

 <b>TELESPAZIO</b> una società LEONARDO e THALES	ID Doc.:	CSC0800000104-ADD01
	Edizione:	2.3
	Data:	20/11/2024

**OPERAZIONI E MANUTENZIONE  
 DELLA RETE ASI-NET – Periodo 2019 – 2022  
 Contratto ASI n. 2019-6-I.0**

**ASI-NET Architectural Design Document**

Livello di Autorizzazioni	Ruolo di Progetto	Nome	Data	Firma
Preparato da	Responsabile Tecnico	F. Turchi		
Verificato da	Resp. U. O. SO-TGI-NMS	A. Gazzara		
Approvato da	Responsabile Tecnico	F. Turchi		
	Assicurazione di Prodotto	P. De Santis		
	Gestione di Configurazione	I. Busiol		
Emesso da	Responsabile di Programma	P. Camponeschi		

Approvazione Cliente		Nome	Data	Firma
Classificazione	A	M. Calabrese	21/11/2024	

 <b>TELESPAZIO</b> una società LEONARDO e THALES	ID Doc.:	CSC0800000104-ADD01
	Edizione:	2.3
	Data:	20/11/2024

## Stato del Documento

ISSUE	DATA	PREPARATO DA	RAGIONE DEL CAMBIO
1.0	05/10/2016	Franco Turchi	Prima Edizione
2.0	07/10/2019	Franco Turchi	Seconda Edizione (prima ed. del contratto 2019-6-I.0)
2.1	03/04/2020	Franco Turchi	Terza Edizione per PSI-4
2.2	23/07/2021	Franco Turchi	Quarta Edizione per PSI-11, PSI-12
2.3	20/11/2024	Franco Turchi	Quinta Edizione

## Storia del Documento

ISSUE	PAGINA	SEZIONE	CAMBI

## Lista Distribuzione

SOCIETÀ	NOME	RUOLO	N. COPIE
ASI	M. Calabrese	Responsabile Unico del Procedimento (RUP)	1
ASI	M. Toninelli	Assistente al RUP	1
Telespazio	P. Camponeschi	Responsabile di Programma Telespazio	1
Telespazio	P. De Santis	Responsabile Assicurazione di Prodotto	1
Telespazio	F. Turchi	Responsabile Tecnico	1
Telespazio	F. Cerone	Responsabile Operativo	1
Telespazio	I. Busiol	Responsabile Gestione di Configurazione	1

 <b>TELESPAZIO</b> <small>una società LEONARDO e THALES</small>	ID Doc.:	CSC0800000104-ADD01
	Edizione:	2.3
	Data:	20/11/2024

## SOMMARIO

<b>1. INTRODUZIONE</b> .....	<b>5</b>
1.1. SCOPO .....	5
<b>2. DOCUMENTI APPLICABILI E DI RIFERIMENTO</b> .....	<b>5</b>
2.1. DOCUMENTI APPLICABILI.....	5
2.2. DOCUMENTI DI RIFERIMENTO .....	5
<b>3. ARCHITETTURA ASI-NET</b> .....	<b>6</b>
<b>4. DESCRIZIONE DELLA RETE</b> .....	<b>14</b>
4.1. NODI DELLA RETE .....	14
4.1.1. <i>Centro Spaziale del Fucino (FSC)</i> .....	15
4.1.2. <i>ALTEC</i> .....	16
4.1.3. <i>JSC</i> .....	17
4.1.4. <i>MATERA</i> .....	18
4.1.5. <i>MSFC</i> .....	19
4.1.6. <i>BSC - MALINDI</i> .....	20
4.1.7. <i>SSDC</i> .....	21
4.1.8. <i>ASI Roma</i> .....	22
4.1.9. <i>ESOC</i> .....	23
4.1.10. <i>KOUROU</i> .....	24
4.1.11. <i>SDSA</i> .....	25
4.1.12. <i>NAPOLI</i> .....	26
4.1.13. <i>ARGOTEC</i> .....	27

 <b>TELESPAZIO</b> <i>una società LEONARDO e THALES</i>	ID Doc.:	CSC0800000104-ADD01
	Edizione:	2.3
	Data:	20/11/2024

## INDICE DELLE FIGURE

Figura 1: Schema a blocchi .....	7
Figura 2: Configurazione BGP proposta .....	10
Figura 3: Nodi ASINet.....	14
Figura 4: nodo FSC.....	15
Figura 5: nodo ALTEC.....	16
Figura 6: nodo JSC .....	17
Figura 7: nodo MATERA .....	18
Figura 8: nodo MSFC .....	19
Figura 9: nodo BSC .....	20
Figura 10: nodo ASDC .....	21
Figura 11: nodo Roma Tor Vergata.....	22
Figura 12: nodo ESOC .....	23
Figura 13: nodo KOUROU.....	24
Figura 14: nodo SDSA.....	25
Figura 15: nodo NAPOLI.....	26
Figura 16: nodo ARGOTEC.....	27

 <b>TELESPAZIO</b> <i>una società LEONARDO e THALES</i>	ID Doc.:	CSC0800000104-ADD01
	Edizione:	2.3
	Data:	20/11/2024

## 1. Introduzione

### 1.1. Scopo

Questo documento vuole dare una descrizione della rete ASI usata come infrastruttura di telecomunicazioni per supportare le missioni MPLM, SWIFT, AGILE, NuSTAR etc., ogni missione prevede l'utilizzo di determinati nodi.

Nel seguito tale rete verrà menzionata come ASINet.

Di seguito viene proposto un documento di architettura per tutti i nodi volto a soddisfare le esigenze legate al contratto ASI n. 2019-6-I.0.

## 2. Documenti applicabili e di riferimento

I documenti applicabili e di riferimento referenziati nei seguenti paragrafi, si intendono nell'edizione corrente.

### 2.1. Documenti Applicabili

Rif.	ID Documento	Titolo
[DA.1]	Contratto ASI n. I/228/00/0	Realizzazione della rete ASI-NET
[DA.2]	Contratto ASI n. I/003/03/0	Operazioni e Manutenzione della rete ASI-NET
[DA.3]	Contratto ASI n. I/002/06/0	Operazioni e Manutenzione della rete ASI-NET
[DA.4]	Contratto ASI n° I/007/08/0	Operazioni e Manutenzione della rete ASI-NET
[DA.5]	Contratto ASI n° I/036/11/0	Operazioni e Manutenzione della rete ASI-NET
[DA.6]	Contratto ASI n° A.A. I/036/11/1	Operazioni e Manutenzione della rete ASI-NET
[DA.7]	Contratto ASI n° A.A. I/036/11/2	Operazioni e Manutenzione della rete ASI-NET
[DA.8]	Contratto ASI n° 2015-051-I.0	Contratto O&M Rete ASINET – Periodo 2016-2018 con ATG
[DA.9]	Contratto ASI n° 2019-6-I.0	Contratto ASI per Operazioni e Manutenzione della Rete ASINET Periodo 2019-2022
[DA.10]	ASINET92-TPZ-06-0004-CMP	Piano di Gestione della Configurazione
[DA.11]	ASINET92-TPZ-05-0003-PAP	Piano di Assicurazione dl Prodotto

### 2.2. Documenti Di Riferimento

Rif.	ID Documento	Titolo
[DR.1]		Space Station Control Center to Italian Space Agency Ground Segment Interface Definition Protocol
[DR.2]	LIS-180221-127-GSN	ASI-Net Acronyms LIS-180221-127-GSN

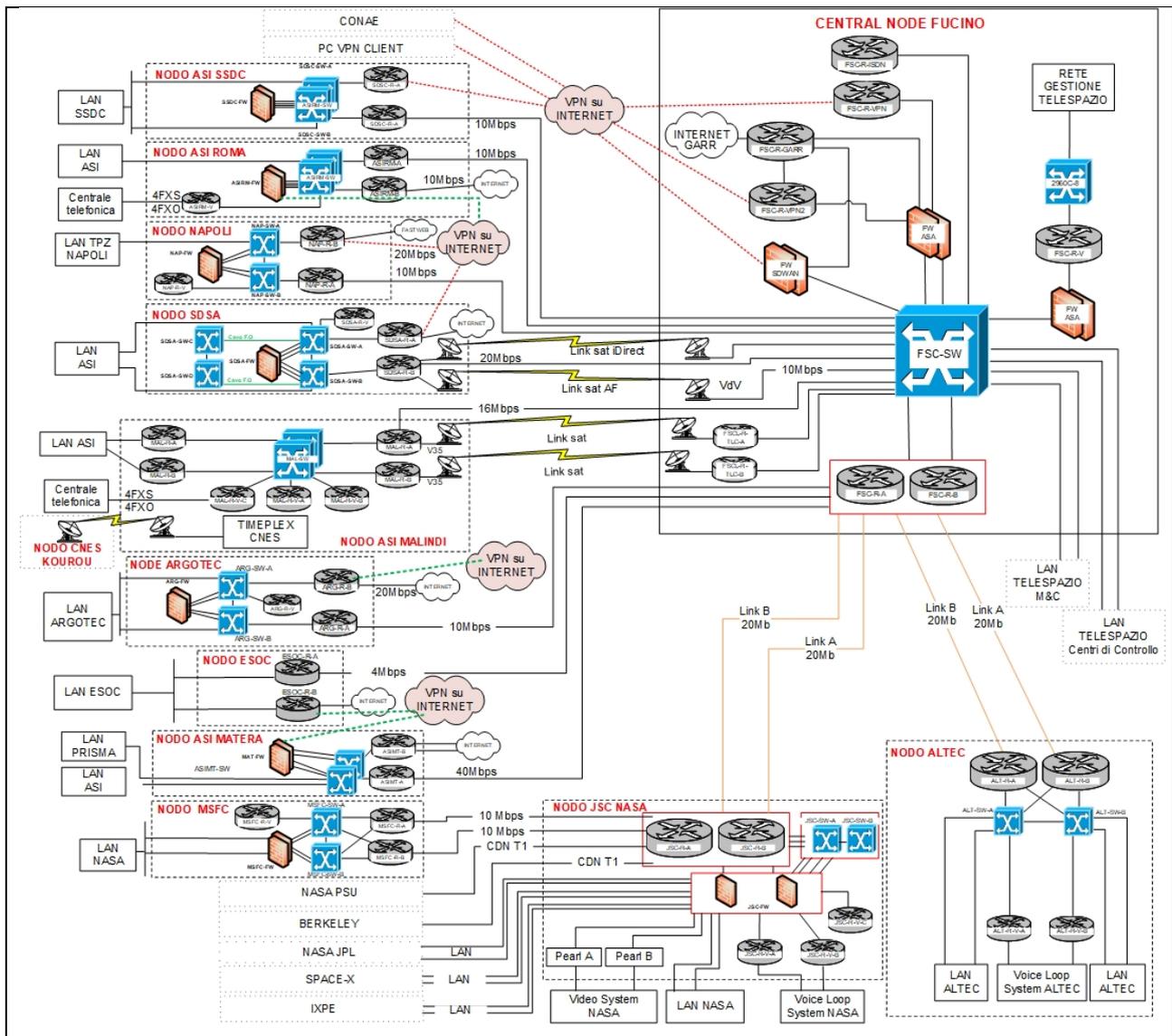
	ID Doc.:	CSC0800000104-ADD01
	Edizione:	2.3
	Data:	20/11/2024

