



Documentazione contrattuale per prestazioni di supporto al committente

Allegato:

- A5 – Documentazione di progetto

Committente	Ufficio Federale delle Strade USTRA
Nome del progetto	SA-CH TP IP-Netz BSA GEIV (F5)
Abbreviazione del progetto	SACHBSA IV
Numero del progetto	200022
Oggetto	Documentazione di appalto per prestazioni di supporto al Committente

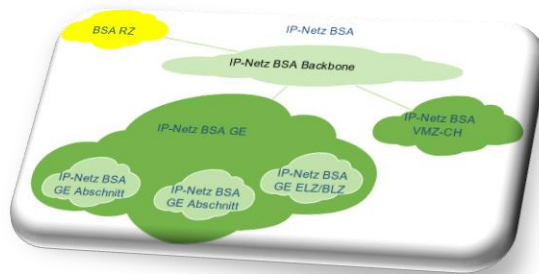


Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Dipartimento federale
dell'ambiente, dei trasporti, dell'energia e delle comunicazioni DATEC

Ufficio federale delle strade USTRA
Filiale Bellinzona

Strada Nazionale N02-N13 / Perimetro UT-IV



N2 Chiasso - Airolo N13 Castione – Roveredo Nord

Cantone /Comune	TI & GR /
Tratta / Km di manutenzione	-
RBBS	-
TdCost	080093
Lotto / Oggetto	-
Numero inventario	21.02.72.899.01
Categoria struttura	K T/G T/U ■ BSA

Studio preliminare

Migrations-Konzept IP – Netz BSA in der GE-IV

Progettista

ingegnara

Via delle Pergole 9
CH-6598 Tenero
www.ingegna.ch

Documento No.

Rev.	Allestito	Indice A	Indice B	Indice C	Indice D	No. interno ufficio:	0067.2
Data	20.11.2019	28.01.2020	28.02.2020			Numero oggetto di inventario:	21.02.72.899.01
Visto	AG	AG	AG			Formato:	A4
Controllo	ES	ES	ES			Scala:	-

Conduzione di progetto

Ufficio federale delle Strade USTRA
Filiale Bellinzona
Via C. Pellandini 2
6500 Bellinzona

Entrata:	-
Verificato / Ing. verificatore:	-
Delibera:	

Concetto di migrazione – Rete IP BSA UT IV

Impressum

Data di creazione / revisione:	20.11.2019 / 28.02.2020
Autore:	Alain Gatti / Enrico Santinelli
Directory / Nome file:	0067.2_Rete IP BSA Concetto di migrazione_UTIV_v1-1
Numero pagine:	51
Approvato il:	
Approvato da:	

Indice delle modifiche

Versione	Data	Autore	Oggetto
0.9	20.11.2019	AG/ES	Prima bozza del documento
1.0	28.01.2020	AG/ES	Bozza rossa dopo prima review
1.1	28.02.2020	AG/ES	Versione definitiva dopo seconda review

Indice

Concetto di migrazione – Rete IP BSA UT IV	2
A. Management summary (IT)	6
1. Introduzione	6
2. Situazione attuale	6
3. Obiettivo strategico Rete IP BSA UT	6
4. Misure e proposte di attuazione	7
5. Costi	7
6. Termini	8
B. Management summary (DE)	9
1. Einleitung	9
2. IST-Zustand	9
3. Strategisches Ziel Migrationskonzept IP-Netze BSA GE	9
4. Massnahmen und Umsetzungsvorschläge	10
5. Kosten	10
6. Termine	11
C. Concetto di migrazione	12
1. Introduzione	12
1.1. Obiettivi e scopo del documento	12
1.2. Destinatari	12
1.3. Documenti di riferimento	12
2. Situazione attuale Rete IP BSA UT IV	13
2.1. Premessa	13
2.2. Introduzione generale	13
2.3. Rete di comunicazione COM	13
2.3.1. Rete dorsale COM	14
2.3.2. Reti di campo	16
2.3.3. Protocolli di routing	18
2.3.4. Concetto SNMP	18
2.3.5. Concetto NTP	18
2.3.6. Integrazione servizi dati, voce e video	18
2.3.7. Concetto QoS, qualità del servizio	18
2.3.8. Integrazione video	19
2.3.9. Connessioni WAN	19
2.3.10. Accesso remoto (RAS) SSL-VPN	20
2.3.11. Collegamento VMZ-CH	21
2.3.12. Accesso a servizi COM da rete VM-CH	21
2.3.13. Integrazione Boschung	22
2.3.14. Interfaccia verso la RSC	22
2.3.15. Interfaccia verso la CECAL	22
2.3.16. Shared DMZ	22

2.4.	Sistemi di gestione e sicurezza	23
2.4.1.	Hardware VMS/NMS	23
2.4.2.	Virtual Machine CT NMS	27
2.4.3.	Virtual Machine Argomon	27
2.4.4.	Virtual Machine SolarWinds NCM (NMS Tools)	27
2.4.5.	Sicurezza	28
2.5.	Infrastruttura passiva	29
2.6.	Infrastruttura attiva	29
2.6.1.	Componenti hardware	29
2.7.	Particolarità della rete COM UT IV	32
2.7.1.	Video Management System (VMS)	32
2.8.	Esercizio	33
3.	Visione futura Rete IP BSA UT IV	34
3.1.	Introduzione	34
3.2.	Rete IP BSA UT IV	34
3.2.1.	Rete dorsale	34
3.2.2.	Rete di campo impianti BSA	36
3.2.3.	Protocolli di routing	37
3.2.4.	Concetto SNMP	37
3.2.5.	Concetto di sincronizzazione della rete	37
3.2.6.	Integrazione Servizi Dati, Voce e Video	37
3.2.7.	Concetto QoS, qualità del servizio	37
3.2.8.	Integrazione video	37
3.2.9.	Connessioni con altre reti	37
3.3.	Sistemi di gestione e sicurezza	38
3.3.1.	NMS	38
3.3.2.	Gestione degli indirizzi IP	38
3.3.3.	Accesso remoto (RAS) SSL-VPN	38
3.3.4.	System Log (Syslog)	39
3.4.	Infrastruttura passiva	40
3.5.	Infrastruttura attiva	40
3.5.1.	Componenti hardware	40
4.	Processo di migrazione e termini	41
4.1.	Tappa 1 – Galleria Mappo-Morettina	41
4.2.	Tappa 2 – Pianificazione migrazione	42
4.3.	Tappa 3 – Realizzazione migrazione COM vs. rete IP BSA	43
4.4.	Termini esterni	47
4.5.	Riassunto delle misure previste	48
5.	Stima costi e pianificazione finanziaria	49
6.	Ripercussioni sull'esercizio	51
6.1.	Organizzazione	51
6.2.	Risorse e competenze	51
6.3.	Costi	51
7.	Prossimi passi	52

8.	Glossario	53
9.	Indici	55
10.	Allegati	56

A. Management summary (IT)

1. Introduzione

Il presente studio preliminare ha lo scopo di mostrare il concetto di migrazione dell'attuale rete IP BSA dell'unità territoriale IV (UT IV), denominata in seguito COM, per renderla conforme alle direttive USTRA.

Il concetto di migrazione indica pertanto le misure da attuare per adempiere a livello tecnico, organizzativo e di esercizio alla direttiva ASTRA 13040 Rete IP BSA [1], definendo allo stesso tempo una tempistica di realizzazione (roadmap) con i relativi costi.

2. Situazione attuale

L'attuale rete COM, appartenente a USTRA, è la rete di comunicazione dorsale che collega tutti gli impianti BSA delle strade nazionali nel perimetro di competenza di UT IV ai sistemi di gestione centralizzati, e che collega tutte le sezioni fra di loro con un'architettura magliata, ridondata e collapsed core-distribution-access.

La rete COM si basa su infrastrutture passive e attive proprie ed è completamente separata dalle reti cantonali, alle quali è però interfacciata per lo scambio di servizi utili all'esercizio delle strade nazionali.

La rete COM è stata rinnovata nel 2018 ed impiega prodotti Cisco della serie 4500 con link da 10 Gbps tra i nodi di comunicazione principali (core) e con link da 1 Gbps verso i nodi di access. Alcuni nodi dislocati (distribution) della serie Cisco 3800 ed alcuni nodi di espansione (access) della serie Cisco 2900 completano l'architettura di rete.

La rete COM dispone solo di poche reti di campo gestite e proprie, le quali utilizzano switch di campo del tipo Cisco IE2000/4000. La maggior parte delle reti di campo non sono gestite e sono messe a disposizione dai singoli impianti BSA.

La sicurezza è garantita da un firewall e da una DMZ.

Come protocollo di trasmissione è impiegato l'IPv4. La versione IPv6 non è impiegata, anche se le componenti di rete principali sono in grado di sopportarla.

La rete COM è gestita e sorvegliata dai tool Argomon/nagios e Solarwinds. La rete integra anche la gestione delle sorgenti e destinazioni video.

La rete COM è realizzata e gestita da un solo fornitore con uno standard omogeneo in tutto il territorio, fornitore che è anche responsabile della sicurezza perimetrale e dell'accesso remoto agli impianti.

Le differenze tra l'attuale rete COM ed i requisiti della futura rete IP BSA UT IV richiesta sono state valutate precedentemente nell'ambito di un'analisi denominata "GAP-Analyse" [4].

3. Obiettivo strategico Rete IP BSA UT

L'obiettivo strategico di USTRA è quello di realizzare per ogni unità territoriale (UT) reti IP BSA standardizzate, proprie e dedicate unicamente agli impianti BSA delle strade nazionali, che coprano dal livello core al livello access, comprese le reti di campo. Le reti dorsali ("Erschliessungsringe") delle singole UT dovranno essere realizzate entro fine 2025.

Secondo la direttiva [1], sono richieste reti Carrier-Grade MPLS con la possibilità di link fino a 100 Gbps tra i nodi principali che saranno interfacciate con il backbone IP-Netz BSA messo a disposizione dalla confederazione. Inizialmente sono consigliati e ammessi link da 10 Gbps tra i nodi principali.

4. Misure e proposte di attuazione

Per poter adempiere alle richieste, sono previste e riassunte le seguenti misure principali:

- Installazione di nuovi router con tecnologia MPLS con, inizialmente, link da 10 Gbps estendibili a 100 Gbps, che supportano IPv6.
- Realizzazione di reti di campo multiutente gestibili e integrabili nell'NMS, che supportano IPv6.
- Fornitura di un sistema di sincronizzazione degli equipaggiamenti all'interno della rete di tipo PTP e SyncE.
- Integrazione della gestione degli indirizzi IP della rete IP BSA UT IV nel tool IPAM centralizzato a livello nazionale.
- Ampliamento dell'NMS per l'integrazione delle funzionalità degli switch/router MPLS.
- Adattamento delle modalità di accesso remoto alla rete da parte di terzi.
- Implementazione del tool NAC messo a disposizione da USTRA.
- Installazione di un server Syslog per la raccolta dei log di tutti gli equipaggiamenti della rete.

L'attuazione delle misure elencate è suddivisa in tre tappe distinte, allo scopo di rispettare i tempi previsti e richiesti da USTRA:

- Realizzazione di due nodi principali MPLS e di due firewall, integrazione in IPAM e integrazione nel backbone IP-Netz BSA svizzero.
- Pianificazione della migrazione con attività preliminari come l'allestimento dei documenti di riferimento, l'adattamento dei sistemi di sicurezza/gestione, la progettazione e la messa in appalto della rete core ("Erschliessungsring") e delle reti di campo.
- Realizzazione della rete core ("Erschliessungsring") e delle reti di campo.

5. Costi

I costi per l'attuazione delle misure indicate (costi di investimento) si aggirano a ca. CHF 9.165 Mio ($\pm 30\%$). Oltre ai costi d'investimento sono da prevedere costi ricorrenti annuali di ca. CHF 400'000.

Per i costi indicati sono necessarie le seguenti precisazioni:

- L'acquisizione e la formazione di personale specialistico non sono considerate nei costi indicati.
- La creazione di un nuovo VMS UT IV, attualmente integrato nella COM, non è considerata nei costi indicati.
- I costi dei nodi principali della sezione Mappo-Morettina non sono considerati nei costi, in quanto a carico del progetto di integrazione della sezione nelle strade nazionali.
- Sono stati considerati moduli ottici per la trasmissione 10 Gbps.
- Il costo per la realizzazione delle reti di campo, attualmente messe a disposizione dai singoli impianti BSA, ammonta a ca. CHF 5.439 Mio ($\pm 30\%$).

6. Termini

La migrazione ed i rispettivi termini sono stati pianificati in base ai termini richiesti da USTRA. Nell'allegato [10] è rappresentato un piano termini generale delle tappe e delle attività previste, dal quale possono essere estrapolati i termini principali seguenti:

- 2020
 - Generazione di progetto e pianificazione dei crediti
- 2021
 - Allestimento documenti di riferimento
 - Fornitura e realizzazione nodi MPLS Galleria Mappo-Morettina
 - Adattamento sistemi di sicurezza/gestione
 - Integrazione backbone IP-Netz BSA, IPAM, NAC
 - Progettazione core UT IV rete IP BSA
- 2022
 - Appalti e aggiudicazione core UT IV rete IP BSA
 - Progettazione reti di campo UT IV
- 2023
 - Appalti e aggiudicazione reti di campo UT IV
- 2024-2025
 - Realizzazione core UT IV ("Erschliessungsring") rete IP BSA e alcune reti di campo UT IV
- 2026-2028
 - Realizzazione reti di campo UT IV restanti

B. Management summary (DE)

1. Einleitung

Ziel der vorliegenden Vorstudie ist es, die Migrationsplanung des bestehenden Netzwerkes der Gebietseinheit IV (GE IV), das sogenannte COM, zu zeigen, um die neue ASTRA-Richtlinie zu erfüllen.

Die Migrationsplanung zeigt demzufolge die Umsetzungsmassnahmen für die technische, organisatorische und betriebliche Erfüllung der Richtlinie ASTRA 13040 IP-Netz BSA [1], welche ebenfalls die entsprechenden Umsetzungstermine (Roadmap) und -kosten zeigt.

2. IST-Zustand

Das bestehende COM (Eigentümer ASTRA) ist das Netzwerk, welches alle BSA der Nationalstrassen innerhalb der GE IV Perimeters mit dem übergeordneten Leitsystem zusammenschliesst. Das Netzwerk verbindet alle Abschnitte mit einer vermaschte, redundante und collapsed core-distribution-access Architektur zusammen.

Das COM-Netzwerk basiert auf eigenen passiven und aktiven Infrastrukturen. Es ist von den kantonalen Netzwerken getrennt. Trotz sind Schnittstellen mit den kantonalen Netzwerken vorhanden, um Austausch von Diensten für den Betrieb der Nationalstrassen zu erlauben.

Das COM wurde im Jahr 2018 erneuert. Es besteht aus Cisco-Komponenten der Serie 4500 mit 10 Gbps Links zwischen den Hauptknoten (Core) und 1 Gbps Links zu den Access-Knoten. Einige abgesetzte Knoten (Distribution) der Serie Cisco 3800 und erweiterte Knoten (Access) der Serie Cisco 2900 vervollständigen die Netzwerkarchitektur.

Das COM verfügt über wenige eigene und verwaltete Feldnetzwerke, welche aus Switches des Typen Cisco IE2000/4000 bestehen. Die meisten Feldnetzwerke sind nicht verwaltet und sind von den einzelnen BSA zur Verfügung gestellt.

Die Sicherheit des Netzwerkes ist von einem Firewall und einem DMZ gewährleistet.

Als Übertragungsprotokoll ist IPv4 verwendet. Die Version IPv6 ist nicht eingesetzt, auch wenn sie von den COM-Komponenten unterstützt wird.

Das Netzwerk ist mit den Tools Argomon/Nagios und Solarwinds verwaltet und überwacht. Die Verwaltung der Video-Quellen und -Senken ist ebenfalls vom Netzwerk gewährleistet.

Das COM-Netzwerk wurde realisiert und ist vom selben Lieferanten verwaltet. Das Netzwerk ist mit demselben Standard überall im Perimeter verwaltet. Der Lieferant ist ebenfalls für die Sicherheit und der BSA-Fernzugriff zuständig.

Die Abweichungen zwischen dem bestehenden COM-Netzwerk und dem zukünftigen IP-Netz BSA wurden in einer vorherigen Phase mittels sogenannter "GAP-Analyse" [4] aufgelistet.

3. Strategisches Ziel Migrationskonzept IP-Netze BSA GE

Das strategische Ziel des ASTRA ist es, für jede Gebietseinheit (GE) standardisierte, eigene und für die BSA der Nationalstrassen dedizierte Netzwerke zu realisieren, welche von der Ebene Core bis zur Ebene Access, inkl. Feldnetzwerken, abdecken. Die Erschliessungsringe der einzelnen GE müssen vor Ende 2025 realisiert werden.

Gemäss Richtlinie [1] sind Carrier-Grade MPLS Netzwerke angestrebt, welche Links bis zu 100 Gbps zwischen den Hauptknoten, die mit dem nationalen Backbone IP-Netz BSA angeschlossen werden, ermöglichen. Anfänglich sind Links von 10 Gbps zwischen den Hauptknoten empfohlen und zugelassen.

4. Massnahmen und Umsetzungsvorschläge

Um die Anforderungen zu erfüllen, sind folgende Hauptmassnahmen vorgesehen und zusammengefasst:

- Installation neuen MPLS-Routers mit Initialbestückung von Links 10 Gbps, erweiterbar bis 100 Gbps, welche IPv6 fähig sind.
- Realisierung von verwaltbaren und ins NMS integrierbaren Feldnetzwerken, welche IPv6 fähig sind.
- Lieferung von einem Synchronisationssystem Typ PTP und SyncE für alle Ausrüstungen innerhalb des Netzwerkes.
- Integration der IP-Adressen Verwaltung des IP-Netzes BSA GE IV ins schweizweite und zentralisierte IPAM-Tool.
- Erweiterung des NMS für die Integration der Funktionalitäten der MPLS-Switches/Routers.
- Anpassung des Netzwerk-Fernzugriffs durch Dritte.
- Umsetzung des vom ASTRA zur Verfügung gestellten NAC-Tools.
- Installation eines Syslog-Servers für die Logsammlung aller Netzwerkausrüstungen.

Die Umsetzung der erwähnten Massnahmen ist, um die geforderten ASTRA-Termine einzuhalten, in drei Etappen geteilt:

- Realisierung von zwei Hauptknoten MPLS und zwei Firewalls, Integration ins IPAM-Tool und Integration in das schweizweite Backbone IP-Netz BSA.
- Migrationsplanung mit vorbereitenden Massnahmen, wie die Erstellung der Referenzdokumente, die Anpassung der Sicherheits-/Verwaltungssysteme, die Projektierung und Ausschreibung des Netzwerkes Erschliessungsring und der Feldnetzwerke.
- Realisierung des Netzwerkes Erschliessungsring und der Feldnetzwerke.

5. Kosten

Die Umsetzungskosten der erwähnten Massnahmen, Investitionskosten, betragen ca. CHF 9.165 (±30%). Zusätzlich sind wiederkehrende jährliche Kosten von ca. CHF 400'000 vorzusehen.

Für die geschätzten Kosten sind folgende Präzisierungen notwendig:

- Die Beschaffung und die Schulung vom Fachpersonal sind nicht in den erwähnten Kosten berücksichtigt.
- Die Realisierung eines neuen VMS GE IV, welches zurzeit in das COM integriert ist, ist nicht in den erwähnten Kosten berücksichtigt.
- Die Kosten der Hauptknoten des Abschnittes Mappo-Morettina sind nicht in den Kosten berücksichtigt, da sie in das Projekt für die Integration des Abschnittes in die Nationalstrassen belasten werden.
- Es wurden optische Module für eine Übertragung von 10 Gbps berücksichtigt.
- Die Kosten für die Feldnetzwerken, welche zurzeit von den einzelnen BSA zur Verfügung gestellt werden, betragen ca. CHF 5.439 Mio (±30%).

6. Termine

Die Migrationsplanung und die entsprechenden Termine wurden gemäss ASTRA-Termine festgelegt. Im Anhang [10] ist ein Terminplan mit den vorgesehenen Etappen und Terminen dargestellt, bei welcher folgende Termine eruiert werden können:

- 2020
 - Projektgenerierung und Kreditanfragen
- 2021
 - Erstellung Referenzdokumente
 - Lieferung und Realisierung MPLS-Knoten Tunnel Mappo-Morettina
 - Anpassung Sicherheits-/Verwaltungssysteme
 - Integration Backbone IP-Netz BSA, IPAM, NAC
 - Projektierung Erschliessungsring IP-Netz BSA GE IV
- 2022
 - Ausschreibung und Vergabe Erschliessungsring IP-Netz BSA GE IV
 - Projektierung Feldnetzwerken GE IV
- 2023
 - Ausschreibung und Vergabe Feldnetzwerken GE IV
- 2024-2025
 - Realisierung Erschliessungsring IP-Netz BSA GE IV und einige Feldnetzwerke GE IV
- 2026-2028
 - Realisierung übrige Feldnetzwerke GE IV

C. Concetto di migrazione

1. Introduzione

1.1. Obiettivi e scopo del documento

USTRA ha avviato da alcuni anni, nell'ambito del programma generale "Architettura di sistema Svizzera (SA-CH)", diversi progetti destinati a uniformare e standardizzare tutti gli equipaggiamenti di esercizio e sicurezza (BSA) delle strade nazionali.

Come è noto gli impianti BSA sono essenziali per la sicurezza dell'utenza su tutte le strade nazionali, siano queste in tunnel o a cielo aperto. Per poter funzionare in maniera efficiente, gli impianti BSA necessitano di sistemi di telecomunicazione performanti, altamente disponibili e omogenei.

Tramite la direttiva ASTRA 13040 Rete IP BSA [1], USTRA vuole uniformare appunto i sistemi di telecomunicazione destinati agli impianti BSA modernizzandoli e orientandoli al futuro. La direttiva mostra l'architettura di rete da realizzare per il backbone svizzero e per le rispettive reti subordinate delle unità territoriali (UT) con le relative interfacce verso gli impianti BSA.

