GB. Inoltre tutti gli switch saranno POE. Per quel che riguarda la telefonia VoIP, non verranno più utilizzati gli ATA se non limitatamente e tutti telefoni saranno saranno IP, compresi i telefoni da laboratorio e nelle sale.

Apparati attivi

Andiamo a descrivere i vari apparati attivi presenti sulla rete, il loro scopo e funzionamento, nonché la loro implementazione. La rete implementata a Brindisi rispecchia per molti aspetti le reti implementate in altre sedi ENEA e anche in altri enti di ricerca. Sicuramente un aspetto in comune con gli altri centri è il collegamento al service provider. La Rete GARR ed i suoi servizi, infatti, sono dedicati alla Comunità della Ricerca e dell'Istruzione Italiana. Attualmente, circa 1200 siti, sono collegati, tra centri di ricerca, università, osservatori, laboratori, biblioteche, musei ed altre infrastrutture.

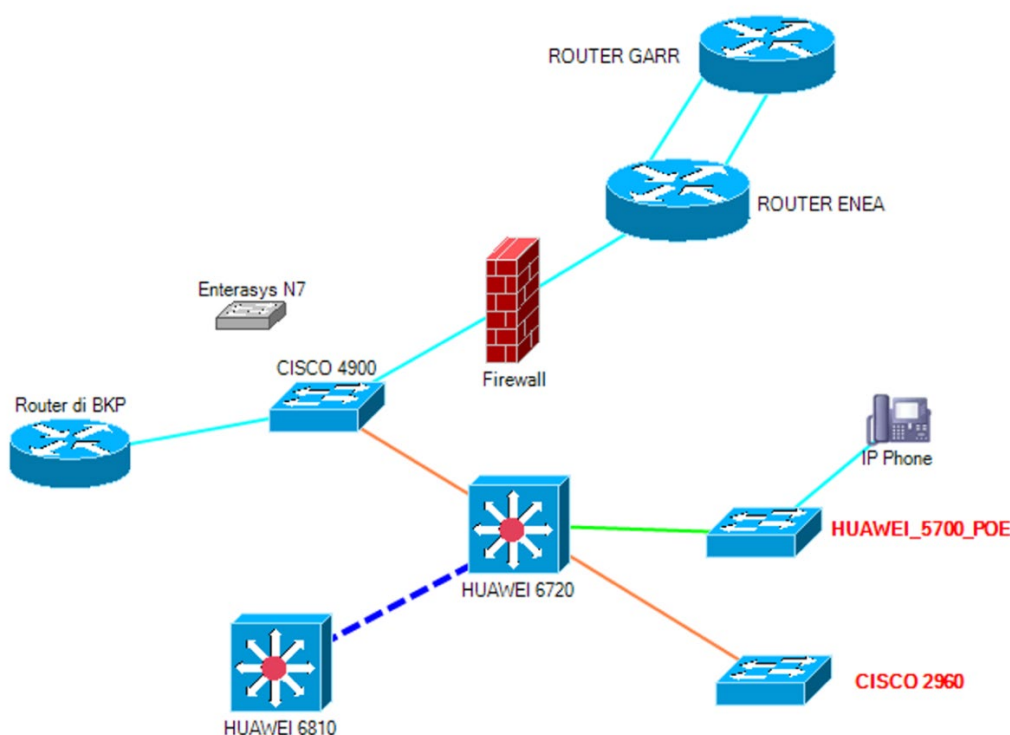


Figura 11: Schema fisico di rete ridotto

1 Il pop Garr

Il centro di Brindisi ospita, tra i suoi locali, il PoP del Consortium GARR che, nell'ambito del progetto GARR-X Progress¹¹, ha effettuato un importante potenziamento del PoP. Il progetto, partito nel luglio del 2013, finanziato attraverso il bando MIUR e destinato alle Regioni della Convergenza, ha realizzato un'infrastruttura digitale integrata sul territorio delle 4 regioni di convergenza, ovvero Calabria, Campania, Puglia e Sicilia, che comprende una rete di nuova generazione completamente in fibra ottica,

¹¹ GARR-X progress – Infrastruttura digitale per promuovere ricerca, istruzione e competitività nel sud

integrando la rete nazionale¹² già in produzione. L'infrastruttura di rete realizzata si basa su apparati di nuova generazione con elevate caratteristiche di scalabilità, velocità e flessibilità, con capacità di trasporto nell'ordine dei 100 Gbps e multipli. Gli accessi delle sedi degli utenti sono stati, di conseguenza, potenziati. All'interno dei PoP sono inoltre installati gli apparati trasmissivi e gli apparati di routing e switching sui quali saranno attestate le fibre ottiche per i collegamenti di accesso degli Enti e delle altre istituzioni GARR servite dal PoP e infine le fibre ottiche di collegamento con gli altri PoP della dorsale. Per consentire l'installazione e l'attivazione degli apparati in questione, è stato necessario eseguire una serie di interventi di adeguamento e potenziamento degli impianti all'interno delle sale che ospitano i PoP. In tale contesto è stato necessario effettuare alcuni interventi di adeguamento degli impianti asserviti al locale che ospita il PoP (quadro elettrico, gruppo di continuità, impianto antincendio, etc.) Tali interventi sono stati effettuati dal gruppo Operations del GARR con il costante supporto degli APM¹³ GARR della sede di Brindisi.

Gli APM forniscono al GARR supporto per gli interventi di adeguamento e potenziamento necessari alla messa in esercizio dell'infrastruttura del progetto GARR-X Progress all'interno dei PoP da completare e in particolare nei seguenti aspetti:

- analizzare le eventuali criticità e valutare gli interventi di adeguamento che si rendano necessari;
- interfacciarsi con l'ufficio tecnico per la richiesta delle specifiche autorizzazioni;
- selezionare le ditte che dovranno effettuare gli interventi suddetti;
- assumere la direzione di eventuali lavori (qualora previsto).

Nel caso in essere si è costituito un Gruppo di Lavoro interdisciplinare coordinato dal sottoscritto con le seguenti: *“Il gruppo seguirà le attività previste nei modi e nei tempi di cui il planning proposto e informerà la Direzione e UTICT-RETE del loro sviluppo”*.

Le opere di Adeguamento sono state le seguenti:

- Allestimento della sala CED per ospitare i nuovi apparati GARR, ovvero l'adeguamento dell'impianto elettrico e la realizzazione della canalizzazione necessaria;
- Compartimentazione dell'area adiacente al CED per la posa della stazione di energia e UPS;

¹² GARR-X è l'ultimo di una serie di upgrade della infrastruttura di rete GARR. La rete è in continua evoluzione, al passo con le esigenze della comunità e le evoluzioni tecnologiche.

¹³ Oltre all'APM per sede, una importante riferimento è l'APA ovvero l'Access Port Administrator, unico per ENEA, che interagisce con la Direzione del GARR ed è una figura con un taglio amministrativo, manageriale, ed ha il compito di assicurare la piena e corretta funzionalità della rete locale dell'ente collegato, secondo le sue specifiche linee gestionali, ed ottimizzare l'uso della Rete GARR da parte delle strutture interne.

- Installazione e configurazione degli apparati trasmissivi e della stazione di energia relativa;
- Installazione e collaudo dell'UPS da 20KVA per gli apparati attivi;
- Fornitura e posa in opera dell'impianto di climatizzatore da realizzarsi nella saletta adiacente al CED e utile al condizionamento degli apparati trasmissivi e dell'UPS.

Di seguito la rete GARR-X nella sua totalità, cui è collegato il Pop di Brindisi.

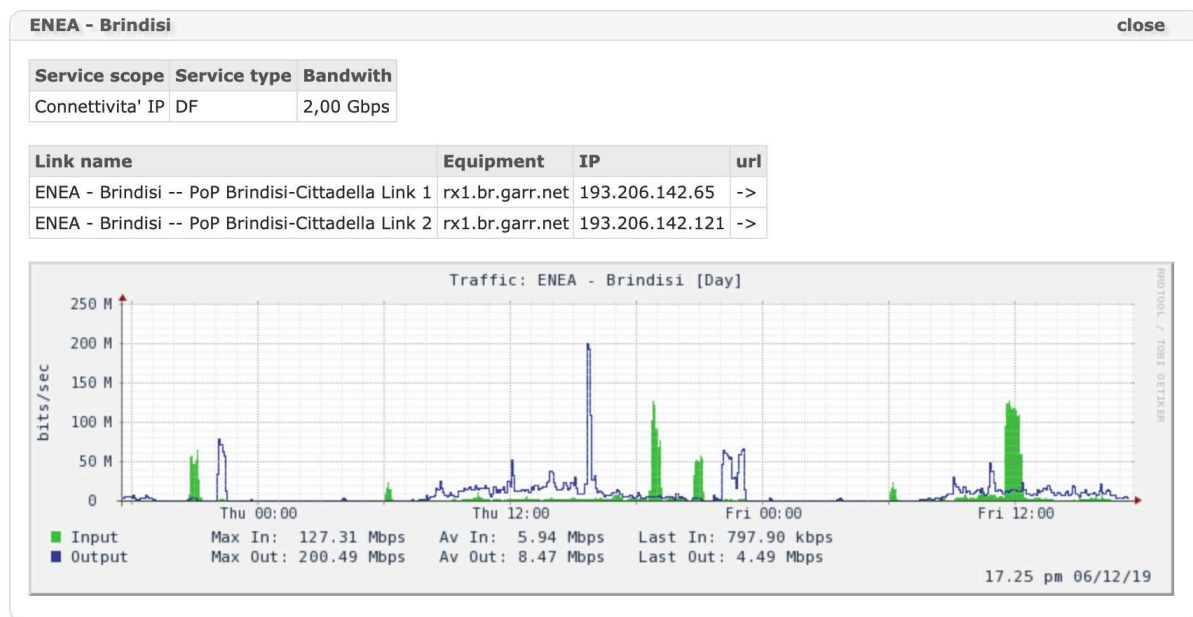


Figura 12: GARR Weathermap: GARRX, Backbone

2 Apparati Layer 3

2.1 Router (GARR)

Il Router Garr rappresenta il punto di collegamento tra l'ente Garr (provider di rete) e l'ente ENEA (client di rete). Il pop di Brindisi, Il router Enea di Brindisi è collegato al Router Garr mediante due uplink ad 1 Gbps ciascuno, in modo da avere almeno un link stabile in caso di guasto.



Il router del GARR è un apparato Juniper MX480 che fornisce connettività mediante 2 link (lambda – λ) con capacità trasmissive di 1 Gbps cadauno. Questa capacità rappresenta un limite impostato dal provider ed è configurabile, con i dovuti upgrade degli apparati e previ accordi tra le parti, per ottenere capacità di banda oltre i 40 Gbps. Vediamo di seguito un estratto della configurazione del Juniper MX480 lato PoP Brindisi-Cittadella¹⁴.

Interfacce VS la LAN – Ovvero le interfacce collegate al router ENEA, la prima configurata con IP 193.206.142.65/30, la seconda con IP 193.206.142.121/30.

```
ge-1/2/1      up    up    enea-brindisi [ODF M5.12]
ge-2/2/0      up    up    enea-brindisi Backup [ODF M7.17]
```

BGP – Di seguito le policy che permettono di accettare gli annunci BGP delle network che vengono inviate da questi link configurati con le opportune P2P.

```
set protocols bgp group ebgp-users neighbor 193.206.142.66 description enea-brindisi
set protocols bgp group ebgp-users neighbor 193.206.142.66 import pol-user-enea-brindisi-import
```

¹⁴ Parte della configurazione e alcuni comandi del Juniper MX480 - GARR.

```

set protocols bgp group ebgp-users neighbor 193.206.142.122 description enea-brindisi
set protocols bgp group ebgp-users neighbor 193.206.142.122 import pol-user-enea-brindisi-bk-import
set policy-options policy-statement pol-user-enea-brindisi-bk-import term enea-brindisi-prefix from route-filter 192.107.88.0/24 exact
set policy-options policy-statement pol-user-enea-brindisi-bk-import term enea-brindisi-prefix then local-preference 80
set policy-options policy-statement pol-user-enea-brindisi-bk-import term enea-brindisi-prefix then community set comm-users
set policy-options policy-statement pol-user-enea-brindisi-bk-import term enea-brindisi-prefix then community add comm-user-enea-brindisi
set policy-options policy-statement pol-user-enea-brindisi-bk-import term enea-brindisi-prefix then accept
set policy-options policy-statement pol-user-enea-brindisi-import term enea-brindisi-prefix from route-filter 192.107.88.0/24 exact
set policy-options policy-statement pol-user-enea-brindisi-import term enea-brindisi-prefix then community set comm-users
set policy-options policy-statement pol-user-enea-brindisi-import term enea-brindisi-prefix then community add comm-user-enea-brindisi
set policy-options policy-statement pol-user-enea-brindisi-import term enea-brindisi-prefix then accept

```

Routes inviate dal garr – La rete 193.206.142.66 viene annunciata con priorità 10, si vince quindi che è la rete di default.

```

inet.0: 787667 destinations, 1575028 routes (787661 active, 6 holddown, 0 hidden)
  Prefix                Nexthop                MED      Lclpref    AS path
* 0.0.0.0/0             Self                  10                I

```

Routes inviate dal garr – La rete 193.206.142.122 viene annunciata con priorità 100.

```

inet.0: 787657 destinations, 1575013 routes (787656 active, 1 holddown, 0 hidden)
  Prefix                Nexthop                MED      Lclpref    AS path
* 0.0.0.0/0             Self                  100                I

```

Routes ricevute dal garr – La rete 192.107.88.0/24 viene inoltrata verso la rete di default, come si evince dalle seguenti tabelle.

```

inet.0: 787638 destinations, 1574976 routes (787638 active, 0 holddown, 0 hidden)
  Prefix                Nexthop                MED      Lclpref    AS path
* 192.107.88.0/24       193.206.142.66         0                64587 I
inet.0: 787656 destinations, 1575012 routes (787656 active, 0 holddown, 0 hidden)
  Prefix                Nexthop                MED      Lclpref    AS path
192.107.88.0/24        193.206.142.122        0

```

2.2 Router (ENEA)

Il router ENEA è un Cisco modello C3925 con interfacce GigabitEthernet e dunque con capacità massime di banda pari a 1 Gbps, è collegato mediante 2 link al router del GARR e svolge funzioni quasi esclusivamente di Routing e NAT. Altri servizi quali DHCP Server e/o Access List permit e Deny, sono relegate ad altre macchine e appliance più specializzati e performanti. Un secondo router della serie

3900 identico in configurazione è utilizzato come backup in caso di guasti. Vediamo di seguito un estratto della configurazione di massima dell'apparato, con un focus sulle parti più interessanti.

Interfacce VS la WAN – Due della quattro interfacce del router sono collegate in uplink al router del GARR. Nella definizione, identica per entrambe interfacce fatto salvo per l'indirizzo IP, oltre ad una banale descrizione, è menzionato l'IP dell'interfaccia Garr interessata, *l'access-group 155 in* che combinata all'*access-list 155 (permit ip any any)* definisce quale traffico è permesso, ovvero tutto il traffico¹⁵ ed infine la definizione di NAT outside e altre politiche di route-map che vedremo in seguito.

```
interface GigabitEthernet0/0/0
description Link Verso GARR
ip address 193.206.142.66 255.255.255.252
ip access-group 155 in
ip nat outside
ip virtual-reassembly in
ip policy route-map pm-calcolo
media-type sfp
!
interface GigabitEthernet0/1/0
description Link Verso GARR
ip address 193.206.142.122 255.255.255.252
ip access-group 155 in
ip nat outside
ip virtual-reassembly in
ip policy route-map pm-calcolo
media-type sfp

access-list 155 permit ip any any
!
```

Interfacce VS la LAN – Una interfaccia del router è collegata in uplink verso il centro stella, lo switch layer 3 huawei P6720. Nella definizione, è menzionata la definizione di NAT inside e altre politiche di route-map che vedremo in seguito.

```
interface GigabitEthernet0/1
description Ethernet vs CR ENEA Brindisi
ip address 192.107.88.254 255.255.255.240
ip nat inside
ip virtual-reassembly in
ip policy route-map packetfence
media-type sfp
!
```

Interfacce VS la LAN – Un'ulteriore interfaccia del router è collegata in uplink verso il centro stella ed è specializzata per veicolare il traffico verso il *“Bypass tra le Reti di Calcolo Enea”* delle varie sedi, ovvero ha scopo bypassare il passaggio dal firewall ottimizzando così le risorse. Nello specifico,

¹⁵ Il Garr non applica nessun filtro e/o limitazione di contenuti di navigazione per le connessioni delle sedi utente. È demandato alle sedi utente il controllo del traffico. Tuttavia il Garr ravvisando un uso non corretto della rete ne può inibire il funzionamento e bloccare ad esempio un IP o una Rete.

l'interfaccia è configurata con un IP specifico ed è proprio l'interfaccia che accetterà tutto il traffico da e verso gli indirizzi IP delle reti di calcolo, ad esempio le reti CRESCO, e altro.

```
!  
interface GigabitEthernet0/2  
  description BYPASS tra RETI CALCOLO ENEA  
  ip address 10.7.12.53 255.255.255.252  
  duplex auto  
  speed auto  
  media-type rj45  
!
```

Tunnel – Uno dei compiti del router è quello di indirizzare il traffico da e verso le reti delle sedi Enea. A questo scopo su tutti i Router delle sedi Enea sono implementate delle interfacce di Tunnel mediante le quali il traffico per l'appunto da e verso le reti Enea, viene veicolato verso il Tunnel in questione senza passare dalla rete del service provider ma in realtà inoculata dentro una rete privata. Il tunnel viene realizzato costruendo una interfaccia Tunnel, una interfaccia di Loopback e impostando delle rotte statiche.

```
interface Loopback1  
  description *** TUNNEL_vs_FRASCATI ***  
  ip address 192.107.88.225 255.255.255.255  
!  
interface Tunnell  
  description *** TUNNEL_vs_FRASCATI ***  
  ip address 10.7.12.49 255.255.255.252  
  ip policy route-map pm-calcolo  
  tunnel source 192.107.88.225  
  tunnel destination 192.107.95.58  
!  
ip route 192.107.100.0 255.255.255.0 Tunnell name PUBB-FRASCATI
```

Questo test di seguito, eseguito mediante traceroute da Brindisi verso Frascati, mostra come sia efficace il Tunnel implementato. Il pacchetto attraversa il router di Brindisi (*192.107.88.254*) che intercetta la rotta statica (*ip router 192.107.100.0 255.255.255.0*) e ruota tutto il traffico verso Tunnell. A questo punto Tunnell mediante la sua interfaccia (*10.7.12.49*) inocula tutto il traffico al Tunnel di destinazione che, opportunamente configurato nella sede di destinazione, riceverà il traffico sulla propria interfaccia (*10.7.12.50*). Il pacchetto arriva poi regolarmente a destinazione (*192.107.100.170*).

```
gc@iMac-di-Giovanni ~ % traceroute 192.107.100.170  
traceroute to 192.107.100.170 (192.107.100.170), 64 hops max, 52 byte packets  
 1  192.168.168.1 (192.168.168.1)  45.308 ms *  45.805 ms  
 2  192.107.88.193 (192.107.88.193)  45.396 ms  44.914 ms  44.852 ms  
 3  192.107.88.254 (192.107.88.254)  45.319 ms  45.109 ms  44.897 ms  
 4  10.7.12.50 (10.7.12.50)  61.024 ms  73.345 ms  61.126 ms  
 5  10.10.252.2 (10.10.252.2)  61.135 ms  61.525 ms  60.742 ms  
 6  10.10.254.5 (10.10.254.5)  72.468 ms  62.586 ms  61.796 ms  
 7  192.107.100.170 (192.107.100.170)  61.358 ms  61.810 ms  61.339 ms
```

In assenza di tunnel il next-hop del router Enea è chiaramente il router Garr e i successivi fino al raggiungimento dell'host di destinazione.

```
gc@iMac-di-Giovanni ~ % traceroute to 192.107.96.118  
 1  192.168.168.1 (192.168.168.1)  245.495 ms *  224.312 ms
```

```

2 192.107.88.193 (192.107.88.193) 43.065 ms 42.737 ms 42.806 ms
3 192.107.88.254 (192.107.88.254) 43.344 ms 43.460 ms 47.428 ms
4 ru-eneabr-l2-rx1-br.br.garr.net (193.206.142.121) 42.945 ms 43.316 ms
5 rx1-br-rx2-ba1.ba1.garr.net (90.147.82.165) 45.029 ms 45.559 ms 283.516 ms
6 rx2-na1-rx2-ba1.ba1.garr.net (90.147.82.110) 52.187 ms 51.869 ms
7 rx3-ba1-rx1-ba1.ba1.garr.net (90.147.82.61) 51.802 ms
8 * * *

```

Bypass Reti Calcolo – La definizione di *route-map* è abbinata ad una o ad una serie di *access-list* contenenti tutti gli IP o reti afferenti alla specifica *access-list*. Nel caso di specie, le *access-list 150* specificano le reti di calcolo. Per queste reti il *next-hop* (ovvero il default gateway) è l'IP *10.7.12.54*, ovvero l'interfaccia che accetterà tutto il traffico da e verso gli indirizzi IP delle reti di calcolo e menzionata di seguito come *Bypass Reti Calcolo*. Vedremo nella sezione successiva come una interfaccia sul centro stella lan sia proprio definita come *Interface Vlanif8, description BYPASS-RETICALCOLO, ip address 10.7.12.54 255.255.255.252*.

```

route-map pm-calcolo permit 10
  match ip address 150
  set ip next-hop 10.7.12.54
!
access-list 150 permit ip 192.107.54.0 0.0.0.255 192.107.88.0 0.0.0.127

```

Bypass Packet Fence – La sezione dedicata al bypass Packet Fence

```

route-map packetfence permit 10
  match ip address 160
  set ip next-hop 193.206.142.65 193.206.142.121
!
access-list 160 permit ip 10.0.1.0 0.0.0.255 192.107.51.0 0.0.0.255

```

BGP – La sezione dedicata al BGP. Il Border Gateway Protocol (BGP) è un protocollo di routing di usato per connettere tra loro più router che appartengono ad Autonomous System distinti e che vengono chiamati router gateway o router di frontiera.