### 3. Architettura ASI-Net

L'architettura della rete ASINet è composta da un nodo centrale ubicato presso la sede Telespazio del Fucino denominato FSC (Fucino Space Centre) al quale sono connessi tutti i nodi italiani e, tramite due link transoceanici a 20Mbps, il nodo NASA del JSC. Tramite quest'ultimo nodo si raggiungono, oltre al nodo NASA presso MSFC (Marshall Space Flight Centre), tutti gli altri utenti situati negli USA come ad esempio la PSU (Pennsylvania state University), la società SpaceX o la UCB (University of California, Berkeley).

La configurazione della rete si basa su due nodi principali: il nodo FSC in Italia ed il nodo JSC negli Stati Uniti. Tutte le connessioni dei rispettivi stati di competenza convergeranno su tali nodi, alle estremità di ciascuna connessione saranno situati dei nodi che potranno accedere a tutti i servizi di rete. I nodi principali si occupano della gestione e del controllo dell'intera rete e dei suoi servizi.

Di seguito viene riportato lo schema generale della rete:



**Figura 1: Schema a blocchi**

Di seguito si riportano le caratteristiche degli apparati ed una breve descrizione dei protocolli utilizzati sulla rete:

- Apparati Modulari che consentono una crescita scalare in termini di volume di traffico e di numero dei nodi;
- Apparecchiature compatibili con tutti i protocolli standard di instradamento;
- Tecnologia VoIP per il miglior instradamento della voce (necessita soltanto di modifica della tabella di instradamento) restringe il know-how sulla rete TCP/IP perché voce e dati coesistono nella rete stessa e nel protocollo IP;
- Il sistema di gestione della rete (Network Management System) voce - dati è integrato;

	ID Doc.:	CSC0800000104-ADD01
	Edizione:	2.3
	Data:	20/11/2024

- Disponibilità della Qualità del Servizio per le priorità di traffico;
- Apparecchiature di streaming Video su protocollo IP con codec H264: adottando l'IP video, il sistema di distribuzione risulta semplificato poiché non vi sono particolari vincoli tecnici sulla posizione dei video client.

Al momento la rete è composta da 13 nodi che sono:

FSC - Telespazio Fucino

JSC – NASA Jhonson Space Center

MSFC – NASA Marshall Space Flight Center

BSC – ASI Broglio Space Center a Malindi

ALTEC – ALTEC Torino

MATERA – ASI Matera

ROMA – ASI Roma Tor Vergata

ASDC – ASI Roma Tor Vergata

ESOC – ESA Darmstradt

CNES – CNES Kourou

SDSA – INAF Cagliari

ARG – ARGOTEC Torino

NAP – Telespazio Napoli

I router Cisco della serie ISR4000 sono stati utilizzati in tutti i nodi della rete avendo un'architettura modulare per consentire al sistema di espandersi in termini di volume di traffico e di numero di interfacce. Sono dei router IP per i dati, ma rappresentano anche un'unica interfaccia per il video, la voce e i dati.

Per la trasmissione dei 4 flussi video della NASA, presso il nodo JSC sono installati due encoder video che permettono di avere in ingresso fino a 4 flussi video HD ed in uscita uno o più flussi in streaming IP utilizzando il Viceo Codec H264.

Il protocollo HSRP viene utilizzato per la ridondanza dei router (in questo caso per gli ISR4000) ed è spesso usato per migliorare la "resiliency" nella rete assegnando, come indirizzo IP di default gateway agli host, quello virtuale configurato tramite il protocollo HSRP.

	ID Doc.:	CSC0800000104-ADD01
	Edizione:	2.3
	Data:	20/11/2024

Per utilizzare entrambi i percorsi dalla rete dagli host ai server, si può configurare il MHSRP fra due router. Essenzialmente, un router è configurato con due gruppi HSRP (chiamiamoli gruppo 1 e gruppo 2) e il secondo router è configurato con i medesimi gruppi HSRP. Sia R1 il router attivo del gruppo 1 e R2 il router in standby sempre del gruppo 1. Per il gruppo 2, sia R2 il router attivo e R1 il router in standby. Poi si configurino metà dei default gateways degli hosts usando l'indirizzo IP virtuale del gruppo 1 e l'altra metà usando l'indirizzo IP virtuale del gruppo 2.

## Protocollo BGP

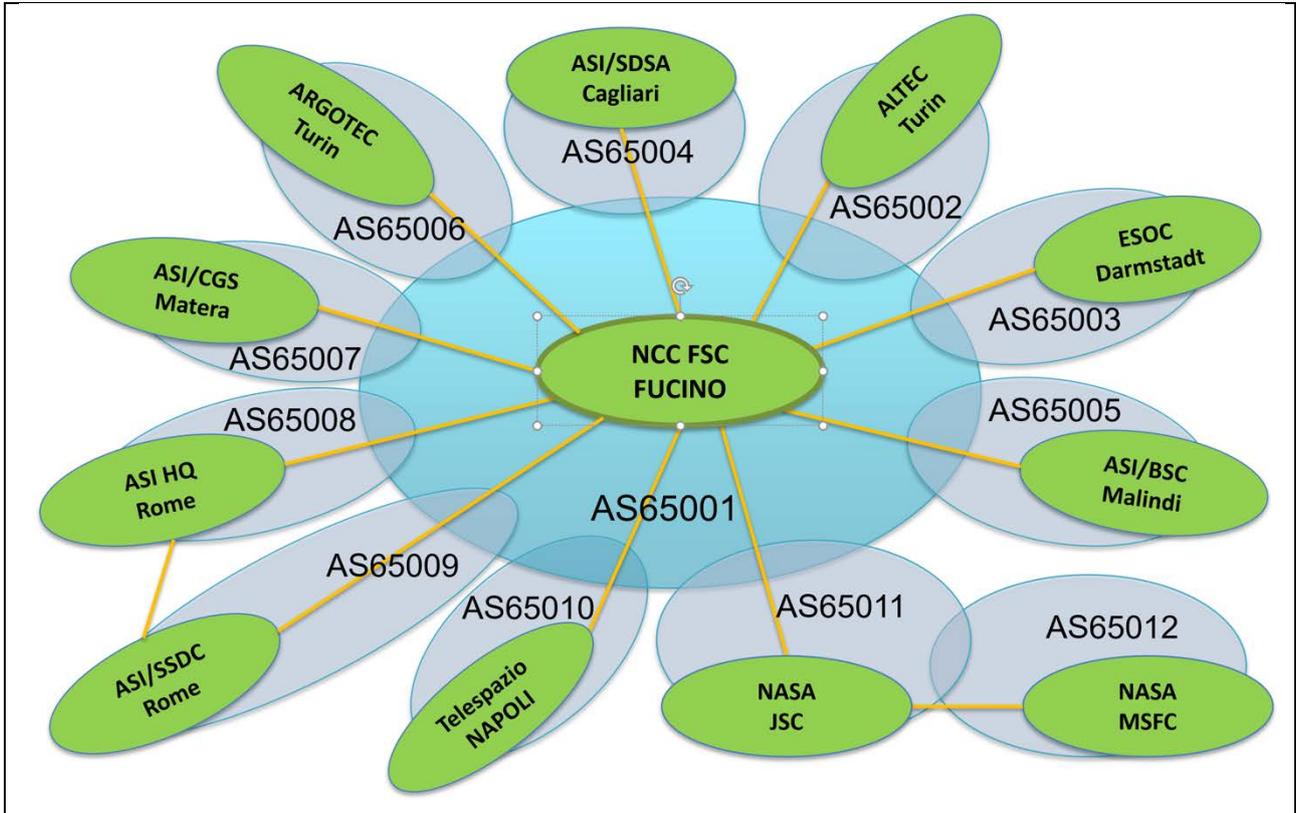
Il Border Gateway Protocol (BGP) è un protocollo di routing dinamico usato per connettere tra loro più router che appartengono a sistemi autonomi (Autonomous System, AS) distinti e che sono chiamati "router gateway" o "boundary router". È quindi un protocollo di routing inter-AS, nonostante possa essere utilizzato anche tra router appartenenti allo stesso AS (nel qual caso è indicato con il nome di iBGP, Interior Border Gateway Protocol), o tra router connessi tramite un ulteriore AS che li separa (eBGP, External Border Gateway Protocol).

Il BGP funziona attraverso la gestione di una tabella di reti IP, o prefissi, che forniscono informazioni sulla raggiungibilità delle diverse reti tra più sistemi autonomi. Si tratta di un protocollo di routing a indicazione di percorso (path vector), che non usa metriche di carattere tecnico ma prende le decisioni di instradamento basandosi su regole ("policy") determinate da ciascuna rete. Se non vengono applicate specifiche regole di controllo sugli apparati, ogni nodo della rete conoscerà tutti i percorsi possibili interni ad ASINet per raggiungere ogni rete annunciata.