Il presente documento ha lo scopo di mostrare il concetto di migrazione dell'attuale rete IP BSA dell'unità territoriale IV (UT IV), denominata in seguito COM, per renderla conforme alle direttive USTRA. Il concetto di migrazione indica pertanto le misure da attuare per adempiere a livello tecnico, organizzativo e di esercizio alla direttiva ASTRA 13040 Rete IP BSA [1], definendo allo stesso tempo una tempistica di realizzazione (roadmap) con i relativi costi.

Il concetto di migrazione delle Rete IP BSA UT IV è stato preceduto da un'analisi delle differenze ("GAP-Analyse") tra l'attuale COM ed i requisiti richiesti da USTRA. Questa analisi ha permesso di creare il documento [4], il quale funge da punto di partenza per la definizione delle misure da attuare.

1.2. Destinatari

Il documento è rivolto ai seguenti destinatari:

- Tecnici specialisti di USTRA
- Specialisti pianificatori della conservazione BSA di USTRA
- Capi progetto BSA di USTRA
- Tecnici specialisti di UT IV
- Progettisti mandatarî BSA per conto di USTRA

1.3. Documenti di riferimento

Il presente documento si basa sui documenti di riferimento seguenti:

- [1] Direttiva ASTRA 13040 IP-Netz BSA V1.2 (edizione 2017 in tedesco/francese)
- [2] Direttiva ASTRA 13030 Sicurezza IT dei sistemi di gestione e comando degli impianti elettromeccanici V1.21 (edizione 2016 in italiano)
- [3] Migrationskonzept IP-Netz BSA V1.2 (edizione del 04.02.2019 in tedesco)
- [4] IP-Netz BSA – GAP-Analyse F5-GEIV V1.0 (edizione del 01.03.2019 in tedesco)
- [5] IP-Netz BSA, IPv6, Adressierungskonzept (edizione del 11.02.2019 in tedesco)
- [6] IP-Netz BSA – FAQ V1.3 (edizione del 31.10.2019 in tedesco e francese)
- [7] Zielarchitektur IP-Netz BSA GE: Beispiele 1-4 V1.1 (edizione del 06.09.2019 in tedesco)

2. Situazione attuale Rete IP BSA UT IV

2.1. Premessa

Per quanto concerne l'infrastruttura stradale del Canton Ticino vi sono tre reti di comunicazione distinte sul territorio alle quali fanno capo i rispettivi servizi:

- Rete COM: rete di comunicazione per tutti gli equipaggiamenti BSA delle strade nazionali appartenente a USTRA.
- Rete RSC: rete di comunicazione per tutti gli equipaggiamenti BSA delle strade cantonali appartenente al Canton Ticino.
- Rete CSI: rete di comunicazione amministrativa appartenente al Canton Ticino utilizzata anche per la Centrale comune d'allarme (CECAL).

Le tre reti di comunicazione si basano su infrastrutture passive e attive proprie e sono completamente separate tra loro, ma interfacciate per lo scambio di servizi utili all'esercizio.

La rete di comunicazione considerata nel presente concetto di migrazione è la rete COM e rientra nel perimetro di competenza di UT IV, comprendendo tutti i nodi di comunicazione sulla N2 Chiasso – Airolo e sulla N13 Gorduno – Roveredo.

Siccome dal 01.01.2020 la galleria Mappo-Morettina (LOG), attualmente appartenente alle strade cantonali ed allacciata alla rete RSC, diventerà di proprietà di USTRA, si è deciso di considerare nel presente concetto anche la sezione LOG. Al momento tra i nodi di comunicazione della sezione LOG ed i nodi di comunicazione della rete COM non vi sono collegamenti.

2.2. Introduzione generale

La rete IP BSA di UT IV è suddivisa in due livelli ben distinti e, in linea di principio, non interconnessi fra loro:

- Rete COM
- Rete di campo

La rete COM è la rete di comunicazione dorsale che collega tutti gli impianti BSA ai sistemi di gestione centralizzati e che collega tutte le sezioni fra di loro con un'architettura magliata e ridondata. La rete COM è realizzata e gestita da un solo fornitore con uno standard omogeneo in tutto il territorio.

Le reti di campo sono normalmente isolate, confinate nel perimetro di un impianto BSA e gestite dal fornitore dell'impianto stesso. Esistono però alcune eccezioni dove la rete COM, a partire dal suo nodo di sezione, è stata estesa con una rete di campo ad anello in grado di servire impianti BSA diversi e naturalmente sezionati virtualmente fra loro.

Il fornitore della rete COM è anche responsabile della sicurezza perimetrale e dell'accesso remoto agli impianti.

2.3. Rete di comunicazione COM

La rete di comunicazione COM è stata messa in servizio nel 2004.

Dal 2014 ha subito diverse espansioni in alcune gallerie con la creazione di reti KNA e nel corso del 2018 sono stati rinnovati integralmente gli switch della dorsale da Chiasso ad Airolo.

La rete COM a larga banda è basata sulla tecnologia Ethernet. Il protocollo IP su Ethernet permette il trasporto dei servizi dati, voce e video in maniera efficace e affidabile.

2.3.1. Rete dorsale COM

L'architettura della rete COM attualmente in servizio è basata sul modello a tre livelli:

1. Il livello dorsale (core layer): È composto dai nodi di rete principali definiti "core" che formano l'asse portante della rete, i quali utilizzano la tecnologia 10 GigabitEthernet (IEEE 802.3aq).
2. Il livello distribuzione (distribution layer): È composto dai nodi di rete secondari definiti "dislocati", o "server farm" per ospitare server, i quali utilizzano la tecnologia GigabitEthernet (IEEE 802.3z).
3. Il livello accesso (access layer): È composto dai nodi di rete definiti di "espansione" utilizzati normalmente per reti KNA, i quali utilizzano le tecnologie FastEthernet (IEEE 802.3 e IEEE 802.3u) e GigabitEthernet (IEEE 802.3z).

La Figura 1 offre una rappresentazione schematica di questi livelli.

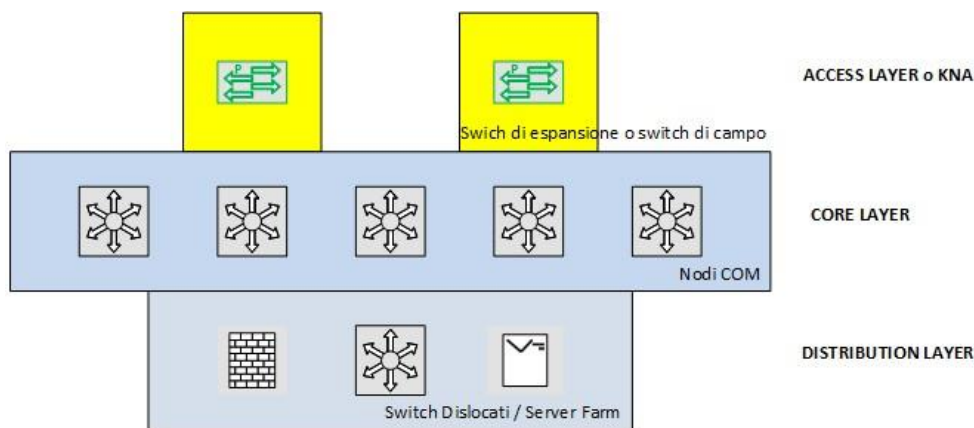


Figura 1: Livelli dell'architettura di rete COM

La prossima figura illustra lo schema di principio della rete COM, i nodi che la formano e i collegamenti tra di essi. I collegamenti tra i nodi sono garantiti da una rete cantonale di fibre ottiche formata da un tracciato di base lungo l'autostrada (dorsale 1 e 2) e un tracciato alternativo attraverso la rete dell'Azienda elettrica ticinese AET (vedi cap. 2.5). Lo stesso schema di principio è rappresentato a livello geografico nell

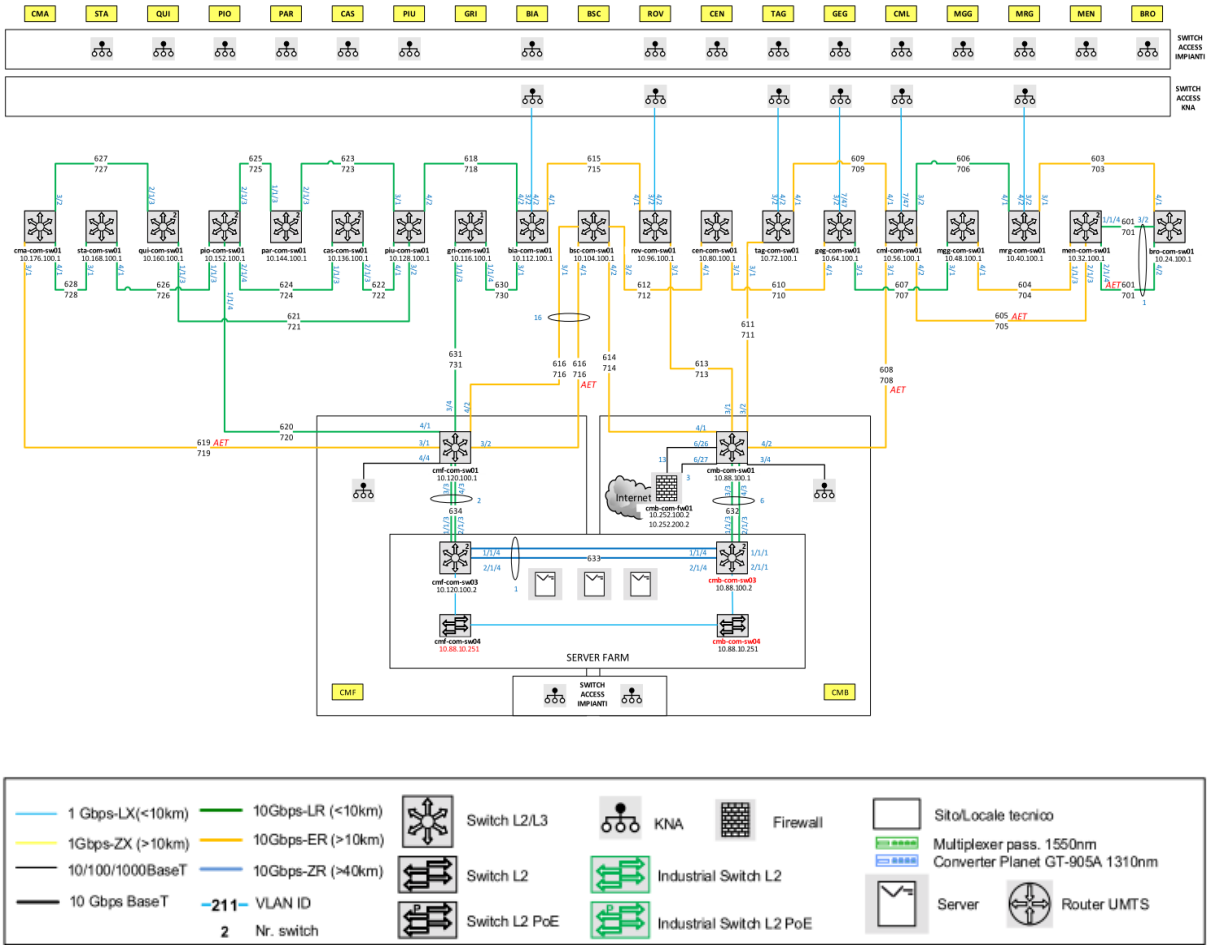


Figura 2: Schema della rete COM – Nodi principali

La rete COM presenta le seguenti caratteristiche di base:

1. È una rete dorsale 10 GigabitEthernet (IEEE 802.3aq) che utilizza in parallelo due tracciati in fibra ottica monomodale, creata utilizzando sistemi della ditta Cisco Systems.
2. Gli switch COM hanno un alto livello d'affidabilità e ridondanza. Sono installati sistemi con alimentazione e processori ridondanti. Inoltre, i tracciati in fibra ottica sono collegati su moduli diversi.
I collegamenti tra i nodi principali (core switch) sono sempre ridondanti tramite due collegamenti core-core.
3. I modelli di switch utilizzati sono i seguenti:

Core	Nodi core	Switch core	Cisco Catalyst 4507R
Distribution	Nodi dislocati	Switch distribution	Cisco Catalyst 3850
Access	Nodi espansione	Switch access	Cisco 2960X
Access	Nodi KNA	Switch di campo	Cisco IE2000/4000
4. I nodi COM Catalyst 4507R hanno un'architettura modulare, predisposti quindi per future espansioni. Anche gli switch Catalyst 3850 (nodi dislocati) permettono un'architettura modulare, in questo caso aggregando switch, in quanto il backplane di questi sistemi può essere collegato in stack con altri dello stesso tipo.
5. Tutti i nodi dislocati sono ridondanti (due switch collegati in stack) tranne a GRI.

6. Lo switch dislocato CMB serve al collegamento del firewall e alle sue DMZ.
7. Diverse gallerie dispongono di un anello locale KNA formato da switch di access e/o di campo per il collegamento dell'impianto locale VTV.
8. Tutti gli switch di campo (access switch) sono anch'essi sempre collegati in maniera ridondata ad altri switch di campo o a un core switch.
9. Utilizzo del protocollo IP per il trasporto di tutti i servizi. Questo permette l'utilizzo di tutti i meccanismi di routing dinamico, di ridondanze e di mantenimento della qualità del servizio, già standardizzati per il protocollo IP.

2.3.2. Reti di campo

Allo stato attuale vi sono reti di campo messe a disposizione dalla rete COM e reti di campo messe a disposizione dai singoli impianti BSA.

2.3.2.1. Reti di campo COM

Le reti di campo per gli impianti BSA messe a disposizione dalla rete COM sono rappresentate nella figura seguente e sono una minima parte rispetto al totale delle reti di campo messe a disposizione dagli impianti BSA (vedi cap. 0).

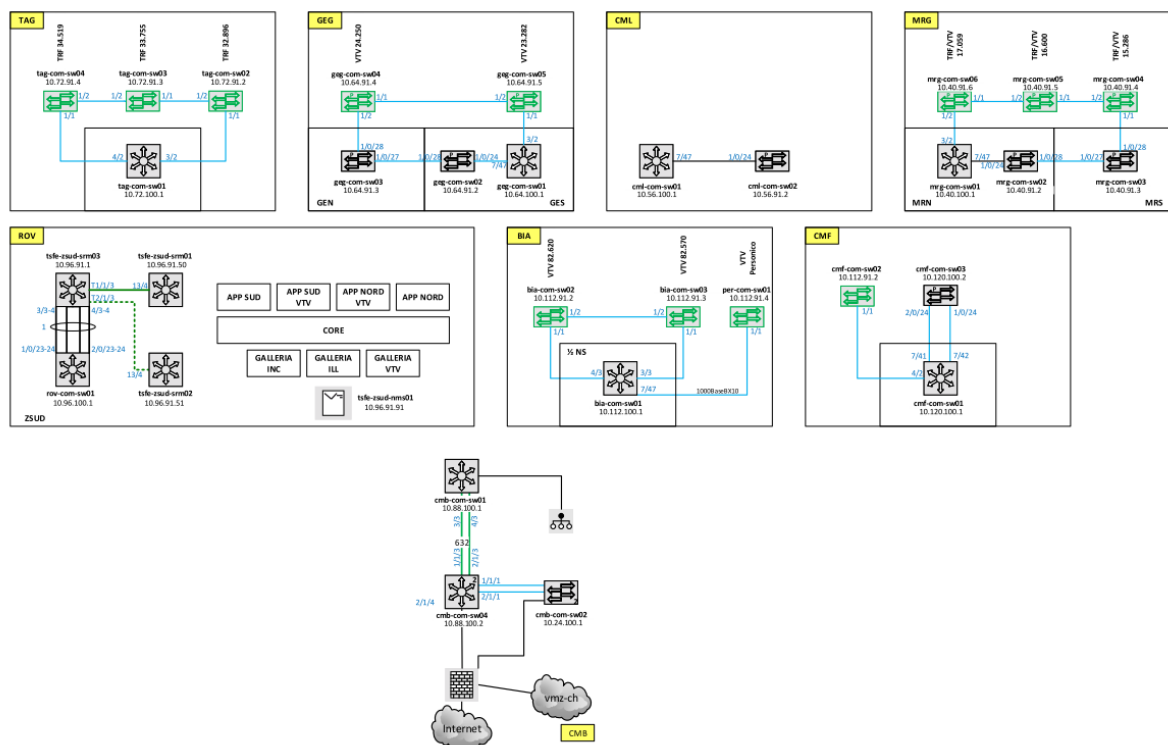


Figura 3: Reti di campo (impianti BSA) messe a disposizione dalla rete COM

Le reti di campo COM sono integrate nell'NMS e sono pertanto gestibili (managed).

2.3.2.2. Reti di campo impianti BSA

Nella maggior parte dei casi le reti di campo degli impianti BSA sono realizzate dagli impianti stessi. Nelle reti di campo degli impianti BSA se ne trovano di diverse tipologie:

- Gestibili (managed)
- Gestibili parzialmente (limited managed)
- Non gestibili (unmanaged)

Rete di campo	Impianto BSA										Totale
	VEN	IAU	ILL	INC	SGE	SOS	TRF	VTV	SVA	KNA	
Managed	1			1		1		6		2	8
BRO								1			1
GEG											0
MGG								1			1
MRG											0
ROV	1			1		1		1		2	6
TAG											0
Limited managed	5	12	5	3		14	12		1		48
BIA		1	1			1					3
CAS		1				1	1				3
CEN	1	1		1		1	1				5
CMB						1			1		2
CMF						1					1
GEG		1				1					2
MEN		1					1				2
MGG	1	1		1		1	1				5
MRG		1	1	1		1					4
PAR	1	1	1			1	1				5
PIO	1	1	1			1	1				5
PIU	1	1	1			1	1				5
QUI						1					1
STA		1				1	1				3
TAG		1				1					2
Unmanaged	1	2	8	6	9			1			27
BIA					1						1
BRO					1						1
BSC					1						1
CAS			1								1
CEN			1								1
CMA					1						1
CMB		1									1
CMF					1						1
CML		1									1
GEG	1		1	1							3
GRI			1		1						2
MGG			1								1
PAR				1	1						2
PIO				1							1
PIU				1	1			1			3
QUI			1		1						2
STA			1	1							2
TAG			1	1							2
Totali	7	14	13	10	9	15	12	7	1	2	83

Tabella 1: Reti di campo impianti BSA

2.3.3. Protocolli di routing

2.3.3.1. Routing unicast

È stato utilizzato il protocollo di routing standard OSPF (OSPFv2 per IPv4, basato sull'RFC2328).

2.3.3.2. Routing multicast

Per il trasporto efficace dei flussi multicast sulla rete COM si utilizza il protocollo di routing PIM-SM (Protocol Independent Multicast Sparse Mode, PIM-SM Version 2, IETF standard – RFC 2362). PIM può essere utilizzato con qualsiasi protocollo di routing unicast. Il protocollo PIM-SM richiede la definizione di “Rendez-vous Points” (RP's), che si occupano di registrare e gestire le sorgenti di flussi multicast. I seguenti nodi COM sono stati definiti come RP's:

- bsc-com-sw01
- cmf-com-sw01

Il protocollo MSDP (Multicast Source Discovery Protocol) si occupa di gestire la comunicazione tra i 2 RP's. I decoder Comerson (destinazioni) e le telecamere IP (sorgenti) utilizzano il protocollo IGMP v2 per associarsi e disassociarsi a un gruppo multicast.

2.3.4. Concetto SNMP

Il concetto SNMP prevede:

- Utilizzo di SNMP RO (read only)
- SNMP RW (read-write) è abilitato unicamente per permettere la configurazione dei nodi COM tramite SolarWinds
- Utilizzo di filtri (ACL) per permettere le query SNMP solo dalle stazioni NMS

2.3.5. Concetto NTP

Tramite il protocollo NTP e un appropriato concetto, viene sincronizzata l'ora di tutte le componenti del COM. Il Server NTP è messo a disposizione dall'SGE.

Tutte le componenti di rete in Ticino sincronizzano l'orologio con il nodo COM cmb-com-sw01. Mentre tutte le componenti della galleria di Roveredo di sincronizzano sul nodo COM rov-com-sw01. L'orologio del nodo COM cmb-com-sw01 viene sincronizzato con il server NTP 10.176.1.5 (cma-sge-ntp1).

2.3.6. Integrazione servizi dati, voce e video

La rete COM integra i servizi dati (SGE/GG, GO e CT), voce (impianti SOS) e video tramite appositi codec.

2.3.7. Concetto QoS, qualità del servizio

L'implementazione della qualità del servizio (QoS: Quality of Service) per la rete COM si basa sul modello DiffServ (Differentiated Service Architecture).

2.3.8. Integrazione video

L'integrazione del servizio video nella rete COM avviene tramite telecamere IP e codec video su IP.

Per gli impianti video rinnovati dopo il 2014 si è proceduto all'installazione di telecamere IP. La compressione video è H.264 con una risoluzione HD720p:1280x720 e un target bitrate di 2 Mbps da 25 fps. Anche le nuove telecamere sono state integrate nel sistema VMS.

Il server VMS installato presso il CMB gestisce l'apertura di flussi video dalle singole telecamere verso i monitor e verso il sistema Videowall installati presso la sala comando di Camorino su comando dell'SGE. Esso è anche responsabile dell'inoltro dei flussi video alle applicazioni video-on-desktop delle postazioni SGE.

A livello locale, le telecamere IP sono integrate in un CT-VTV, responsabile del rilievo dello stato delle stesse e tramite l'interfaccia MI (OPC server > OPC client) può inviare alla GO locale il nuovo stato della telecamera per consentire l'animazione delle icone delle telecamere sul sistema SGE.