Il BGP mette a disposizione di ciascun router strumenti per ottenere informazioni sulla propria raggiungibilità, determinare i percorsi ottimi e propagare le informazioni a tutti i router interni ad un Autonomous System.

```

router bgp 64587
  bgp log-neighbor-changes
  network 192.107.88.0
  aggregate-address 192.107.88.0 255.255.255.0 summary-only
  neighbor 193.206.142.65 remote-as 137
  neighbor 193.206.142.65 soft-reconfiguration inbound
  neighbor 193.206.142.121 remote-as 137
  neighbor 193.206.142.121 soft-reconfiguration inbound
  maximum-paths 2
  auto-summary

```

Indirizzi per il NAT – In questa sezione viene semplicemente definito un pool di indirizzi IP pubblici da dedicare al NAT¹⁶ definendo una *source list* di IP privati che saranno tradotti.

```
!  
ip nat pool cisbri-natpool 192.107.88.250 192.107.88.251 netmask 255.255.255.240  
ip nat inside source list 1 pool cisbri-natpool overload
```

Route statiche - In questa sezione vengono definite tutte le route statiche.

```
ip route 10.0.1.0 255.255.255.0 192.107.88.253  
!
```

Access list – Di seguito vengono analizzate le *access list* dedicate al NAT (acl-1), Accesso al Firewall in caso di attacchi bruce-force (acl-2), Accesso al Firewall (acl-23) e Accesso al Bypass e Calcolo (acl-155)

```
access-list 1 permit 192.168.168.0 0.0.0.255  
access-list 2 permit 192.168.0.0 0.0.255.255 log  
access-list 2 permit 192.107.0.0 0.0.255.255 log  
access-list 2 deny any log  
access-list 2 remark attiva in caso di attacchi brute-force  
access-list 23 permit 192.168.0.0 0.0.255.255 log  
access-list 23 permit 192.107.0.0 0.0.255.255 log  
access-list 23 deny any log  
access-list 23 remark attiva sempre  
access-list 155 permit udp 192.107.54.0 0.0.0.255 any eq ntp  
access-list 155 deny udp any any eq ntp log  
access-list 155 permit ip any any
```

2.3 Centro Stella (Huawei P6720)

Gli apparati di switching sono il cuore della rete lan e hanno una configurazione che si focalizza prevalentemente sulle interfacce di distribuzione della rete e sulle interfacce di uplink verso gli altri apparati. Il centro stella della lan è il centro stella principale della rete di Brindisi, si occupa di smistare il traffico sugli altri apparati quali switch periferici (foglie) e su altri centri stella specializzati (centro stella calcolo). Il centro stella è un apparato Huawei modello P6720 di ultima generazione con interfacce XGigabitEthernet (10 Gbps) e due interfacce 40GE (40 Gbps). La quasi totalità di foglie è collegata con link da 10 Gbps.

Bypass Calcolo

```
acl number 3003  
rule 15 permit ip source 192.107.88.0 0.0.0.127 destination 192.107.70.0 0.0.0.255  
rule 35 permit ip source 192.107.88.0 0.0.0.127 destination 90.147.99.0 0.0.0.255  
#  
traffic classifier c1 operator or
```

¹⁶ Il meccanismo del NAT è diventato fondamentale nel momento in cui gli indirizzi IP del protocollo IPv4 hanno cominciato a scarseggiare. L'aumento esponenziale dei dispositivi connessi alla Rete ha fatto sì che gli indirizzi disponibili in questo spazio di rete (4 miliardi e 300 milioni circa) si esaurissero in fretta. Il NAT è stato quindi utilizzato per poter nascondere dietro un unico indirizzo pubblico migliaia di indirizzi privati.

```

if-match acl 3003
#
traffic behavior bypass
  redirect ip-nexthop 10.7.12.53
  statistic enable
#
traffic policy bypass match-order config
  classifier cl behavior bypass
#
free-rule-template name default_free_rule
#
portal-access-profile name portal_access_profile
#
drop-profile default
#

```

AAA (authentication, authorization, accounting)

```

aaa
authentication-scheme default
authentication-scheme radius
  authentication-mode radius
authorization-scheme default
accounting-scheme default
local-aaa-user password policy administrator
  password history record number 0
  password expire 0
domain default
  authentication-scheme radius
  radius-server default
domain default_admin
  authentication-scheme default

```

VLAN – La definizione e configurazione delle vlan è una tra le implementazioni principali degli switch. Le vlan vengono definite su tutti gli switch su cui passa traffico che fa parte di quello vlan, inoltre è possibile definire una interface Vlan a cui viene assegnato un indirizzo IP.

```

vlan 1
  description APPARATI
#
interface Vlanif100
  description LAN
  ip address 192.168.173.253 255.255.254.0

```

Interfacce definite Trunk – Sono quelle interfacce per cui è permesso traffico da tutte le vlan. Sono tipicamente definite come interfacce trunk tutte quelle interfacce configurate come uplink verso altri apparati. E' vero infatti che attraverso di esse deve essere consentito tutto il traffico. La configurazione può variare significativamente come sintassi da un brand all'altro, tuttavia il concetto rimane invariato. Nel caso di specie del brand Huawei, la sintassi prevede che tutte le vlan siano menzionate, quindi una porta trunk sarà definita allow-pass su tutte le vlan, dalla 2 alla 4094.

```

#
interface XGigabitEthernet0/0/4
  description LINK TO CENTROSTELLA
  port link-type trunk

```

```
port trunk allow-pass vlan 2 to 4094
```

Interfacce definite Access – Sono quelle interfacce per cui è permesso traffico unicamente da alcune vlan. Sono tipicamente le porte specializzate, degli host. E' vero infatti che attraverso di esse deve passare solo ed esclusivamente il traffico della vlan in questione. Anche in questo caso la configurazione può variare significativamente. Nel caso di specie del brand Huawei, la sintassi è banale, ovvero una porta access su una vlan sarà definita come port default vlan 100 (Esempio per la vlan 100).

```
#
interface XGigabitEthernet0/0/25
description LINK-6720-NEWROUTER
port link-type access
port default vlan 6
loopback-detect enable
```

Interfacce a 40 Gbps – Il centro stella è dotato di porte a 40 Gbps che saranno utilizzate come uplink verso il centro stella di Calcolo, e verso lo Storage.

```
interface 40GE0/0/1
#
interface 40GE0/0/2
#
```

Interfacce vxlan – Sono definite interfacce VXLAN un tipo di vlan che operano a livello di WAN e non solo di LAN. Nell'esempio descritto vediamo come un indirizzo della rete di Brindisi (*192.168.175.60*) è definito come sorgente per comunicazioni su IP della rete di Trisaia (*192.168.254.90* e), e viceversa, il tutto utilizzando esclusivamente indirizzi IP privati e non pubblici. Le vxlan sono in fase di studio e test per permettere la comunicazione tra le sedi di Brindisi e Trisaia. L'obiettivo è far comunicare i due centri in modo che gli host presenti in Trisaia possano autenticarsi mediante il server Packet Fence presente a Brindisi. Sono utilizzate a questo scopo tre vlan dedicate.

```
#
bridge-domain 11
 12 binding vlan 11
 vxlan vni 10011
 statistics enable
#
bridge-domain 150
 12 binding vlan 150
 vxlan vni 10150
 statistics enable
#
interface LoopBack1
 ip address 192.168.175.60 255.255.255.255
#
interface Nve1
 source 192.168.175.60
 vni 10150 head-end peer-list 192.168.254.90
 vxlan statistics peer 192.168.254.90 enable
```

```
#
bridge-domain 11
 12 binding vlan 11
 vxlan vni 10011
 statistics enable
#
bridge-domain 150
 12 binding vlan 150
 vxlan vni 10150
 statistics enable
#
interface LoopBack1
 ip address 192.168.254.90 255.255.255.255
#
interface Nve1
 source 192.168.254.90
 vni 10011 head-end peer-list 192.168.175.60
 vni 10150 head-end peer-list 192.168.175.60
 vxlan statistics peer 192.168.175.60 enable
```

Rotte Statiche – Tutto il traffico ove non veicolato verso il bypass o altre destinazioni, viene infine veicolato verso il Firewall. La route statica definita con la notazione *0.0.0.0 0.0.0.0 Vlanif4 10.0.2.254* significa che tutto il traffico deve essere veicolato sul firewall.

```
#
ip route-static 0.0.0.0 0.0.0.0 Vlanif4 10.0.2.254 description default router su
FIREWALL
```

2.4 Centro Stella Calcolo (Huawei P6810)

Il centro stella Calcolo è un apparato di ultima generazione del brand Huawei modello P6810. L'apparato dispone di 48 interfacce 10GE e di 4 interfacce 40GE. Lo switch è utilizzato come centro stella calcolo e per il collegamento in alta affidabilità degli storage dell'hill di cui dispone il centro per la distribuzione di servizi mediante il cloud, ovvero l'infrastruttura virtuale del centro.

Le interfacce a 10 Gbps – sono collegate ai due Data Hill in modo ridondante e con doppio collegamento incrociato, su vlan dedicata (9 - Storage) . Le interfacce collegano anche tutti gli switch della sala calcolo.

```
#
interface 10GE1/0/33
description vs DH02 Contr. A Port 1
port default vlan 9
loopback-detect enable
device transceiver 10GBASE-COPPER
#
interface 10GE1/0/34
description vs DH02 Contr. B Port 1
port default vlan 9
loopback-detect enable
device transceiver 10GBASE-COPPER
#
interface 10GE1/0/35
description vs DH01 Contr. A Port 1
port default vlan 9
loopback-detect enable
device transceiver 10GBASE-COPPER
#
interface 10GE1/0/36
description vs DH01 Contr. B Port 1
port default vlan 9
loopback-detect enable
device transceiver 10GBASE-COPPER
```

Le interfacce a 40 Gbps –utilizzate per i collegamenti in uplink verso il centro stella LAN.

2.5 Centro Stella (Cisco 4900M)

Centro stella VS Firewall – Il centro stella Cisco 4900 è stato per molto tempo il centro stella lan della rete di Brindisi. L'apparato, anche esso di layer 3, e sostanzialmente con le medesime funzionalità dell'attuale centro stella LAN, dispone di interfacce GigabitEthernet, e TenGigabitEthernet installabili mediante schede di rete modulari. L'apparato dispone anche di porte rame con capacità di 1 GBps che sono opportunamente collegate al firewall poiché anche quest'ultimo dispone di sole porte rame con capacità di 1 Gbps. Dunque, il Cisco 4900 è attualmente utilizzato come interfaccia di collegamento tra in centro stella ed il firewall.

```
!  
interface GigabitEthernet3/1  
  description FWWG-NUOVO-VLAN20-MNGT  
  switchport access vlan 20  
  switchport mode access  
!  
interface GigabitEthernet3/4  
  description FWWG-NUOVO-4900  
  switchport access vlan 4  
  switchport mode access  
!  
interface GigabitEthernet3/6  
  description FWWG-NUOVO-DMZ  
  switchport access vlan 3  
  switchport mode access
```

DHCP Server – Il Cisco 4900 è utilizzato anche come default dhcp server per alcune vlan e/o per test.

```
!  
ip dhcp pool vlan1  
  network 10.0.1.0 255.255.255.0  
  domain-name brindisi.enea.it  
  dns-server 192.168.173.200  
  netbios-name-server 192.168.173.202  
  netbios-node-type p-node  
  option 42 ip 192.168.173.208  
  default-router 10.0.1.254  
  lease 3  
!  
ip dhcp pool BYPASS_LAN  
  network 192.168.169.0 255.255.255.0  
  domain-name brindisi.enea.it  
  dns-server 192.168.173.200  
  netbios-name-server 192.168.173.202  
  netbios-node-type p-node  
  option 42 ip 192.168.173.208  
  default-router 192.168.169.254  
  lease 3  
!
```

3 Apparati Layer 2

Negli anni il corredo di apparati del centro è cresciuto per numerosità di apparati e l'upgrade della infrastruttura in termini di banda e prestazioni ha permesso di sostituire numerosi apparati. Ciò nonostante alcuni di essi sono ancora attivi, più che altro per scopi di testing e/o per utilizzo limitato. Gli switch di piano sono dedicati alla distribuzione capillare della rete in tutti gli edifici. Nella primissima infrastruttura comparivano apparati di brand Enterasys, sostituiti nel 2012 da apparati del brand Cisco. Attualmente in produzione, questi, sono stati affiancati da apparati del brand Huawei. Vedremo le configurazioni più significative sugli apparati e ci soffermeremo sull'implementazione delle funzionalità di LLDP e CDP, AAA per Packet Fence sui due brand attualmente in produzione.

Brand	Modello	N. Porte	2018	2020	Velocità	Host	Uplink	PoE
Enterasys	V2H124	24	No	No	Megabit	Megabit	Gigabit	No
Enterasys	C1G124	24	Si	No	Gigabit	Gigabit	Gigabit	No
Enterasys	B5G124	24	Si	No	Gigabit	Gigabit	Gigabit	No
Cisco	WS-C4948	48	Si	No	Gigabit	Gigabit	Gigabit	No
Cisco	WS-C3750	48	Si	Si	Gigabit	Gigabit	TenGigabit	No
Cisco	WS-C2960	48	Si	Si	Gigabit	Gigabit	TenGigabit	No
Huawei	S5700	48	Si	Si	Gigabit	Gigabit	TenGigabit	No
Huawei	S5720	48	Si	Si	Gigabit	Gigabit	TenGigabit	Si

3.1 Cisco WS-C2960, WS-C3750

Definizione del server di AAA, Packet Fence

```
aaa group server radius packetfence
  server 192.168.175.120 auth-port 1812 acct-port 1813
  deadtime 1
!
aaa authentication login default local
aaa authentication dot1x default group packetfence
aaa authorization network default group packetfence
aaa accounting update newinfo
aaa accounting dot1x default start-stop group packetfence
aaa accounting network default start-stop group packetfence
!
aaa server radius dynamic-author
  client 192.168.175.120 server-key *****
  port 3799
```

Sezione dedicate ai protocolli cdp e lldp

```
device-sensor filter-list lldp list lldp-list
  tlv name system-description
!
device-sensor filter-list cdp list cdp-list
  tlv name version-type
  tlv name platform-type
```

```

!
network-policy profile 12
 voice vlan 12
vlan internal allocation policy ascending
!
lldp run
!

```

Interfacce VS i client

```

!
interface GigabitEthernet1/0/1
 switchport access vlan 11
 switchport mode access
 network-policy 12
 authentication event fail action authorize vlan 13
 authentication event server dead action authorize vlan 100
 authentication event server dead action authorize voice
 authentication event server alive action reinitialize
 authentication host-mode multi-auth
 authentication order dot1x mab
 authentication priority dot1x mab
 authentication port-control auto
 authentication periodic
 authentication timer restart 10800
 authentication timer reauthenticate 10800
 authentication violation replace
 mab
 no snmp trap link-status
 mls qos trust cos
 dot1x pae authenticator
 dot1x timeout quiet-period 2
 dot1x timeout tx-period 3
 spanning-tree portfast
!

```

Definizione del radius server

```

!
radius-server dead-criteria time 30 tries 20
radius-server host 192.168.175.120 auth-port 1812 acct-port 1813 test username
dummy
radius-server deadtime 1
radius-server key *****
radius-server vsa send authentication
!