In pratica il BGP mette a disposizione di ciascun router un modo per:

- Ottenere informazioni sulla raggiungibilità dei prefissi di sottorete da parte dei sistemi confinanti
- Determinare i percorsi ottimi verso le sottoreti sulla base delle politiche del sistema e sulle informazioni di raggiungibilità
- Propagare le informazioni a tutti i router interni ad un AS

Per implementare il protocollo BGP nella rete ASINet, o per essere più precisi il protocollo iBGP, ad ogni nodo è stato assegnato un numero di AS univoco come riportato nella figura seguente:



**Figura 2: Configurazione BGP proposta**

Di seguito la tabella di assegnazione AS per nodo:

Numero AS	Descrizione
65001	Nodo del Fucino
65002	Nodo ALTEC
65003	Nodo ESOC
65004	Nodo SDSA
65005	Nodo MALINDI
65006	Nodo ARGOTEC
65007	Nodo MATERA
65008	Nodo ASI ROMA
65009	Nodo SSDC
65010	Nodo NAPOLI

 <b>TELESPAZIO</b> una società LEONARDO e THALES	ID Doc.:	CSC0800000104-ADD01
	Edizione:	2.3
	Data:	20/11/2024

65011	Nodo JSC
65012	Nodo FSC

## SD-WAN

In alcuni nodi della rete è stato implementato il protocollo SD-WAN per supportare il “load-balancing” del traffico dati su tutti i link disponibili in modo da utilizzare la capacità trasmissiva di tutti i link WAN disponibili.

SD-WAN è un’architettura di rete WAN definita da un software (chiamato controller SD-WAN) che consente, tramite la configurazione di opportune regole, di controllare il traffico dati verso le reti WAN. Quindi il controllo del traffico dati non viene più gestito da apparati fisici (come i router) ma dal Software. In ASINet il controllo del traffico è demandato ai firewall FORTIGATE installati nei nodi.

Con SD-WAN è possibile:

- unire due diversi link, anche di tipo diverso (fibra, xDSL, fixed wireless, 4G...) e di operatori diversi, permettendo sia di fare load-balancing dei link sia di configurare il percorso preferenziale per un’applicazione in modo da privilegiare le applicazioni critiche per il business (ad esempio VoIP e Telemetria);
- limitare la banda per applicazioni non critiche (ad esempio l’Internet browsing);
- monitorare in tempo reale le prestazioni di ogni singolo collegamento.

## SPANNING TREE

Lo spanning tree è un Protocollo di comunicazione standard utilizzato per realizzare reti complesse (a Livello fisico) con percorsi ridondanti utilizzando tecnologie di Livello datalink (il livello 2 del modello OSI). Lo spanning tree viene eseguito dagli switch e dai router, e mantiene inattive alcune interfacce in modo da garantire che la rete rimanga connessa ma priva di loop.

Gli apparati scambiano messaggi BPDU fra loro per rivelare i loop nella rete che vengono poi rimossi portando in uno stato di "BLOCKING" alcune delle loro interfacce di rete.

## Qualità del Servizio (QoS)

Tale concetto fa riferimento alla capacità di una rete di fornire un servizio migliore per un traffico di rete selezionato con le varie tecnologie, incluse le reti Frame Relay, ATM, Ethernet, 802.1, SONET, e le reti IP-che possono usare tutte queste tecnologie. Gli scopi

	ID Doc.:	CSC0800000104-ADD01
	Edizione:	2.3
	Data:	20/11/2024

primari della QoS comprendono la banda dedicata, lo jitter controllato, il ritardo di trasmissione (richiesto da alcuni tipi di traffico interattivo e in tempo reale) e migliori caratteristiche delle perdite. Le tecnologie di QoS offrono gli elementari blocchi costitutivi che saranno usati per future applicazioni di tipo “affari” in campus, WAN, e reti dei fornitori di servizi.

#### Caratteristiche e benefici offerti dal Cisco IOS QoS.

Questa funzione abilita reti complesse al controllo e prevedibilmente al servizio di una varietà di applicazioni e tipi di traffico in rete. Quasi ogni rete può avvantaggiarsi della QoS per un’ottima efficienza, sia piccole o grandi reti aziendali sia un fornitore di servizi Internet. Questo software offre questi benefici:

- **Controllo delle risorse** — Si possono controllare le risorse in uso. Per esempio si può limitare la banda consumata su un collegamento principale tramite dei trasferimenti FTP o dando priorità ad un importante accesso a basi di dati.
- **Uso più efficiente delle risorse di rete** — Usando gli strumenti gestionali di analisi e di contabilità della rete Cisco, si può conoscere la ragione dell’uso della rete e quali servizi vengono fruiti dalla parte più significativa del traffico generato da un’utenza “affari”.
- **Servizi personalizzati** — Il controllo e la visibilità dati da QoS abilita i fornitori di servizi Internet ad offrire ai loro clienti diversi gradi di servizio attentamente personalizzati alla loro clientela.
- **Coesistenza di applicazioni critiche per le missioni** — Le tecnologie Cisco di QoS certificano che la vostra WAN in uso sia usata efficientemente dalle applicazioni critiche per le missioni più importanti per i vostri affari, che siano disponibili la banda e i ritardi minimi richiesti dalle applicazioni vocali e multimediali e che altre applicazioni che usano il collegamento abbiano un buon servizio senza interferire con il traffico critico della missione.

#### NAT (Network Address Translator)

Il NAT opera su un router che interconnette due reti fra loro; una di queste reti (chiamata interna) è indirizzata sia con indirizzi privati che obsoleti che devono essere convertiti in indirizzi accettati prima che i pacchetti siano trasferiti all’altra rete (chiamata esterna). La traduzione opera insieme con l’instradamento così che il NAT può essere semplicemente abilitato, quando lo si desidera, su un router d’accesso Internet lato utente. L’uso di un NAT offre la traduzione di indirizzi di rete su una piattaforma router in modalità congruenti con la RFC 1631. Lo scopo del NAT è quello di fornire delle funzionalità come se la rete privata avesse globalmente degli indirizzi unici e il NAT non fosse presente. La RFC 1631 rappresenta un sottoinsieme delle funzionalità del NAT Cisco IOS. Il NAT Cisco IOS

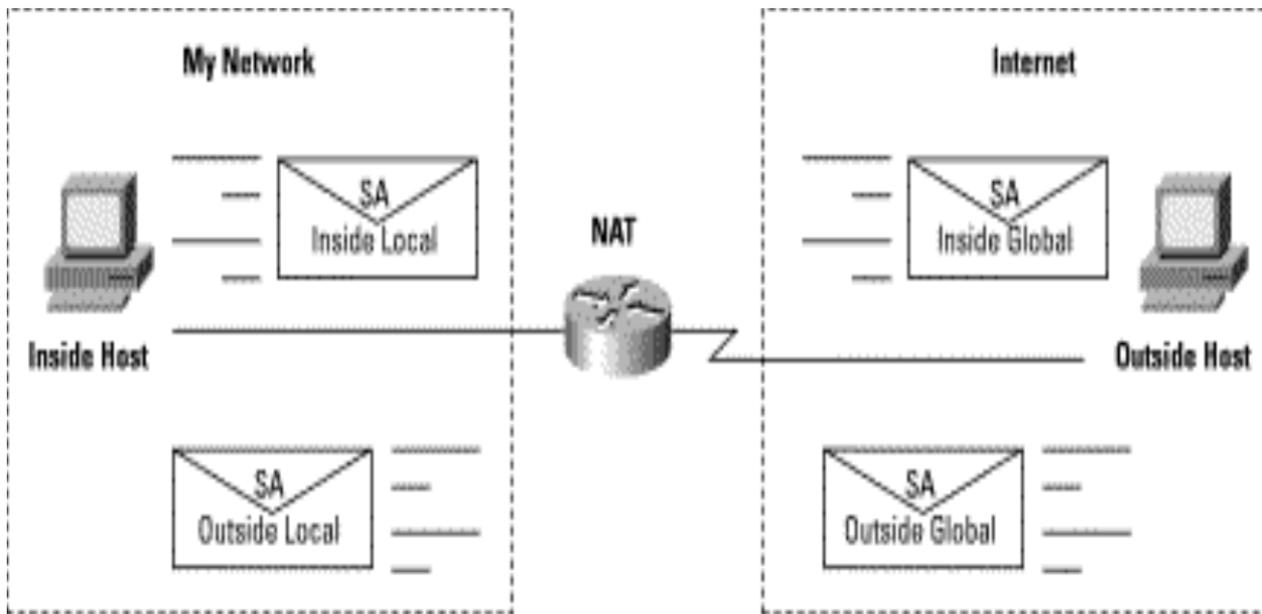
ID Doc.:	CSC0800000104-ADD01
Edizione:	2.3
Data:	20/11/2024

supporta la “traduzione bi-direzionale” mediante l’uso simultaneo delle traduzioni a “sorgente interna” e a “sorgente esterna”.

### Terminologia NAT

Interna: L’insieme delle reti che sono soggette a traduzione.

Esterna: Tutte le altre. Di solito queste hanno indirizzi validi in Internet.



An IP Address is Either Local or Global  
Local IP Addresses are Seen in the  
Inside Network  
Global IP Addresses are Seen in the Outside Network

 una società LEONARDO e THALES	ID Doc.:	CSC0800000104-ADD01
	Edizione:	2.3
	Data:	20/11/2024

## 4. DESCRIZIONE DELLA RETE

In questo paragrafo viene analizzata la configurazione di ogni singolo nodo.