Presso la galleria della Biaschina l'integrazione del servizio video nella rete COM avviene ancora tramite codec video su IP, alloggiati in cestelli, del sistema di gestione VMS e delle funzioni che consentono le commutazioni video.

Il compressore video fornito è il modello netCOM della Comerson basato sulla tecnologia wavelet, in grado di elaborare 50 fields/sec PAL e 60 fields/sec NTSC.

L'interfaccia video del codec verso gli utenti video (telecamere o monitor) è del tipo PAL/CCIR, connettore BNC 75 Ohm, tranne che per i posti di lavoro collegati alla rete LAN che utilizzano un decoder software. L'interfaccia LAN del Codec è del tipo 10/100BaseT.

Il decoder è provvisto di generatore di caratteri in grado di sovrapporre all'immagine un codice di identificazione o il nome della telecamera visualizzata. Encoder e decoder sono sviluppati su piattaforma embedded e sistema operativo Linux.

2.3.9. Connessioni WAN

Nel corso degli anni la rete COM ha dovuto allestire dei collegamenti fisici esterni per l'interconnessione a servizi necessari al funzionamento della rete o per portare servizi della rete COM presso altri enti (p.es. video). Tutti i collegamenti fisici sono centralizzati presso il CMB.

Tutte le connessioni dei servizi sono basate sul protocollo IP e controllate da un firewall che ne garantisce la sicurezza.

La tabella che segue illustra, a blocchi, i servizi implementati o previsti.

Denominazione	Zona Firewall	Servizi
Provider	Public addresses (untrust)	Collegamenti internet
Shared services	Incoming services DMZ Outgoing services DMZ Authentication services (futuro)	DMZ o zona demilitarizzata per servizi interni che necessitano di accedere ad internet
Comunication DMZ	Local DMZ Regional DMZ USTRA DMZ	Collegamenti verso altri enti

Tabella 2: Servizi connessioni WAN

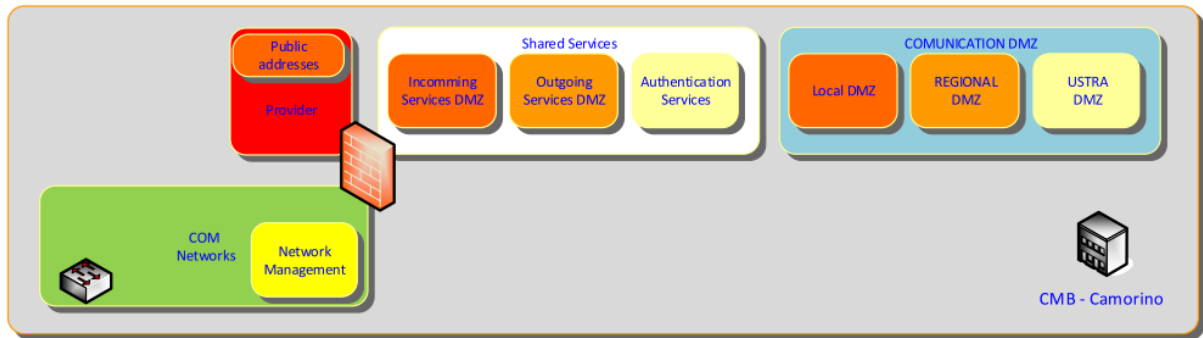


Figura 4: Schema a blocchi connessioni esterne

Oltre ai collegamenti sopra menzionati esiste un collegamento indiretto con la GE V (Grigioni) visto che UT IV per la galleria di Roveredo, dove è stato integrato un nodo COM, ne gestisce la tecnica, mentre la Polizia dei Grigioni ha la gestione operativa (Polizia).

Collegamento definito "indiretto", visto che entrambe le unità territoriali possono arrivare sulla rete KNA, ma nessun traffico "diretto" tra le due unità territoriali è permesso.

2.3.10. Accesso remoto (RAS) SSL-VPN

È possibile accedere alla rete COM attraverso un portale SSL-VPN accessibile unicamente attraverso un sistema di autenticazione sicuro (one time password). L'accesso SSL-VPN è garantito a tutti i fornitori degli impianti di gestione autostradale connessi alla rete COM (circa 20).

L'infrastruttura di accesso e autenticazione è gestita e garantita dal fornitore del servizio di manutenzione (oggi Argonet SA). Il fornitore del servizio di accesso remoto SSL-VPN si interfaccia a sua volta in modo sicuro tramite linea noleggiata con i firewall Fortinet della rete COM al CMB.

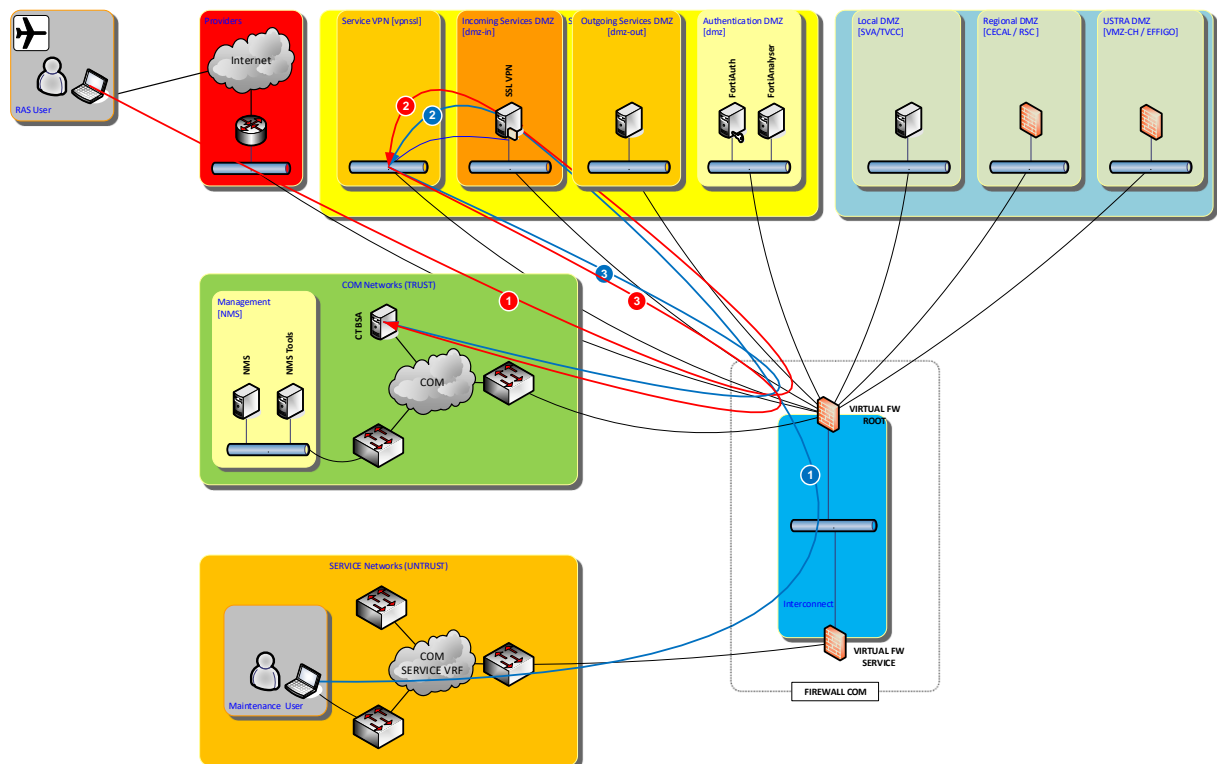


Figura 5: Schema di accesso RAS

2.3.11. Collegamento VMZ-CH

Per la visualizzazione delle immagini video all'interno della rete COM è definito uno stream IP principale (firststream) ad alta qualità sulle telecamere IP. Per VMZ a Emmen è stato definito un secondo streaming (secondstream) sulle telecamere a qualità ridotta a disposizione delle richieste dalla centrale VTV di Emmen.

Questo collegamento transita tra il cluster di firewall COM ed il router del BIT al CMB (figura sottostante).

Per permettere l'inoltro dei flussi sulla rete VM-CH è stato necessario:

- Eseguire la traslazione di tutti gli IP delle telecamere in un IP VM-CH tramite il protocollo NAT sul firewall CMB.
- Mettere in comunicazione multicast le due reti tramite il protocollo MSDP (Multicast Source Discovery Protocol), che permette l'interconnessione di molteplici domini di PIM-SM (Sparse Mode).

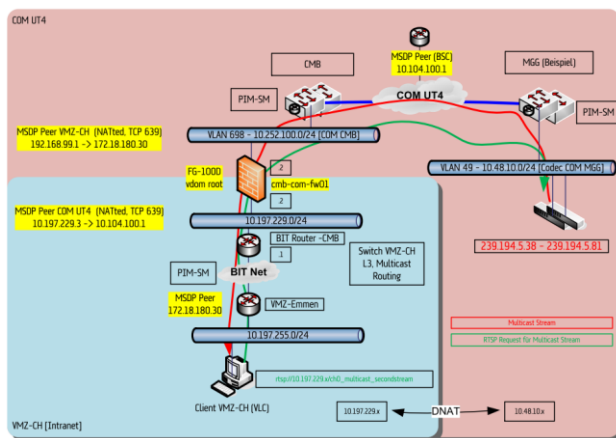


Figura 6: Schema di principio globale dell'integrazione con VM-CH

La visualizzazione nella centrale VTV di Emmen avviene tramite un player standard (p.es. VLC, QuickTime, ecc.).

2.3.12. Accesso a servizi COM da rete VM-CH

Per l'integrazione con la rete VM-CH si è proceduto a collegare il firewall cmb-com-fw00 con il router di VM-CH già presente al CMB. Tramite questo collegamento vengono messi a disposizione alla centrale di Emmen diversi servizi della rete COM:

- Accesso ai dati Boschung
- Accesso a postazione SGE presso il CMB e accesso al sistema PMV
- Accesso a sistema Misura 4 e controllo veicoli pesanti

Le due reti COM e VTV utilizzano entrambe la stessa classe di indirizzamento IP privato, vale a dire 10.0.0.0.

Per evitare problemi di instradamento di rete e per non dover configurare delle route statiche si è deciso di utilizzare la funzione di Network Address Translation (NAT).

VMZ-CH ha messo a disposizione alcuni dei suoi indirizzi IP riservati a Bellinzona per la connessione ai vari servizi. Tramite il Firewall COM questi IP vengono convertiti negli IP reali dei sistemi.

2.3.13. Integrazione Boschung

Per l'integrazione della rete impianto ghiaccio nella rete COM si è seguito lo standard già utilizzato per gli altri impianti. In sostanza ogni componente di rete Boschung è stata configurata in una rete IP già esistente in ogni località (usando l'IP dell'impianto meteo MET).

USTRA ha assegnato 2 indirizzi IP della sua rete per permettere alla ditta Boschung di collegarsi da remoto ai server di Airolo e Bellinzona.

Lo schema di principio è il seguente.

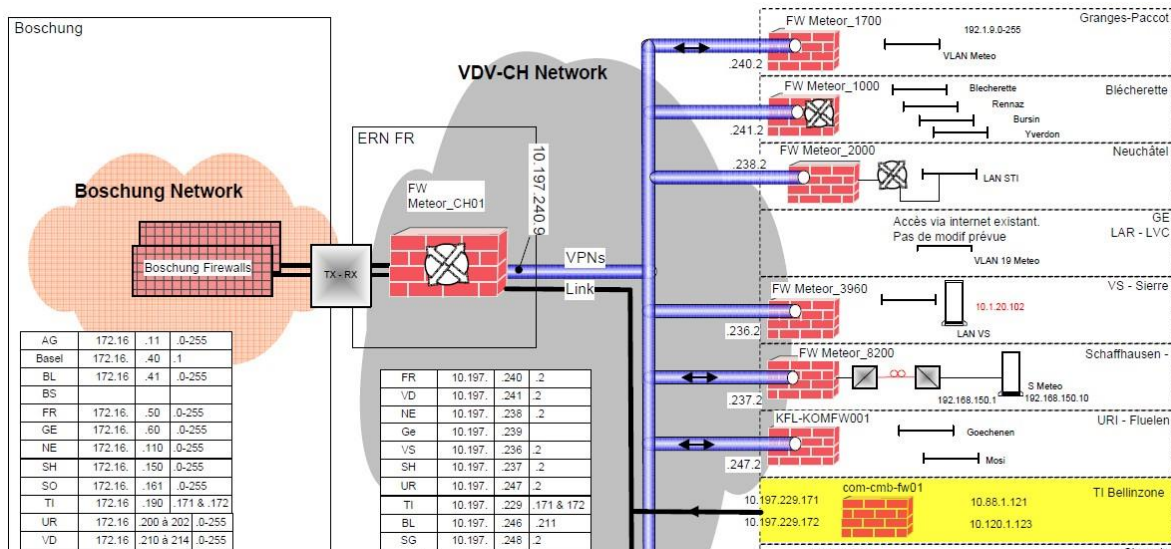


Figura 7: Collegamento COM VDV-CH per Boschung

2.3.14. Interfaccia verso la RSC

La connessione alla rete di comunicazione delle strade cantonali RSC avviene tramite un collegamento in rame al CMB tra i firewall COM e RSC per la gestione UT IV.

2.3.15. Interfaccia verso la CECAL

L'inoltro di immagini video dall'impianto delle strade nazionali verso la centrale comune di allarme CECAL avviene tramite un collegamento in fibra ottica al CMB tra firewall COM e firewall CSI.

2.3.16. Shared DMZ

Sotto questa denominazione rientrano le DMZ che necessitano di accedere a internet. I collegamenti sono i seguenti:

- DMZ TVCC: rete web server
- DMZ IN/OUT: reti che ospitano sistemi che devono accedere a internet

Nella DMZ TVCC sono posizionati i web server che si occupano dell'invio continuo di immagini delle varie telecamere della rete COM al CSI. Queste immagini sono poi messe a disposizione dell'applicazione della Polizia per smartphone.

Nella DMZ IN/OUT vengono posizionate devices che necessitano di accedere a Internet come Server per l'aggiornamento antivirus o il sistema contromano.

Nota: Dove non è stato possibile posizionare i devices in DMZ è stato permesso l'accesso diretto a Internet. Per il momento questo servizio è permesso solo all'impianto conta-traffico della galleria di Maroggia che utilizza il servizio americano Inrix.

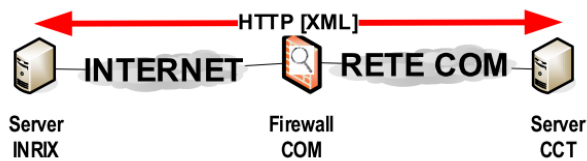


Figura 8: Collegamento Inrix

2.4. Sistemi di gestione e sicurezza

La gestione della rete di comunicazione è suddivisa in due sistemi distinti:

- Parte network, basata sui sistemi NMS e NMS tools (Argomon/nagios e SolarWinds)
- Parte video, basata su sistema VMS

Gli applicativi NMS e VMS sono installati sulle macchine virtuali (VM) ridondanti al CMB:

- cmb-com-ctn01 [Engine NMS]
- cmb-com-ctn02 [IUM NMS]
- cmb-com-ctv01 [Engine+IUM VMS]

Gli host cmb-com-ctn01 e cmb-com-ctv01 gestiscono anche la comunicazione tra COM e SGE (funzione di OPC server per la trasmissione dei punti-dato).

L'applicativo SolarWinds, impiegato unicamente per la manutenzione delle apparecchiature Cisco (gestione delle configurazioni e delle versioni software), è installato su un server dedicato presso il CMB (cmb-com-uti01).

L'applicativo Argomon, impiegato per le statistiche di traffico e allarmistica di tutte le apparecchiature è anch'esso installato su un server dedicato presso il CMB (cmb-com-mon01).

2.4.1. Hardware VMS/NMS

I server e gli storage NMS/VMS ridondanti sono installati presso il CMB. È prevista la ridondanza dislocata al CMF che non è ancora stata realizzata ma lo sarà entro fine 2019.

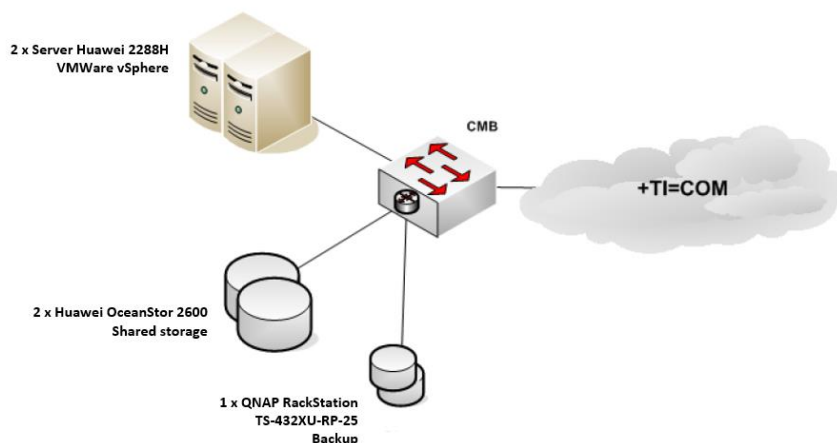


Figura 9: Architettura server NMS/VMS

La soluzione è formata da server Huawei 2288H e due storage Huawei OceanStor 2600. I server non dispongono di dischi fisici. Tramite la rete essi accedono ai dischi virtuali che sono ospitati sugli storage.

Le Virtual Machines (VMs) delle applicazioni (p.es. NMS o VMS) installate sui dischi virtuali sono gestite tramite una software VMware (vSphere) che permette di bilanciarne il servizio tra i due server. In caso di problemi, la funzionalità VMware vMotion permette di spostare le VMs da un server all'altro.

Gli storage sono composti da una serie di dischi fisici (array). Tramite il management degli storage, questi array vengono suddivisi in più unità logiche o partizioni (LUN).

Le VMs delle applicazioni sono ospitate in queste LUN. Anche gli storage hanno una software che permette di spostare le LUN da un sistema all'altro in tempo reale senza interruzioni del servizio.

I due sistemi di storage sono completamente ridondanti e replicati in tempo reale. La consistenza e replicazione dei dati viene gestita autonomamente dai due sistemi.

La figura che segue rappresenta la struttura di una soluzione ridondante sia a livello di VMs che di storage.

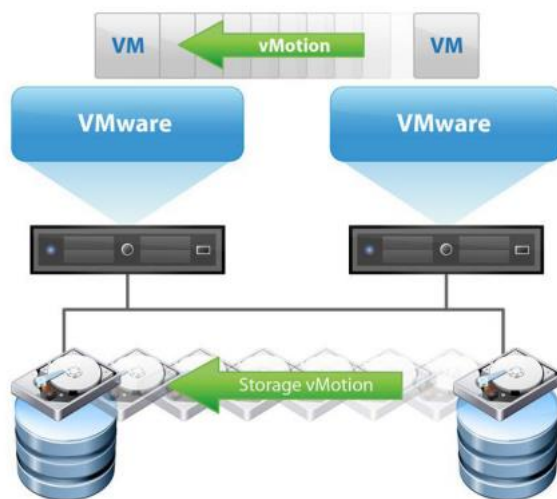


Figura 10: Schema di principio ridondanza livello VMWare e Storage

Inoltre, i dati delle singole VM vengono salvaguardati mediante un sistema di backup VEEAM sulle due appliances. In caso di guasto i dati aggiornati sono sempre a disposizione sui secondi sistemi dell'infrastruttura.

Il design della soluzione prevede l'installazione di un server ed uno storage al CMB e la medesima installazione viene replicata al CMF. Tramite la nuova rete COM a 10 Gbps la sincronizzazione dei dati tra le due sedi è garantita in tempo reale.

Sia i server che gli storage dispongono di collegamenti dedicati in fibra ottica agli switch.

Le differenti VMs possono essere attive in uno dei due datacenter, a scelta o in caso di guasto possono venir attivate sull'altra sede.

Il sistema di storage collegato in rete permette facilmente future espansioni e può venir messo a disposizioni ad altri servizi (rappresentati dai server X nella figura seguente).

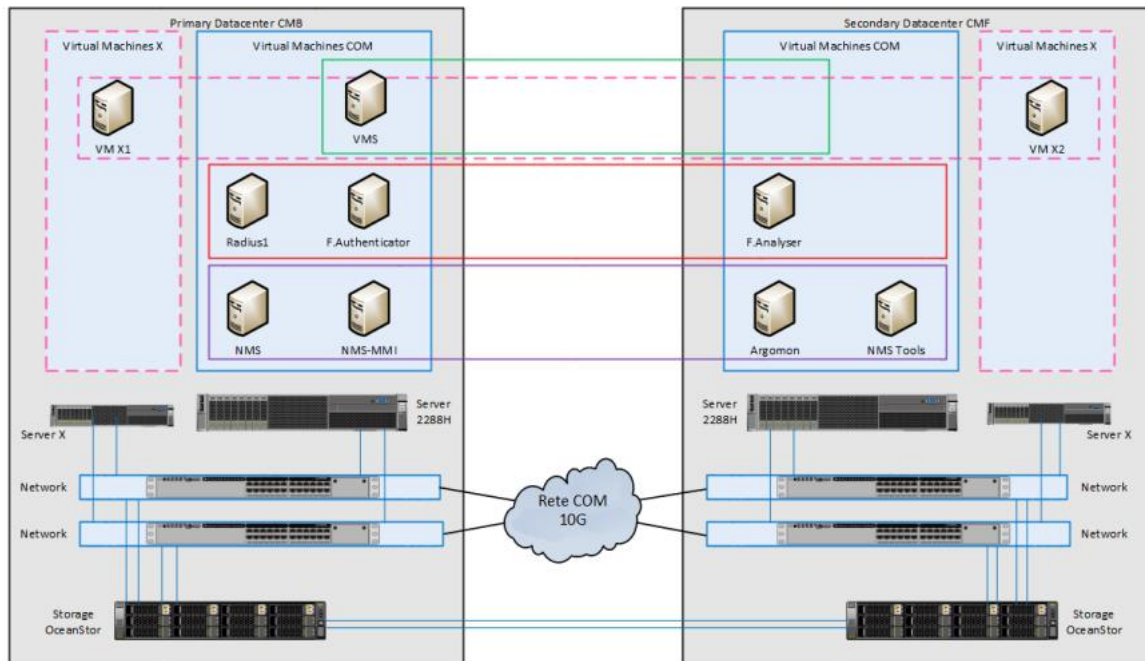


Figura 11: Schema logico installazione CMB-CMF

Il software del sistema di storage, con i dischi logici (LUNs) sono accessibili contemporaneamente dalle due località (modalità active/active). In caso di guasto di uno dei sistemi, le relative LUNs rimangono accessibili attraverso il secondo sistema.