```

3.2 Huawei S5700, S5720

```

authentication-profile name default_authen_profile
authentication-profile name dot1x_authen_profile
authentication-profile name mac_authen_profile
authentication-profile name portal_authen_profile
authentication-profile name dot1xmac_authen_profile
authentication-profile name multi_authen_profile
authentication-profile name packetfence
 dot1x-access-profile packetfence
 mac-access-profile packetfence
 authentication mode multi-authen max-user 10
 authentication event authen-server-down action authorize vlan 100
 authentication event authen-server-up action re-authen
 authentication dot1x-mac-bypass

```

```

authentication device-type voice authorize
authentication mac-move enable vlan all
authentication mac-move detect enable
#
domain pf
#
l2protocol-tunnel user-defined-protocol 802.1x protocol-mac 0180-c200-0003 group-
mac 0100-0000-0002
#
trace mac enable
#
radius-server dead-count 1
radius-server dead-detect-condition by-server-ip
#
http server load s5720si-v200r011c10spc600.008.web.7z

```

```

Access Point radius-server template default
radius-server template packetfence
radius-server shared-key cipher %^%#|mXsSnX)3+q[;|Yvwm:2|rMj71x2FQ![D~JqJdbN%^%#
radius-server authentication 192.168.175.120 1812 weight 80
radius-server accounting 192.168.175.120 1813 weight 80
radius-server retransmit 2
radius-server dead-time 1
radius-server detect-server interval 30
radius-server testuser username gigio password cipher
%^%#wuh75z>9H>|Vf18Lj@:30Y<\/[cP/71vZ/*PzmSQ%^%#
radius-server session-manage any
radius-server authorization 192.168.175.120 shared-key cipher
%^%#Hf4jGud/;SDa'dU!*`'0aM6~RZMZ{C!C2}~ZLkvJ%^%# server-group packetfence
#
pki realm default
certificate-check none
#
free-rule-template name default_free_rule
#
portal-access-profile name portal_access_profile
#

#
aaa
authentication-scheme default
authentication-scheme radius
authentication-mode radius
authentication-scheme abc
authentication-mode radius
authorization-scheme default
accounting-scheme default
accounting-scheme abc
accounting-mode radius
local-aaa-user password policy administrator
password history record number 0
password expire 0
service-scheme abc
domain default
authentication-scheme radius
radius-server default
domain default_admin
authentication-scheme default
domain pf
authentication-scheme abc
accounting-scheme abc
service-scheme abc

```

```

radius-server packetfence
local-user admin password irreversible-cipher
local-user admin privilege level 15
local-user admin ftp-directory flash:
local-user admin service-type telnet terminal ssh ftp x25-pad http
local-user cisco password irreversible-cipher
local-user cisco privilege level 15
local-user cisco service-type telnet terminal ssh ftp x25-pad http
local-user packetfence password irreversible-cipher
local-user packetfence privilege level 15
local-user packetfence service-type telnet terminal ssh ftp x25-pad http

```

Interfacce VS i client

```

interface GigabitEthernet0/0/8
port link-type hybrid
voice-vlan 12 enable
voice-vlan legacy enable
port hybrid pvid vlan 11
port hybrid tagged vlan 12
port hybrid untagged vlan 11 20 100
authentication-profile packetfence
dhcp snooping enable
dhcp option82 insert enable

```

3.2.1 PoE

Tutti gli switch installati nell'ultima ristrutturazione hanno modulo PoE per l'alimentazione dei telefoni VoIP.

```

<HUAWEI_5700_3>display poe power-state
PORTNAME      POWERON/OFF  ENABLED  FAST-ON  PRIORITY  STATUS
-----
GigabitEthernet0/0/6    on         enable   -        Low       Powered
GigabitEthernet0/0/7    off        enable   -        Low       Detecting

```

3.3 Enterasys C1, A2, B5, N7

In questa sezione vediamo la sintassi di alcuni comandi e implementazioni su apparati Enterasys che vale la pena sottolineare poiché hanno una struttura diversa dai tipici comandi di cisco e huawei.

Creazione e configurazione di interfacce su vlan e in trunk, la prima differenza consiste nella nomenclatura della interfaccia che tipicamente è detta interfaccia mentre Enterasys la chiama “*porta*”.

In questo esempio le porte da 1 a 46 sono in modalità access su vlan 100, la porta 47 è in modalità trunk.

- Creazione delle vlan
- Verifica delle porte da configurare come uplink mediante interrogazione dello switch (chi sono i neighbors – Es. router o altri switch). Le porte ad essi collegate saranno porte di uplink.
- Verifico della grandezza dello switch. Uno switch può essere composto da stack di apparati.
- Pulizia delle vlan (1) mediante comando clear vlan 1 delle porte specializzate su vlan.
- Settaggio della porta trunk

- Settaggio delle porte vlan 100
- Assegnazione delle porte a vlan 100
- Riavvio delle porte

```
set vlan create 100
set vlan name 100 "LAN"
show neighbors
show port
clear vlan egress 1 ge.1.1-46
set vlan egress 100 ge.1.47 tagged
set vlan egress 100 ge.1.1-46 untagged
set port vlan ge.1.1-46 100
set port disable ge.1.1-46
set port enable ge.1.1-46
```

3.4 Enterasys VH2402S

Gli apparati VH2402S sono degli apparati obsoleti ma tuttavia presenti, in modo molto limitato, in alcune sedi Enea. Riportiamo un esempio di configurazione delle vlan in modalità access e trunk, che può risultare difficoltosa senza una utile guida. La prima differenza che si nota dagli apparati meno datati è l'assenza di CLI per le configurazioni, che vengono effettuate da un menù controllato solo da tastiera, senza ausilio di mouse.

Port Assignment VLAN Configuration

Unit	Port	PVID	802.1Q Trunk	Ingress Filter
1	1	100	NO	FALSE
1	2	100	NO	FALSE
1	3	100	NO	FALSE
1	4	100	NO	FALSE
1	5	100	NO	FALSE
1	6	100	NO	FALSE
1	7	100	NO	FALSE
1	8	100	NO	FALSE
1	9	100	NO	FALSE
1	10	100	NO	FALSE

Unit ID : 1 [Show]
Port ID : 1 [More]

<APPLY> <OK> <CANCEL>

Port Assignment VLAN Configuration

Unit	Port	PVID	802.1Q Trunk	Ingress Filter
1	21	100	NO	FALSE
1	22	100	NO	FALSE
1	23	100	NO	FALSE
1	24	100	NO	FALSE
1	25	1	NO	FALSE
--	--	----	----	-----
--	--	----	----	-----
--	--	----	----	-----
--	--	----	----	-----
--	--	----	----	-----

Unit ID : 1 [Show]
Port ID : 21 [More]

<APPLY> <OK> <CANCEL>

802.1Q VLAN Current Table Information

Deleted VLAN Entry Counts : 0

VID	Creation Time	Status
1	0 (0 day 0 hr 0 min 0 sec)	Permanent

Unit Current Egress Ports Current Untagged Ports

1 000000000000 000000000000 1---

Sorted by VID : 1
[Show] [More]

<OK> <PREV UNIT> <NEXT UNIT>

802.1Q VLAN Current Table Information

Deleted VLAN Entry Counts : 0

VID	Creation Time	Status
100	0 (0 day 0 hr 0 min 0 sec)	Permanent

Unit Current Egress Ports Current Untagged Ports

1 111111111111 111111111111 1---

Sorted by VID : 1
[Show] [More]

<OK> <PREV UNIT> <NEXT UNIT>

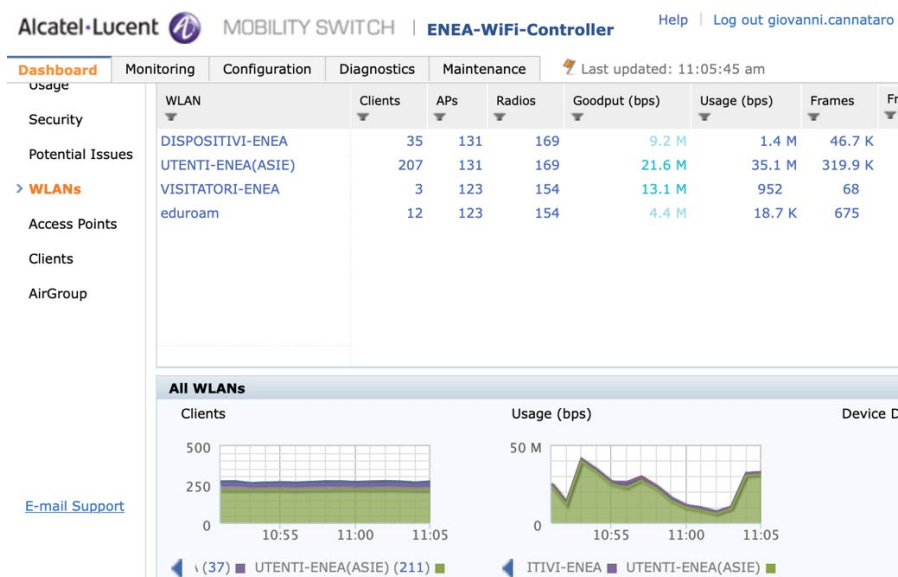
4 Controller Wi-Fi

Nei principali Centri di Ricerca Enea la rete Wi-Fi è implementata mediante tre diverse brand, Controller Alcatel-Lucent, Controller WatchGuard, Controller Huawei. In tutti i centri vengono trasmessi in broadcast i medesimi SSID e le stesse modalità di autenticazione:

SSID	tipo di autenticazione	
UTENTI-ENEA(ASIE)	credenziali ASIE	
VISITATORI-ENEA(ASIE)	credenziali ASIE	
VISITATORI-ENEA	in funzione del Controller ¹⁷	
Eduroam	RADIUS server federato con Eduroam	

4.1 Alcatel-Lucent

I controller Alcatel-Lucent sono centralizzati e localizzati nel centro ricerche di Casaccia, tuttavia il controllo del traffico varia in base all'SSID di riferimento. Il traffico generato dai device collegati come UTENTI-ENEA(ASIE) è trattato come interno alla lan del centro in cui è ubicato l'AP, mentre il traffico generato dai device collegati come VISITATORI-ENEA(ASIE), VISITATORI-ENEA ed Eduroam è inoculato in un tunnel verso Casaccia e questo consente il controllo del traffico differenziando i dipendenti dagli ospiti.



¹⁷ In dismissione

4.2 WatchGuard

I controller WatchGuard sono gestiti dai firewall XTM810, presenti nella quasi totalità dei centri Enea, in modalità decentralizzata per quanto riguarda la gestione degli AP, del traffico di rete, e per gli aspetti logistici, ma in modalità centralizzata ed organizzata per quanto riguarda la pubblicazione dei SSID, rigorosamente omogenea per tutti i centri Enea. Da una delle numerose sezioni del firewall è possibile abilitare il Gateway Wireless Controller e gestire gli AP, rigorosamente del brand WatchGuard. La sezione è molto ricca di impostazioni possibili quali Notification, Logging Settings, vlan, Advanced Deployment, Alarms, MAC Access Control, alcuni utilizzati, altri demandati ad altri apparati (vlan, Mac Address Control, ecc.).

Access Points

SSIDs

Settings

Notification

Paired Access Points

☐	NAME 	SSIDS	NETWORK SETTINGS	RADIO 1	RADIO 2	LOCATION
☐	AP200_1	AP200	192.168.175.30	2.4GHz - G/N	5GHz - N	UFFICIO CANNATARO
☐	AP200_2	AP200	192.168.175.31	2.4GHz - G/N	5GHz - N	UFFICIO GIACINTO
☐	AP200_3	AP200	192.168.175.32	2.4GHz - G/N	5GHz - N	Sala Rizzo - Edificio 6 Piano 1
☐	AP200_4	UTENTI-ENEA(ASIE)	192.168.228.251	2.4GHz - G/N	5GHz - N	UFFICI BARI
☐	AP200_5		192.168.175.34	2.4GHz - G/N	5GHz - N	
☐	AP200_6		192.168.175.35	2.4GHz - G/N	5GHz - N	

4.3 Huawei

I controller Huawei AC6005 sono decentralizzati in più centri Enea, per garantire ridondanza e resilienza ai guasti. Ogni controller di fatto può gestire tutti gli apparati presenti in Enea, ma per ottimizzare le risorse i controller registrano gli AP della lan in cui si trovano, ovvero in modalità predefinita. È possibile, quindi, configurare l'AP sia in modo che abbia un suo Controller di riferimento¹⁸ a prescindere da dove esso sia installato, che contatterà dopo aver ricevuto un IP dal DHCP, sia in modo che si registri al controller di riferimento nella lan in cui è installato l'AP. I controller sono presenti ed in produzione nei centri Enea maggiori, mentre sono da poco installati e in fase di collaudo presso il centro di Brindisi.

¹⁸ L'AP contatterà il Controller o i Controller che gli sono stati configurati. Su ogni AP, infatti, è possibile configurare fino a 4 Controller di riferimento.

4.4 Access Point

4.4.1 OAW-AP68

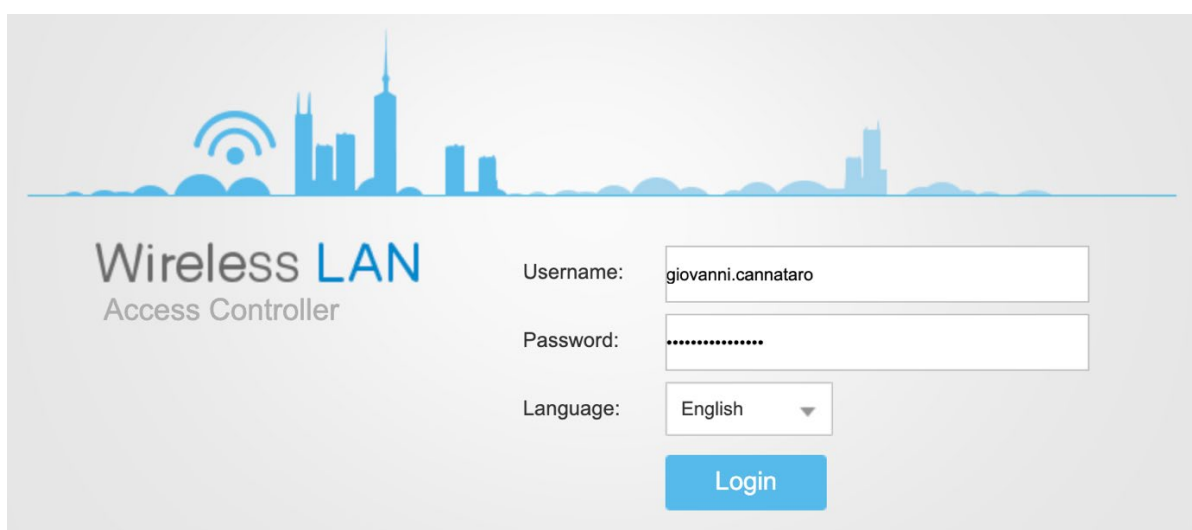
Gli access point AP68 sono gestiti direttamente dall'interfaccia del controller Alcatel-Lucent del centro di Casaccia. Questa appliance, ridondata e distribuita sui centri più grandi, controlla in modo centralizzato tutti gli AP Enea distribuiti sul territorio, attualmente nel numero di circa 160 e gestisce ogni giorno circa 300 accessi utente.

4.4.2 AP200

Gli access point AP200 sono gestiti direttamente dall'interfaccia dei firewall WatchGuard delle varie sedi mediante la sezione Gateway Wireless Controller. Questi AP vanno a coprire aree di competenza Enea rimasti parzialmente scoperti dall'installazione degli AP Alcatel per la sede di Brindisi, mentre per altre sedi sono distribuiti in modo capillare e coprono le aree di competenza Enea. Questi AP, assieme ai nuovi AP Huawei andranno a sostituire gradualmente gli AP Alcatel-Lucent man mano che questi diventeranno obsoleti.

4.4.1 AP5130DN

Gli access point AP5130DN sono gestiti direttamente dal controller Huawei che all'avvio dell'AP rileverà la sua presenza in rete e lo abiliterà mediante opportune configurazioni. Una volta rilevato e inserito nella lista degli AP questo sarà gestito e abilitato, disabilitato, messo in black list, ecc. Gli AP Huawei andranno a sostituire gradualmente gli AP Alcatel-Lucent man mano che questi diventeranno obsoleti.



The image shows a login interface for a 'Wireless LAN Access Controller'. At the top, there is a blue graphic of a city skyline with a Wi-Fi signal icon. Below the graphic, the text 'Wireless LAN' is displayed in a large, bold, blue font, with 'Access Controller' in a smaller, grey font underneath. To the right of the logo, there are three input fields: 'Username:' with the value 'giovanni.cannataro', 'Password:' with a masked password '.....', and 'Language:' with a dropdown menu showing 'English'. Below these fields is a blue 'Login' button.

5 Firewall

Il firewall attualmente in produzione è un Firewall del brand WatchGuard Modello XTM 810. E' dotato di 10 interfacce da 1 Gbps in rame. E' un dispositivo di sicurezza molto potente e versatile e di facile utilizzo. Il firewall è attualmente configurato nella modalità host-based e network-based firewall, con regole di allow/deny, tuttavia ha diverse potenzialità e features di ultima generazione e può funzionare come firewall su livello applicativo. Questa scelta è dettata da un aspetto economico di convenienza, visti i costi molto elevati delle licenze per l'attivazione delle suddette features. Nella prossima ristrutturazione della rete sono già previsti firewall applicativi. Il firewall è veramente molto completo e presenta un menù vasto di cui vedremo solo alcune parti più interessanti.

DASHBOARD	SYSTEM STATUS	NETWORK	FIREWALL	SUBSCRIPTION SERVICES	AUTHENTICATION	VPN	SYSTEM
Front Panel	ARP Table	Interfaces	Firewall Policies	Application Control	Hotspot	Branch Office VPN	Information
Subscription Services	Authentication List	ARP Entries	Mobile VPN IPSec Policies	WebBlocker	Servers	BOVPN Virtual Interfaces	Feature Key
FireWatch	Blocked Sites	Link Aggregation	Aliases	spamBlocker	Settings	Phase 2 Proposals	NTP
Interfaces	Checksum	VLAN	Proxy Actions	Gateway AV	Users and Groups	IKEX2 Shared Settings	SNMP
Traffic Monitor	Components List	Bridge	Traffic Management	Geolocation	Web Server Certificate	Mobile VPN with IPSec	Managed Device
Gateway Wireless Controller	DHCP Leases	Loopback	Scheduling	IPS	Single Sign-On	Mobile VPN with PPTP	Logging
Geolocation	Diagnostics	Multi WAN	SNAT	Quarantine Server	Terminal Services	Mobile VPN with SSL	Diagnostic Log
	Dynamic DNS	Dynamic DNS	Default Packet Handling	Reputation Enabled Defense	Authentication Portal	Mobile VPN with LZTP	Global Settings
	Hotspot Clients	NAT	Blocked Sites	Botnet Detection		Global Settings	Certificates
	Processes	Routes	Blocked Ports	Dataloss Prevention			Proxy Auto-Configuration
	Routes	Dynamic Routing	Quotas	APT Blocker			Upgrade OS
	Server Connection	Gateway Wireless Controller		Threat Detection			Backup Image
	Traffic Management						Restore Image
	Users and Roles						Technology Integrations
	Quotas						USB Drive
	VPN Statistics						Users and Roles
							Configuration File
							Login Disclaimer
							About

- La Dashboard mostra le statistiche di navigazione come top clients, top destination, e ancora top policies ed altro. Un'altra statistica interessante viene mostrata nella sezione FireWatch, che mostra tutte le connessioni per i parametri source, destination, policy, interface (In), interface (Out). Nella sezione Interfaces possiamo vedere le connessioni espresse come bandwidth di tutte le interfacce in produzione, i pacchetti inviati e ricevuti da ciascuna interfaccia. Traffic Monitor è la sezione più interessante per quel che riguarda il troubleshooting sul firewall. Da questa interfaccia possiamo infatti vedere in presa diretta tutto il traffico che attraversa il firewall. Per ogni tupla del db ci viene mostrato timestamp, action (allow o deny), IP sorgente, IP destinatario, porta TCP/UDP o altro, Interfaccia, Regola intercettata ed altri codici.

```
2019-12-10 00:35:01 Deny 192.168.173.168 119.201.79.56 8621 61807 1-LAN 0-OUT Denied 129 62 (Unhandled Internal Packet-00)
2019-12-10 00:35:01 Allow 192.107.88.4 192.107.88.200 47784 53 1-LAN 2-DMZ Allowed 67 62 (Tutto aperto tra le reti locali-00)
```

Sempre dalla Dashboard principale abbiamo accesso al Gateway Wireless Controller, ovvero il controller degli access point WatchGuard, e nel caso di specie, gestiamo un piccolo numero di AP 200 di cui vedremo la configurazione in una sezione successiva.