### 4.1. Nodi della Rete

Nel seguito vengono descritti i nodi che sono connessi alla rete ASI-Net:

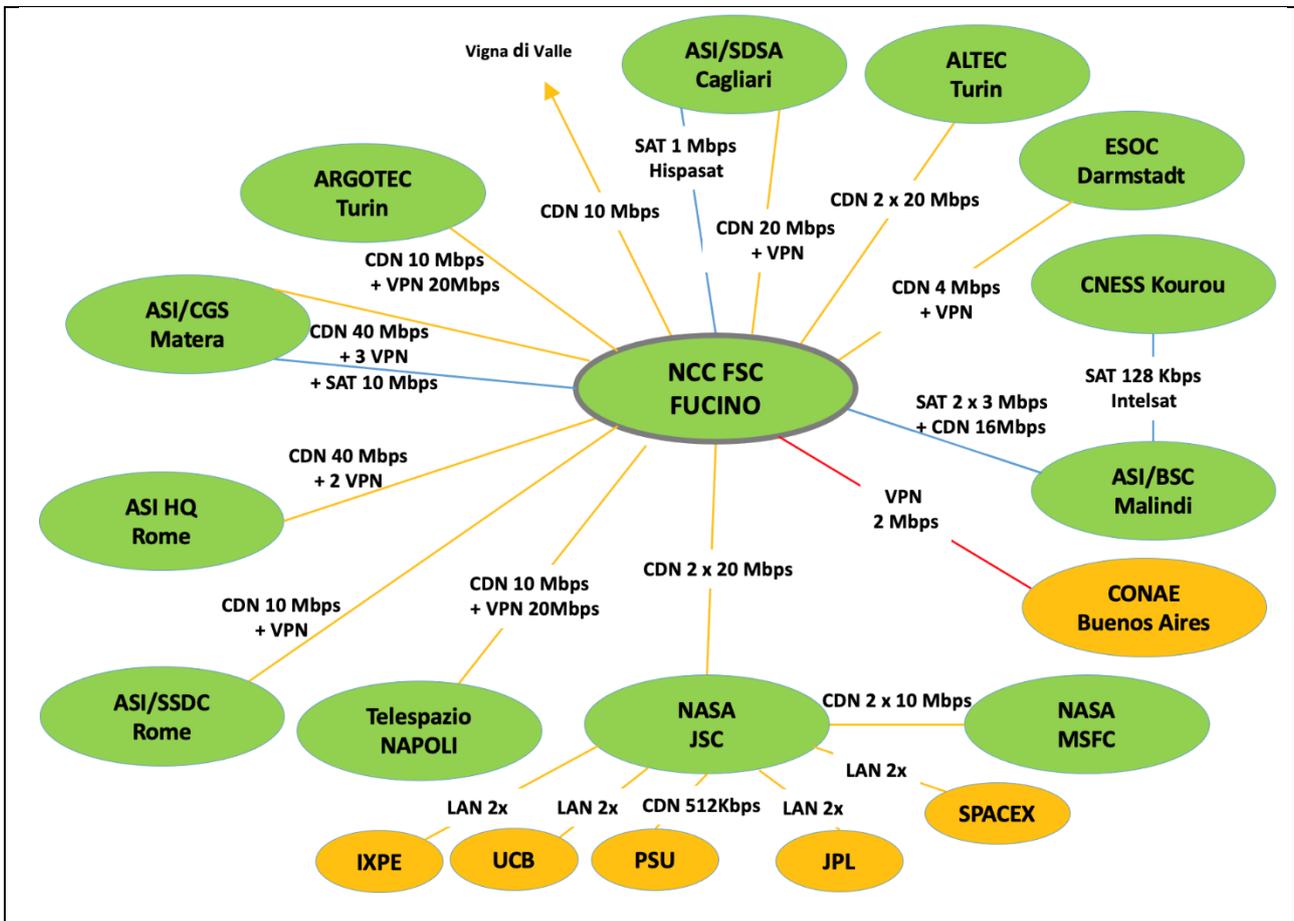


Figura 3: Nodi ASINet

 una società LEONARDO e THALES	ID Doc.:	CSC0800000104-ADD01
	Edizione:	2.3
	Data:	20/11/2024

#### 4.1.1. Centro Spaziale del Fucino (FSC)

FSC è il nodo centrale che controlla la corretta operatività dell'intera rete e in cui risiede il sistema di gestione della rete stessa: qui il personale operativo raccoglie dati e statistiche sulle reali prestazioni e caratteristiche operative.

I Firewall CISCO della serie ASA5500X installati in questo nodo proteggono il sistema di gestione della rete da accessi indesiderati. Oltre a questi sono installati anche due firewall FORTINET FG-601E utilizzati per i collegamenti in secure SD-WAN verso i nodi dove sono installati firewall FORTINET e per terminare VPN IPsec negli altri ove previsto.

Tutti i collegamenti LAN/WAN degli altri nodi sono attestati ad entrambi i router centrali (Primario e Secondario) per migliorare l'affidabilità della rete e la disponibilità del servizio.

I collegamenti satellitari sono attestati al nodo sulle porte seriali sincrone dei router.

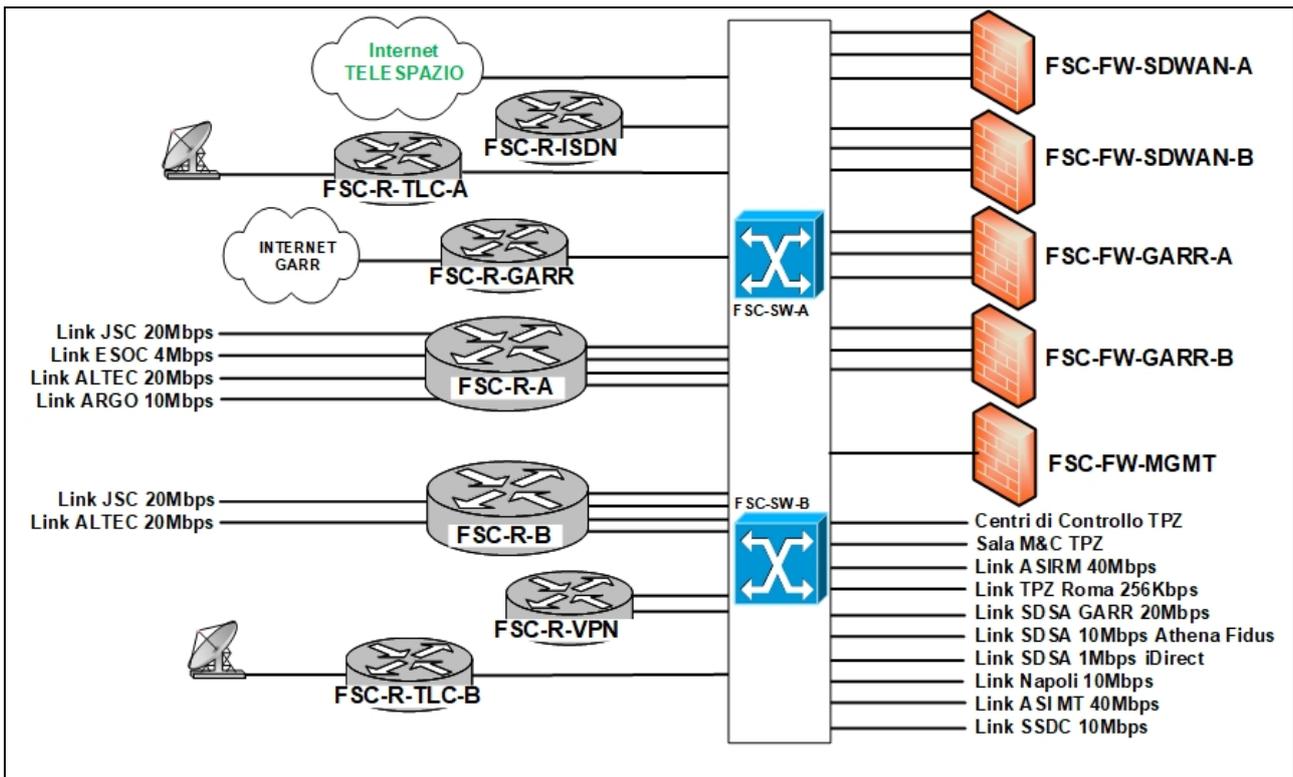


Figura 4: nodo FSC

### 4.1.2. ALTEC

ALTEC è un utente dei servizi ASI-Net.

A questo nodo arrivano dati, voce e video provenienti dal nodo JSC.

Inoltre, per il progetto EXOMARS, il nodo è stato anche collegato logicamente con due canali a 2Mbps al nodo di ESOC.

Qui di seguito è riportato lo schema del nodo:

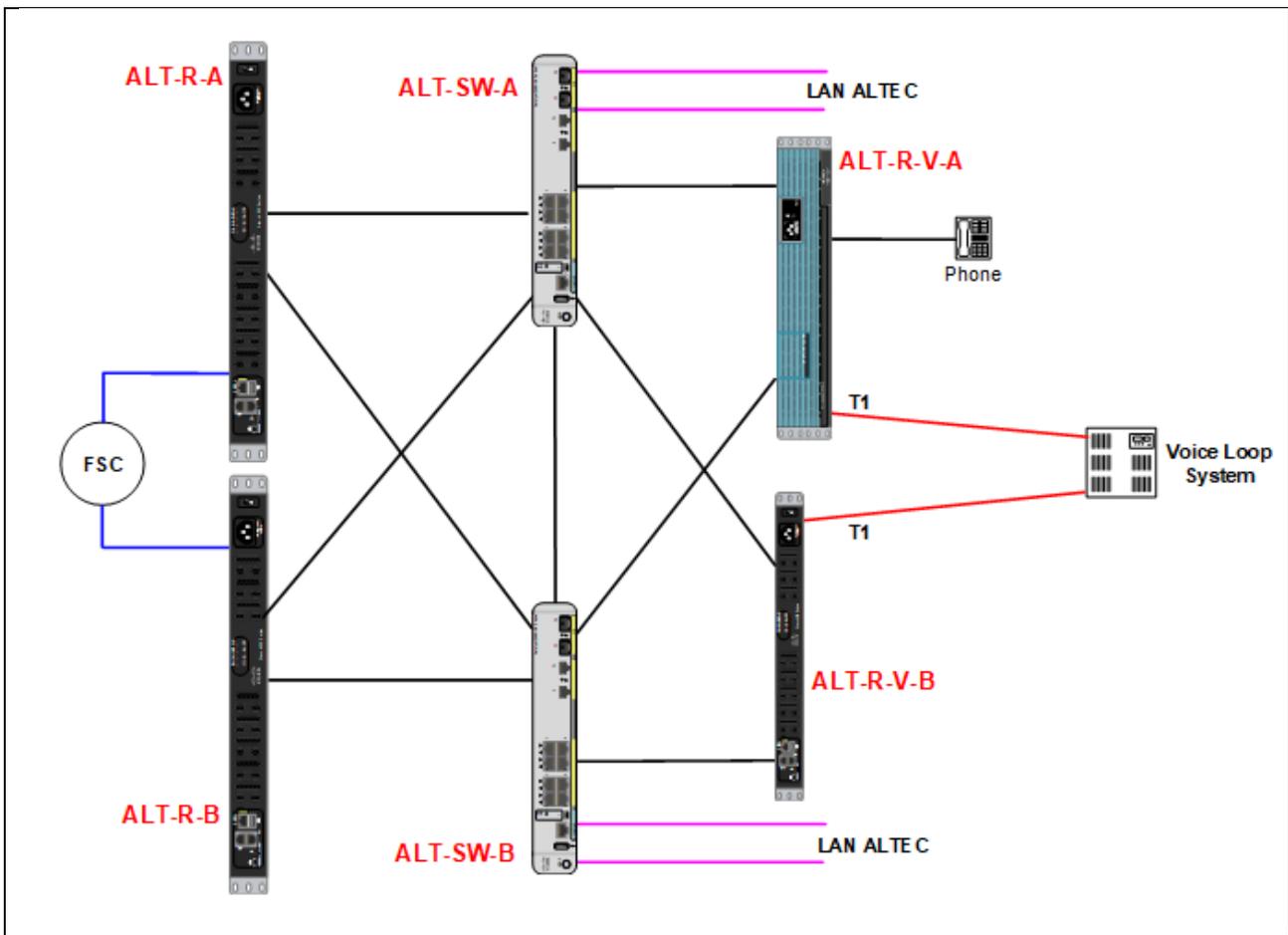


Figura 5: nodo ALTEC

### 4.1.3. JSC

A questo nodo sono connessi alcuni siti della NASA, ovvero il MSFC, il PSU e il JPL. Inoltre al nodo sono connessi la Società SPACE-X e l'UCB (University of California Berkeley). Il nodo JSC è connesso al nodo FSC, per mezzo di due link EVC a 20Mbps, in Secure SD-WAN tramite i firewall Fortigate FG-101F. Inoltre sempre in Secure SD-WAN è collegato al nodo MSFC.