Alfine di gestire un'eventuale interruzione dei tracciati in fibra ottica tra le due sedi viene installata una workstation indipendente che ospita un servizio di controllo chiamato Quorum.

L'applicazione Quorum/Witness, installata su una macchina virtuale esterna ai sistemi, ha il compito di arbitrare l'accesso ai dati, garantendone la consistenza anche nel caso venisse a mancare completamente la comunicazione tra le due sedi. Nel caso venga a mancare la comunicazione tra i due sistemi sincronizzati, questi richiedono al Quorum quale dei due deve continuare a gestire i dati, impedendo che tutti e due continuino indipendentemente l'uno dall'altro causando una perdita di consistenza dei dati.

Nell'immagine che segue è rappresentato lo schema di principio della soluzione (sito 1 = CMB, sito 2 = CMF, sito 3 da definire).

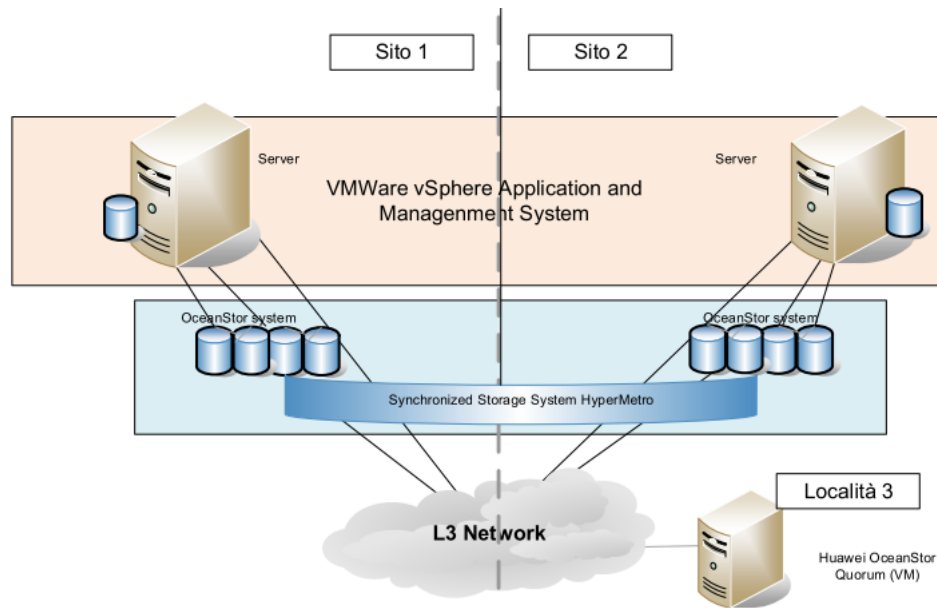


Figura 12: Schema di principio della soluzione server-storage

La soluzione è configurata come segue.

Server Huawei 2288H:

- 2 U Chassis con 24x2.5" Slot per dischi
- 2 CPU Intel Xeon Gold 6134 con 8 Cores
- 4x32 GB RAM Memoria (2656 Ghz), in totale 128 GB Memory
- 2xNVMe M.2 Disk 32 GB (per booting ESXi)
- 2x10 GE SFP+ e 2xGE
- Alimentazione ridondante da 550W

Storage Huawei OceanStor 2600:

- Storage system OceanStor 2500 V3
- Doppio controller con 32 GB di cache memory
- Interfaccia di rete con 2 volte 4x10 GE [SFP+] e 2 volte 6x1 GE
- 25 disk enclosures 2.5"
- 8 disk SAS con 900GB 10K RPM
- Alimentazione ridondante

Il sistema Quorum:

- Workstation Intel NUC (Linux e software Huawei)

I sistemi Huawei includono anche i seguenti software di sistema:

- Basic software
- HyperMetro per la sincronizzazione active/active dei dati

2.4.2. Virtual Machine CT NMS

Le principali funzionalità del CT NMS sono l'interfacciamento con SGE e il monitoraggio dello stato delle componenti attive di rete:

- Verifica stato delle componenti attive di rete tramite SNMP trap o SNMP get
- Elaborazione, filtraggio e registrazione dei messaggi di stato in una banca dati
- Polling di alcuni parametri (contatori) relativi ai volumi di traffico sulla rete
- Registrazione dei valori di traffico raccolti in una banca dati
- Visualizzazione grafica dello stato della rete tramite interfaccia web
- Visualizzazione dello stato dei codec, accedendo ai dati disponibili sul sistema VMS
- Visualizzazione (anche grafica) dei dati di traffico
- Rilevamento automatico di nuovi elementi di rete
- Interfacciamento con SGE

2.4.3. Virtual Machine Argomon

Tramite l'applicativo Argomon (basato sul software open-source Nagios), è possibile visualizzare diverse statistiche di traffico, carico CPU, temperatura, occupazione dischi, memoria, ecc. È inoltre possibile visualizzare statistiche sui tempi di risposta dei diversi sistemi monitorati.

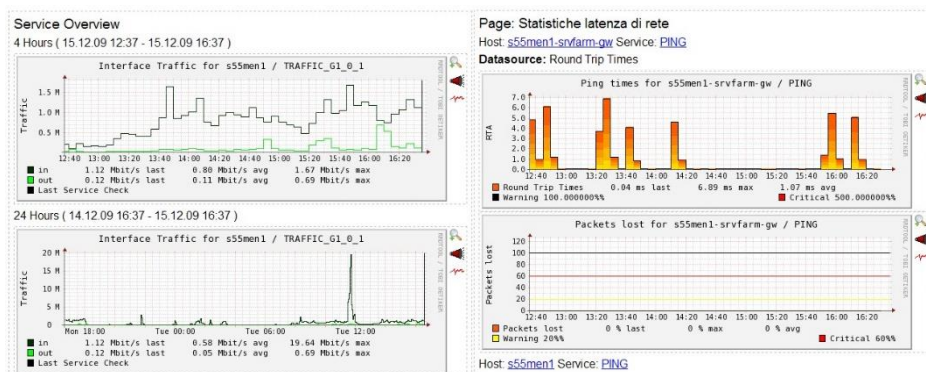


Figura 13: Argomon, esempio grafici di traffico e tempi di risposta

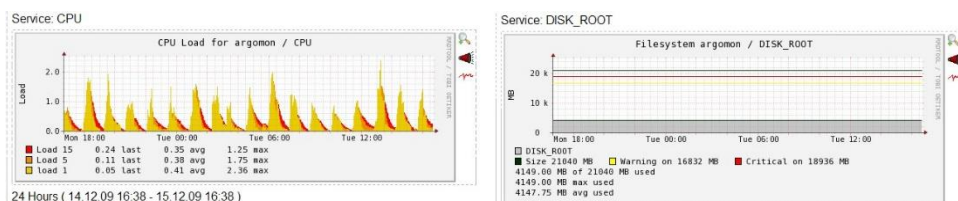


Figura 14: Argomon, esempio carico CPU e utilizzo dischi fissi

2.4.4. Virtual Machine SolarWinds NCM (NMS Tools)

I sistemisti di rete dispongono del software SolarWinds Network Configuration Manager DL200 per le seguenti funzioni:

- Gestione automatica dei backup delle configurazioni degli switch Cisco e dei firewall con possibilità di confrontare le differenze tra la configurazione attiva e quelle precedenti.
- Sistema di logging.

2.4.5. Sicurezza

Lo schema fisico delle connessioni dei firewall è raffigurato nell'immagine seguente.

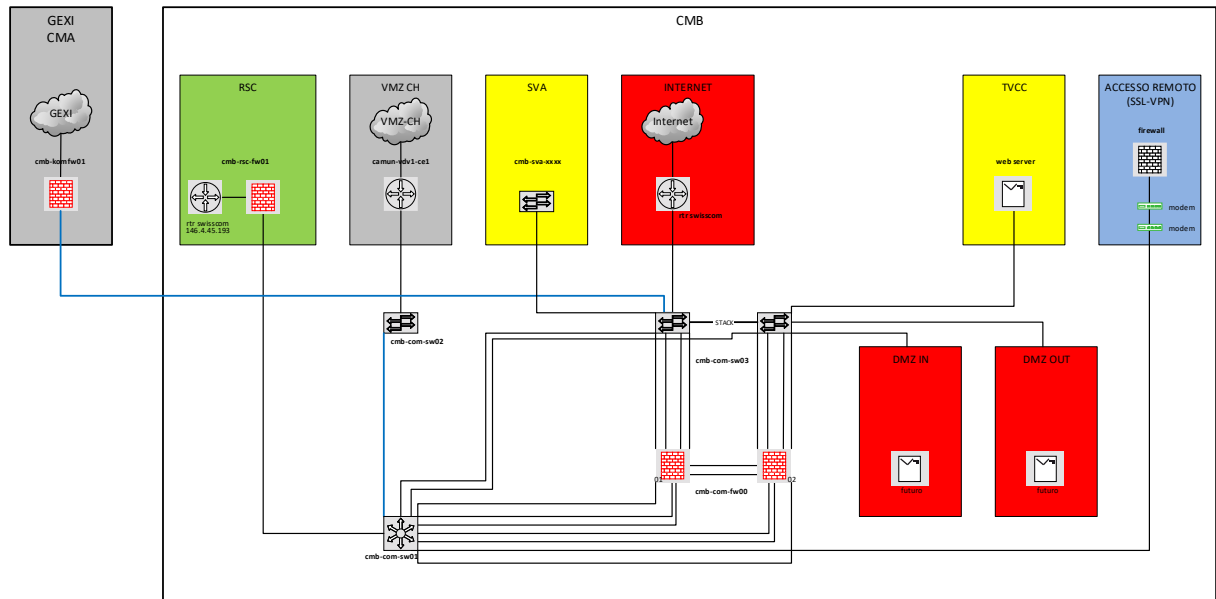


Figura 15: Connessioni dei firewall

Lo schema logico delle connessioni dei firewall è raffigurato nell'immagine seguente.

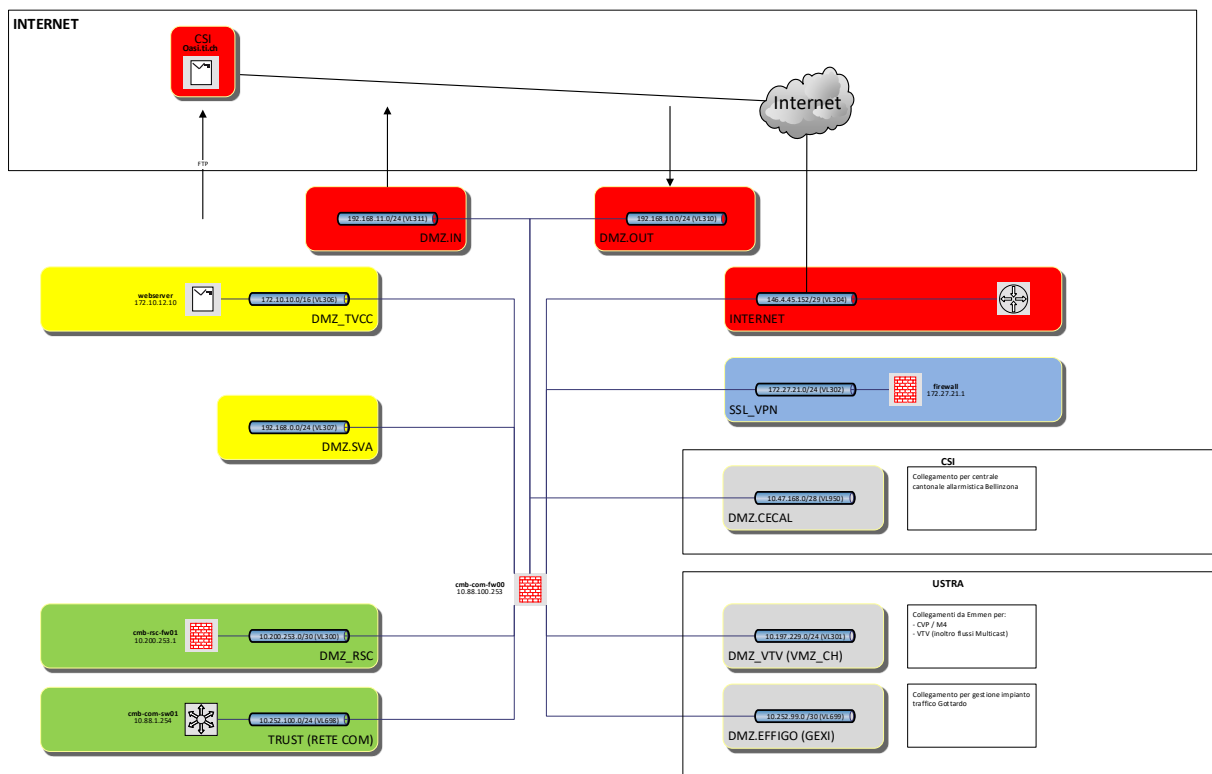


Figura 16: Schema logico di connessione del firewall

2.5. Infrastruttura passiva

Lungo tutta l'autostrada N2 Chiasso – Airolo e N13 Gorduno – Roveredo sono disponibili collegamenti in fibra ottica monomodale (singlemode) appartenenti a USTRA. Queste fibre ottiche permettono la realizzazione di due dorsali tra i nodi di comunicazione per l'architettura magliata e ridondata della rete di comunicazione. Si tratta in particolare di:

- Due cavi distinti da 96 fibre ottiche singlemode tra Chiasso e Airolo. Laddove progetti di manutenzione (EP) sono stati eseguiti, sono stati creati due tracciati separati sulle due carreggiate sud-nord e nord-sud, nei quali sono stati posati cavi da 144 fibre ottiche singlemode. È disponibile un tracciato cavi doppio sulle seguenti tratte:
 - N2 Coldrerio Nord – Mendrisio
 - N2 Melide – Gentilino
 - N2 Varenzo – AiroloPer le altre tratte delle N2 i due cavi FO sono alloggiati nel medesimo tracciato cavi.
- Due cavi distinti da 144 fibre ottiche singlemode tra Gorduno e Roveredo. Tra Gorduno e Castione i due cavi alloggiati nel medesimo tracciato, mentre tra Castione e Roveredo sono presenti due tracciati separati sulle due carreggiate sud-nord e nord-sud, cosicché i due cavi FO si trovano in due tracciati distinti.
- Per ovviare ai tracciati unici della N2 dove transitano i due cavi FO, è stata creata un'ulteriore ridondanza attraverso l'infrastruttura AET tra Chiasso, Mendrisio, Lugano-Noranco, Camorino, Biasca, Faido e Airolo.

Per il collegamento tra la sezione Mappo-Morettina ed il centro di manutenzione di Camorino, la situazione è più complessa, in quanto esiste unicamente un cavo relativamente vecchio da 16 fibre ottiche in gran parte occupato dai diversi servizi integrati. Il progetto di integrazione della sezione Mappo-Morettina nel sistema di gestione SGE delle strade nazionali si occuperà di prevedere le future fibre ottiche necessarie alla COM.

Nota: È opportuno segnalare che tutte le fibre ottiche disponibili di USTRA e quelle ridondanti transitano su tracciati comuni per accedere ai locali tecnici di BRO, CML, CMB, CMF e CMA. Ciò significa che questi punti di accesso sono un potenziale punto debole dell'infrastruttura passiva.

2.6. Infrastruttura attiva

2.6.1. Componenti hardware

Nella tabella seguente è indicata la lista degli elementi hardware principali installati in ogni luogo. Come indicato nella premessa iniziale, la galleria Mappo-Morettina (LOG) viene considerata nell'ambito del presente progetto, non vengono però indicati i componenti hardware utilizzati in quanto essi saranno sostituiti nell'ambito dell'integrazione della sezione nelle strade nazionali.

ID	Luogo	Catalyst 4507R+E	Catalyst 3850	Cisco 2960X	Cisco IE2000/4000 Moxa ICS-G7852A, EDS-510E, -P510	Fortinet 100D	Decoding station	Encoder	NMS+VMS, server e storage Huawei	Nagios, SolarWinds (software)
1	BRO	1								
2	MEN		2							
3	MRG	1		1	3					
4	MGG	1								
5	CML	1			1		2			
6	GEG	1		2	2					
7	TAG	1			3					
8	CEN	1								
9	CMB	1	4			2	27	2	2	1
10	SFE		2		106					
11	BSC	1								
12	BIA	1			3			2		
13	GRI		1							
14	CMF	1	2				2			
15	PIU	1						22		
16	CAS		2							
17	PAR		2							
18	PIO		2							
19	QUI		2							
20	STA	1								
21	CMA	1								
Totali		14	19	3	118	2	31	26	2	1

Tabella 3: Elenco del materiale principale installato

2.6.1.1. Switch COM Catalyst 4507R+E

I nodi COM sono sistemi Cisco della serie Catalyst 4500. Lo chassis Catalyst 4507R+E è equipaggiato con alimentazione e processore ridondante normalmente come segue (esempio non esaustivo):

- WS-C4507R+E: Catalyst4500E 7 slot chassis for 48 Gbps/slot, fan, no power supply
- C4500E-IP-ES: Paper IP to ent services license
- WS-X45-SUP8-E: Catalyst 4500 E-Series supervisor 8-E
- WS-X45-SUP8-E/2: Catalyst 4500 E-Series redundant supervisor 8-E
- WS-X4648-RJ45-E: Catalyst 4500 E-Series 48-Port 10/100/1000 (RJ45)
- PWR-C45-1400AC: Catalyst 4500 1400W AC power supply (data only)
- PWR-C45-1400AC/2: Catalyst 4500 1400W AC power supply redundant (data only)

Inoltre, per la rete COM sono stati utilizzati i seguenti moduli ottici:

- GLC-LH-SMD=C: SFP 1000BASE-LX singlemode 1310nm 10Km DOM
- SFP-10G-LR=C: SFP+ 10GBASE-LR singlemode 1310nm 10Km DDM
- SFP-10G-ER=C: SFP+ 10GBASE-ER singlemode 1550nm 40Km DDM
- SFP-10G-ZR=C: SFP+ 10GBase-ZR singlemode 1550nm 80Km DDM
- GLC-ZX-SM: SFP 1000BASE-ZX, singlemode 1550nm ZR/80km/24dB

2.6.1.2. Switch dislocati

Come switch dislocati sono utilizzati switch della serie Catalyst 3750. Si è deciso di utilizzare dei sistemi layer 3, per garantire la massima flessibilità. Gli switch dislocati sono collegati in gigabit ethernet ai nodi COM tramite fibra ottica monomodale.

Il modello utilizzato per tutti i nodi dislocati è il seguente:

- WS-C3850-24T-E: Cisco Catalyst 3850 24 port data IP services
- C3850-NM-4-10G: Cisco Catalyst 3850 4x10 GE network module
- PWR-C1-350WAC/2: 350W AC config 1 secondary power supply

Per i moduli ottici fare riferimento al capitolo precedente.

2.6.1.3. Switch di espansione

Dove le porte degli switch di core non erano sufficienti si è proceduto ad installare uno switch della serie Catalyst 2960X. Sono dei sistemi layer 2 e anch'essi come gli switch dislocati sono collegati ai nodi COM tramite fibra ottica monomodale.

Il modello utilizzato per tutti i nodi dislocati è il seguente:

- WS-C2960X-24PS-L: Catalyst 2960-X 24 GigE PoE 370W, 4x1G SFP, LAN base

Come per i GBIC, anche per i transceiver SFP, sono utilizzati due tipi a dipendenza della lunghezza della tratta in fibra ottica:

- GLC-LH-SMD=C: SFP 1000BASE-LX singlemode 1310nm 10Km DOM
- GLC-LX-SM-RGD-C: SFP 1000Base-LX singlemode 1310nm 10Km industrial temperature / Cisco

2.6.1.4. Switch di campo rete COM

Per gli switch di campo messi a disposizione dalla rete COM che vengono utilizzati dagli elementi degli impianti BSA, sono stati utilizzati diversi modelli di switch.

- IE-4000-4S8P4G-E: IE 4000 4xSFP 100M with 8xPoE, 4x1G Combo, LAN base
- IE-2000-8TC-G-B: IE 8 10/100 2 T/SFP base
- Moxa ICS-G7852A
- Moxa EDS-510E
- Moxa EDS-P510

2.6.1.5. Switch di campo reti impianti BSA

I diversi impianti BSA, che mettono a disposizione le proprie reti di campo, utilizzano prodotti provenienti da diversi fornitori.

- Cisco Catalyst 2960x
- Cisco IE4000
- Cisco IE2000
- Planet IGS-10020MT
- Planet WGS-4215-8P2S
- Moxa EDS 405/408A-xxxxx
- Moxa EDS-728
- Schneider 499NOS17100
- Siemens Scalance XB205-3LD
- Hirschmann RS20-0800M2/NS-205
- Hirschmann RSB20-0800S2S2AAB
- Microsens MS400870M
- D-Link DES-3226S

2.6.1.6. Codec video

Per la codifica e decodifica del traffico video in flussi IP è utilizzato il compressore video Com-merson netCOM, basato sulla tecnologia wavelet, in grado di elaborare 50 field/sec PAL o 60 field/sec NTSC.

Le schede sono alloggiate in cestelli rack da 19" e 5 unità completi di ventilazione. Ogni cestello può contenere fino ad un massimo di 12 schede codec. L'alimentazione dei rack che contengono le schede netCOM è garantita da alimentatori ridondanti.