- Il menù System Status, così come la Dashboard ci mostra una vista sullo stato attuale del firewall, dai siti bloccati agli indirizzi IP rilasciati dal dhcp interno (attivato solo su alcune specifiche vlan), e ancora ci mostra i client collegati agli hotspot ed altro ancora.

- Network è sicuramente la sezione che ci interessa di più, parlando di reti, poiché è proprio da qui che andiamo a configurare le varie interfacce network del firewall, ne definiamo il tipo (external per le reti pubbliche, trusted per le reti interne), l'indirizzo IP, ecc. Sempre da questa sezione andiamo a configurare opzionalmente tutte quei servizi tipici di una rete, quali vlan, bridge, loopback, DNS, NAT, routes ed altro ancora. Nella rete di Brindisi alcuni dei servizi appena citati sono svolti da altri apparati (DNS Server su linux, NAT e vlan dal centro stella, ecc. tuttavia in questa sezione vengono definite le rotte statiche in uscita dal firewall, fondamentali per il suo funzionamento, è implementato il servizio di NAT per le reti esterne collegate al Firewall per cui abbiamo deciso di definire un indirizzo di NAT diverso da quello per la rete di Brindisi, vedi Vlan 15 (Ditne) – 10.0.4.0/24. Infine dal menù Network è possibile abilitare e configurare il Gateway Wireless Controller e definire la configurazione degli Access Point, i SSIDs delle reti Wi-Fi, ecc.
- Firewall è la sezione centrale dell'apparato, da qui è possibile configurare le politiche di sicurezza, definire Alias e azioni da intraprendere. È possibile utilizzare un alias per identificare un gruppo di host o reti con un nome univoco, ed è molto consigliato l'utilizzo degli alias al posto dei meri indirizzi IP o reti. All'atto della creazione di una regola (policy) l'interfaccia si presenta così come in figura.

Firewall Policies / Edit

Name ☒ Enable

Settings Traffic Management Scheduling Advanced

Connections are

Policy Type TCP4500

PORT	PROTOCOL
4500	UDP

FROM

TO

Figura 13: Creazione di una regola (policy) sul firewall

Sostanzialmente per ogni policy creata ne definiamo:

- il nome, definiamo un nome simbolico il più attinente possibile alla regola stessa;
- il tipo di connessione, Allowed/Denied;
- la porta ed il protocollo, 443/TCP;
- sorgente, From;
- destinazione, To;

La policy di sicurezza citata nell'esempio si chiama TPC4500 (Name) ed è una regola che consente (Allow) a tutti (From Any) di instaurare connessioni UDP/ 4500 (Protocol/Port) verso vpnserver (To). Infine la regola è abilitata e funzionante (Enable). Tutte le policy hanno sostanzialmente la stessa struttura, variano le porte ed i protocolli, gli alias che sono coinvolti ecc. Per ogni policy possono ulteriormente essere definiti:

- TAG, che ne identificano l'appartenenza ad una tipologia di regole;
- Logging, tutte le policy su cui è abilitato il logging verranno visualizzate sulla interfaccia Ttraffic Monitor;

Inoltre si può scegliere dal menù generale se fare logging su un Log Server esterno o interno. Le regole più significative o sulle quali si fa troubleshooting sono menzionate e il log viene conservato su server esterno. Wachguard consente lo storage dei Log su un server proprietario di nome Dimension, abilitato e funzionante nella rete di Brindisi.

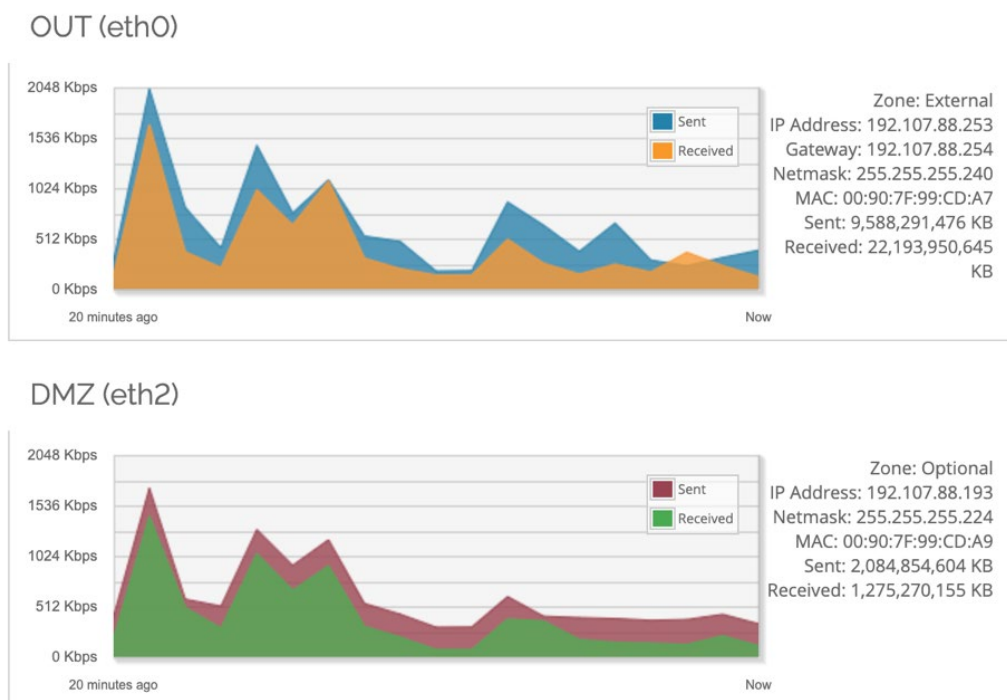


Figura 14: Statistiche di utilizzo di banda

Schema logico

Dopo aver affrontato nella primissima parte del documento, la realizzazione del cablaggio strutturato, fondamentale per la realizzazione di una buona rete dati e successivamente, affrontato e descritto lo schema fisico di rete, ovvero come gli apparati sono distribuiti e in che modo e con che tipologia e topologia essa è strutturata, nella seguente sezione andremo ad affrontare un tema molto importante per le reti, ovvero lo schema logico di rete.

Lo schema logico di rete è uno schema che sintetizza in che modo una rete è implementata a livello logico, dunque è una astrazione dal livello fisico della rete e permette al gestore di implementarla secondo una sua idea di sicurezza, affidabilità, resilienza e accessibilità. La buona riuscita della implementazione di una rete necessita dello studio e realizzazione di un buon schema logico della stessa. Una rete organizzata in un certo modo e con una certa resilienza e affidabilità a livello logico, non può prescindere dall'utilizzo di determinate applicazioni e metodologie di implementazione, senza le quali, altrimenti, la rete non avrebbe le suddette caratteristiche.

Il primo strumento ed il più importante è l'utilizzo di vlan che ci permettono di segmentare la rete e dividerla, in modo logico, e non soltanto fisicamente.

Una rete informatica può funzionare senza l'utilizzo di alcuna vlan, ma la sua gestione e sicurezza è pesantemente compromessa e complicata, nonché vetusta, non conforme ai moderni standard di sicurezza, ed obbiettivamente scomoda nella sua gestione.

Nativamente tutti gli apparati di rete hanno una sola vlan default (1) abilitata su tutte le interfacce e di fatto l'utilizzo di una sola vlan equivale sostanzialmente a non utilizzarle. Di contro vedremo, come, l'utilizzo di molteplici vlan, ci permette di ottimizzare il traffico di rete, segmentare, parzializzare, dividere la rete in modo logico, aumentando sicurezza e fruibilità, con il piccolo scotto di complicare un po' la configurazione della rete stessa.

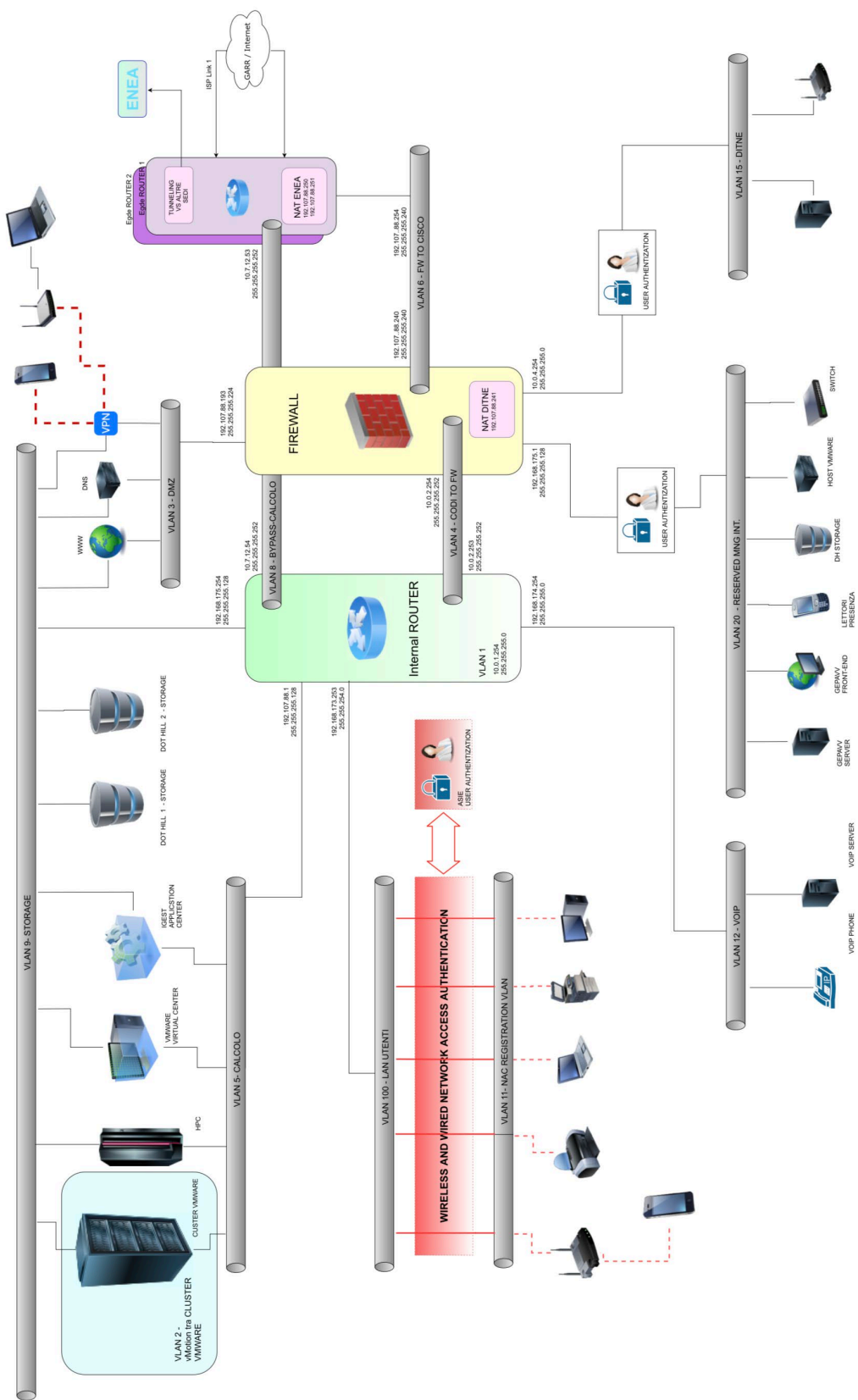


Figura 15: Network Logical Diagram

1 Indirizzamento IP

L'infrastruttura di rete di Brindisi è concepita e strutturata affinché il suo funzionamento sia quanto più sicuro, tanto più coerente con gli standard di sicurezza imposti. Uno degli obiettivi perseguiti è quello di utilizzare dove possibile indirizzamento privato affinché le macchine e la rete in generale sia il più possibile protetta da intrusioni malevoli. La sede di Brindisi dispone di un totale di 16 reti di classe C¹⁹ per gestire tutte le varie configurazioni e necessità ed ulteriori reti private di classe A²⁰ utilizzabili a piacere.

1.1 IP Privati

SUBNET	MASK	SIZE	ROLE
10.0.1.0	255.255.255.0	254	ex centralino nortel, ex cisco
10.0.2.252	255.255.255.252	2	Codi to Fw /Fw to Codi
10.0.3.0	255.255.255.0	254	vmotion vmware
10.0.4.0	255.255.255.0	254	rete ditne
10.0.5.0	255.255.255.0	254	registration_vlan
10.0.6.0	255.255.255.0	254	isolation_vlan
10.0.7.0	255.255.255.0	254	fwgw_mng
10.0.8.0	255.255.255.0	254	bypass_vlan_voice
10.50.1.0	255.255.255.0	254	gpfs-calcolo
10.50.2.0	255.255.255.0	254	gpfs-calcolo
10.7.12.004	255.255.255.252	2	tunneling brindisi-bologna
10.7.12.008	255.255.255.252	2	tunneling brindisi-palermo
10.7.12.012	255.255.255.252	2	tunneling brindisi-sede
10.7.12.016	255.255.255.252	2	tunneling brindisi-portici
10.7.12.020	255.255.255.252	2	tunneling brindisi-trisaia
10.7.12.024	255.255.255.252	2	tunneling brindisi-bari
10.7.12.028	255.255.255.252	2	tunneling brindisi-brasimone
10.7.12.032	255.255.255.252	2	tunneling brindisi-saluggia
10.7.12.044	255.255.255.252	2	tunneling brindisi-ispra
10.7.12.048	255.255.255.252	2	tunneling brindisi-frascati

¹⁹ L'enea ha adottato la suddivisione tra i centri della rete privata di classe B con IP 192.168.0.0/16. Ogni centro, in base alle esigenze, utilizza una porzione di IP privati ad esso assegnati cosicché si crei una macro LAN distribuita nell'ottica della raggiungibilità tra le sedi. Brindisi utilizza il range di IP dal 192.168.168.0 al 192.168.175.0, ovvero 16 reti di classe C.

²⁰ Gli IP di classe A con IP 10.0.0.0/8 sono utilizzabili a piacere da ogni centro, tuttavia è obiettivo del Laboratorio organizzare anche il loro utilizzo in virtù della raggiungibilità tra centri.

10.7.12.052	255.255.255.252	2	bypass tra router wan e centro stella calcolo
10.7.12.056	255.255.255.252	2	vmotion tra servizi01 e servizi02
192.168.160.0	255.255.248.0	2040	utilizzi futuri
192.168.168.0	255.255.255.0	254	vpn
192.168.169.0	255.255.255.0	254	bypass lan
192.168.170.0	255.255.255.0	254	blade calcolo
192.168.171.0	255.255.255.0	254	blade calcolo
192.168.172.0	255.255.254.0	512	lan
192.168.174.0	255.255.255.0	254	voip
192.168.175.0	255.255.255.128	126	management
192.168.175.128	255.255.255.128	126	storage

Tabella 3: Indirizzamento IP Privati

1.2 IP Pubblici

Il centro di Brindisi detiene l'utilizzo di una rete pubblica di classe C con indirizzamento 192.107.88.0/24²¹ opportunamente subnettata per soddisfare le esigenze del centro. L'utilizzo di IP pubblici è consentito per l'indirizzamento delle DMZ dei servizi di Centro e di Calcolo, per gli uplink di tunneling tra le sedi, per il collegamento tra Router e Firewall e per il NAT. In linea generale sono utilizzati solo ed esclusivamente dove necessitano strettamente.

SUBNET	MASK	SIZE	ROLE
192.107.88.0	255.255.255.128	126	dmz calcolo
192.107.88.128	255.255.255.224	30	libera
192.107.88.128	255.255.255.192	62	libera
192.107.88.160	255.255.255.224	30	libera
192.107.88.192	255.255.255.224	30	dmz centro
192.107.88.224	255.255.255.240	14	tunneling
192.107.88.240	255.255.255.240	14	router-firewall

Tabella 4: Indirizzamento IP Pubblici

²¹ La rete 192.10.7.88.0/24 fa parte di un range di classi di ip pubblici più ampio ed utilizzati da ENEA senza soluzione di continuità dalla rete 192.107.51.0/0 alla rete 192.107.100.0/24 chiamata anche NET-ENEATCPNET-[1-50]. L'Enea detiene l'utilizzo di altre reti pubbliche, ad esempio per l'indirizzamento dei nodi di CRESCO.

2 VLAN

2.1 Introduzione

In telecomunicazioni e informatica il termine VLAN (Virtual Local Area Network) indica un insieme di tecnologie che permettono di segmentare il dominio di broadcast, che si crea in una rete locale basata su switch, in più reti locali logicamente non comunicanti tra loro, ma che condividono globalmente la stessa infrastruttura fisica di rete locale. Le applicazioni di questa tecnologia sono tipicamente legate ad esigenze di separare il traffico di gruppi di lavoro o dipartimenti di un'azienda, per applicare diverse politiche di sicurezza informatica.

I vantaggi di una vlan, sono molteplici:

- **Isolamento di un gruppo di dispositivi** – con una vlan si può fare in modo che alcuni sistemi e dispositivi possano "colloquiare" fra loro e connettersi alla rete Internet senza che la rete virtuale nella quale essi sono inseriti offra visibilità sugli altri host della lan (o delle altre vlan) e senza che questi possano avere a loro volta visibilità sui "membri" della vlan.
- **Migliore gestione del traffico** – impostando una vlan si possono definire molto facilmente politiche per la gestione del traffico che permettano ad esempio di limitare la banda messa a disposizione dei sistemi collegati alla rete virtuale, quindi, è possibile ricorrere a QoS (Quality of Service) per definire una politica di gestione del traffico.
- **Ottimizzazione dell'utilizzo delle infrastrutture ed elevata scalabilità** – per creare una vlan e isolare una subnet non si dovranno acquistare nuovi switch o router ma basterà isolare semplicemente alcune porte presenti sullo switch. L'utilizzo delle vlan permette inoltre di creare configurazioni di rete fortemente scalabili: l'espansione di una rete esistente diventa così facile, veloce e molto economica.

Le vlan consentono di creare differenti domini di broadcast: ogni volta che un client invia una richiesta a livello hardware sulla rete per conoscere qual è il mac address corrispondente a un determinato IP privato, viene effettuata un'operazione broadcast. Grazie alla segmentazione che può essere impostata ricorrendo alle vlan, il traffico di broadcast può essere circoscritto all'interno della vlan stessa. I benefici sono evidenti perché le richieste broadcast di una vlan non vanno più a impattare sulle prestazioni dell'intera rete locale. Mediante le vlan, infatti, si possono mettere in comunicazione solo quei dispositivi che necessitano di colloquiare tra loro. Le vlan possono essere estese anche oltre i limiti fisici del singolo switch, nel caso in cui si abbia una rete che si sviluppa su più piani o edifici

È possibile utilizzare le lan virtuali per dividere la rete in aree logiche separate. Le vlan possono anche essere considerate domini di broadcast. Qualsiasi porta dello switch può appartenere a una vlan e i pacchetti unicast, broadcast e multicast vengono inoltrati e inondati solo alle stazioni terminali in quella

vlan. Ogni vlan è considerata una rete logica e i pacchetti destinati alle stazioni che non appartengono alla vlan devono essere inoltrati attraverso un router.

Le vlan sono generalmente associate a subnet IP. Ad esempio, tutte le stazioni terminali in una particolare sottorete IP appartengono alla stessa vlan. Per comunicare tra vlan, è necessario instradare il traffico.