Il nodo JSC è connesso al nodo FSC per mezzo di due link EVC da 20Mbps ciascuno.

Schema del nodo:

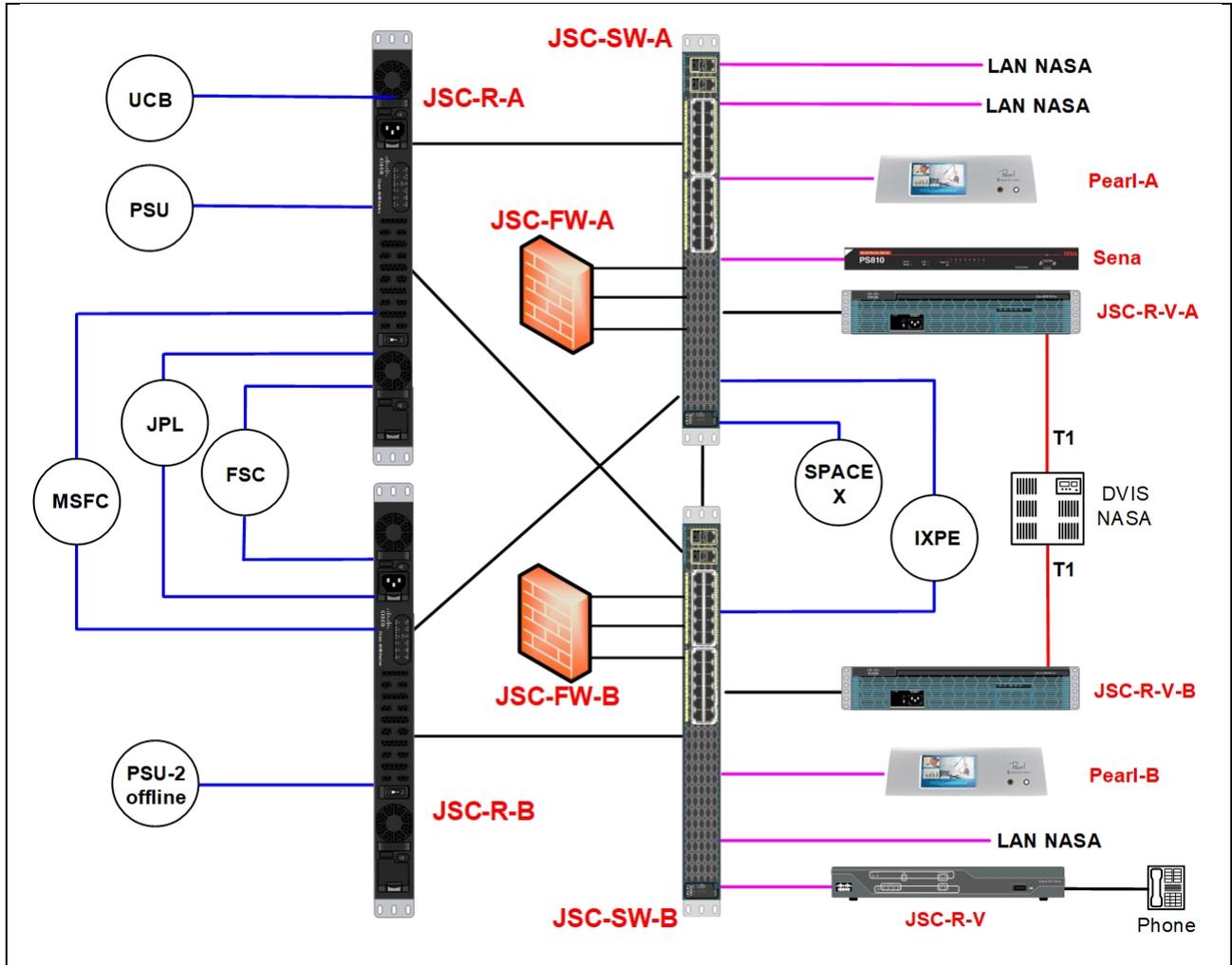


Figura 6: nodo JSC

 <b>TELESPAZIO</b> una società LEONARDO e THALES	ID Doc.:	CSC0800000104-ADD01
	Edizione:	2.3
	Data:	20/11/2024

#### 4.1.4. MATERA

Il nodo di Matera è formato da due router CISCO serie isr4000, due switch CISCO 9200 e da due firewall Fortigate FG-101F. Il nodo è collegato al nodo centrale di Fucino con una linea CDN a 40Mbps, un collegamento satellitare a 10Mbps e da una VPN via Internet.

Inoltre tra il nodo di Matera ed il nodo del Fucino, tramite i firewall Fortigate, è configurata una Secure SD-WAN.

Di seguito lo schema di rete del nodo di Matera:

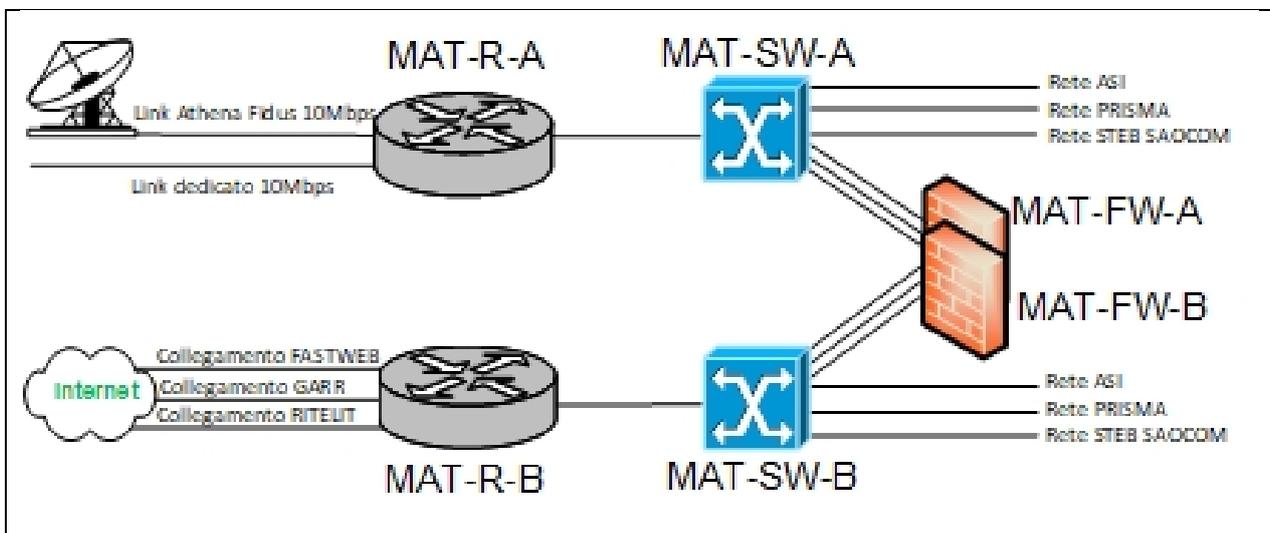


Figura 7: nodo MATERA

 <b>TELESPAZIO</b> una società LEONARDO e THALES	ID Doc.:	CSC0800000104-ADD01
	Edizione:	2.3
	Data:	20/11/2024

#### 4.1.5. MSFC

La configurazione implementata al nodo MSFC (Marshall Space Flight Center) è al momento una configurazione tipo, composta da due router Cisco della serie ISR4000, da due switch CISCO serie 2900, da due firewall Fortigate Fg-101F ed un voice router Cisco C881.

Il nodo è collegato al nodo JSC tramite due linee CDN a 10Mbps; inoltre tra il nodo MSFC ed il nodo JSC è configurata una Secure SD-WAN tramite i firewall Fortigate.

Lo schema seguente mostra la configurazione presso il nodo.