Per il video on desktop, è utilizzato un decoder software. Il plug-in netCOM per NetStation, è il software che consente la visualizzazione delle immagini live.

2.6.1.7. Firewall

Per l'accesso RAS e per l'accesso alle reti esterne (p.es. VM-CH), sono stati utilizzati 2 firewall della ditta Fortinet in cluster installati al CMB. In particolare, è stato impiegato il modello Forti-gate 100D.

2.7. Particolarità della rete COM UT IV

2.7.1. Video Management System (VMS)

Nell'architettura della rete COM di UT IV in origine è stato inserito anche l'impianto VMS con i suoi codec ed è stato installato sullo stesso hardware dei sistemi di gestione COM.

Le principali funzionalità del VMS per la gestione dei codec e delle telecamere sono:

- Inizializzazione dei codec video con parametri di default per il frame/rate del flusso video, per il livello di compressione (6 livelli di compressione) e per il tipo di trasmissione (TCP o MTP).
- Monitoraggio dello stato dei codec (controllo della vita di tutte le periferiche installate) e richiesta presenza segnale video agli encoder.
- Attribuzione dei flussi video generati dagli encoder verso uno o più decoder per la visualizzazione sui monitor sovra-imprimendo una scritta configurabile a video.
- Controllo stato telecamere IP e decoder.
- Telecamera IP up/down.
- Attribuzione sorgenti video tramite le pagine in SGE.

Inoltre, il VMS consente di effettuare attivazioni di layout video sul videowall e sulle postazioni (cioè più attribuzioni in parallelo telecamera-monitor), di sequenze video (cioè ciclico di telecamere a tempo definito su un monitor), gestione delle avarie dei codec e dei video-loss, storico delle avarie e dei comandi effettuati dagli operatori.

La figura seguente rappresenta l'architettura del sistema di Video Management System (VMS).

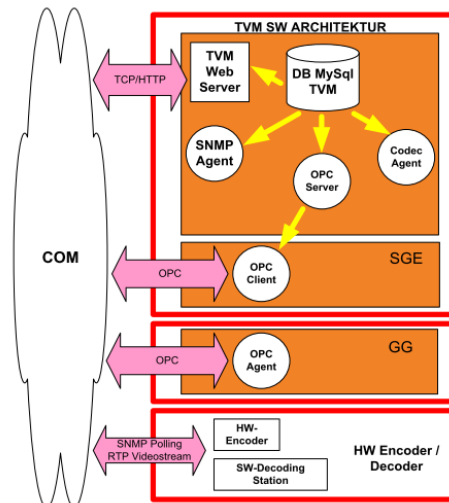


Figura 17: Architettura software VMS

Il CT COM VMS include, oltre alla possibilità di gestire i codec Netcom wavelet, anche la possibilità d'integrare codec H.264. Questo, di fatto, permetterebbe d'integrare nella gestione autostradale anche le telecamere mobili, ora gestite su un server VMS dedicato. Il CT COM VMS rispetto alla versione precedente è installato su una macchina virtuale dedicata, separata dal CT COM NMS. È possibile visualizzare su monitor e videowall telecamere provenienti sia da equipaggiamenti wavelet (codec) sia da equipaggiamenti H.264 (codec e telecamere).

2.8. Esercizio

L'esercizio della rete COM e dei propri servizi, comprese le reti di campo COM, è assicurato da UT IV tramite i propri sistemisti e tramite un contratto di manutenzione stipulato con il fornitore Argonet SA, che garantisce un servizio di picchetto in lingua italiana 24 ore su 24 e 7 giorni su 7, giorni festivi inclusi. Il fornitore garantisce inoltre i seguenti tempi di reazione, intervento e ripristino:

- Tempo massimo di reazione: 2 ore
- Tempo massimo di intervento: 4 ore
- Tempo massimo di ripristino: 12 ore

L'esercizio delle reti di campo impianti BSA è assicurato anch'esso dai sistemisti UT IV e, a seconda del tipo di impianto, tramite contratti di manutenzione stipulati da UT IV con i singoli fornitori. Servizi di picchetto, tempi di reazione, intervento e ripristino dipendono dall'importanza dell'impianto.

3. Visione futura Rete IP BSA UT IV

3.1. Introduzione

La rete IP BSA UT IV dovrà rispettare la direttiva USTRA 13040 [1] che ha lo scopo di standardizzare l'infrastruttura di comunicazione delle strade nazionali su tutto il territorio svizzero. In estrema sintesi, essa descrive l'architettura di rete destinata alla dorsale svizzera (backbone IP-Netz BSA) e alle infrastrutture di comunicazione locali nelle unità territoriali (UT), comprese le interfacce con i centri di calcolo BSA (BSA RZ), VMZ-CH, altre UT, reti cantonali e federali, reti di partner (p.es. Swisscom) e altre reti esterne attraverso internet.

Nella nuvola tratteggiata della figura seguente è mostrata la delimitazione della rete IP BSA UT IV.

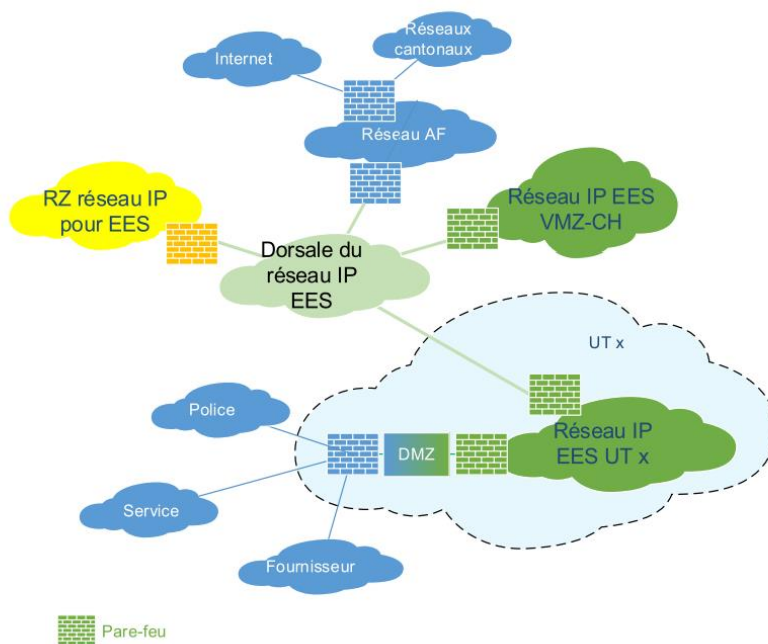


Figura 18: Delimitazione rete IP BSA UT IV

In base all'applicazione della direttiva 13040 [1] e delle altre direttive afferenti ad essa, come ad esempio la 13030 [2] relativa alla sicurezza, nei capitoli seguenti è descritta la situazione desiderata alla fine del processo di migrazione.

Alla fine di ogni capitolo viene già fornita un'indicazione sulla differenza ("gap") fra situazione attuale e situazione desiderata, come pure un'indicazione sulle proposte per colmare questa differenza.

3.2. Rete IP BSA UT IV

3.2.1. Rete dorsale

La rete dorsale (core) permette di collegare fra loro le diverse sezioni ed il sistema di gestione. Ad essa sono connesse le reti di campo (access) alle quali sono allacciati gli impianti BSA.

L'architettura attuale della rete COM è già compatibile con quella proposta dalla direttiva 13040 [1], mentre le caratteristiche seguenti richiedono una sostituzione dei router attualmente in servizio.

- È immediatamente richiesto MPLS come protocollo di routing verso il backbone IP-Netz BSA e in futuro su tutti i router della dorsale.
- Sulla dorsale sono richiesti link a 100 Gbps. Per l'interfacciamento con le reti di campo sono sufficienti interfacce a 10 Gbps.

- Sulla dorsale è richiesto l'indirizzamento IPv6.
- Sul singolo router non è richiesta la ridondanza interna (p.es. alimentazione, controller e schede d'interfaccia di rete).
- Il raddoppio dei router è suggerito nelle sezioni con gallerie ma non è obbligatorio.

L'architettura della dorsale sarà la seguente, dove ogni router core avrà almeno due Link verso un secondo router core (vedi anche allegato [9]).

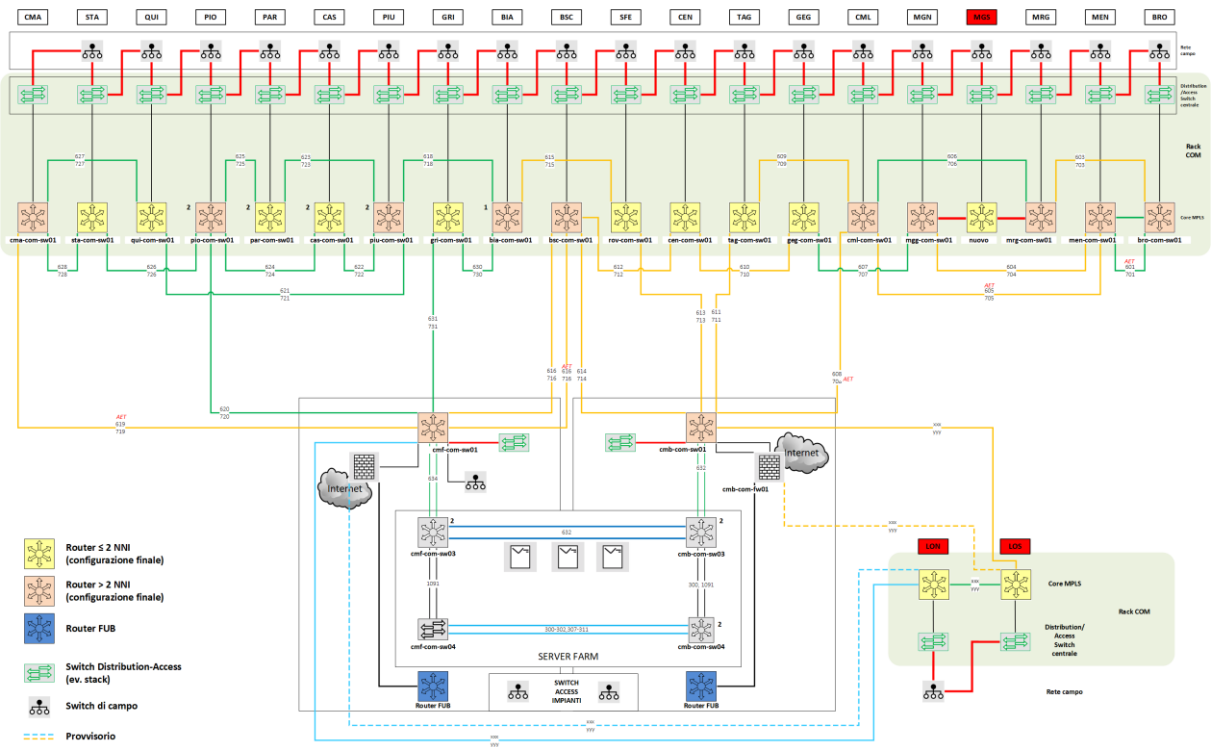


Figura 19: Nuova dorsale rete IP BSA UT IV

In UT IV, i router delle sezioni con le gallerie più importanti verranno raddoppiati, in particolare:

- Galleria Mappo-Morettina (nei locali LON e LOS)
- Galleria Melide-Grancia (nei locali MGN e MGS)

I punti finali scelti per l'interconnessione verso il backbone IP-Netz BSA sono Camorino e Faido (CMB e CMF).

Sintesi del gap fra situazione attuale e desiderata, identificabile quale misura da attuare:

Situazione attuale	Richiesta USTRA secondo [1] e [2]
Link 10 Gbps	Possibilità di link fino a 100 Gbps.
Routing OSPF	Routing MPLS
IPv4	IPv6

Per poter raggiungere la situazione desiderata è necessario acquistare nuovi router. L'architettura resta comunque simile a quella attuale.

3.2.2. Rete di campo impianti BSA

La rete di campo dove sono allacciati tutti gli impianti BSA permette il collegamento fra tutti gli elementi di campo di un impianto, i suoi sistemi di controllo o di comando e l'interconnessione con la rete dorsale per la comunicazione con altri impianti o con i sistemi di gestione centralizzati.

Nella direttiva 13040 [1] si tende a favorire il concetto di una sola rete ben ridondata per tutti gli impianti BSA piuttosto che numerose reti diverse (una per impianto, come attualmente nel perimetro UT IV).

Gli switch access delle reti di campo dovranno essere layer 2 managed con interfacce verso l'utente da 1 Gbps per poter connettere qualsiasi tipo di impianto.

L'interconnessione verso la dorsale dovrà invece prevedere interfacce 10 Gbps e gli anelli degli switch di campo dovranno terminare in due nodi di comunicazione principali differenti come mostrato nella figura seguente.

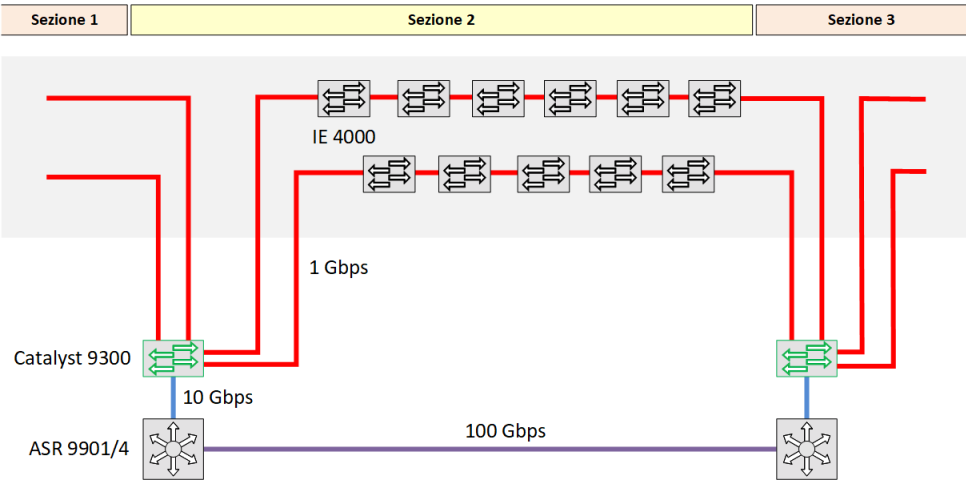


Figura 20: Principio d'integrazione reti di campo nella dorsale rete IP BSA UT IV

Sintesi del gap fra situazione attuale e desiderata, identificabile quale misura da attuare:

Situazione attuale	Richiesta USTRA secondo [1] e [2]
Prevalentemente reti singole per ogni impianto	Rete di campo unica multiutente
Reti di campo prevalentemente non collegate alla dorsale COM	Collegamento fra rete di campo e dorsale della nuova rete IP BSA UT IV
Alcune reti di campo sono collegate ad un solo nodo COM	Tutte le reti di campo collegate su due nodi della nuova rete IP BSA UT IV
Switch non gestiti	Switch gestiti (managed)
IPv4	IPv6 (IPv4 comunque possibile)
Anelli di campo con più di 7 Switch	Anelli di campo con massimo 7 Switch

Per poter raggiungere la situazione desiderata, è necessario intervenire in modo importante praticamente in tutte le reti di campo.

Il processo ideale è quello di installare la nuova rete di campo multifunzionale predisposta per connettervi tutti gli impianti e poi eseguire la commutazione degli impianti dalle reti esistenti verso la nuova rete.

3.2.3. Protocolli di routing

Il protocollo di routing previsto è MPLS fino alla dorsale della nuova rete. Gli switch delle reti di campo lavorano in layer 2.

Sintesi del gap fra situazione attuale e desiderata, identificabile quale misura da attuare:

Situazione attuale	Richiesta USTRA secondo [1] e [2]
OSPF	MPLS

3.2.4. Concetto SNMP

Le componenti della rete di campo BSA devono poter essere gestite e sorvegliate da un sistema di monitoring centralizzato tramite protocollo SNMP.

I sistemi della dorsale COM sono già oggi monitorati tramite Argomon, che può essere esteso per monitorare i nuovi elementi della rete di campo.

3.2.5. Concetto di sincronizzazione della rete

PTP e SyncE devono essere distribuiti fino al livello sezione.

Sintesi del gap fra situazione attuale e desiderata, identificabile quale misura da attuare:

Situazione attuale	Richiesta USTRA secondo [1] e [2]
NTP	PTP e SyncE

Per descrivere il concetto di sincronizzazione della rete è in preparazione presso USTRA il documento "83044 IP-Netz BSA: Zeit- und Taktverteilung".

Le sorgenti di sincronizzazione della rete saranno rese disponibili alle UT tramite il backbone IP-Netz BSA con protocolli SyncE e PTP.

Quasi tutte le apparecchiature BSA connesse alla rete di campo continueranno comunque a sincronizzarsi tramite NTP.

3.2.6. Integrazione Servizi Dati, Voce e Video

La rete prevista nella direttiva 13040 [1] permette l'integrazione dei servizi già attiva sulla dorsale COM attuale.

3.2.7. Concetto QoS, qualità del servizio

La rete prevista nella direttiva 13040 [1] permette di mantenere i principi della QoS già attiva sulla dorsale COM attuale.

3.2.8. Integrazione video

La rete prevista nella direttiva 13040 [1] permette l'integrazione video già attiva sulla dorsale COM attuale.

3.2.9. Connessioni con altre reti

Connessioni con altre reti locali sono possibili ma da limitare allo stretto necessario. Esse devono essere eseguite secondo la direttiva 13030 [2].

L'interconnessione con le altre UT è possibile attraverso i 2 router MPLS che collegano la dorsale della rete IP BSA UT IV al backbone IP-Netz BSA al CMB e al CMF.

3.3. Sistemi di gestione e sicurezza

3.3.1. NMS

Il sistema NMS deve essere fornito sulla rete IP BSA dell'UT. Quello attualmente in servizio è considerato idoneo.

3.3.2. Gestione degli indirizzi IP

Per la gestione degli indirizzi IP verrà messo a disposizione un sistema IPAM che però necessita comunque localmente di un server DHCP e di un server DNS. Attualmente questi sistemi in UT IV non esistono.

Sintesi del gap fra situazione attuale e desiderata, identificabile quale misura da attuare:

Situazione attuale	Richiesta USTRA secondo [1] e [2]
Nessuna gestione indirizzi IP	IPAM centralizzato (CH)
Nessun server DHCP/DNS	Installazione server DHCP/DNS

È necessario installare un server DHCP e un server DNS. Possono essere macchine virtuali sul sistema di virtualizzazione già attivo per la gestione della dorsale.

3.3.3. Accesso remoto (RAS) SSL-VPN

L'accesso remoto ai sistemi BSA (segnatamente al CT) di ciascun fornitore d'impianto, avviene oggi tramite un servizio RAS offerto da Argonet su infrastrutture proprie ubicate presso la sua sede. Si desidera sostituire questa modalità di accesso remoto tramite un sistema gestito da UT IV e ubicato all'interno del perimetro USTRA.

Sintesi del gap fra situazione attuale e desiderata, identificabile quale misura da attuare:

Situazione attuale	Richiesta USTRA secondo [1] e [2]
Accesso remoto (RAS) tramite servizio esterno	Accesso remoto interno gestito da UT IV

La soluzione proposta è quella di replicare lo stesso tipo d'infrastruttura nella rete UT IV in modo da sciogliere le dipendenze dall'infrastruttura situata oggi presso Argonet.

Il nuovo flusso di accesso alla rete viene rappresentato dalla seguente grafica:

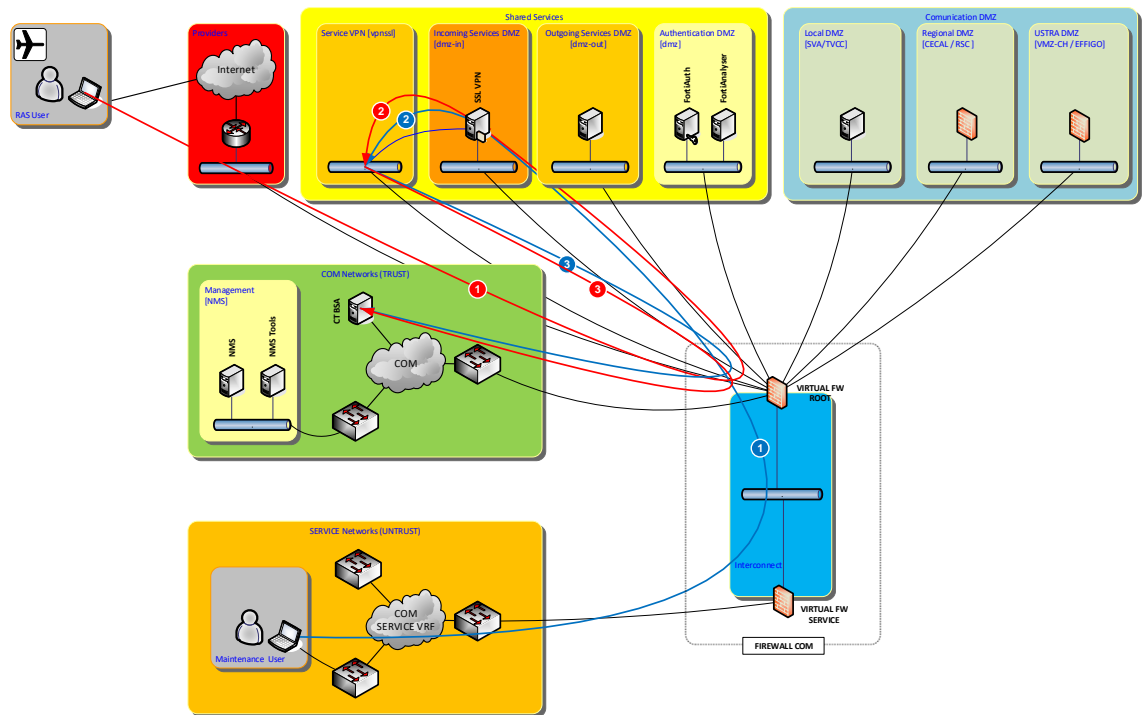


Figura 21: Accesso remoto (RAS)

Un utente esterno, per esempio un fornitore che deve accedere al CT del suo impianto, si collega tramite applicativo VPN (client Fortinet) dal proprio laptop al terminatore VPN su canale securizzato (SSL-VPN).