Le vlan sono numerate da 1 a 4094. Tutte le porte configurate appartengono alla vlan predefinita al primo avvio dello switch. La vlan predefinita (1) utilizza solo valori predefiniti e non è possibile creare, eliminare o sospendere l'attività nella vlan predefinita²².

Le vlan appena create rimangono inutilizzate fino a quando le porte non vengono assegnate alla vlan specifica. Tutte le porte sono assegnate a vlan (1) per impostazione predefinita.

Nella rete di Brindisi, come vedremo, la vlan 1 viene ancora utilizzata solo per il raggiungimento di alcuni apparati di rete, che sono comunque raggiungibili su un'altra vlan apposita.

2.2 VLAN Interface

Le vlan sono create sul centro stella e su tutte le foglie su cui le devono transitare, oltre che, ovviamente, su apparati di transito o altri centro stella. Per ogni vlan viene creata una “vlan interface” ovvero un'interfaccia virtuale sull'apparato che farà da default gateway per la specifica vlan. Tipicamente sul centro stella vengono create tante vlan interfaces quante sono le interfacce ad esso collegato. Successivamente le porte degli switch vengono in gergo specializzate assegnandogli una vlan creata. Da quel momento in poi quella porta assegnata alla vlan accetterà solo traffico taggato con quella specifica vlan.

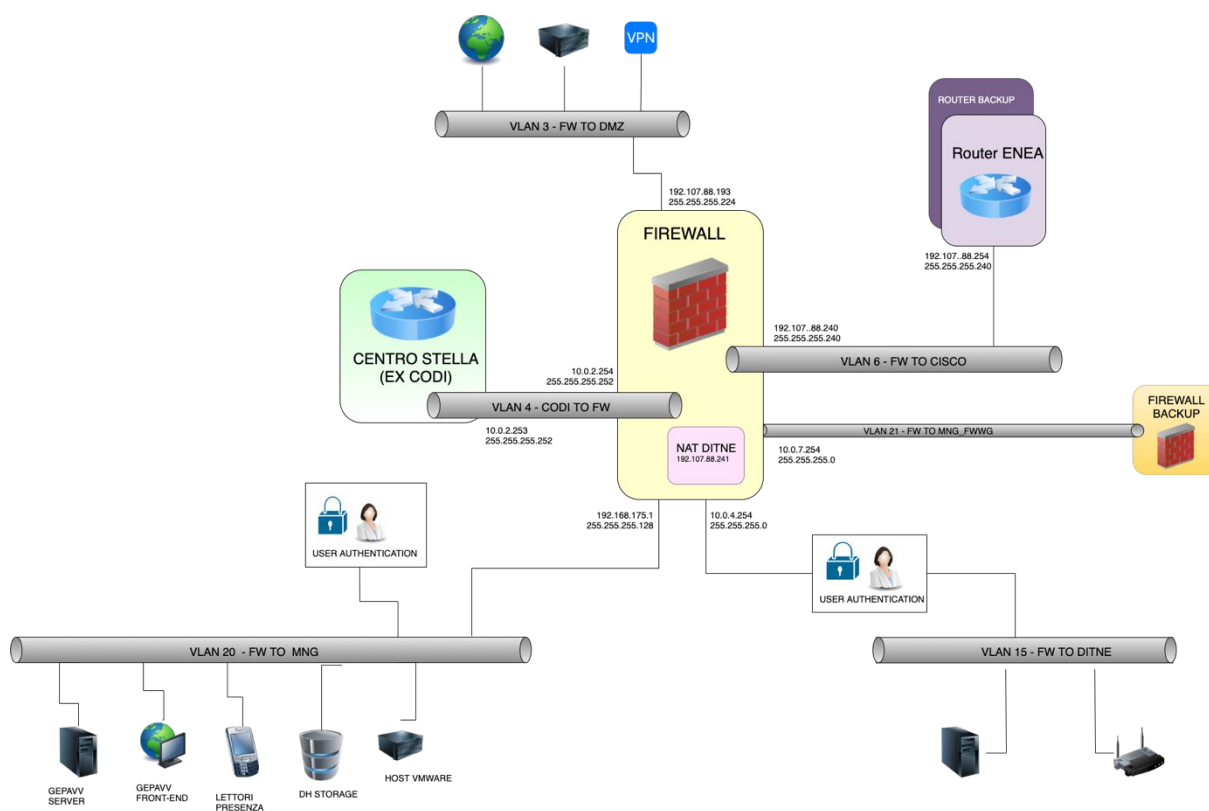
Nr.	Nome	descrizione	IP Default Gateway	Interfacce terminate sul		
				Centro Stella	Firewall	NAC
1	vlan 1	apparati	10.0.1.254	X		
2	vlan 2	vmotion_vmware				
3	vlan 3	dmz	192.107.88.193		X	
4	vlan 4	codi-fw	10.0.2.253	X		
		fw-codi	10.0.2.254		X	
5	vlan 5	dmz-calcolo	192.107.88.1	X		
6	vlan 6	fw-routergbt	192.107.88.253		X	
7	vlan 7	gpfs-calcolo				
8	vlan 8	bypass-reticalcolo	10.7.12.54	X		
9	vlan 9	storage	192.168.175.254	X		

²² Mediante qualche accorgimento è possibile farlo.

10	vlan 10	isolation_vlan				X
11	vlan 11	registration_vlan				X
12	vlan 12	voice	192.168.174.254	X		
13	vlan 13	guest				X
14	vlan 15	ditne	10.0.4.254		X	
15	vlan 20	mng	192.168.175.1		X	
16	vlan 21	fw-mng	10.0.7.254		X	
17	vlan 100	lan	192.168.173.253	X		
18	vlan 110	bypass_lan	192.168.169.254	X		
19	vlan 112	bypass_vlan_voice	10.0.8.254	X		
20	vlan 150	vxlan_test				X
21	vlan 210	isolation_pf_cluster				X
22	vlan 211	registration_pf_cluster				X

Tabella 5: Lista completa delle Vlan definite

2.3 Interfacce terminate sul firewall



2.3.1 Vlan 3 (Dmz) – 192.107.88.193/27

Nell'ambito della sicurezza informatica una zona demilitarizzata è una sottorete isolata, fisicamente o logicamente, che contiene dei servizi informatici offerti ed accessibili sia dalle reti esterne non protette (WAN), sia da reti interne (intranet), configurata con lo scopo di far usufruire questi servizi nella maniera più sicura possibile, senza compromettere la sicurezza della rete e degli utilizzatori. In questa “zona”, taggate con vlan 3 sono confinate la maggior parte dei servizi di rete quali siti internet, dns, servizi di videoconferenza punto-punto, e dei server che erogano vpn, radius, sip.

2.3.2 Vlan 6 (FW to Router) – 192.107.88.240/28

Questa vlan è utilizzata con indirizzamento pubblico per il collegamento diretto tra router-firewall.

2.3.3 Vlan 20 (Mng) - 192.168.175.1/25

LA vlan 20 è implementata per dare maggiore sicurezza e robustezza alla rete. In particolare nasce da una precisa scelta dei gestori, intenzionati a confinare in un'area ben definita della rete, sicura, controllata e poco facilmente accessibile, le interfacce di management di tutti dispositivi di rete e di tutti i server che offrono servizi al personale.

Sono indirizzati con IP *192.168.175.0/25* su vlan 20 tutti i dispositivi di rete come switch e access point, le interfacce di management degli host ESXi²³ VMware e dei controller dei dothill, le interfacce dei lettori di badge per il controllo presenze e apriporta. Infine sono

Infine, tutti i servizi del personale, dopo esser stati migrati su macchine virtuali, sono stati confinati su questa vlan con enormi vantaggi quali:

- **Maggiori performance** – Virtual Machine sempre disponibili, performanti, sempre aggiornate all'ultima release, in alta affidabilità e con sicurezza di backup. NON utilizzo di SAMBA;
- **Maggiore sicurezza** – Cartelle non sono rese disponibili in rete, solo l'utente/i abilitato ha la possibilità di accedervi;
- **Maggiore usabilità** – Chiavi hardware di licenza sono installate sugli host ESXi e rese disponibili.

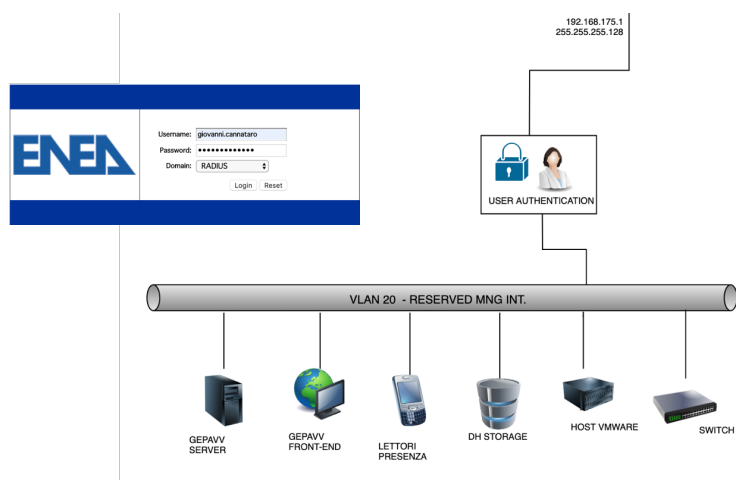
L'accesso alle VM avviene esclusivamente previa autenticazione²⁴ su Radius Server mediante credenziali ASIE dall'interfaccia del firewall <https://fw:4100/logon.shtml>.

2019-12-13 01:06:55 admd Authentication of Firewall user [giovanni.cannataro@RADIUS] from 192.168.168.5 accepted id="1100-0004"

²³ Le funzionalità e le prestazioni di VMware ESX ed ESXi sono le stesse; la differenza tra i due hypervisor risiede nell'architettura del packaging e nella gestione operativa, tuttavia ESXi ha un'architettura superiore.

²⁴ Regole ad-hoc sono state scritte per abilitare al login i soli utenti amministratori.

2019-12-13 01:06:55 sessiond Firewall user giovanni.cannataro@RADIUS from 192.168.168.5 logged in id="3E00-0002"
 2019-12-13 01:08:21 Allow 192.168.168.5 192.168.175.20 57334 22 2-DMZ 4 MNGT Allowed 64 6 (Autorizzati_VLAN20_Management-00)
 proc_id="firewall" rc="100" msg_id="3000-0148" tcp_info="offset 11 S 1221488439 win 65535" src_user="giovanni.cannataro@RADIUS"

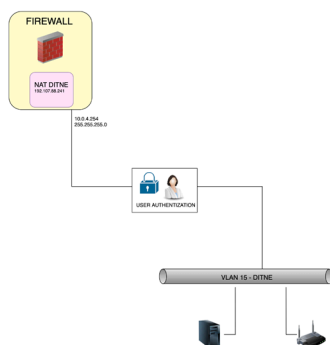


2.3.4 Vlan 21 (Mng_FWWG) – 10.0.7.254/24

La vlan 21 è di uso interno, utilizzata per la piena raggiungibilità degli apparati in stato di configurazione test e pre-rilascio. Uno fra tanti è il firewall per la sede di Bari, attualmente in uplink alla rete locale di Brindisi.

2.3.5 Vlan 15 (Ditne) – 10.0.4.0/24

Il Ditne è un ente esterno che si trova nel comprensorio della Cittadella della Ricerca in attesa di connettersi alla rete Garr. Il centro di Brindisi fornisce connettività mediante una vlan dedicata e con limitazioni. In generale questa tipologia di vlan è da considerarsi come caso d'uso standard per le connessioni una tantum per eventi quali conferenze, workshop ecc, da tenersi in ambienti della cittadella e non che hanno un collegamento fisico con il PoP garr di Brindisi.



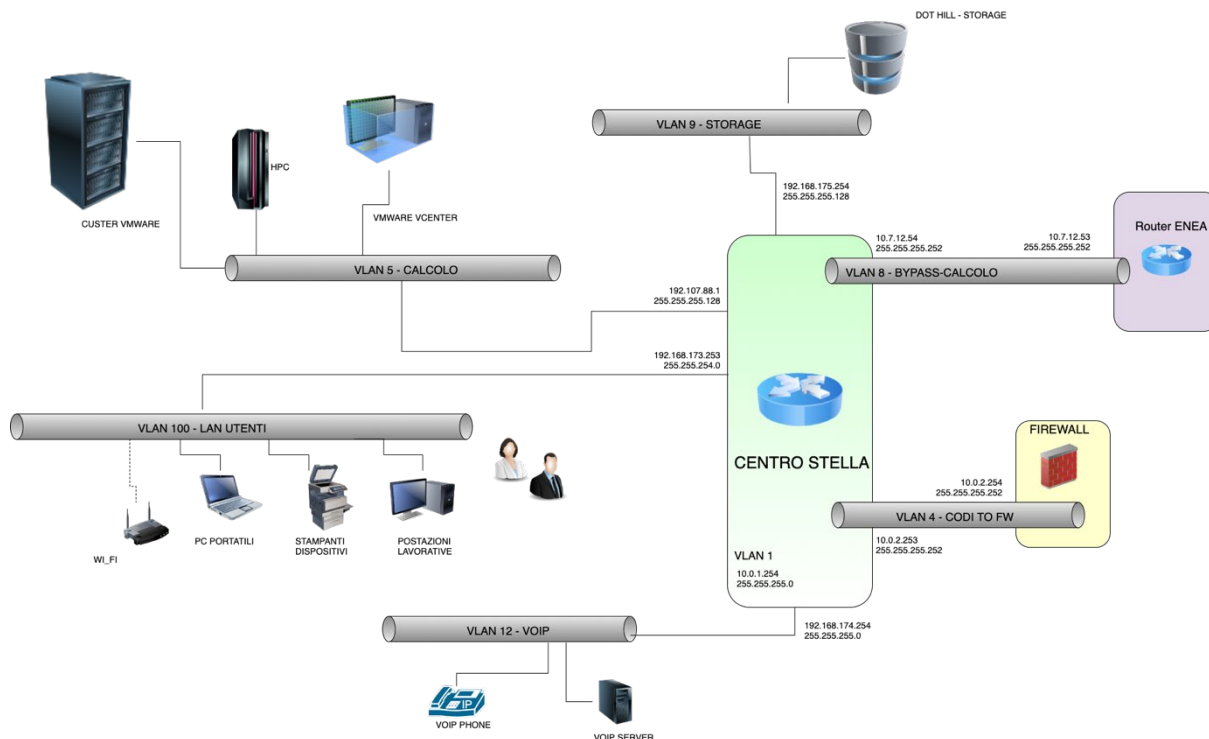
L'accesso avviene esclusivamente previa autenticazione su Firebox²⁵ mediante credenziali create ad-hoc, dall'interfaccia del firewall <https://fw:4100/logon.shtml>

Per una maggiore sicurezza:

Sono state implementate regole ad hoc e delle limitazioni sul firewall sia per la navigazione in internet, sia per la banda disponibile, l'IP di NAT diverso da quello ENEA

²⁵ Sono stati creati dei Firebox Users ad-hoc per gli utenti del Ditne poiché essi, non essendo dipendenti ENEA, non hanno credenziali Active Directory e non possono fare autenticazione Radius.

2.4 Interfacce terminate sul centro stella



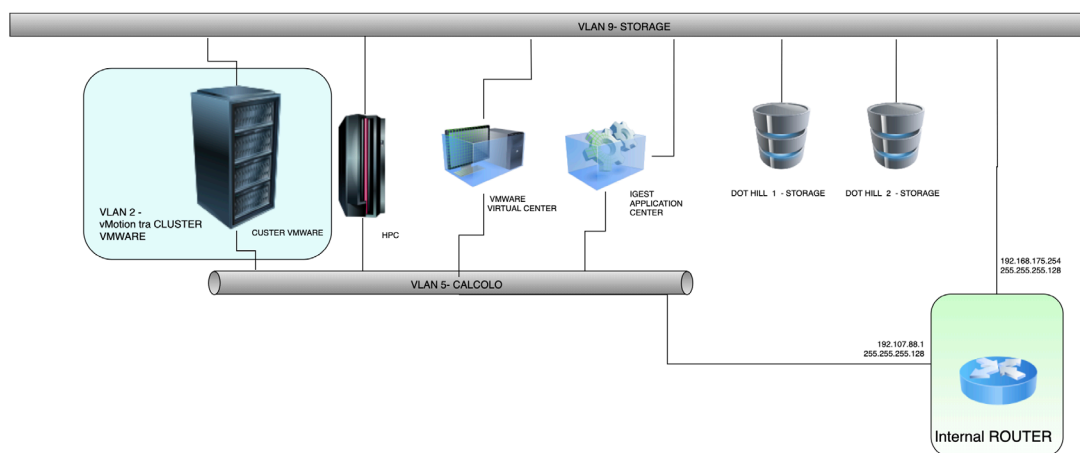
2.4.1 Vlan 1 (Apparati) – 10.0.1.254/24

La vlan 1, di default su tutti gli apparati di rete al loro primo avvio, è tutt'ora attiva sugli apparati di rete quali centro stella e NAC. Indirizzi IP della rete *10.0.1.0/254* sono presenti attualmente su tutti gli apparati di rete raggiungibili oltre che su vlan 20 anche su vlan 1. Tuttavia, si sta migrando verso una infrastruttura in cui tali apparati non saranno più raggiungibili su vlan default.

2.4.2 Vlan 4 (CODI to FW) – 10.0.2.253/24

Questa vlan è utilizzata con indirizzamento privato per il collegamento diretto tra codi4900-firewall.

2.4.3 Vlan 5 (Calcolo) - 192.107.88.1/25



2.4.4 Vlan 8 (Bypass Calcolo) – 10.7.12.54/30

Il laboratorio RETI, orientato da sempre all’ottimizzazione delle risorse e alla sicurezza delle reti, ha definito delle attività allo scopo di avere piena visibilità tra centri Enea. Le configurazioni dei router hanno al loro interno delle interfacce dedicate al “*Bypass tra le Reti di Calcolo Enea*”. *Queste interfacce* veicolano il traffico di alcune reti, in particolare le reti che generano traffico dei cluster di calcolo scientifico, facendolo bypassare dal firewall, aumentando notevolmente la velocità delle comunicazioni tra centri. Per questo traffico è utilizzata la vlan 8 su indirizzamento privato.

2.4.5 Vlan 9 (Storage) - 192.168.175.128/25

La vlan gestisce gli accessi alle interfacce iSCSI degli host ESXI Vmware e alle interfacce dei controller dei dothill.