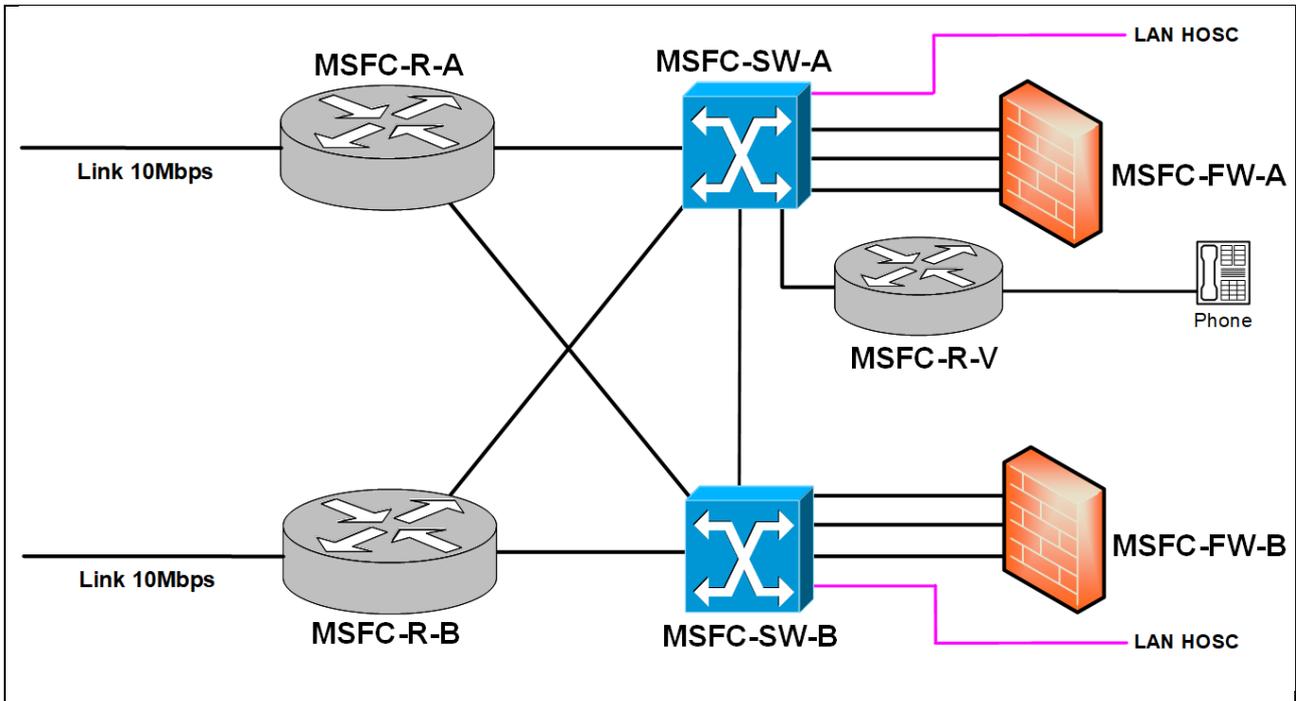


Figura 8: nodo MSFC

 una società LEONARDO e THALES	ID Doc.:	CSC0800000104-ADD01
	Edizione:	2.3
	Data:	20/11/2024

#### 4.1.6. BSC - MALINDI

ASI-Net raggiunge questo nodo tramite due collegamenti satellitari che sono del tutto indipendenti fra loro anche dal punto di vista degli apparati di terra

Lo schema seguente mostra la configurazione presso il nodo.

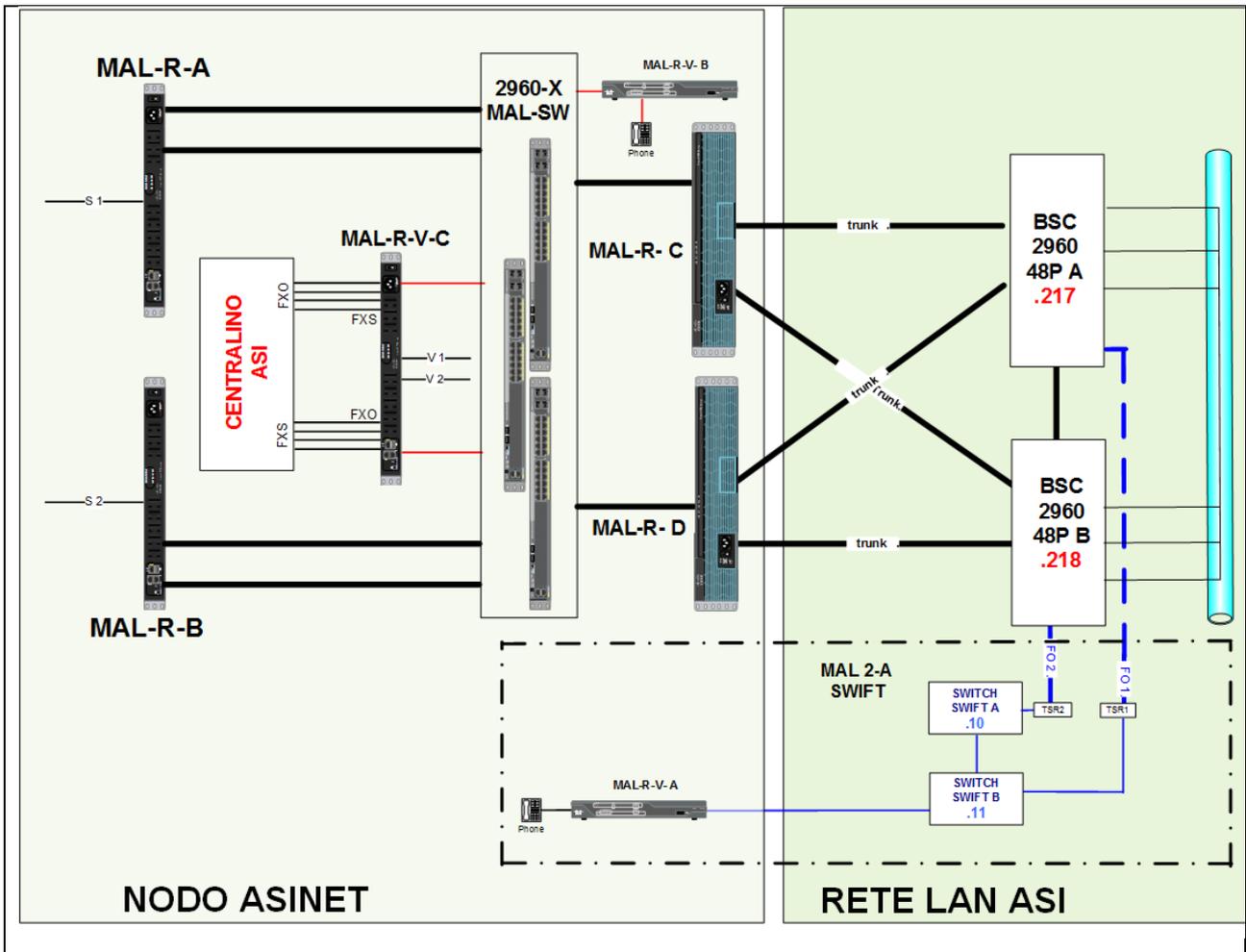


Figura 9: nodo BSC

 una società LEONARDO e THALES	ID Doc.:	CSC0800000104-ADD01
	Edizione:	2.3
	Data:	20/11/2024

#### 4.1.7. SSDC

L'architettura del nodo prevede sempre l'utilizzo di macchine modulari Cisco come filosofia consolidata nella rete, gli apparati installati sono CISCO ISR4331, switch CISCO serie 2960 e firewall Fortigate FG-101F.

Il nodo è collegato al nodo centrale di Fucino con una linea CDN a 10Mbps e da una VPN via Internet.

Inoltre tra il nodo SSDC ed il nodo del Fucino, tramite i firewall Fortigate, è configurata una Secure SD-WAN.

Lo schema seguente mostra la configurazione presso il nodo:

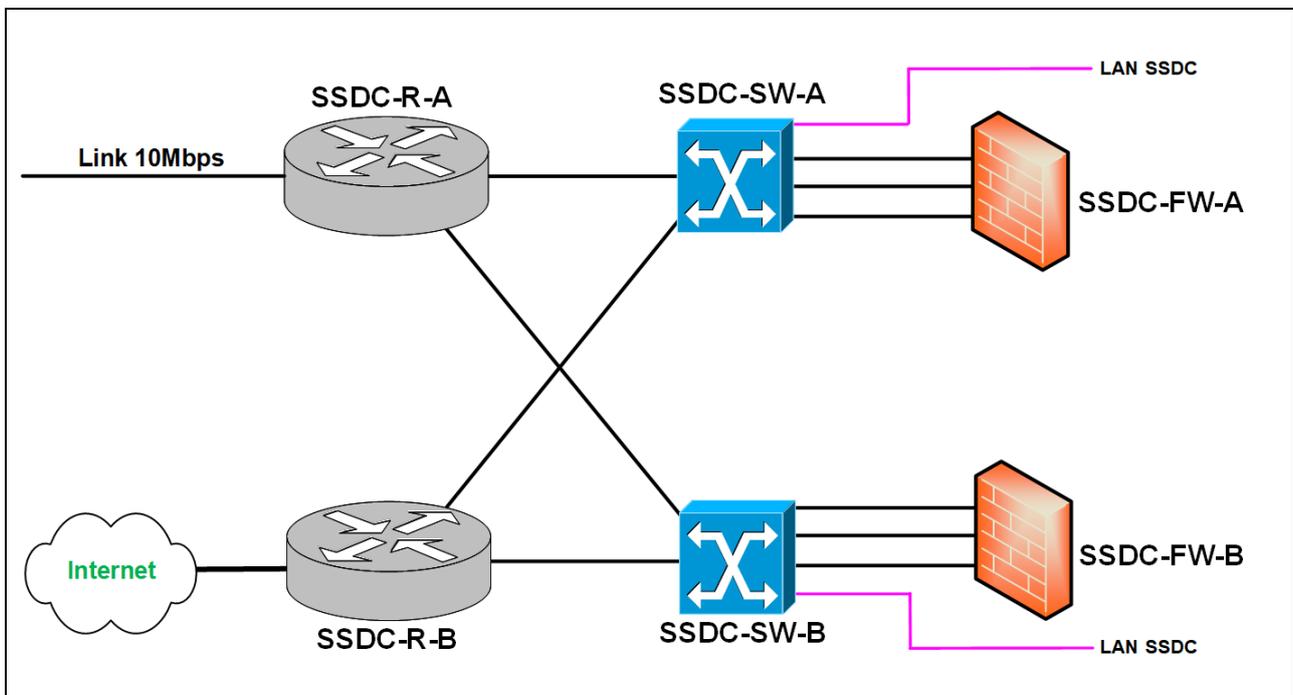


Figura 10: nodo ASDC

 <b>TELESPAZIO</b> una società LEONARDO e THALES	ID Doc.:	CSC0800000104-ADD01
	Edizione:	2.3
	Data:	20/11/2024

#### 4.1.8. ASI Roma

Questo nodo ha la funzione di connettere la sede ASI di Roma Tor Vergata con la rete ASINet sia per i collegamenti Voce/Video che dati.

L'architettura del nodo prevede sempre l'utilizzo di macchine modulari Cisco come filosofia consolidata nella rete, gli apparati installati sono CISCO ISR4331, switch CISCO serie 9200 e firewall Fortigate FG-101F.

Il nodo è collegato al nodo centrale di Fucino con una linea CDN a 10Mbps e da una VPN via Internet.

Inoltre tra il nodo di ASIRM ed il nodo del Fucino, tramite i firewall Fortigate, è configurata una Secure SD-WAN.