All'utente si presenta una maschera di immissione delle credenziali che richiede una prima autenticazione con il classico binomio username/password (primo fattore) nonché l'immissione di un token di strong authentication (secondo fattore). Il token, rispetto a quello fisico impiegato oggi, sarà virtuale per le nuove utenze mentre quello fisico (chiavetta RSA) resterà in funzione ma non verrà più estesa se non in casi particolari come locali senza copertura mobile.

Il terminatore VPN verificherà le credenziali di accesso con Fortiauthenticator. Se le credenziali sono valide, all'utente esterno si presenterà un portale web dedicato con tutti gli applicativi che necessita per lavorare. Questo portale è anche chiamato toolbox. Il prodotto che funge da terminatore di VPN raccomandato è PulseSecure.

Naturalmente dovranno essere memorizzati tutti i log degli accessi e questo può essere fatto tramite Fortianalyzer.

3.3.4. System Log (Syslog)

Un importante tassello per l'implementazione delle misure di sicurezza è la capacità di raccogliere centralmente tutti gli eventi che i sistemi operativi tracciano, chiamati anche logs. Ogni log fornisce importanti informazioni riguardo il funzionamento del sistema, le operazioni che sta eseguendo (giornale), allarmi, allerte, informazioni generali, ecc.

I sistemi sono spesso configurati per mostrare i log sul sistema operativo ma questi possono pure essere trasmettessi ad un database centrale tramite protocollo Syslog.

Una volta raccolte centralmente tutte le informazioni nel database, il Syslog server permette di analizzarle in base alle soglie di allerta e allarme configurate e inizializzare delle azioni specifiche.

Sintesi del gap fra situazione attuale e desiderata, identificabile quale misura da attuare:

Situazione attuale	Richiesta USTRA secondo [1] e [2]
Nessun server Syslog	Introduzione server Syslog

Per poter soddisfare i requisiti della direttiva 13030 [2] proponiamo il prodotto Orion Solarwinds, che permette la raccolta di log sulla parte infrastrutturale e su connessioni di rete, switch di campo, server BSA.

3.4. Infrastruttura passiva

Sull'infrastruttura passiva non è necessario nessun intervento. Tutti i percorsi delle fibre ottiche saranno separati dagli EP per permettere la dovuta ridondanza. Un'ulteriore ridondanza sarà garantita laddove necessario attraverso terzi.

3.5. Infrastruttura attiva

3.5.1. Componenti hardware

Per analogia alla Tabella 3 relativa al materiale installato per la rete COM, nella tabella seguente viene elencato il materiale ipotizzabile per adempiere alle richieste USTRA ed i quantitativi previsti per la nuova rete IP BSA di UT IV. Il principio di utilizzo e collegamento del materiale principale previsto è rappresentato nella Figura 20.

ID	Luogo	Router > 2 NNI (p.es. NCS serie 5500)	Router ≤ 2 NNI (p.es. NCS serie 500)	Switch Distribution-Access (p.es. Cisco serie 9000)	Switch di campo (p.es. IE4000)
1	BRO	1		2	3
2	MEN	1		1	6
3	MRG	1		2	17
4	MGG	1	1	2	42
5	CML	1		1	4
6	GEG		1	2	13
7	TAG		1	1	3
8	CEN		1	1	16
9	CMB	1		5	10
10	SFE		1	1	100
11	BSC	1		1	0
12	BIA	1		1	13
13	GRI		1	1	2
14	CMF	1		1	0
15	PIU	1		2	13
16	CAS		1	1	5
17	PAR		1	1	6
18	PIO	1		1	10
19	QUI		1	1	3
20	STA		1	1	25
21	CMA	1		1	0
22	LOG		2	2	80
Totali		12	12	32	371

Tabella 4: Elenco del materiale principale previsto

4. Processo di migrazione e termini

Il processo di migrazione della rete COM verso la rete IP BSA uniformata secondo le richieste di USTRA si basa sostanzialmente sui principi formulati nel documento di riferimento [3]:

- Principio 1: Protezione dell'investimento
- Principio 2: Migrazione adattata al ciclo di vita
- Principio 3: Passaggio alla conformità

Dai principi elencati ne deriva un piano termini presentato nell'allegato A03 [10] e completato con i commenti dei seguenti capitoli.

4.1. Tappa 1 – Galleria Mappo-Morettina

La prima tappa permette di integrare la sezione LOG (tratta stradale Magadino – Locarno, comprendente la galleria Mappo-Morettina) nei sistemi delle strade nazionali (vedi cap. 2.1) e simultaneamente di creare i primi due nodi di comunicazione della rete IP BSA UT IV. In particolare, saranno eseguite le seguenti attività:

- ID 4: Come menzionato nella premessa iniziale al cap. 2.1, la galleria Mappo-Morettina cambia di proprietà divenendo a tutti gli effetti una strada nazionale. Un progetto di migrazione verso i sistemi delle strade nazionali è già stato avviato da USTRA filiale 5. Siccome bisognerà creare nuovi nodi di comunicazione per la sezione Mappo-Morettina, nell'ambito del progetto citato si propone di realizzare i nuovi nodi secondo le richieste di USTRA per la rete IP BSA UT IV (p.es. MPLS, ecc.), in modo da poter essere da subito conformi secondo il principio 3 alle direttive emesse. Questo offre la possibilità di approcciare a gradi questa nuova tecnologia, permettendo così ai sistemisti di UT IV di assimilare l'esperienza necessaria alla futura rete IP BSA del territorio di loro competenza ("learning by doing").
- ID 5: La rete COM permette già sin d'ora di implementare i sistemi di sicurezza e di gestione secondo le direttive 13030 [2] e 13040 [1] di USTRA. Per poter interfacciare la rete COM al backbone IP-Netz BSA nazionale è auspicabile installare già durante questa fase i nuovi firewall previsti al CMB e al CMF per la rete IP BSA UT IV finale.
- ID 6+7+8: A partire dal momento che il tool IPAM ed il backbone IP-Netz BSA a livello svizzero saranno disponibili è opportuno integrare la rete COM attuale, da una parte per uniformare la gestione e dall'altra per permettere lo smantellamento della rete VDV-CH. I due nuovi nodi COM della sezione LOG, conformi alle nuove direttive, saranno pertanto allacciati ai nodi del backbone IP-Netz BSA situati al CMB ed al CMF. Queste attività saranno seguite e accompagnate dal progettista specializzato per tutte le attività preliminari (ID 7, 8, 16 e 17).

Le attività appena descritte sono riassunte nello schema di principio seguente.

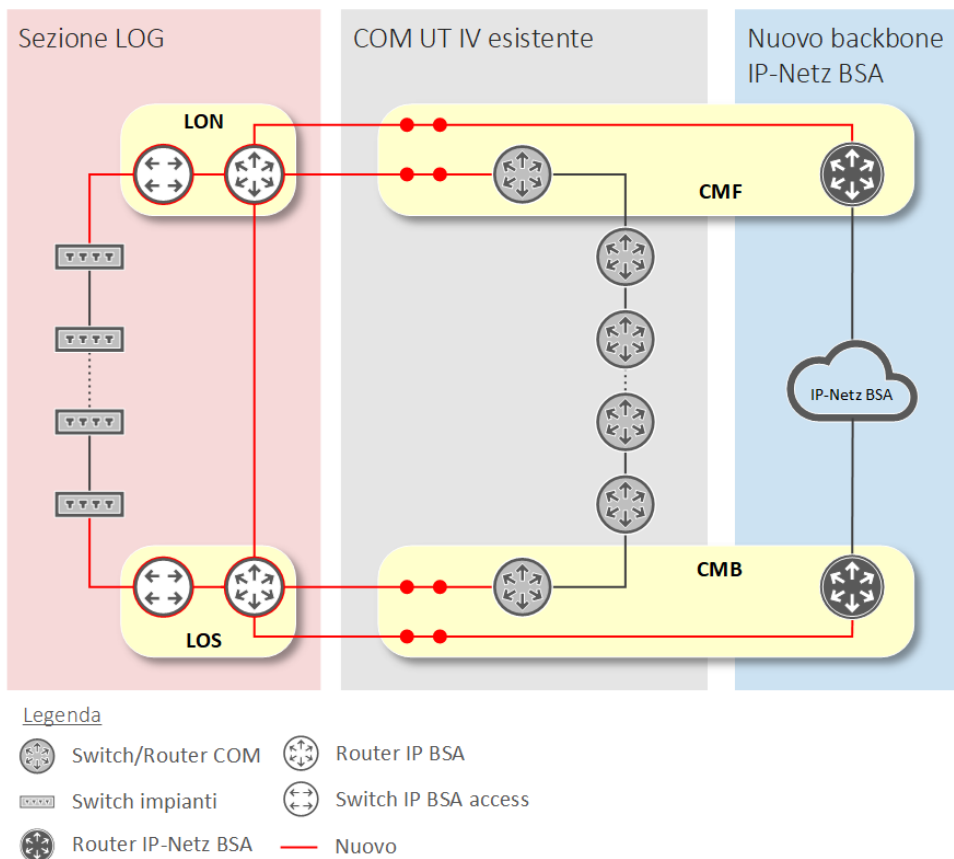


Figura 22: Tappa 1, nuovi nodi principali LOG e integrazione backbone IP-Netz BSA

4.2. Tappa 2 – Pianificazione migrazione

La seconda tappa permette di pianificare in dettaglio la migrazione, così come la preparazione di tutti i documenti di riferimento e l'allestimento degli appalti necessari per la realizzazione della nuova rete IP BSA UT IV nella sua totalità. In particolare, saranno eseguite le seguenti attività:

- ID 12+13: Il committente ha espresso la necessità di essere accompagnato lungo tutta la migrazione della rete COM verso la rete IP BSA UT IV. È pertanto necessario assegnare l'incarico di accompagnamento BHU subito all'inizio del progetto.
- ID 15: Delle attività preliminari sono necessarie per poter adattare la rete COM ed integrarla rapidamente nel backbone IP-Netz BSA svizzero. Queste attività preliminari dovranno essere assegnate ad un progettista specializzato. Queste attività preliminari prevedono anche le attività ID 7+8.
- ID 16: La realizzazione della nuova rete IP BSA UT IV deve essere supportata da documenti di riferimento univoci e completi. I documenti di riferimento hanno lo scopo di mettere a disposizione una base documentale che descriva come strutturare le reti di campo, quale tipologia di equipaggiamenti utilizzare per il rinnovo delle stesse e dei nodi di comunicazione principali, come assegnare gli indirizzi IP e altri aspetti specifici in modo da adempiere nelle fasi successive al principio 3. Prima di poter mettere in appalto le opere relative alla rete è pertanto necessario allestire i nuovi documenti di riferimento.

- ID 17: Appena USTRA mette a disposizione il tool centrale NAC, è possibile adattare l'accesso remoto della rete COM così da allinearsi alla direttiva 13030 [2].
- ID 19: Per poter rispettare il piano termini stabilito è opportuno poter attribuire il mandato di progettazione, allestimento appalti e direzione lavori del core UT IV ("Erschliessungsring") della rete IP BSA entro metà del 2021. Il progettista dovrà avere conoscenze tecniche approfondite nelle reti di comunicazione.
- ID 20+21: La fase di progettazione permette di specificare i dettagli tecnici della migrazione dei nodi di comunicazione core ("Erschliessungsring"), così come di pianificare in dettaglio la migrazione. A seconda dei lotti definiti durante la progettazione e della procedura di acquisizione stabilita da parte di USTRA, si possono allestire gli appalti necessari alla realizzazione completa della nuova rete IP BSA UT IV. L'attribuzione dei singoli mandati definisce di fatto l'inizio vero e proprio della migrazione dall'attuale rete COM alla futura rete IP BSA.
- ID 23: Per completare la rete IP BSA UT IV secondo le richieste è necessario poter attribuire il mandato di progettazione, allestimento appalti e direzione lavori delle reti di campo UT IV. Il progettista dovrà avere conoscenze tecniche approfondite nelle reti di comunicazione.
- ID 24+25: La fase di progettazione permette di specificare i dettagli tecnici, così come di pianificare in dettaglio la realizzazione delle reti di campo di ogni sezione. A seconda dei lotti definiti durante la progettazione e della procedura di acquisizione stabilita da parte di USTRA, si possono allestire gli appalti necessari alla realizzazione delle reti di campo UT IV. L'attribuzione dei singoli mandati definisce l'inizio della realizzazione di reti di campo uniformi e gestite centralmente, così come richiesto da USTRA.

4.3. Tappa 3 – Realizzazione migrazione COM vs. rete IP BSA

La terza ed ultima tappa permette di realizzare la nuova rete IP BSA UT IV nella sua totalità. La realizzazione è suddivisa come indicato nel piano termini. In particolare, le attività si svolgeranno come segue:

- ID 28+29+30: Nell'ambito di alcuni EP, ritenuti interessanti a livello di tempistiche previste, vengono realizzati i nodi di comunicazione principali ed i nodi di access, nonché le reti di campo nelle rispettive sezioni stradali. Passo dopo passo la rete di comunicazione COM comincia la sua migrazione verso la rete IP BSA e può essere messa in servizio gradualmente. Gli impianti BSA delle sezioni vengono man mano adattati e commutati sulla nuova rete ed i componenti della vecchia rete possono essere smantellati ed immagazzinati come materiale di riserva. Le figure seguenti mostrano la situazione attuale ed il principio di realizzazione della nuova rete e di commutazione degli impianti BSA.

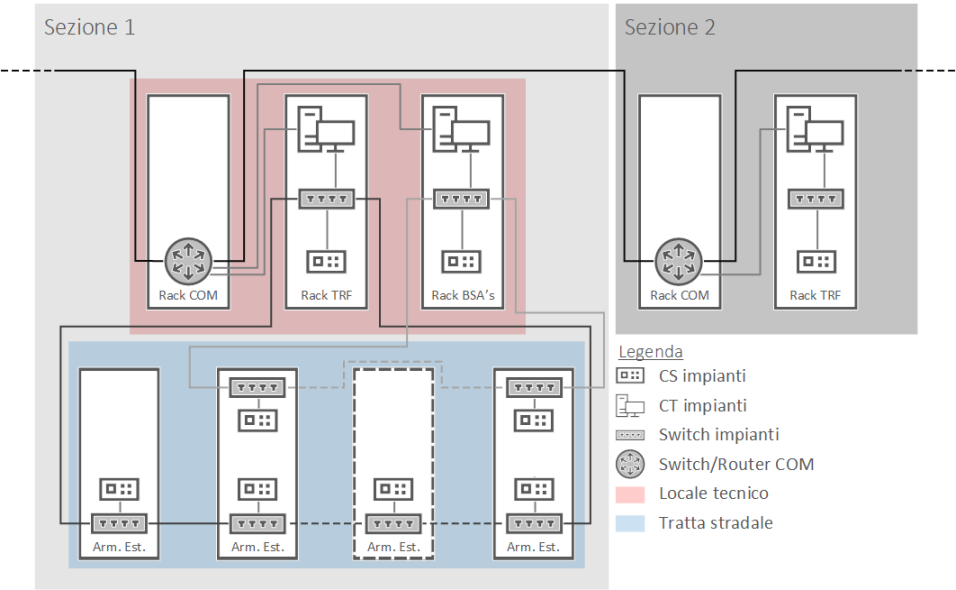


Figura 23: Schema di principio di una sezione (esistente)

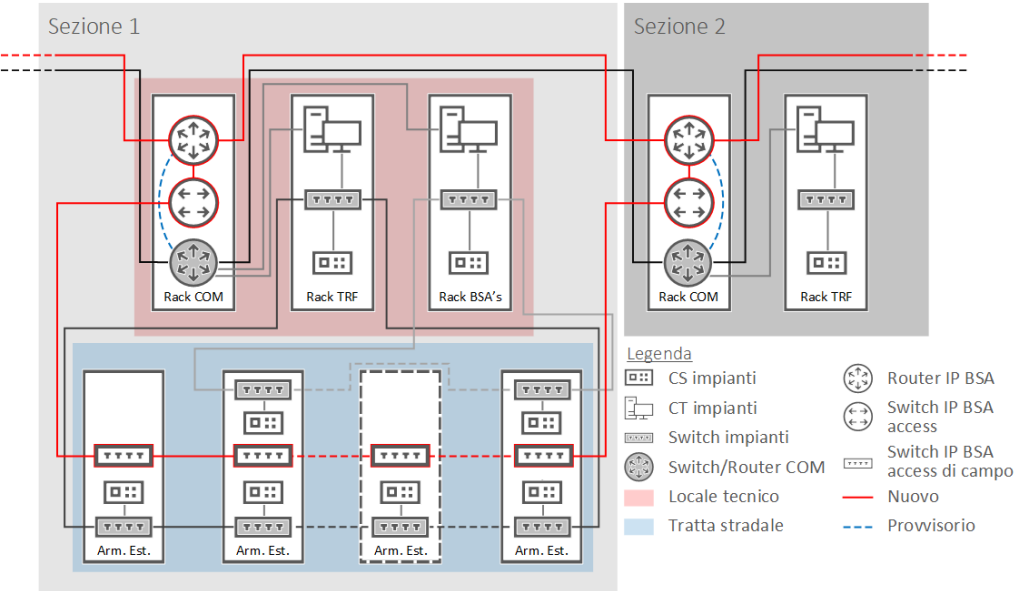


Figura 24: Schema di principio realizzazione rete IP BSA di una sezione

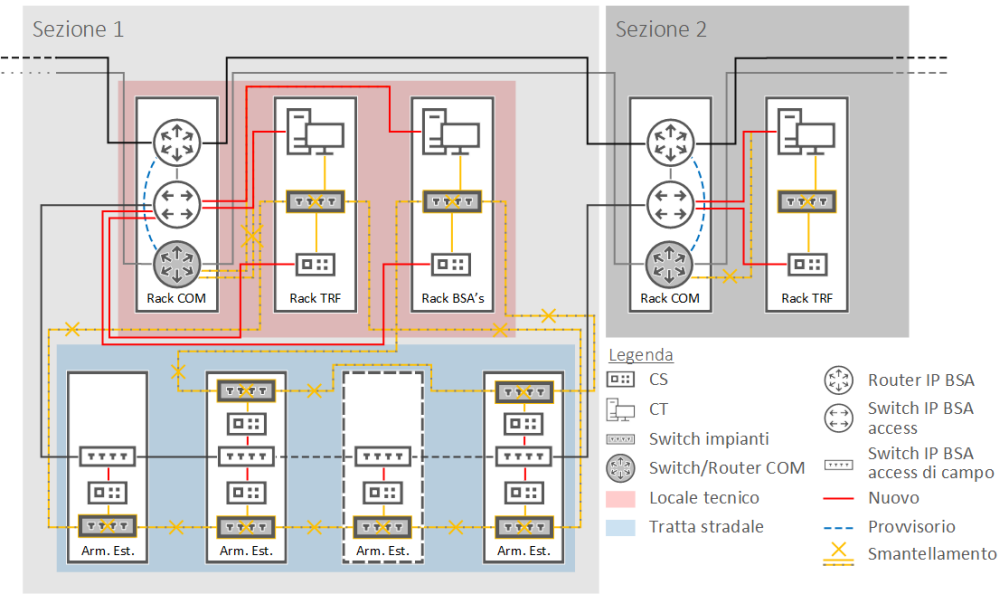


Figura 25: Principio di commutazione impianti BSA su rete IP BSA di una sezione

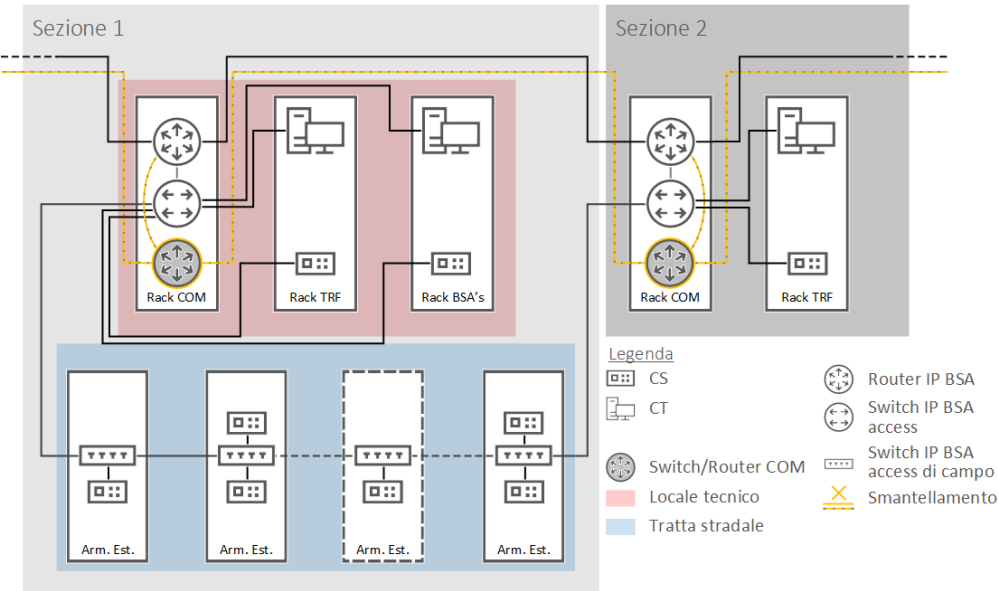


Figura 26: Schema di principio smartellamento rete COM

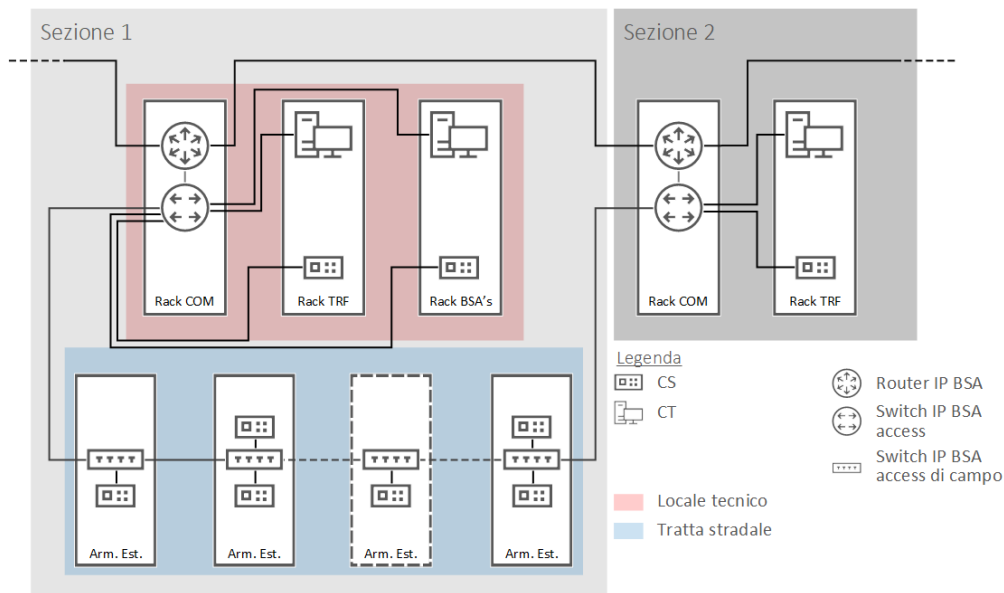


Figura 27: Schema di principio stato finale rete IP BSA UT IV di una sezione

- ID 31+32: Nelle rimanenti sezioni autostradali di UT IV, analogamente a quanto raffigurato nelle figure precedenti, viene creato dapprima il resto della dorsale della nuova rete IP BSA ("Erschliessungsring") ed in seguito i rispettivi nodi di accesso (access), così come vengono create tutte le reti di campo nelle singole sezioni. Prioritariamente vengono realizzati tutti i nodi principali (core) in modo da metterli in esercizio nella loro totalità. In seguito, ogni sezione può essere messa in esercizio autonomamente adattando e commutando man mano sulla nuova rete IP BSA gli impianti BSA. L'interfacciamento della rete IP BSA UT IV verso il backbone IP-Netz BSA nazionale, può venire ripreso dai nodi di comunicazione del CMB e CMF come stabilito nel progetto e secondo la figura seguente. I nodi principali della galleria Mappo-Moretina ritornano ad occuparsi solo della sezione d'appartenenza. I nuovi firewall installati nell'attività ID 5 sono configurati per il loro funzionamento finale e secondo le direttive.