NAME	IPV4 ADDRESS	MAC ADDRESS	ROLE
DOTHILL01	192.168.175.130	00:c0:ff:38:00:a5	Controller A Port 0
DOTHILL01	192.168.175.131	00:c0:ff:38:00:a4	Controller A Port 1
DOTHILL01	192.168.175.132	00:c0:ff:37:ff:bd	Controller B Port 0
DOTHILL01	192.168.175.133	00:c0:ff:37:ff:bc	Controller B Port 1
iSCSI_1 su VmWbri01	192.168.175.134	00:50:56:6a:e6:5e	Porta Per iSCSI_1
iSCSI_1 su VmWbri02	192.168.175.135	00:50:56:63:cf:c5	Porta Per iSCSI_1
iSCSI_2 su VmWbri01	192.168.175.136	00:50:56:61:17:f4	Porta Per iSCSI_2
iSCSI_2 su VmWbri02	192.168.175.137	00:50:56:6f:1b:d8	Porta Per iSCSI_2

Tabella 6: Indirizzamento IP Vlan Storage

Schema di realizzazione di una VLAN dedicata per lo storage

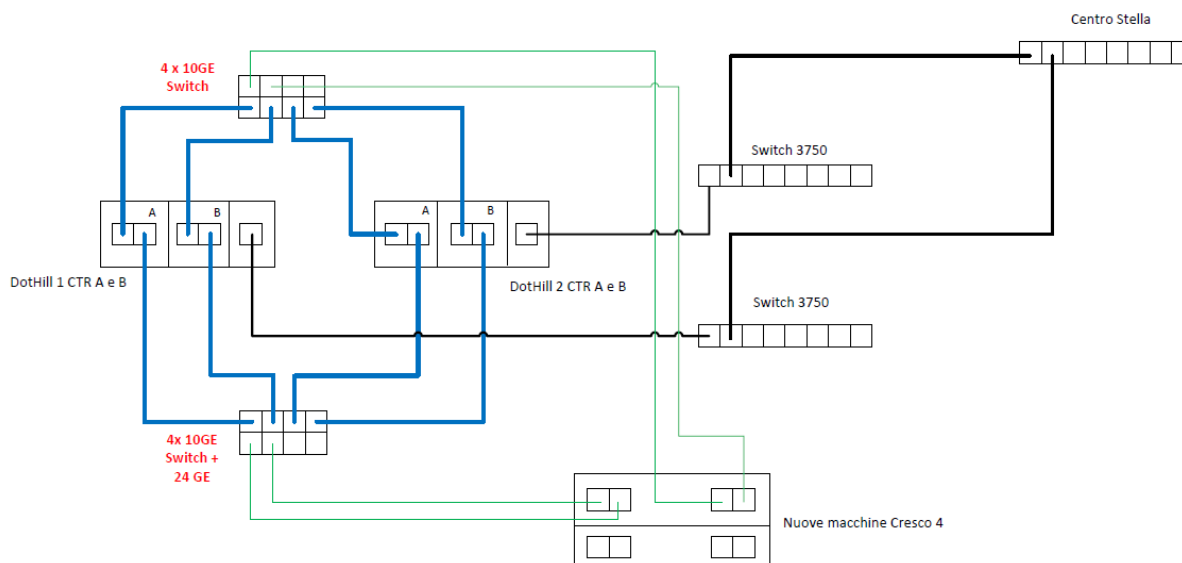


Figura 16: Schema di realizzazione Storage Network

2.4.6 Vlan 12 (Voice) - 192.168.174.0/24

La vlan 12 è utilizzata per il traffico generato dalla telefonia VoIP. Nella prima fase di test della centrale telefonica, per l'indirizzamento dei telefoni VoIP sono stati utilizzati IP dalla rete LAN. Successivamente, fin dal primo rilascio, su pochi utenti, abbiamo studiato e implementato soluzioni per il riconoscimento, la gestione e la configurazione e provisioning automatico dei telefoni VoIP, e per la separazione del traffico comune dal traffico telefonico.

- Implementazione di una vlan (voice) per la gestione del traffico telefonico.
- Il riconoscimento degli apparati che si collegano in rete, avviene mediante protocollo LLDP, presente nativamente, anche se non abilitato di default, su tutti gli switch di Brindisi e ritenuto molto performante per l'identificazione di un apparato come telefono ed istruito per assegnare la vlan dedicata (voice);
- Il riconoscimento degli apparati che non “parlano” LLDP avviene mediante l'utilizzo di un Server DHCP implementato ad hoc per la gestione dei Telefoni e degli apparati della rete VoIP con indirizzamento diverso dalla LAN, su vlan dedicata. L'implementazione si fa utilizzando il comando *match if substring* – passando come parametro una “sottostringa” del mac-address (appunto i primi tre ottetti) e verificando che sia identica alla stringa a noi nota (vedi telefoni appartenenti ai vari brand). Una volta verificata la corrispondenza, il mac-address in questione sarà catalogato come facente parte della classe “voip”.

VLAN 12 (VOICE) – Implementazione su Cisco

```
network-policy profile 12
voice vlan 12
network-policy 12
```

VLAN 12 (VOICE) – Implementazione su Huawei

```
vlan 12
description VOICE
voice-vlan 12 enable
voice-vlan legacy enable
port hybrid tagged vlan 12
```

Protocollo LLDP – Implementazione su Cisco

```
lldp run
#sh lldp neighbors
```

Device ID	Local Intf	Hold-time	Capability	Port ID
GXP2130_00:0b:82:7f:Gi1/0/10		106	B,T	000b.827f.22e9
GXP2130_00:0b:82:7f:Gi1/0/4		95	B,T	000b.827f.22fd

Protocollo LLDP – Implementazione su Huawei

```
lldp compliance cdp txrx
lldp compliance cdp receive
>display lldp local
```

System information

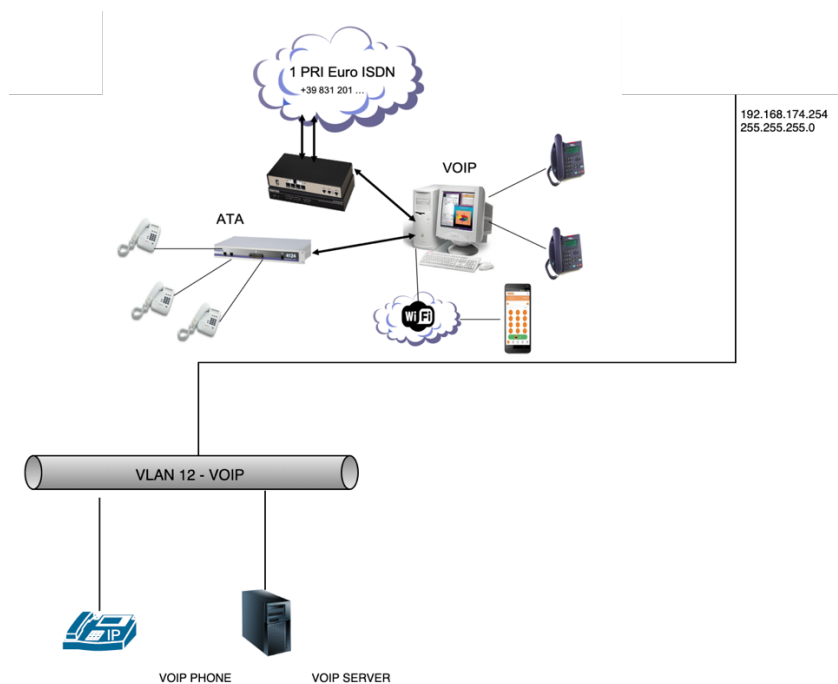
LLDP Up time :2019-03-20 17:20:43+02:00 DST

```
>display lldp neighbor brief
```

Local Intf	Neighbor Dev	Neighbor Intf	Exptime(s)
GE0/0/1	GXP2130_00:0b:82:7f:2...	000b-827f-25a6	97
GE0/0/2	GXP2130_00:0b:82:7f:2...	000b-827f-25aa	93

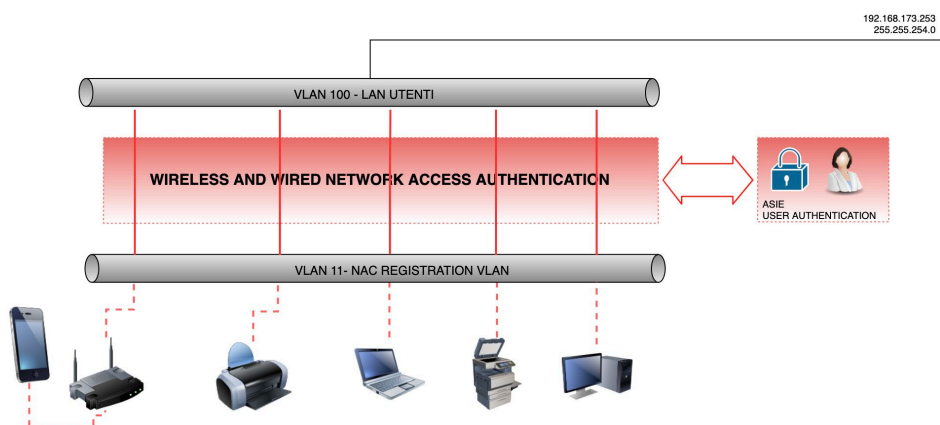
DHCP SERVER

```
subnet 192.168.174.0 netmask 255.255.255.0 {
    option subnet-mask 255.255.255.0;
    option broadcast-address 192.168.174.255;
    option routers 192.168.174.254;
    option sip-server 01:c0:a8:ae:fc;
    option tftp-server-name "192.168.174.200";
class "voip" {
    match if substring (hardware,1,3) = 00:0b:82 or
    substring (hardware,1,3) = 34:db:fd or
    substring (hardware,1,3) = 00:08:5d or
# hardware GRANDSTREAM 00:0b:82:62:da:76;
# hardware CISCO 34:db:fd:5f:fb:70;
# hardware Aastra 00:08:5d:49:dc:b7;
# hardware NOVAFON 00:90:33:03:10:c5;
```



2.4.7 Vlan 100 (Lan) – 192.168.172.0/23

La vlan 100 è utilizzata per il traffico della lan su indirizzamento 192.168.172.0/23 tramite dhcp e dopo autenticazione mediante NAC²⁶. Le politiche di sicurezza vengono implementate tramite i dispositivi di rete, gestendone la configurazione delle porte (vlan enforcement) in modo che i client non autenticati (assegnati alla vlan registration) non possano effettivamente fare nulla (dalla semplice navigazione fino a tentativi di attacco, scansioni di porte, DoS, ecc.) finché non siano stati ammessi in rete.



²⁶ Una spiegazione più approfondita è resa nel paragrafo 2.5.4

2.4.8 Vlan 110 (Bypass Lan) – 192.168.169.254/24

Le vlan bypass Lan e Bypass Voice, ed in generale, se presenti, altre vlan con nomenclatura simile, sono implementate per il NAC e per ovviare a problematiche relative all'autenticazione. In verità si tratta di vlan che intervengono quando qualcosa va storto e per un motivo qualsiasi l'autenticazione non avviene perché la macchina dell'utente è senza protocollo 802.1X, non riesce a fare login sul captive portal, non riesce a contattare il Radius Server, ecc., in generale non riesce a terminare il processo di AAA.

2.4.9 Vlan 112 (Bypass Vlan Voice) – 10.0.8.254/24

Come Vlan 110 (Bypass Lan) – 192.168.169.254/24

2.4.10 Vlan 150 (VXLAN test)

La vlan 150 è utilizzata per le vxlan.

2.1 Interfacce terminate su Packet Fence

2.1.1 Vlan 10 (Isolation) – 10.0.6.0/24

La vlan isolation è pensata per ospitare tutte quelle macchine (host) che per un qualsiasi motivo sono state ritenute, dai meccanismi di discovery della rete, insicure, non aggiornate, deprecate o altro e per tali motivi non riscono a fare AAA. Queste macchine sono per l'appunto isolate dal resto della lan in attesa di essere verificate.

2.1.2 Vlan 11 (Registration) – 10.0.5.0/24

Usata per il NAC (Network Access Control) mediante il l'implementazione di Packet Fence. Il Nac è un approccio alla sicurezza informatica che tenta di unificare la tecnologia di sicurezza degli endpoint (come antivirus, prevenzione delle intrusioni dei computer e valutazione delle vulnerabilità), all'autenticazione dell'utente o del sistema e il rafforzamento della sicurezza di rete

Il processo di autenticazione avviene nel seguente modo:

- Un client sconosciuto viene associato alla vlan di Registration, PacketFence (DHCP) assegna un indirizzo IP e come DNS il suo indirizzo.
- Se sul client è attiva l'autenticazione 802.1x parte il processo di autenticazione (FreeRADIUS) al termine della quale il PacketFence restituisce allo switch la vlan da assegnare.
- In assenza di un supplicant 802.1x sul client, lo switch, scaduto un timeout, termina l'invio di pacchetti 802.1x ed effettua un fallback all'autenticazione MAC (Stampanti e Telefono VoIP).

- Tutti i client, se non ancora autenticati, vengono reindirizzati verso il Captive Portal per l'autenticazione.
- Utenti di dominio ASIE²⁷ : integrazione con l'Active Directory ENEAIT²⁸

2.1.3 Vlan 13 (guest)

La vlan guest è pensata per ospitare tutte quelle macchine che per un qualsiasi motivo non riescono a fare AAA²⁹. Vi sono determinate condizioni per cui un utente, in fase di autenticazione, non riesce a terminare il meccanismo di autenticazione. Queste macchine potrebbero essere utenti noti o non abilitati all'autenticazione ma comunque utenti validi da trattare con cautela ma senza in qualche modo inibirne il collegamento come accade per la vlan isolation. Questa vlan, al contrario della vlan isolation, ha una azione più moderata.

2.1.4 Vlan 210 (isolation_pf_cluster)

Le vlan 210 e 211 rappresentano le versioni per il NAC, ma implementato su Packet Fence in modalità Cluster.

2.1.5 Vlan 211 (registration_pf_cluster)

Come Vlan 210 (isolation_pf_cluster).

²⁷ ASIE, Accesso Servizi Informatici ENEA, è il sistema di autenticazione per accedere alle risorse e ai servizi sviluppati e resi disponibili da ICT. Per utilizzare ASIE è necessario disporre di una Username e di una Password, indicate come "credenziali ASIE". Di norma lo username ASIE corrisponde al proprio nome e cognome nella seguente forma: nome.cognome

²⁸ Per l'autenticazione degli utenti sarà necessario utilizzare le proprie credenziali ASIE nel formato più generico possibile: ENEAIT\nome.cognome

²⁹ authentication event fail action authorize vlan 13. Per i dettagli vedere ad esempio la configurazione del Cisco WS-C2960, WS-C3750

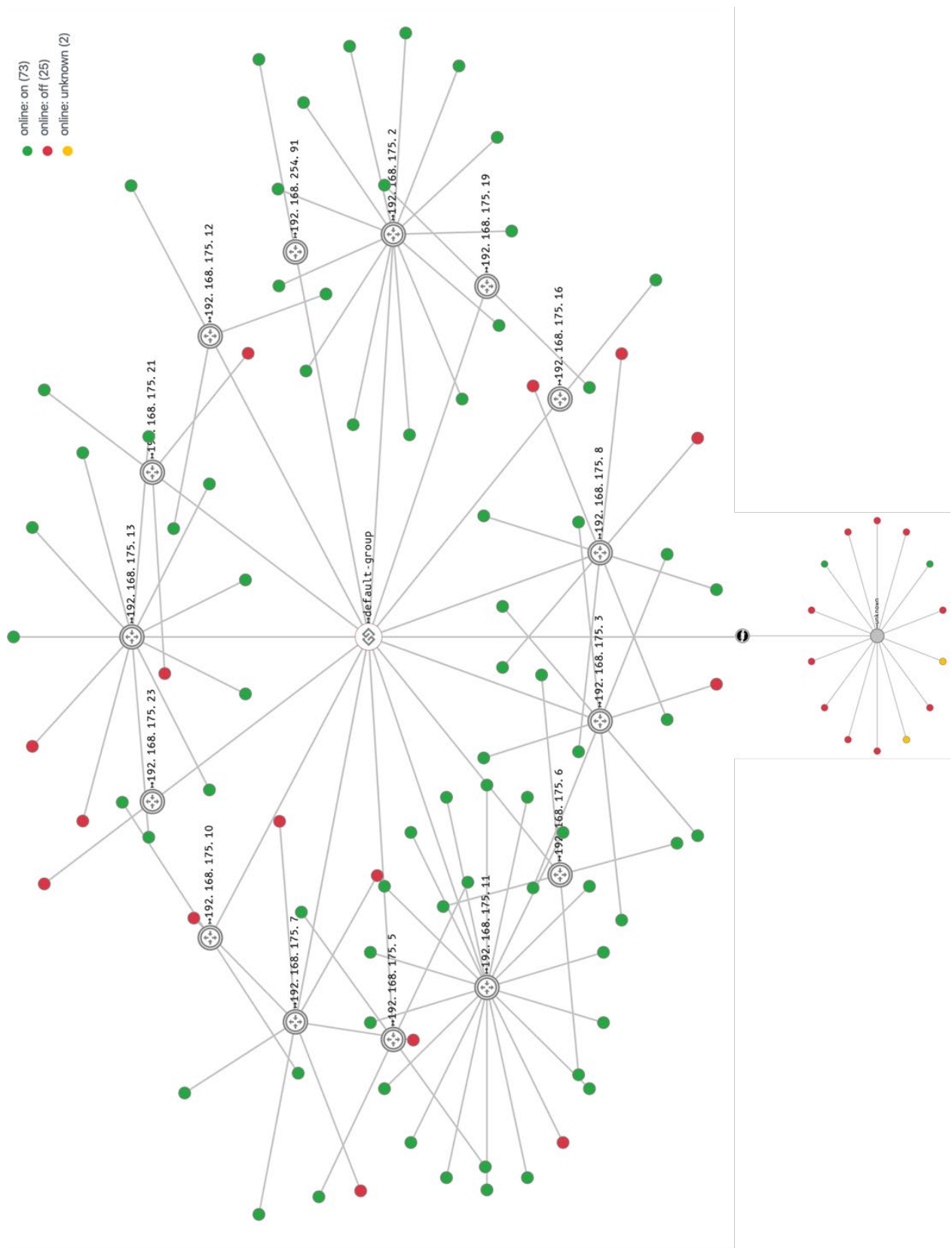


Figure 17: Packet Fence Network view

2.2 Interfacce interne

2.2.1 Vlan 2 (vMotion VmWare) – 10.0.3.0/24

Il vMotion è una tecnologia fondamentale e consente la migrazione live delle macchine virtuali in produzione, da un server fisico a un altro con tempi di inattività pari a zero, disponibilità continua del servizio e completa integrità della transazione. Alcuni dei vantaggi del vMotion sono:

- l'ottimizzazione e allocazione automaticamente di interi pool di risorse per un utilizzo ottimale dell'hardware con conseguente flessibilità e disponibilità delle risorse stesse;
- la manutenzione automatica dell'hardware senza tempi di inattività programmati;
- la migrazione proattiva delle macchine virtuali da server con errori o prestazioni insufficienti.

Le migrazioni vMotion utilizzano una **rete dedicata** per trasferire lo stato della macchina virtuale tra gli host di origine e quelli di destinazione. È necessario configurare tale rete per ciascun host che verrà utilizzato per le migrazioni. Inoltre, la migrazione in real-time di una macchina virtuale da un server fisico ad un altro, è possibile grazie a tre tecnologie sottostanti:

- Lo stato di una macchina virtuale è contenuto in un set di file archiviati su un archivio condiviso come Fibre Channel, iSCSI, Storage Area Network (SAN) o Network Attached Storage (NAS). Il VMFS (Virtual Machine File System) del cluster VMware permette quindi a più installazioni di ESXI Server di accedere ai file della stessa Virtual Machine contemporaneamente.
- La memoria attiva e lo stato di esecuzione della macchina virtuale vengono rapidamente trasferiti su una rete ad alta velocità, consentendo alla macchina virtuale di passare istantaneamente dallo stato di esecuzione sul server ESXI di origine allo stato di esecuzione sul server ESXI di destinazione. Per l'utente il periodo di trasferimento è impercettibile poiché vMotion tiene traccia delle transazioni in corso in memoria. Una volta che l'intera memoria e lo stato del sistema sono stati copiati nel Server di destinazione, vMotion sospende la macchina virtuale di origine, copia eventuali variazioni sul server ESXI di destinazione e ripristina il virtuale macchina sul server ESXI di destinazione. L'intero processo richiede meno di due secondi su una rete Gigabit Ethernet.
- Le reti utilizzate dalla macchina virtuale sono anch'esse virtualizzate e questo garantisce che anche dopo la migrazione, la configurazione e lo stato della rete della macchina virtuale vengano conservate.