Si riporta di seguito lo schema relativo al nodo ASI di Roma Tor Vergata:

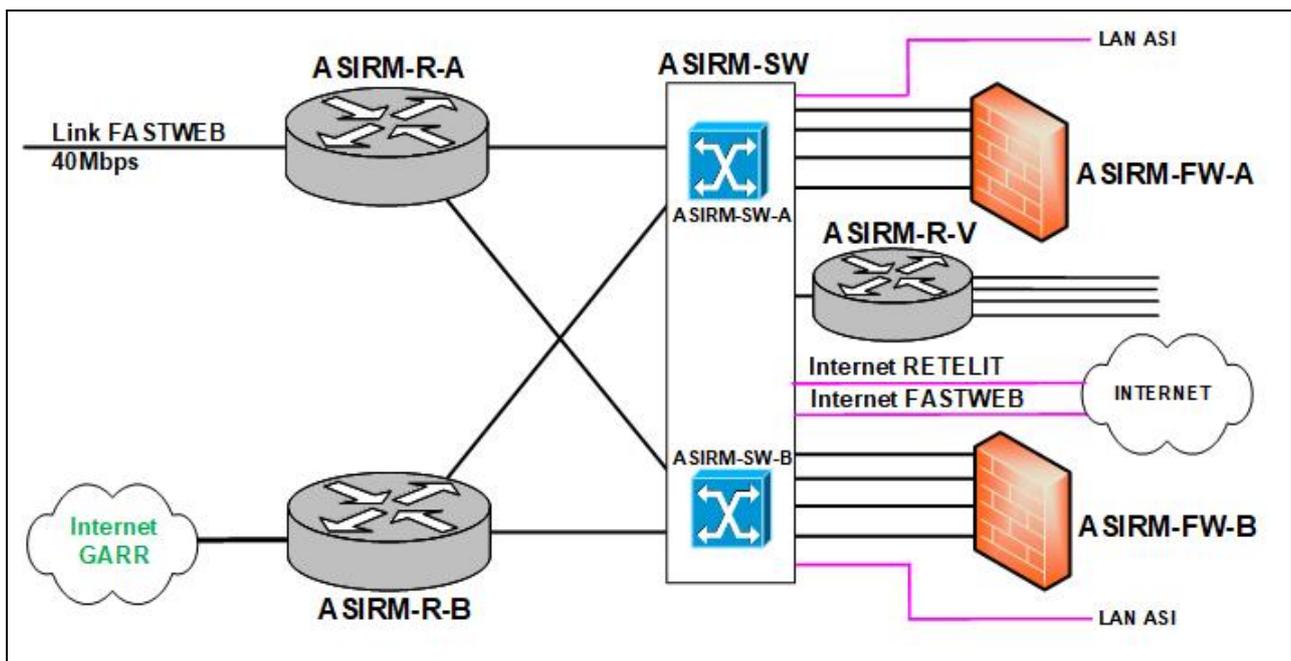


Figura 11: nodo Roma Tor Vergata

 una società LEONARDO e THALES	ID Doc.:	CSC0800000104-ADD01
	Edizione:	2.3
	Data:	20/11/2024

#### 4.1.9. ESOC

L'architettura del nodo ESOC prevede sempre l'utilizzo di macchine modulari Cisco come filosofia consolidata nella rete, gli apparati sono della famiglia isr4300.

Si riporta di seguito lo schema relativo al nodo ASI di ESOC:

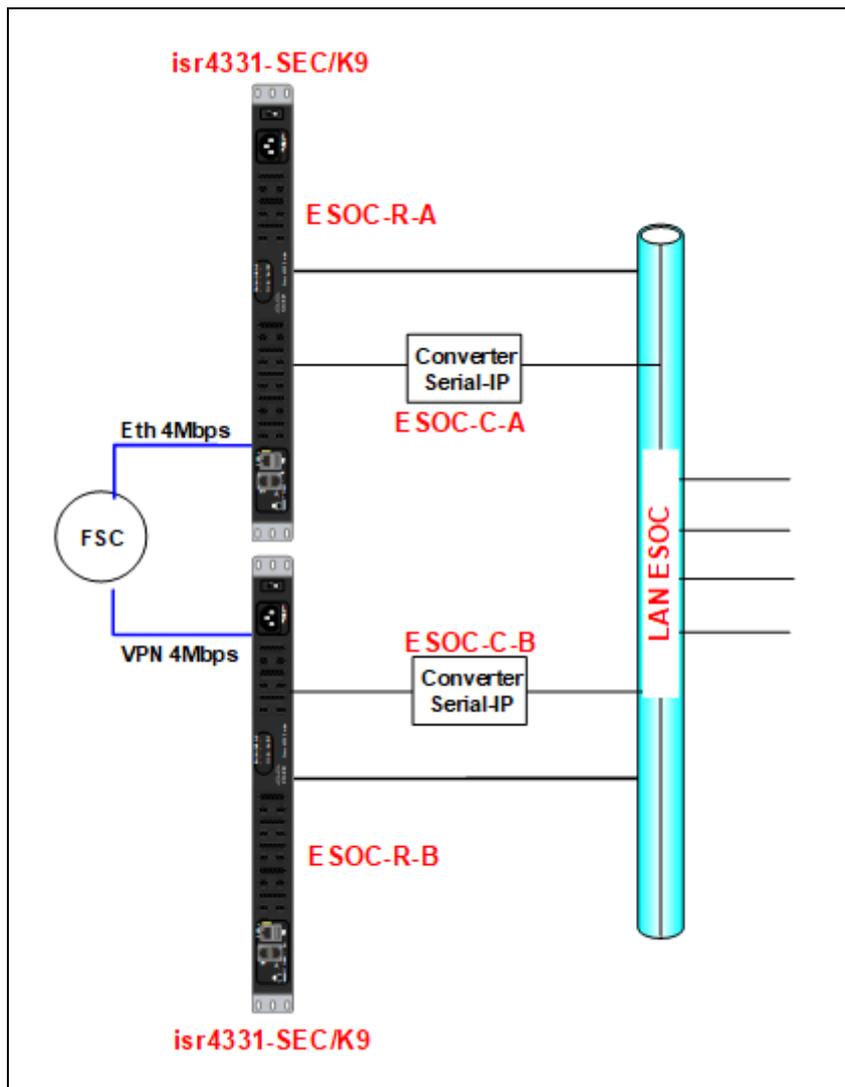


Figura 12: nodo ESOC

 una società LEONARDO e THALES	ID Doc.:	CSC0800000104-ADD01
	Edizione:	2.3
	Data:	20/11/2024

#### 4.1.10. KOUROU

Nel nodo di Kourou non è previsto alcun apparato IP ma solo una stazione VSAT per collegarsi in V35 con Malindi ad una velocità di 128Kbps.

Di seguito si riporta lo schema:

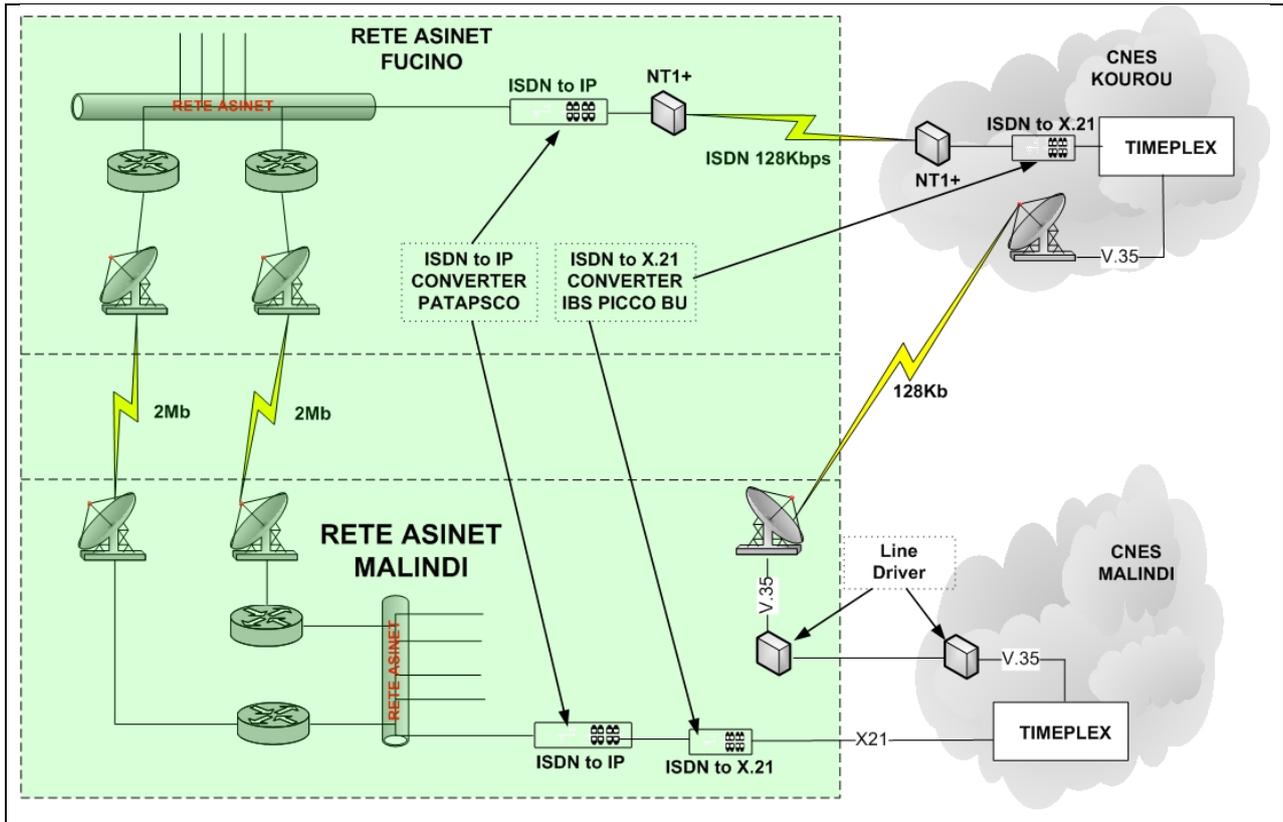


Figura 13: nodo KOUROU

 una società LEONARDO e THALES	ID Doc.:	CSC0800000104-ADD01
	Edizione:	2.3
	Data:	20/11/2024

#### 4.1.11. SDSA

Questo nodo ha la funzione di connettere la sede ASI presso il SRT (Radio Telescopio Sardinia) per i collegamenti Voce e dati con il JPL ed ESOC.