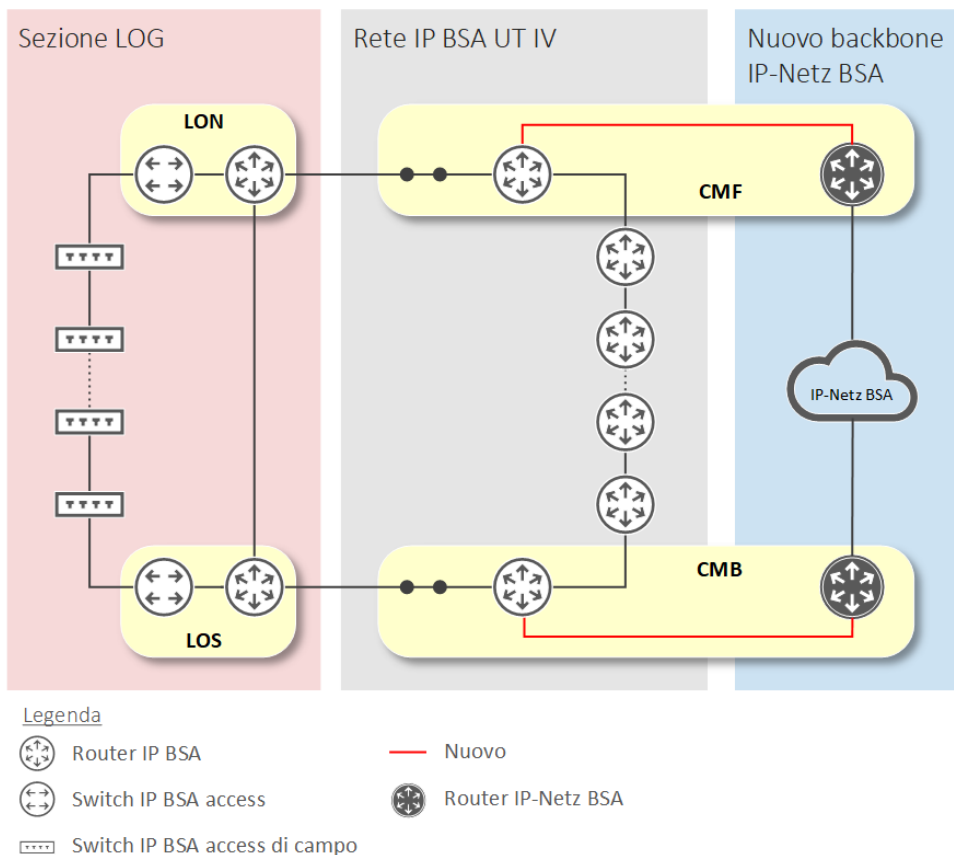


Figura 28: Interfacciamento finale rete IP BSA UT IV con backbone IP-Netz BSA

Nota: I nodi di comunicazione della rete COM sono stati rinnovati nel 2018. La loro durata di vita ipotetica è di circa 10 anni e applicando il principio 1 di protezione dell'investimento ed il principio 2 relativo al ciclo di vita degli equipaggiamenti installati, essi dovrebbero essere sostituiti non prima della fine dell'anno 2028. La pianificazione stabilita permette di adempiere parzialmente a questi principi, in quanto gli switch/router principali saranno sostituiti anzitempo (entro la fine del 2025). Ciononostante, e considerando i tempi necessari a realizzare in seguito tutte le reti di campo, si ritiene che questo compromesso sia accettabile.

4.4. Termini esterni

I termini delle tre tappe descritte nei capitoli precedenti sono stati stabiliti considerando i seguenti termini esterni:

- ID 37+38+39+40+41+42: Questi termini esterni sono stati comunicati durante l'elaborazione del presente concetto di migrazione e sono stati dichiarati come obiettivi inderogabili di USTRA. Essi hanno ripercussioni e sono fondamentali sulle attività elencate precedentemente, in particolare per l'integrazione della rete IP BSA UT IV e dei rispettivi servizi nel backbone IP Netz BSA nazionale.
- ID 43+44+45: La realizzazione della nuova rete IP BSA UT IV (core, access e reti di campo) in alcune sezioni avverrà all'interno dei progetti EP08, EP28 e EP18, in modo da sfruttare le sinergie che questi EP metteranno a disposizione.

4.5. Riassunto delle misure previste

Nella seguente tabella vengono ripresi i punti dell'analisi delle differenze ("GAP-Analyse") tra l'attuale COM ed i requisiti richiesti da USTRA [4] e riassunte le rispettive misure previste per adempiere a tutte le esigenze.

Tema	Misura
Separazione rete strade nazionali (SN) e rete strade cantonali (SC)	<ul style="list-style-type: none"> Nessuna misura prevista.
Architettura secondo cap. 2 della direttiva [1]	<ul style="list-style-type: none"> Installazione di nuovi router con tecnologia MPLS per tutti i nodi principali della rete IP BSA UT IV. Realizzazione di reti di campo multiutente (una rete comune per tutti gli impianti BSA) direttamente integrate alla dorsale della rete IP BSA UT IV. Collegamento di ogni rete di campo multiutente ad almeno due nodi principali distinti. Creazione di anelli di reti di campo con al massimo 7 switch.
Equipaggiamenti di rete secondo cap. 3 della direttiva [1]	<ul style="list-style-type: none"> Fornitura di nuovi switch/router carrier grade MPLS che permettono l'utilizzo di link da 100 Gbps. Inizialmente e secondo quanto stabilito nel progetto saranno utilizzati link da 10 Gbps. Fornitura di nuovi switch delle reti di campo gestibili e integrabili nell'NMS della rete IP BSA UT IV. Fornitura di un sistema di sincronizzazione degli equipaggiamenti all'interno della rete di tipo PTP e SyncE.
Equipaggiamenti di rete IPv6	<ul style="list-style-type: none"> Fornitura di nuovi switch/router principali IPv6. Fornitura di nuovi switch delle reti di campo IPv6.
Tools secondo cap. 5-9 della direttiva [1] e sicurezza secondo la direttiva [2]	<ul style="list-style-type: none"> Integrazione della gestione degli indirizzi IP della rete IP BSA UT IV nel tool IPAM centralizzato a livello nazionale. A tale scopo è prevista l'installazione all'interno della nuova rete di un server DHCP e di un server DNS. Ampliamento dell'NMS per l'integrazione delle funzionalità degli switch/router MPLS. Adattamento delle modalità di accesso remoto alla rete da parte di terzi, in maniera che equipaggiamenti e gestione sottostiano al controllo di UT IV. Implementazione del tool NAC messo a disposizione da USTRA. Installazione di un server Syslog per la raccolta dei log di tutti gli equipaggiamenti della rete.

Tabella 5: Riassunto delle misure previste

5. Stima costi e pianificazione finanziaria

A seguito dell'analisi della soluzione e della tecnologia da adottare per la nuova rete IP BSA di UT IV, sono stati stimati i costi con una precisione del $\pm 30\%$, i quali sono rappresentati nella tabella seguente.

Pos.	Descrizione	Tipo	Qtà	Costo unitario [CHF]	Costo per posizione [CHF]	Costo totale investimento [CHF]
1	Accompagnamento Committente (BHU)					140'000
1.1	Prestazioni di supporto al Committente (BHU)	gl	1	140'000	140'000	
2	Attività preliminari (prestazioni di servizio)					190'000
2.1	Allestimento documenti di riferimento	gl	1	60'000	60'000	
2.2	DL adattamento sistemi di sicurezza e di gestione	gl	1	50'000	50'000	
2.3	DL integrazione backbone IP-Netz-BSA, IPAM, NAC	gl	1	30'000	30'000	
2.4	Prestazioni UT IV	gl	1	50'000	50'000	
3	Attività preliminari (forniture e fornitori)					530'000
3.1	Server DNS/DHCP	gl	1	10'000	10'000	
3.2	Firewall	pz	2	200'000	400'000	
3.3	Monitoring e Syslog	gl	1	10'000	10'000	
3.4	Accesso remoto	gl	1	30'000	30'000	
3.5	Configurazioni sicurezza e integrazione backbone IP-Netz-BSA, IPAM, NAC	gl	1	80'000	80'000	
4	Prestazioni di servizio core UT IV rete IP BSA					210'000
4.1	Progettazione core UT IV rete IP BSA	gl	1	20'000	20'000	
4.2	Appalti, aggiudicazione e DL core UT IV rete IP BSA	gl	1	100'000	100'000	
4.3	Prestazioni UT IV	gl	1	90'000	90'000	
5	Fornitura e installazione core UT IV rete IP BSA					2'390'000
5.1	Router ≤ 2 NNI	pz	10	25'000	250'000	
5.2	Router > 2 NNI	gl	12	120'000	1'440'000	
5.3	Interfacce 10 Gbps	gl	1	300'000	300'000	
5.4	Prestazioni fornitore per realizzazione e attivazione	gl	1	400'000	400'000	
6	Prestazioni di servizio reti di campo UT IV					900'000
6.1	Progettazione reti di campo UT IV	gl	1	100'000	100'000	
6.2	Appalti, aggiudicazione e DL reti di campo UT IV	gl	1	300'000	300'000	
6.3	Prestazioni UT IV	gl	1	500'000	500'000	
7	Fornitura e installazione reti di campo UT IV					4'150'000
7.1	Costo globale materiale	gl	1	2'650'000	2'650'000	
7.2	Prestazioni fornitori per realizzazione e attivazione	gl	1	1'500'000	1'500'000	
Totale parziale CHF (IVA esclusa)						8'510'000
IVA					7.70%	655'270
Totale CHF (IVA inclusa)						9'165'270

Tabella 6: Stima costi rete IP BSA UT IV

Note relative alla Tabella 6:

- Come discusso durante le riunioni di progetto, le ripercussioni finanziarie sugli impianti BSA dovute alla nuova rete IP BSA non devono essere considerate. È comunque importante segnalare che nella nuova rete IP BSA non è contemplato nessun

VMS per la gestione delle sorgenti-destinazioni video (nella rete COM attuale il VMS è parte integrante della rete). Durante la progettazione della nuova rete IP BSA bisognerà pertanto avviare un progetto per la realizzazione di un nuovo VMS UT IV.

- Pos. 3.2: Infrastruttura firewall comprendente Fortianalyzer, Fortiauthenticator, ecc.
- Pos. 3.4: Accesso remoto comprendente RAS, SSL-VPN.
- Pos. 5.1: I costi dei nodi principali della sezione Mappo-Morettina non vengono considerati nel presente concetto di migrazione, in quanto a carico del progetto di integrazione della sezione nelle strade nazionali.
- Pos. 5.3: I moduli ottici per la trasmissione 10 Gbps si differenziano a seconda delle distanze da coprire. La quantità totale prevista per questi moduli si attesta a 82 unità. La progettazione finale sarà in grado di quantificare con precisione le quantità necessarie. Se si volessero già inserire le interfacce a 100 Gbps, i costi andrebbero moltiplicati per un fattore 5.
- Pos. 6.3: Sono considerate tutte le prestazioni di accompagnamento dei fornitori nei diversi luoghi. Eventuali sinergie e ottimizzazioni con EP o progetti specifici permetterebbero di contenere questi costi.
- Pos. 7.1: Viene definito un costo globale sulla base della quantità di switch attualmente presenti per le reti da campo. Sarà il progetto di dettaglio a stabilire il quantitativo esatto necessario per ogni rete di campo. In questa posizione è compreso il costo degli switch access nei locali tecnici dove è installato lo switch core.
- Pos. 7.2: Nelle prestazioni dei fornitori sono comprese tutte le prestazioni per recarsi nei diversi luoghi (ca. 370 luoghi), scollegare le reti di campo esistenti e attivare le nuove reti di campo. Oltre al fornitore della rete IP BSA, dovranno essere coinvolti anche i diversi fornitori degli impianti BSA.

Sulla base dei costi stimati nella Tabella 6 ed applicando il piano termini proposto [10] è possibile stabilire la pianificazione finanziaria sull'arco degli anni per le voci principali delle misure previste.

Pos.	Descrizione	2020	2021	2022	2023	2024	2025	2026	2027	2028
1	Accompagnamento Committente (BHU)	-	0.023	0.023	0.023	0.023	0.015	0.015	0.015	0.015
2	Attività preliminari (prestazioni di servizio)	-	0.205	-	-	-	-	-	-	-
3	Attività preliminari (forniture e fornitori)	-	0.571	-	-	-	-	-	-	-
4	Prestazioni di servizio core UT IV rete IP BSA	-	0.046	0.067	-	0.057	0.057	-	-	-
5	Fornitura e installazione core UT IV rete IP BSA	-	-	-	-	0.528	2.046	-	-	-
6	Prestazioni di servizio reti di campo UT IV	-	-	0.135	0.059	0.086	0.086	0.215	0.215	0.172
7	Fornitura e installazione reti di campo UT IV	-	-	-	-	0.670	0.223	1.341	1.341	0.894
Totali per anno [Mio. CHF], IVA inclusa		-	0.844	0.225	0.082	1.363	2.428	1.571	1.571	1.081

Tabella 7: Pianificazione finanziaria delle misure previste

Note relative alla Tabella 7:

- Le posizioni della tabella si riferiscono alle posizioni principali della stima costi.
- I totali indicati negli anni sono in milioni di CHF, comprendenti di IVA al 7.70%.

6. Ripercussioni sull'esercizio

6.1. Organizzazione

La struttura organizzativa di UT IV è predisposta per l'esercizio e la manutenzione delle strade nazionali, indipendentemente dalle tipologie e tecnologie degli impianti BSA presenti sul terreno.

Attualmente la rete COM è gestita dai sistemisti di UT IV con competenze basilari delle reti ethernet e con una formazione apposita relativa agli strumenti messi a disposizione dall'attuale rete COM. La gestione è accompagnata da un contratto di manutenzione con il fornitore della rete.

L'introduzione di una nuova tecnologia di rete ha evidentemente ripercussioni sul know-how acquisito negli anni da parte dei sistemisti di UT IV, i quali dovranno essere formati specificamente sulla nuova rete IP BSA (questo però avviene per ogni nuovo impianto BSA).

6.2. Risorse e competenze

Con la nuova rete IP BSA è consigliato potenziare il team UT IV con personale specializzato nelle reti informatiche e nella specifica tecnologia. Questo potenziamento non è però obbligatorio, bensì potrebbe essere attuato con i sistemisti esistenti attraverso una formazione ed una istruzione specifica durante la realizzazione della nuova rete IP BSA.

A tale proposito nel presente concetto è stato proposto di realizzare presso la galleria Mappo-Morettina i due nuovi nodi di comunicazione già conformi alle direttive e richieste USTRA (secondo il principio 3, vedi cap. 4). Ciò permetterebbe ai sistemisti di avvicinarsi a piccoli passi alla nuova tecnologia della rete in modo da acquisire know-how sufficiente per quando ci sarà la migrazione totale della rete COM verso la rete IP BSA.

6.3. Costi

Oltre ai costi di investimento indicati nel cap. 5 sono ipotizzabili ulteriori costi:

- Acquisizione di personale specialistico da parte di UT IV: ca. CHF 100'000 all'anno per persona (salario annuo, esclusi oneri e prestazioni sociali da parte del datore di lavoro). Un'unità supplementare per UT IV dovrebbe essere sufficiente, se un piano di formazione/istruzione dei sistemisti esistenti viene messo in atto.
- Aumento dei costi del contratto di manutenzione con il futuro fornitore della rete IP BSA. I futuri costi di manutenzione dipenderanno dal livello di servizio richiesto, ma sicuramente sarà necessario inizialmente un supporto allargato. I costi di manutenzione possono essere stimati a ca. CHF 400'000 all'anno per tutta la nuova rete IP BSA e le nuove reti di campo (oggi non considerate nel contratto di manutenzione del fornitore della rete COM).
- L'aumento dei costi del personale rispettivamente del contratto di manutenzione della rete di comunicazione hanno evidentemente una ricaduta sul contratto di prestazioni tra UT IV e USTRA. Anche in questo caso bisogna considerare un aumento dei costi per USTRA. Una quantificazione non è però per il momento fattibile.

7. Prossimi passi

Il concetto di migrazione proposto e le rispettive tempistiche richiedono dei lavori preliminari da parte di USTRA elencati qui di seguito:

1. Generazione di progetto e pianificazione dei crediti di progettazione e realizzazione della rete IP BSA.
2. Richiesta d'offerta e attribuzione di un mandato di accompagnamento al committente (BHU).
3. Richiesta d'offerta per la ricerca di un progettista specializzato per le attività preliminari della rete IP BSA (integrazione rete COM in IPAM e nel backbone IP-Netz BSA, allestimento documenti di riferimento, adattamento sistemi di sicurezza/gestione).
4. Attribuzione del mandato di progettista specializzato per le attività preliminari della rete IP BSA.
5. Richiesta d'offerta per la ricerca di un progettista specializzato per la progettazione, appalti e direzione lavori del core ("Erschliessungsring") della rete IP BSA di UT IV.
6. Attribuzione del mandato di progettista specializzato per la progettazione, appalti e direzione lavori del core della rete IP BSA di UT IV.
7. Richiesta d'offerta per la ricerca di un progettista specializzato per la progettazione, appalti e direzione lavori delle reti di campo UT IV.
8. Attribuzione del mandato di progettista specializzato per la progettazione, appalti e direzione lavori delle reti di campo UT IV.

Una volta attribuiti i mandati di BHU e di progettazione specialistica, bisognerà seguire le attività previste nel piano termini [10] per poter mantenere i milestone previsti dal presente concetto di migrazione.