Per il centro di Brindisi è stata implementata una vlan dedicata con rispettivo indirizzamento IP.

Connectee	MAC Address	Port Group	State	VLAN ID
vmwbri3.brindisi.enea.it - vmk3	00:50:56:6a:ad:36	VMotion	Link Up	VLAN access: 2
vmwbri1.brindisi.enea.it - vmk3	00:50:56:65:db:a7	VMotion	Link Up	VLAN access: 2
vmwbri2.brindisi.enea.it - vmk3	00:50:56:65:90:5d	VMotion	Link Up	VLAN access: 2
servizi3.brindisi.enea.it - vmk3	00:50:56:6e:92:00	VMotion	Link Up	VLAN access: 2
servizi6.brindisi.enea.it - vmk3	00:50:56:62:8b:6b	VMotion	Link Up	VLAN access: 2
servizi7.brindisi.enea.it - vmk3	00:50:56:60:12:6f	VMotion	Link Up	VLAN access: 2
servizi8.brindisi.enea.it - vmk3	00:50:56:6b:1c:ac	VMotion	Link Up	VLAN access: 2
servizi9.brindisi.enea.it - vmk3	00:50:56:65:5a:1c	VMotion	Link Up	VLAN access: 2

Tabella 7: Indirizzamento IP Vlan vMotion VmWare

2.2.2 Vlan 7 (gpfs calcolo) – 10.50.1.0/24

La vlan 7 è utilizzata per il traffico gpfs calcolo.

2.3 Evoluzioni future

La rete è in continua evoluzione e al momento della pubblicazione del presente documento sono allo studio possibili cambiamenti e migliorie nell'ottica di una ristrutturazione della rete, con lo scopo di conferire sempre maggiore sicurezza e robustezza. In particolare si pensa di spostare la vlan 12 – VOICE, dedicata al traffico VoIP, in una area della rete meno vulnerabile, ovvero terminarla sul firewall anziché sul centro stella. Questa scelta è dettata dalla alta attenzione che si deve al traffico proveniente da questa vlan. Altre evoluzioni saranno trattate in un prossimo documento.

Parco Macchine

1 Infrastruttura Fisica

L'infrastruttura fisica conta di pochissimi Server per la distribuzione di servizi dal momento che quasi tutti i servizi e applicazioni sono migrati e distribuiti dall'infrastruttura virtuale mediante Virtual Machines.

Server e Workstation – Vi sono presenti ancora invece diversi server dislocati per tutto il centro al servizio dei vari laboratori di ricerca, perlopiù workstation con applicativi proprietari a corredo della strumentazione, server di grosse dimensioni con hardware specializzato ecc. Il centro presenta molti laboratori per la preparazione e trattamento di materiali e per la caratterizzazione macroscopica, microstrutturale e microanalitica di materiali, con annessa strumentazione per misure termomeccaniche e termoanalitiche, spettrometri e microscopi, e molto spesso workstation grafiche e di vario utilizzo e supporto alla strumentazione. Alcuni esempi:

- Laboratorio Caratterizzazione Materiali da Recupero utilizza una Workstation grafica Dell Precision 3620, equipaggiato con processore Xeon® E3-1200 a 8 core e 64 GB di RAM, scheda grafica 3D midrange AMD Firepro W5100 e archiviazione mediante due dischi da 1 TeraByte;
- Laboratorio Prove Meccaniche utilizza una Workstation corredata da software per macchine di trazione, del microscopio;
- Laboratorio Test Sensori utilizza un Server Dell PowerEdge R320, equipaggiato con processore Intel Xeon® a 6 core e 16 Gigabyte di memoria RAM. Per l'archiviazione dei dati vengono utilizzati 6 dischi da 500 GB in configurazione raid5, mentre il sistema operativo Debian GNU Linux gira su due dischi sempre da 500 GB in mirror;
- In sala Archita è presente una Workstation Grafica a servizio dei Laboratori DTE-ICT con sistema operativo Ubuntu Server e Windows Server, ambiente di sviluppo CUDA con 2880 Core della GPU Nvidia Quadro k6000.

Appliance Fisiche – L'infrastruttura fisiche conta oltre che di Server anche di tutta una serie di appliance fisiche, che difficilmente possono essere virtualizzate. Escludendo per ovvie ragioni tutti gli apparati che possono considerarsi di “rete”, già descritti in precedenza, e/o apparati afferenti alla centrale telefonica, quali Gateway VoIP e ATA, non rimangono che due appliance fisiche presenti, ovvero il Firewall perimetrale ed i Controller Wi-Fi centralizzati di cui vedremo il funzionamento nelle sezioni dedicate.

Nodi di Calcolo – Sono presenti Server Fisici utilizzati per l'installazione di nodi di calcolo CRESCO (224 nodi di calcolo su Portici per 5.376 cores, 10 nodi su Brindisi per 240 cores), oltre che

l'installazione di storage e l'installazione di sistemi front end e visualizzazione 3D a supporto dei nodi di calcolo.

Server Esxi – L'infrastruttura fisica più corposa riguarda il parco macchine Server su cui è installata la distribuzione VMware ESXi per la virtualizzazione e implementazione del Cloud per la distribuzione de servizi. Il parco macchine, che ospita l'infrastruttura virtuale è composta dalle seguenti macchine:

Q.tà	Modello	Processori Logici	RAM	Nome Host	Laboratorio
1	Dell Poweredge R620	32	64	Servizi[03]	ISER
1	IBM3850	16	64	Servizi[02]	RETE
3	IBM3850	16	64	Vmwabri[01...03]	IGEST
5	Intel-S7000FC4UR	16	64	Servizi[1...5]	RETE
4	Supermicro_6028TR-HTR	32	64	Servizi[6...9]	RETE

Tabella 8: Parco macchine servizi Brindisi

2 Infrastruttura Virtuale

Il centro ENEA di Brindisi, ha una infrastruttura Virtuale basata su VMware® vSphere®. Un Virtual Center Server può contenere più Datacenter. Le grandi aziende organizzate per unità, dipartimenti e/o dislocate su un vasto territorio, utilizzano più datacenter per rappresentare le unità organizzative. Esso offre una piattaforma centralizzata per la gestione degli ambienti VMware vSphere, consentendo di automatizzare e distribuire un'infrastruttura virtuale in tutta sicurezza. I servizi di Rete sono erogati essenzialmente da due vCenter importanti, il primo a cui è annesso il centro di Brindisi, insieme a quello di Frascati, Sede e Bologna, il secondo che annette ad esso i centri di Casaccia, Portici, Trisaia e Palermo. Il Datacenter Brindisi ha ad oggi:

- **5 Cluster** – Un cluster è un gruppo di host che condivide le risorse e un'interfaccia di gestione. Quando si aggiunge un host ad un cluster, le risorse dell'host diventano parte delle risorse del cluster. Il cluster gestisce le risorse di tutti gli host al suo interno. Avere gli host organizzati per cluster garantisce soluzioni come il vSphere Distributed Resource Scheduler (DRS) che bilancia continuamente i carichi di lavoro delle macchine virtuali sugli host e vSphere High Availability (HA) che consente alle macchine virtuali in esecuzione di ripristinare automaticamente gli errori dell'host.
- **13 Host di cui 12 in HA** – Un host è un computer che utilizza il software di virtualizzazione per eseguire macchine virtuali. Gli host forniscono la CPU e le risorse di memoria utilizzate dalle VM e consentono loro di accedere a storage e reti. L'aggiunta di un host al vCenter Server ci consente di gestirlo e di gestire tutte le VM sono eseguite su di esso.

- **Oltre 100 Virtual Machine** – Una Virtual Machine è una istanza di tipo software di un computer fisico. In altre parole così come un computer fisico, una VM esegue un sistema operativo e delle applicazioni, ha un sistema operativo installato, ha dispositivi virtuali che forniscono le stesse funzionalità dell'hardware fisico e dunque un quantitativo di CPU e memoria, schede video, accesso allo storage e connettività di rete.
- **Più di 15 Datastore** – Un datastore è un contenitore logico che contiene i file della macchina virtuale e altri file necessari per le operazioni della macchina virtuale. Esistono diversi tipi di storage fisico tra i quali, lo storage locale – solitamente non utilizzato – iSCSI, Fibre Channel NFS ecc
- **Oltre 20 Networks** – In vsphere la rete viene gestita utilizzando due tipologie di oggetto:
 - vSphere Standard switch che gestiscono le VM a livello di host e funzionano come dei semplici switch fisici, ovvero rilevando quali macchine virtuali sono connesse a ciascuna delle sue porte virtuali e utilizzando tali informazioni per inoltrare il traffico alle macchine virtuali corrette. Uno o più gruppi di porte si connettono a uno Standard Switch e specificano le opzioni di configurazione delle porte come larghezza di banda e tagging VLAN per ciascuna porta membro. Ciascun NIC della macchina virtuale può essere assegnato a un gruppo di porte.
 - vSphere Distributed Switch che gestiscono la VM a livello di data center. Un Distributed Switch funge da switch virtuale su tutti gli host associati e consente alle macchine virtuali di mantenere una configurazione di rete coerente durante la migrazione tra gli host. Un Distributed Switch può instradare il traffico internamente tra macchine virtuali o collegarsi a una rete esterna. A un Distributed Switch vSphere possono essere assegnati più gruppi di porte distribuite.

Il vCenter FraBol nella sua totalità ospita 4 Datacenter con 40 Host e più di 350 Virtual Machine ed è equipaggiato con hardware con capacità totali di CPU di 1 THz, memoria di 3 TB e storage di 170 TB.

2.1 Networking in vSphere

La gestione della rete in una infrastruttura virtuale gioca un ruolo fondamentale tanto quanto quella che si fa in una infrastruttura fisica. Non di meno, le due infrastrutture, devono avere le stesse caratteristiche e peculiarità, fondamentali per una gestione ottimale della rete. Appare dunque logico e sensato che se in una rete fisica si utilizzano alcune vlan, le stesse dovranno essere pubblicate sull'infrastruttura

virtuale. Tuttavia, come abbiamo appena letto, ci sono più modalità di gestione della rete in vsphere, ed in particolare di gestione degli oggetti noti come virtual switch.

Abbiamo visto che ci sono due tipologie di oggetto ma essi possono essere utilizzati in tre diverse modalità operative.

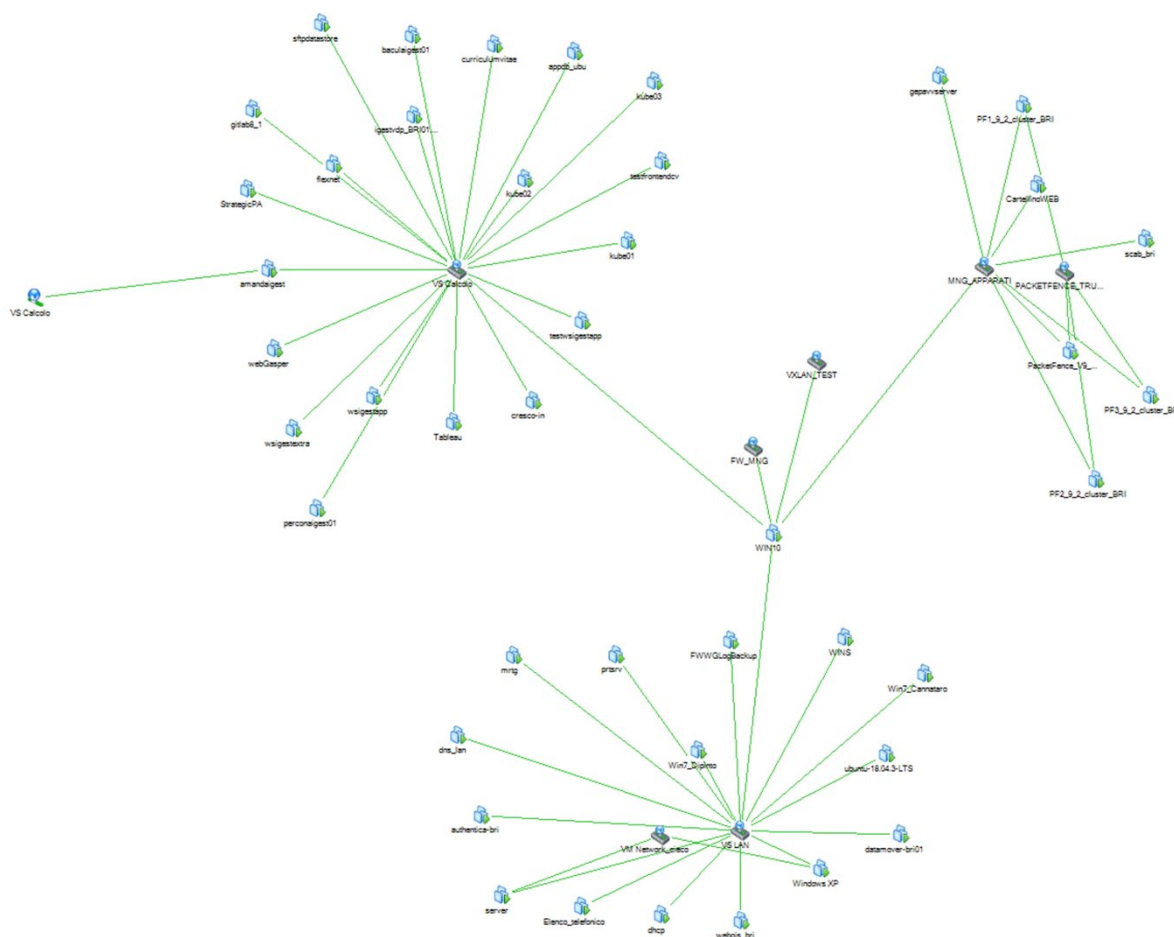


Figura 18: VM to Network (Datacenter di Brindisi)

2.1.1 vSphere Standard Switch

vSphere Standard Switch senza ausilio di VLAN – In questo caso, viene creato un oggetto di tipo standard Switch che non ha nessuna specializzazione e nessun tagging vlan. Lo switch in questione non essendo taggato è in trunk e fa passare tutto il traffico e rimane compito dello switch a valle della porta o gruppo di porte a cui lo standard switch è associato, taggare il traffico e assegnare eventuali VLAN. Questa modalità operativa è meno consigliata ma ben si presta se la macchina fisica sulla quale è installata l'istanza di vMware Esxi, risulta fornita di numerose porte ethernet, maggiori in numero delle VLAN presenti nella rete, ognuna delle quali può essere specializzata su una specifica vlan. Lo svantaggio vero di questa modalità è la gestione onerosa dal punto di vista sistemistico e che impone al

gestore della rete un lavoro manualmente sugli switch fisici e l'onere di dover tenere traccia puntuale delle varie configurazioni sulle porte degli switch.

Name	Type	Network Protocol Profile	VM Count	Host Count	VC
VM Network	Standard network		1	10	FraBol

Tabella 9: vSphere Standard Switch

vSphere Standard Switch con ausilio di VLAN – In questo caso, vengono creati molteplici oggetti di tipo standard Switch che sono specializzati, ovvero sono tagged su una specifica VLAN. Si possono vari switch virtuali, ognuno dei quali sarà specializzato su una VLAN. Rimane compito dello switch a valle della porta o gruppo di porte a cui lo standard switch è associato, non taggare il traffico ed essere configurata come porta trunk. Questa modalità operativa è molto utilizzata e consigliata, in particolar modo a chi si affaccia all'utilizzo di infrastruttura virtuali da poco tempo. Il vantaggio vero di questa modalità è la gestione molto poco onerosa dal punto di vista della configurazione degli apparati, che, di fatto, possono essere configurati in modo tale da avere tutte le porte trunk. Sarà compito degli Standard Switch veicolare il traffico nelle vlan specifiche.

Name	Type	Network Protocol Profile	VM Count	Host Count	VC
VM Network	Standard network		1	10	FraBol
CIECO	Standard network		0	3	FraBol
VS CALCOLO	Standard network		2	0	FraBol
VS DMZ	Standard network		1	0	FraBol

Tabella 10: vSphere Standard Switch tagged

2.1.2 vSphere Distributed Switch

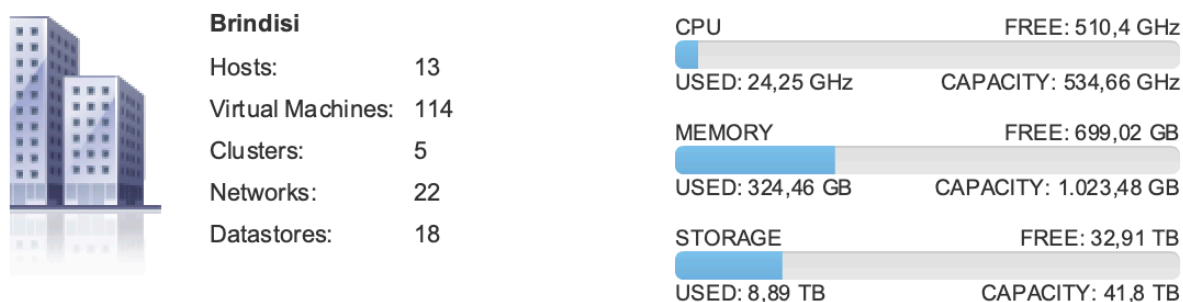
vSphere Distributed Switch – In questo caso, viene creato un oggetto di tipo distributed Switch che conterrà al suo interno una serie di **Distributed Port Group** ovvero un gruppo di porte associato a un Distributed Switch ognuno dei quali specifica le opzioni di configurazione delle porte, in particolar modo la VLAN associata. Esisterà un Distributed Port Group per ogni standard Switch che vogliamo specializzare, che sia tagged su una specifica VLAN. All'interno dell'oggetto appena creato sarà contenuto anche un oggetto di tipo **Uplink Port Group** ovvero un gruppo di porte associate a uno Distributed Switch. Questa modalità operativa è ampiamente utilizzata e consigliata, in particolar modo dagli utilizzatori più esperti. I vSphere Distributed Switch gestiscono la Virtual Machine a livello di datacenter e non solo di host. Questo significa che all'aggiunta di un nuovo host in un datacenter non sarà necessario aggiungere e configurare switch locali. Un Distributed Switch funge da switch virtuale

su tutti gli host associati e consente alle macchine virtuali di mantenere una configurazione di rete coerente durante la migrazione tra gli host. L'implementazione degli Switch Distribuiti rispetto agli Switch Standard introduce inoltre una serie di innumerevoli vantaggi tra i quali i più significativi:

- **Gestione centralizzata dal vCenter** – gestione più semplice, veloce e sicura perché non ho bisogno di ricreare gli stessi Switch Standard su tutti i nodi del Cluster, con relativa riduzione degli errori di configurazione;
- **Gestione del traffico** – Inbound e Outbound traffic shaping, VM Port Blocking, VLAN e Private VLAN, Traffic Filtering
- **Network vMotion** – consente la migrazione live delle macchine virtuali in produzione, da un server fisico a un altro con tempi di inattività pari a zero, disponibilità continua del servizio e completa integrità della transazione. Il vMotion è una tecnologia fondamentale per la creazione di un data center dinamico e automatizzato. Le migrazioni vMotion utilizzano una rete dedicata per trasferire lo stato della macchina virtuale tra gli host di origine e quelli di destinazione. È necessario configurare tale rete per ciascun host che verrà utilizzato per le migrazioni di vMotion. Per ulteriori dettagli vedi paragrafo 2.5.1
- Cisco Discovery Protocol (CDP) e Link Layer Discovery Protocol (LLDP)

Name	Type	VM Count	Host Count	VC
cieco_vlan_trunk	Distributed port group	2	13	FRABOL
dvSwitch_BRI_Int-DVUplinks	Uplink port group	0	13	FRABOL
FW-TO-ROUTER	Distributed port group	1	13	FRABOL
FW_MNG	Distributed port group	1	13	FRABOL
iSCSI_1	Distributed port group	0	13	FRABOL
iSCSI_2	Distributed port group	0	13	FRABOL
Management_Interf_Vlan_3	Distributed port group	0	13	FRABOL
Management_Interf_Vlan_5	Distributed port group	0	13	FRABOL
MNG_APPARATI	Distributed port group	17	13	FRABOL
PACKETFENCE_TRUNK_VLAN	Distributed port group	10	13	FRABOL
PACKETFENCE_VLAN_1	Distributed port group	1	13	FRABOL
VLAN_VOICE	Distributed port group	6	13	FRABOL
CIECO	Distributed port group	16	13	FRABOL
VMotion	Distributed port group	0	13	FRABOL
VS Calcolo	Distributed port group	40	13	FRABOL
VS DMZ	Distributed port group	20	13	FRABOL
VS LAN	Distributed port group	33	13	FRABOL
VXLAN_TEST	Distributed port group	1	13	FRABOL

Tabella 11: vSphere Distributed Switch



Conclusioni

La realizzazione di una infrastruttura tecnologicamente avanzata e innovativa e la virtualizzazione dei servizi e delle macchine permette ai gestori dei servizi erogati di concentrarsi sugli aspetti di gestione e implementazione dei servizi e sulla ricerca di soluzioni innovative e ancora sulla standardizzazione dei servizi, sulla automatizzazione delle operazioni sistemiche e così di tralasciare altri aspetti più di basso livello legati alle macchine fisiche e ai guasti che essi si portano inesorabilmente dietro.