L'architettura del nodo prevede sempre l'utilizzo di macchine modulari Cisco come filosofia consolidata nella rete, gli apparati sono gli ISR4331.

Si riporta di seguito lo schema relativo al nodo SDSA:

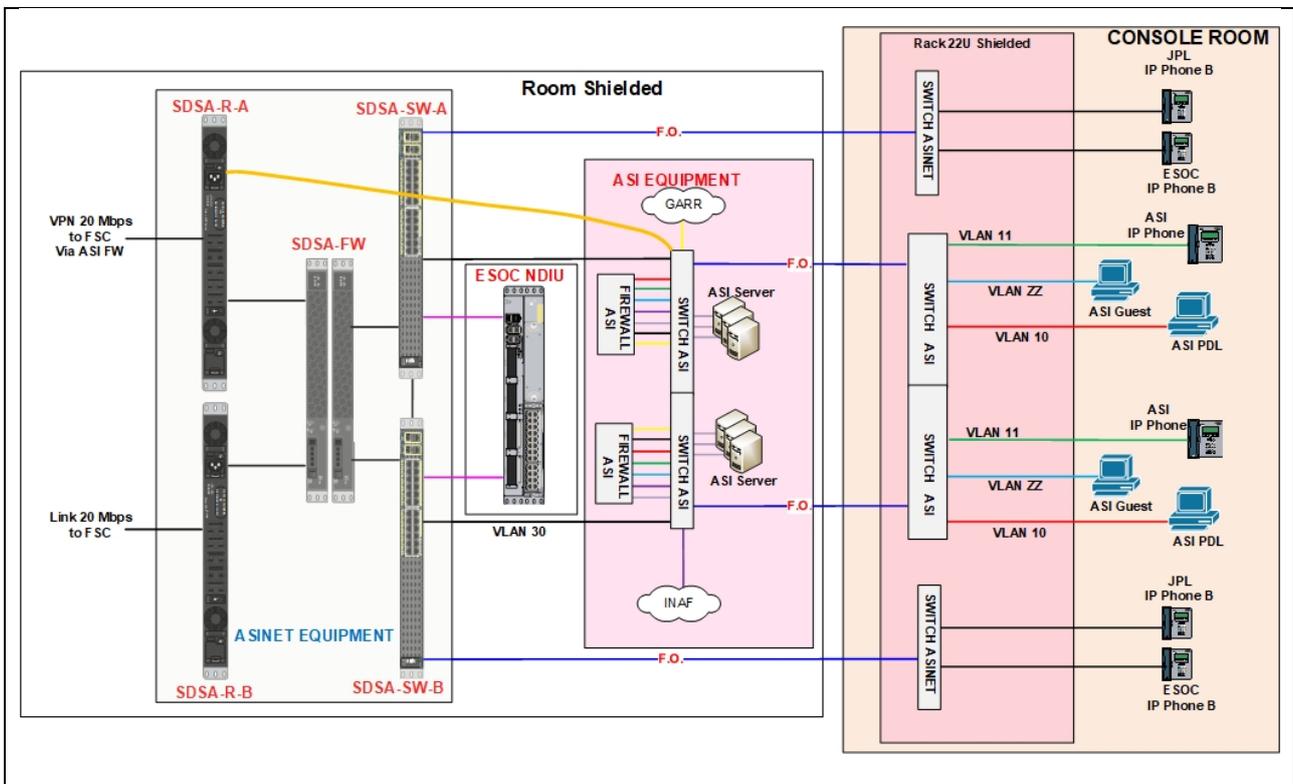


Figura 14: nodo SDSA

#### 4.1.12. NAPOLI

Il nodo di Telespazio Napoli ha una configurazione tipo, composta da due router Cisco ISR4331, da due switch CISCO 2960CX, da due firewall NGF CISCO ASA5506X ed un voice router Cisco C881. Il nodo è collegato al nodo del Fucino con un link a 10Mbps ed una VPN IPSec via Internet

Lo schema seguente mostra la configurazione presso il nodo.

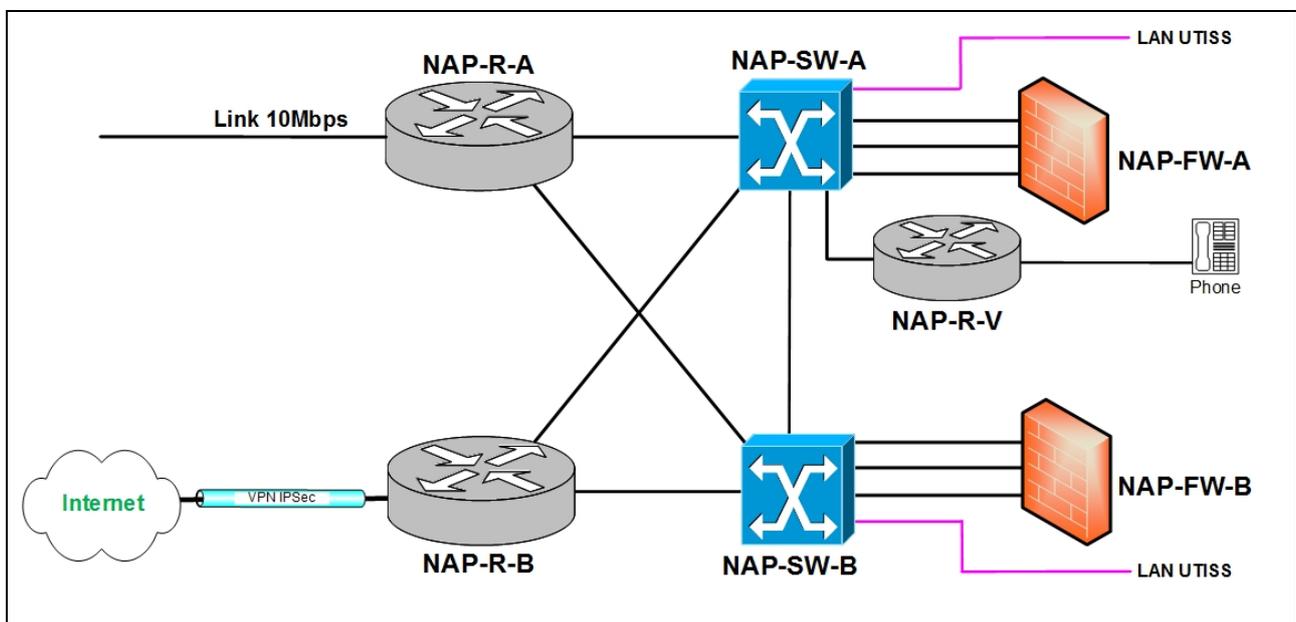


Figura 15: nodo NAPOLI

 <b>TELESPAZIO</b> <i>una società LEONARDO e THALES</i>	ID Doc.:	CSC0800000104-ADD01
	Edizione:	2.3
	Data:	20/11/2024

#### 4.1.13. ARGOTEC

Il nodo di ARGOTEC ha una configurazione tipo, composta da due router Cisco ISR4331, da due switch CISCO 2960CX, da due firewall NGF CISCO ASA5506X ed un voice router Cisco C881. Il nodo è collegato al nodo del Fucino con un link a 10Mbps ed una VPN IPSec via Internet.

Lo schema seguente mostra la configurazione presso il nodo.

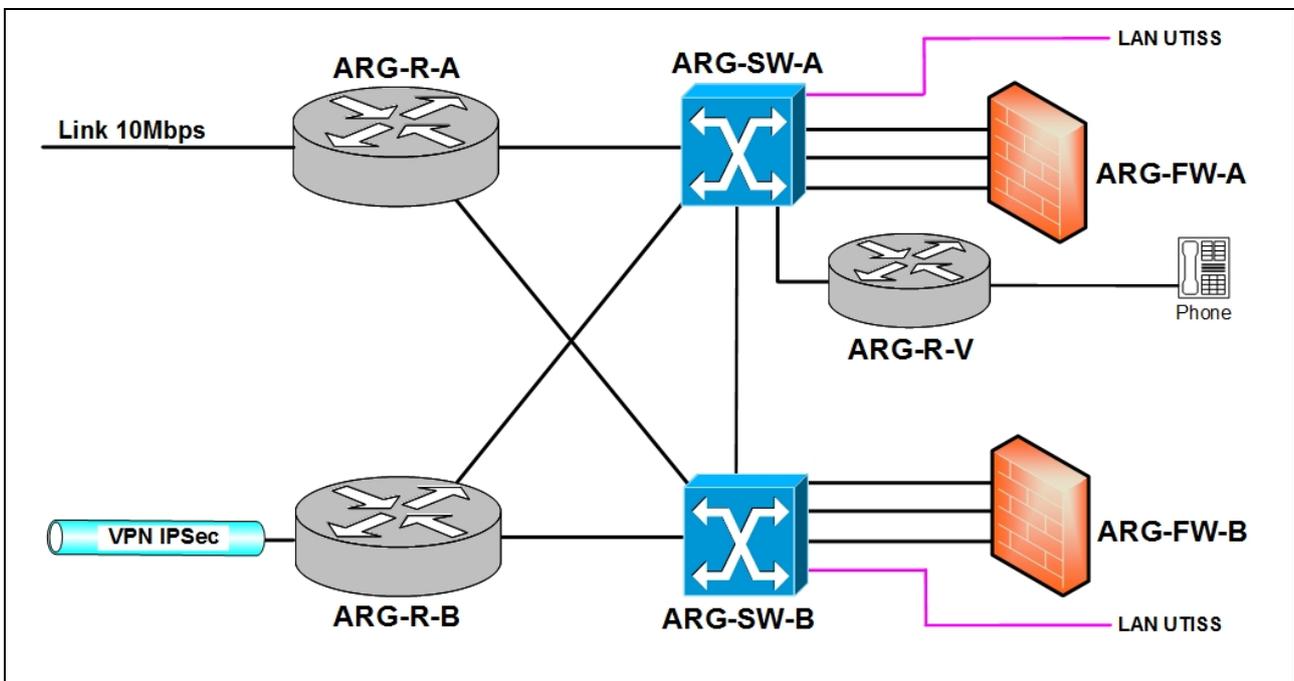


Figura 16: nodo ARGOTEC