La gestione di una infrastruttura Cloud è indubbiamente più interessante e appagante, la ricerca di soluzioni tecnologiche e innovative per la gestione e remotizzazione dei servizi legati al mondo della ricerca, della pubblica amministrazione, delle aziende è di grande attualità. Sempre più aziende e pubbliche amministrazioni realizzano progetti di telelavoro, co-working, collaborazioni tra diversi paesi, servendosi di reti ad alta efficienza e servizi di cloud computing.

Sitografia

<https://www.vmware.com>

<https://www.garr.it>

<https://www.enea.it>

<https://www.cisco.com>

Indice delle Figure

Figura 1: Schema di rete del cablaggio strutturato	10
Figura 2: Stralcio della planimetria generale Cittadella della Ricerca con riferimento agli spazi ENEA	11
Figura 3: Planimetria Edificio A2 PT Blocco 4	12
Figura 4: Distribuzione delle postazioni di lavoro doppie cat. 6° all'interno del Campus.....	13
Figura 5: Planimetria Edificio a2_PT Blocco 4	14
Figura 6: Planimetria Edificio 6_P1.....	15
Figura 7: Schema fisico, apparati attivi 2004	16
Figura 8: Schema fisico, apparati attivi 2012	18
Figura 9: Schema fisico, apparati attivi 2018	19
Figura 10: Schema fisico, apparati attivi 2020	20
Figura 11: Schema fisico di rete ridotto	21
Figura 13: GARR Weathermap: GARRX, Backbone	23
Figura 15: Creazione di una regola (policy) sul firewall.....	43
Figura 14: Statistiche di utilizzo di banda	44
Figura 16: Network Logical Diagram	46
Figura 17: Schema di realizzazione Storage Network	56
Figura 19: Packet Fence Network view	61
Figura 20: VM to Network (Datacenter di Brindisi).....	67

Indice delle Tabelle

Tabella 1: Cablaggio strutturato: tabella riassuntiva	9
Tabella 2: Cablaggio strutturato: distribuzione.....	10
Tabella 3: Indirizzamento IP Privati	48
Tabella 4: Indirizzamento IP Pubblici	48
Tabella 5: Lista completa delle Vlan definite	51
Tabella 6: Indirizzamento IP Vlan Storage.....	55
Tabella 7: Indirizzamento IP Vlan vMotion VmWare	63
Tabella 8: Parco macchine servizi Brindisi.....	65
Tabella 9: vSphere Standard Switch	68
Tabella 10: vSphere Standard Switch tagged	68
Tabella 11: vSphere Distributed Switch	70
Tabella 12: Lista Componenti Rete LAN (Passiva) – Realizzazione 2004.....	73
Tabella 13: Lista Componenti Rete LAN (Passiva) – Ampliamento 2012	74
Tabella 14: Lista Componenti Rete LAN (Passiva) – Ampliamento 2013	74
Tabella 15: Lista Componenti Rete LAN (Attiva) – Realizzazione 2018.....	75
Tabella 16: Lista Componenti Rete LAN (Attiva) – Realizzazione 2019.....	76
Tabella 17: Lista Componenti Rete LAN (Attiva) – Realizzazione 2020.....	76

Appendice

Lista Componenti	Q.tà
Descrizione	
CONSIP - Apparat UPS - UPS	
1000 VA	7
3000 VA	1
CONSIP - Attrezzaggi	
Canalizzazioni sospese, secondo le specifiche di cui al paragrafo 5.1.1 di dimensioni 200x75	700
Canalizzazioni di raccordo a battiscopa secondo le specifiche di cui al paragrafo 5.1.2	2500
CONSIP - Cablaggio Strutturato - Armadi a Rack	
Basetta di messa a terra	9
Ripiano fisso	9
Armadio rack 19" da 42U, profondo 800 mm, completo di telaio 19"	7
Gruppo di ventilazione a tetto	9

Armadio rack 19" da 42U, profondo 600 mm, completo di telaio 19"	2
Canalina di alimentazione ed interruttore magnetotermico con 6 prese schuko	9
CONSIP - Cablaggio Strutturato - Attestazioni	
Attestazione di cavi a 4 coppie ad una estremità	1008
PIGTAIL SC/UPC SIMPLEX, CERAMIC, FIBRAOTTICA MONOMODALE, 0.9 MM, COLORE BLU	140
CONSIP - Cablaggio Strutturato - Cavi in rame	
Cavo UTP cat 6, 1000hm, rivestito con guaina esterna LSZH	25315
Cavo telefonico 50 coppie in cat 3, guaina esterna LSZF	1120
Cavo telefonico 100 coppie in cat 3, guaina esterna LSZF	160
CONSIP - Cablaggio Strutturato - Fibre Ottiche	
Cavo a 8 fibre ottiche monomodali 9/125 micron, protezione anti roditore dielettrica e guaina LSZH	1610
CONSIP - Cablaggio Strutturato - Patch Cord	
Patch cord 1xIDC-1xRJ45, a due coppie, 1000hm, lunga mt 1,5 o mt 3, telefonica	20
Patch cord 1xIDC-1xIDC, ad una coppia, 1000hm, lungi mt 1,5 o mt 3, telefonica di dorsale	292
Patch cord 1xIDC-1xRJ45, ad una coppia, 1000hm, lungo mt 1,5 o mt 3, telefonica	232
CORDONE DI PERMUTA UTP KM8 CAT.6LSZH RJ45-RJ45 (L.=2,0)	280
CORDONE DI PERMUTA UTP KM8 CAT.6LSZH RJ45-RJ45 (L.=3,0 MT.)	280
CONSIP - Cablaggio Strutturato - Patch panel e accessori	
Guida patch orizzontale altezza 1U	32
Patch panel per l'attestazione 24 f.o. su connettore sc monomodale di tipo precaricato	11
Patch panel altezza 1 U equipaggiato con 24 porte RJ45 non schermati di cat 6	23
CONSIP - Cablaggio Strutturato - Prese	
Piastrine predisposte per l'installazione su scatole tipo UNI503 da esterno	252
Piastrine predisposte per l'installazione su scatole tipo UNI503 da esterno	1

Tabella 12: Lista Componenti Rete LAN (Passiva) – Realizzazione 2004

Descrizione Articolo Convenzione	Q.tà
Fornitura Patch panel altezza 1 U non schermato, di tipo precaricato, equipaggiato con 24 porte RJ45 di cat. 6A, per cavi UTP cat. 6A	17
Installazione Patch panel altezza 1 U non schermato, di tipo precaricato, equipaggiato con 24 porte RJ45 di cat. 6A, per cavi UTP cat. 6A	17
Fornitura in opera Patch cord UTP RJ45, cat.6 da mt 1, 1000hm, rivestito con guaina esterna LSZH	177
Fornitura in opera Patch cord UTP RJ45, cat.6 da mt 2, 1000hm, rivestito con guaina esterna LSZH	177
Fornitura in opera Patch cord UTP RJ45, cat.6 da mt 3, 1000hm, rivestito con guaina esterna LSZH	354
Fornitura Cavo UTP cat.6A, 1000hm, rivestito con guaina esterna LSZH	21000
Installazione Cavo UTP cat.6A, 1000hm, rivestito con guaina esterna LSZH	21000
Lavori di rimozione delle parti passive - 1% del totale della sola fornitura di parti passive	1

Fornitura in opera Connettore fibra ottica SC 9/125 micron	8
Installazione Pigtail in fibra ottica, SC, single-mode, 1 metro	8
Fornitura Piastrina per scatole tipo UNI503 da esterno, da incasso o su facciata di torretta a pavimento complete di modulo con 2 connettori RJ45 di cat. 6A UTP, cornice, cestello e scatole	177
Installazione Piastrina per scatole tipo UNI503 da esterno, da incasso o su facciata di torretta a pavimento complete di modulo con 2 connettori RJ45 di cat. 6A UTP, cornice, cestello e scatole	177
Lavori di realizzazione di opere civili accessorie alla fornitura - Materiali	1
Lavori di realizzazione di opere civili accessorie alla fornitura - Servizi	1
Fornitura in opera Guida patch orizzontale altezza 1U	17

Tabella 13: Lista Componenti Rete LAN (Passiva) – Ampliamento 2012

Q.tà	Marca	DESCRIZIONE
10	Alcatel-Lucent	OmniAccess AP68 wireless access point 10/100/1000Base-T (RJ-45)
10	Alcatel-Lucent	1 Port 802.3af PoE Midspan 10/100/1000 15.4W.
10	Alcatel-Lucent	Power Cord for ITALY, 220VAC, 10A, 2.5M, black

Tabella 14: Lista Componenti Rete LAN (Passiva) – Ampliamento 2013

Q.tà	Codice	DESCRIZIONE
		CENTRO STELLA DI CAMPUS: 12 Gbit in monomodale 60 utenze 100/1000 rame
1	7C107	Matrix N7 Chassis
2	6C207-3	Matrix E7 and Matrix N7 1600 Watt AC Power Supply
1	7G4202-60	Distributed Forwarding Engine (Platinum) with 60 10/100/1000Base-TX ports via RJ45
1	7G4270-12	Distributed Forwarding Engine (Platinum) with 12 1000Base-X ports via mini-GBIC
12	MGBIC-LC09	1000Base-LX Mini GBIC w/LC connector
		EDIFICIO A2 p.t. - 3/4 blocco: stack da 4 V2 con uplink verso CED fino 96 utenze
4	V2H124-24	Matrix V2 with 24 10/100Base-TX ports via RJ45 and 2 expansion slots
4	V2STACK	Matrix V2 Stacking Module with required stacking cables
1	V2G112-2	Matrix V2 Uplink Module with 1 10/100/1000Base-TX "Combo" port via RJ-45 or mini-GBIC
1	MGBIC-LC09	1000Base-LX Mini GBIC w/LC connector
		EDIFICIO A2 p.t. - 1 blocco: stack da 2 V2 con uplink verso CED e fino a 48 utenze
2	V2H124-24	Matrix V2 with 24 10/100Base-TX ports via RJ45 and 2 expansion slots
2	V2STACK	Matrix V2 Stacking Module with required stacking cables
1	V2G112-2	Matrix V2 Uplink Module with 1 10/100/1000Base-TX "Combo" port via RJ-45 or mini-GBIC
1	MGBIC-LC09	1000Base-LX Mini GBIC w/LC connector
		EDIFICIO A2 p.1 - 4 blocco: stack da 2 V2 con uplink verso CED e fino a 48 utenze

2	V2H124-24	Matrix V2 with 24 10/100Base-TX ports via RJ45 and 2 expansion slots
2	V2STACK	Matrix V2 Stacking Module with required stacking cables
1	V2G112-2	Matrix V2 Uplink Module with 1 10/100/1000Base-TX "Combo" port via RJ-45 or mini-GBIC
1	MGBIC-LC09	1000Base-LX Mini GBIC w/LC connector
		EDIFICIO A2 p.1 - 3 blocco: un V2 con uplink verso CED e fino a 24 utenze
1	V2H124-24	Matrix V2 with 24 10/100Base-TX ports via RJ45 and 2 expansion slots
1	V2G112-2	Matrix V2 Uplink Module with 1 10/100/1000Base-TX "Combo" port via RJ-45 or mini-GBIC
1	MGBIC-LC09	1000Base-LX Mini GBIC w/LC connector
		EDIFICIO C : un V2 con uplink verso CED e fino a 24 utenze
1	V2H124-24	Matrix V2 with 24 10/100Base-TX ports via RJ45 and 2 expansion slots
1	V2G112-2	Matrix V2 Uplink Module with 1 10/100/1000Base-TX "Combo" port via RJ-45 or mini-GBIC
1	MGBIC-LC09	1000Base-LX Mini GBIC w/LC connector
		EDIFICIO AE: stack da 2 V2 con uplink verso CED e fino a 48 utenze
2	V2H124-24	Matrix V2 with 24 10/100Base-TX ports via RJ45 and 2 expansion slots
2	V2STACK	Matrix V2 Stacking Module with required stacking cables
1	V2G112-2	Matrix V2 Uplink Module with 1 10/100/1000Base-TX "Combo" port via RJ-45 or mini-GBIC
1	MGBIC-LC09	1000Base-LX Mini GBIC w/LC connector
		EDIFICIO 9: stack da 2 V2 con uplink verso CED e fino a 48 utenze
2	V2H124-24	Matrix V2 with 24 10/100Base-TX ports via RJ45 and 2 expansion slots
2	V2STACK	Matrix V2 Stacking Module with required stacking cables
1	V2G112-2	Matrix V2 Uplink Module with 1 10/100/1000Base-TX "Combo" port via RJ-45 or mini-GBIC
1	MGBIC-LC09	1000Base-LX Mini GBIC w/LC connector
		EDIFICIO 6: stack da 2 V2 con uplink verso CED e fino a 48 utenze
2	V2H124-24	Matrix V2 with 24 10/100Base-TX ports via RJ45 and 2 expansion slots
2	V2STACK	Matrix V2 Stacking Module with required stacking cables
1	V2G112-2	Matrix V2 Uplink Module with 1 10/100/1000Base-TX "Combo" port via RJ-45 or mini-GBIC
1	MGBIC-LC09	1000Base-LX Mini GBIC w/LC connector
		EDIFICIO 6: switch 24 porte 100/1000 con 4 uplink verso CED e 20 utenze rame
1	C1G124-24	Matrix C1 with 24 10/100/1000Base-TX ports via RJ45 and four 1000Base-X "Combo" ports (alternative to four RJ45 ports) via mini-GBIC
4	MGBIC-LC09	1000Base-LX Mini GBIC w/LC connector

Tabella 15: Lista Componenti Rete LAN (Attiva) – Realizzazione 2018

APPARATI / CENTRI	cod. convenzione	Q.tà
TRANSCEIVER 10Gb BASE T		8
TRANSCEIVER 1000 BASE T	RL6L1_SFP-1000BaseT	10
OMXD3000 TRANSCEIVER SFP+ 10G MULTI-MODE LC	RL6L1_OMXD30000	4
OSX010000 TRANSCEIVER SFP+ 10G SINGLE-MODE LC	RL6L1_OSX010000	8

TRANSCEIVER SFP 1G SINGLE-MODE		
LC-LC DUPLEX 50/125 PATCH CORD 2MT (MULTI-MODE)	RL6L1_HOPLCOM3020LC253	
LC-LC DUPLEX 50/125 PATCH CORD 10MT (MULTI-MODE)	RL6L1_HOPLCOM3100LC253	
LC-LC DUPLEX 8/125 PATCH CORD 2MT (SINGLE-MODE)	RL6L1_HOPLC008020LC203	
LC-LC DUPLEX 8/125 PATCH CORD 6MT (SINGLE-MODE)	RL6L1_HOPLC008060LC203	
HUAWEI S5720-52X-SI-AC-C	RL6L1_S5720-52X-SI-AC-C	1
HUAWEI S5720-52X-PWR-SI-ACF-C	RL6L1_S5720-52X-PWR-SI-ACF-C	4
HUAWEI S5720-28TP-PWR-LI-AC		
FIREWALL CON 2/4 PORTE 10Gb		1
ROUTER WAN CON 2/4 PORTE 10Gb		1

Tabella 16: Lista Componenti Rete LAN (Attiva) – Realizzazione 2019

APPARATI / CENTRI	cod. convenzione	Q.tà
HUAWEI 6720-54C-EI-48S-AC (router di LAN)	RL6L1_6720-54C-EI-48S-AC-C	1
PAC-600WA-B	RL6L1_PAC-600WA-B	1
TRANSCEIVER 1000 BASE T	RL6L1_SFP-1000BaseT	0
OMXD3000 TRANSCEIVER SFP+ 10G MULTI-MODE LC	RL6L1_OMXD30000	8
OSX010000 TRANSCEIVER SFP+ 10G SINGLE-MODE LC	RL6L1_OSX010000	8
TRANSCEIVER QFSP-40G-ISR4 MULTI-MODE 0,15KM	RL6L1_QSFP-40G-iSR4	4
TRANSCEIVER QFSP-40G-LR4 SINGLE-MODE 0,15KM	RL6L1_QSFP-40G-iLR4	0
LC-LC DUPLEX 50/125 PATCH CORD 2MT (MULTI-MODE)	RL6L1_HOPLCOM3020LC253	4
LC-LC DUPLEX 50/125 PATCH CORD 10MT (MULTI-MODE)	RL6L1_HOPLCOM3100LC253	4
LC-LC DUPLEX 8/125 PATCH CORD 2MT (SINGLE-MODE)	RL6L1_HOPLC008020LC203	4
LC-LC DUPLEX 8/125 PATCH CORD 6MT (SINGLE-MODE)	RL6L1_HOPLC008060LC203	4
HUAWEI S5720-52X-SI-AC-C	RL6L1_S5720-52X-SI-AC-C	0
HUAWEI S5720-52X-PWR-SI-ACF-C	RL6L1_S5720-52X-PWR-SI-ACF-C	0

Tabella 17: Lista Componenti Rete LAN (Attiva) – Realizzazione 2020

ENEA
Servizio Promozione e Comunicazione
www.enea.it

Stampa: Laboratorio Tecnografico ENEA - C.R. Frascati
maggio 2020