8. Glossario

Abbreviazione	Significato
AET	Azienda Elettrica Ticinese
ASTRA	Bundesamt für Strassen
BHU	Supporto al committente
BIA	Sezione Biaschina
BIT	Bundesamt für Informatik und Telekommunikation
BRO	Sezione Chiasso-Brogeda
BSA	Equipaggiamenti di esercizio e sicurezza
BSC	Sezione Biasca
CAS	Sezione Casletto
CCIR	Consultative Committee on International Radio
CECAL	Centrale Comune di Allarme
CEN	Sezione Ceneri
CMA	Sezione Airolo
CMB	Sezione centro manutenzione Bellinzona-Camorino
CMF	Sezione centro manutenzione Faido
CML	Sezione centro manutenzione Lugano (Noranco)
COM	Rete di comunicazione nel perimetro di competenza UT IV
CPU	Central Processing Unit
CSI	Centro sistemi informativi
CT	Controllore di testa (comando impianto)
DHCP	Dynamic Host Configuration Protocol
DiffServ	Differentiated Service Architecture
DL	Direzione lavori
DMZ	Demilitarized Zone
DNS	Domain Name System
EP	Erhaltungsprojekt (progetto di manutenzione)
FO	Fibra ottica
Fps	Frames per second
Gbps	Gigabit per second
GE	Gigabit-Ethernet
GE V	Unità territoriale V
GEG	Sezione Gentilino
GG	Gestione Generale
GO	Gestione Oggetto (sezione)
GRI	Sezione Gribbiasca
IEEE	Institute of Electrical and Electronics Engineers
IGMP	Internet Group Management Protocol
IP	Internet Protocol
IPAM	IP Address Management
KBU	Piccola manutenzione strutturale
KNA	Kommunikationsnetzwerk Abschnitt / Rete comunicazione sezione

Abbreviazione	Significato
LAN	Local Area Network
LOG	Sezione Mappo-Moretina
LON	Locale tecnico Locarno nord
LOS	Locale tecnico Locarno sud
LUN	Logical Unit Number
MEN	Sezione Mendrisio
MET	Impianto meteo
MGG	Sezione Melide-Grancia
MGN	Locale tecnico Melide-Grancia nord
MGS	Locale tecnico Melide-Grancia sud
MI	Modulo Interfaccia
MRG	Sezione Maroggia
MSDP	Multicast Source Discovery Protocol
MSDP	Multicast Source Discovery Protocol
NAC	Network Access Control
NAT	Network Address Translation
NCM	Network Configuration Manager
NMS	Network Management System
NTP	Network Time Protocol
NTSC	National Television Standards Committee
OPC	Open Platform Communications
OSPF	Open Shortest Path First
PAL	Phase Alternating Line
PAR	Sezione Pardorea
PIM-SM	Protocol Independent Multicast Sparse Mode
PIO	Sezione Piottino
PIU	Sezione Piumogna
PMV	Pannello messaggio variabile
PoE	Power over Ethernet
PTP	Precision Time Protocol
QoS	Quality of Service
QUI	Sezione Quinto
RAS	Remote Access Service
ROV	Sezione Roveredo
RSC	Rete comunicazione strade cantonali
RZ	Rechenzentrum (centro di calcolo)
SA-CH	Architettura di sistema Svizzera
SC	Strade cantonali
SGE	Sistema di gestione
SN	Strade nazionali
SNMP	Simple Network Management Protocol
SOS	Impianto SOS
SSL-VPN	Secure Sockets Layer Virtual Private Network
STA	Sezione Stalvedro
SyncE	Synchronous Ethernet
Syslog	System Log
TAG	Sezione Taverne

Abbreviazione	Significato
TRF	Impianto traffico
UMTS	Universal Mobile Telecommunications System
USTRA	Ufficio federale delle strade
UT IV	Unità territoriale IV
VDV-CH	Verkehrsdatenverbund Schweiz (infrastruttura per lo scambio di dati operativi)

Abbreviazione	Significato
VLAN	Virtual LAN
VM	Virtual Machine
VM-CH	Gestione traffico Svizzera
VMS	Video Management System
VMZ-CH	Centrale gestione traffico Svizzera
VTV	Impianto video
WAN	Wide Area Network

Tabella 8: Abbreviazioni

9. Indici

Indice delle figure

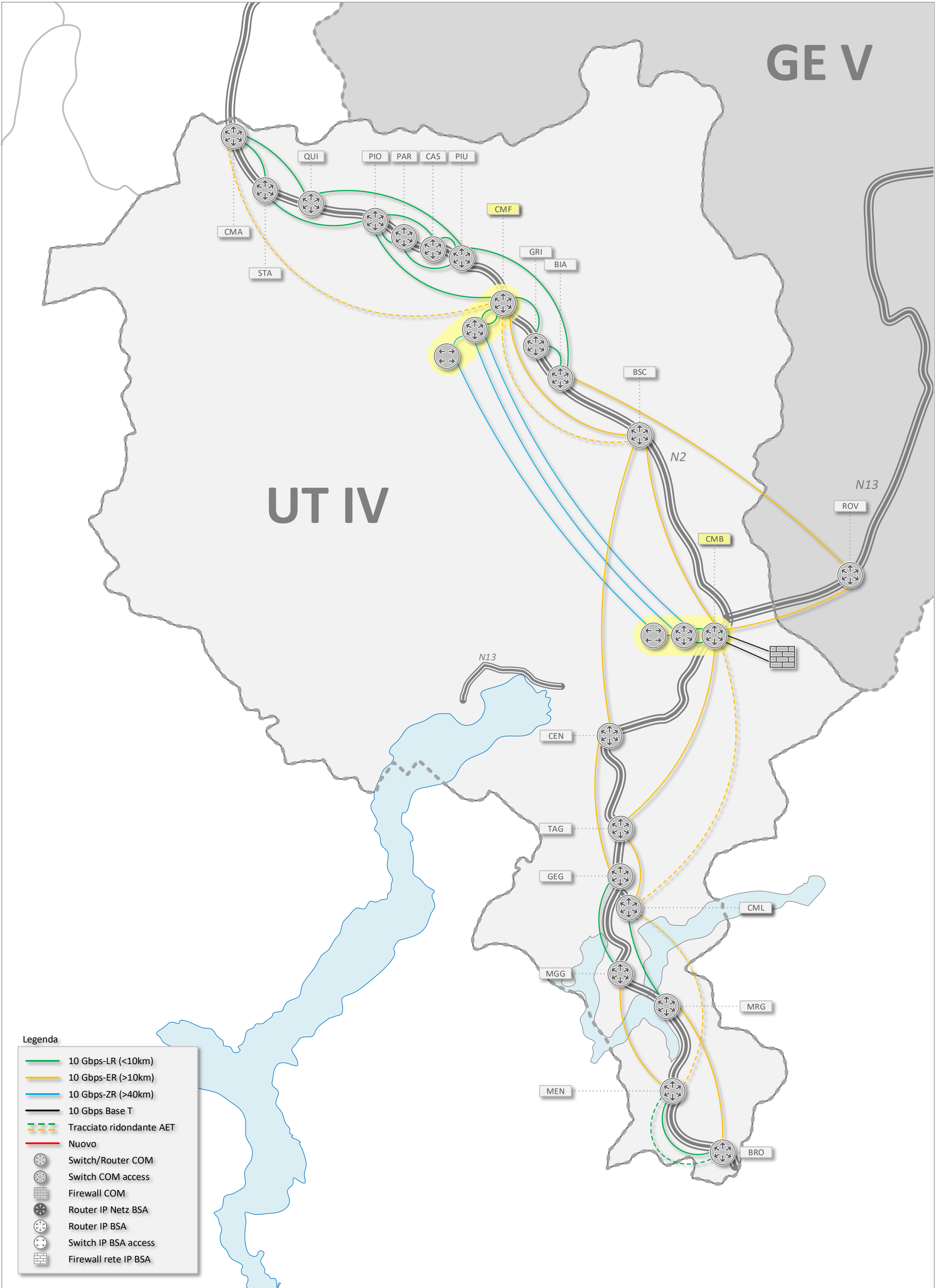
Figura 1: Livelli dell'architettura di rete COM.....	14
Figura 2: Schema della rete COM – Nodi principali.....	15
Figura 3: Reti di campo (impianti BSA) messe a disposizione dalla rete COM.....	16
Figura 4: Schema a blocchi connessioni esterne	20
Figura 5: Schema di accesso RAS.....	20
Figura 6: Schema di principio globale dell'integrazione con VM-CH.....	21
Figura 7: Collegamento COM VDV-CH per Boschung	22
Figura 8: Collegamento Inrix.....	23
Figura 9: Architettura server NMS/VMS	23
Figura 10: Schema di principio ridondanza livello VMWare e Storage	24
Figura 11: Schema logico installazione CMB-CMF	25
Figura 12: Schema di principio della soluzione server-storage.....	26
Figura 13: Argomon, esempio grafici di traffico e tempi di risposta.....	27
Figura 14: Argomon, esempio carico CPU e utilizzo dischi fissi	27
Figura 15: Connessioni dei firewall	28
Figura 16: Schema logico di connessione del firewall	28
Figura 17: Architettura software VMS	33
Figura 18: Delimitazione rete IP BSA UT IV.....	34
Figura 19: Nuova dorsale rete IP BSA UT IV	35
Figura 20: Principio d'integrazione reti di campo nella dorsale rete IP BSA UT IV.....	36
Figura 21: Accesso remoto (RAS).....	39
Figura 22: Tappa 1, nuovi nodi principali LOG e integrazione backbone IP-Netz BSA.....	42
Figura 23: Schema di principio di una sezione (esistente)	44
Figura 24: Schema di principio realizzazione rete IP BSA di una sezione	44
Figura 25: Principio di commutazione impianti BSA su rete IP BSA di una sezione	45
Figura 26: Schema di principio smantellamento rete COM	45
Figura 27: Schema di principio stato finale rete IP BSA UT IV di una sezione	46
Figura 28: Interfacciamento finale rete IP BSA UT IV con backbone IP-Netz BSA.....	47

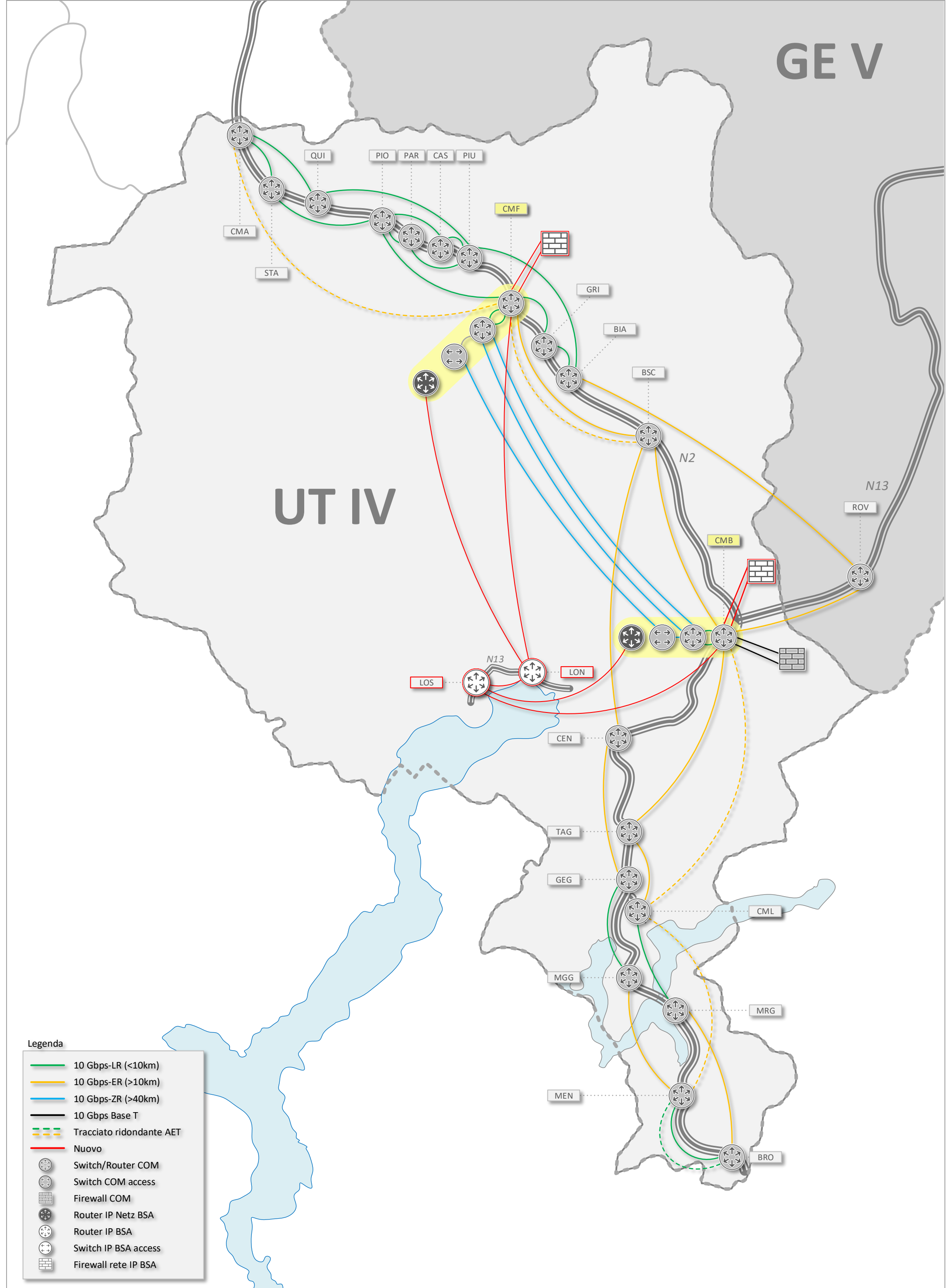
Indice delle tabelle

Tabella 1: Reti di campo impianti BSA	17
Tabella 2: Servizi connessioni WAN	19
Tabella 3: Elenco del materiale principale installato.....	30
Tabella 4: Elenco del materiale principale previsto	40
Tabella 5: Riassunto delle misure previste.....	48
Tabella 6: Stima costi rete IP BSA UT IV	49
Tabella 7: Pianificazione finanziaria delle misure previste.....	50
Tabella 8: Abbreviazioni.....	54

10. Allegati

- [8] Allegato A01 – Schema geografico della rete COM
- [9] Allegato A02 – Schema di rete COM e KNA
- [10] Allegato A03 – Piano termini





Legenda

10 Gbps-LR (<10km)

10 Gbps-ER (>10km)

10 Gbps-ZR (>40km)

10 Gbps Base T

Tracciato ridondante AET

Nuovo

Switch/Router COM

Switch COM access

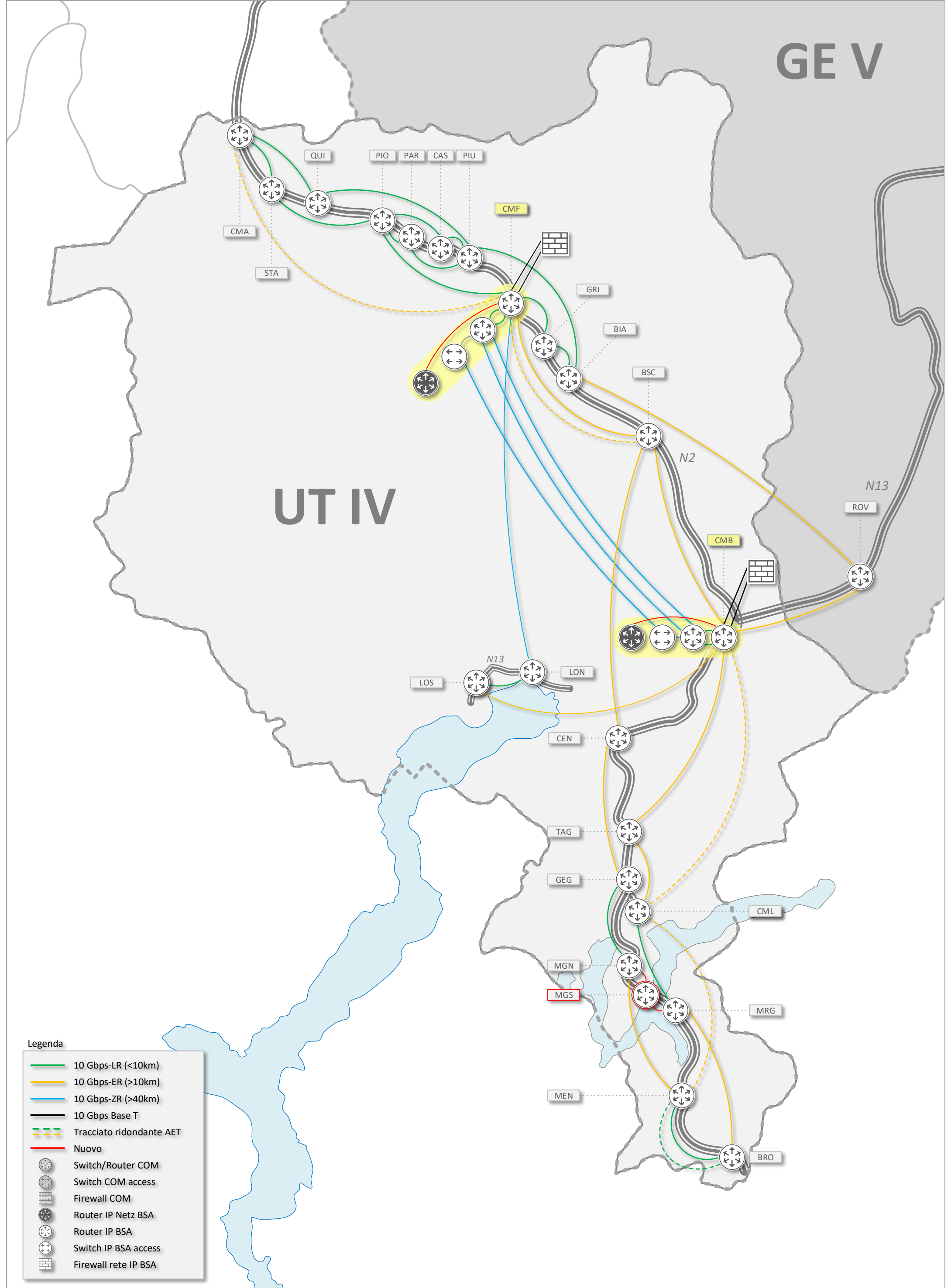
Firewall COM

Router IP Netz BSA

Router IP BSA

Switch IP BSA access

Firewall rete IP BSA



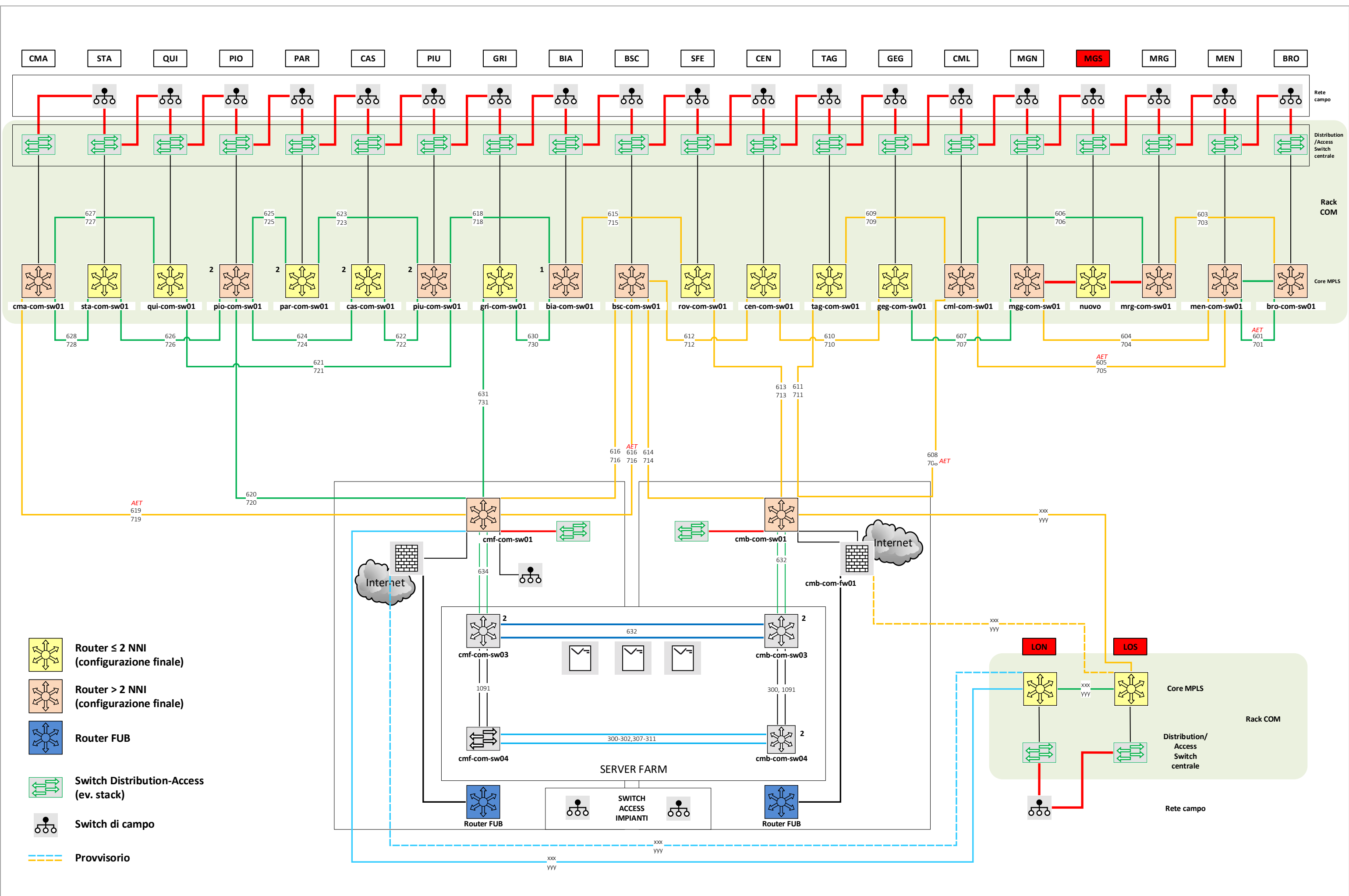
GE V

UT IV







Legenda

- 10 Gbps-LR (<10km)
- 10 Gbps-ER (>10km)
- 10 Gbps-ZR (>40km)
- 10 Gbps Base T
- Tracciato ridondante AET
- Nuovo
- Switch/Router COM
- Switch COM access
- Firewall COM
- Router IP Netz BSA
- Router IP BSA
- Switch IP BSA access
- Firewall rete IP BSA

AUTORE	Gino Gatti	ALLEGATO A01 – Schema geografico della rete UT IV			
DATA	28.02.2020	Nome File	0067.2-001_Rete COM N2 Chiasso-Airolo_v1-1.vsd		
FORMATO	A3	N. PIANO	0067.2-001	VERSIONE	1.1
		PAGINA 3 DI 3			



ID		Attività	Durata	Inizio	Fine																								
						2020 S1	S2	2021 S1	S2	2022 S1	S2	2023 S1	S2	2024 S1	S2	2025 S1	S2	2026 S1	S2	2027 S1	S2	2028 S1	S2	2029 S1	S2				
1		Rete IP BSA UT IV - Concetto di migrazione	2035 g	lun 01.06.20	ven 02.06.28																								
2																													
3		Tappa 1 - Galleria Mappo-Morettina	248 g	lun 01.06.20	ven 21.05.21																								
4		Realizzazione nuova rete IP BSA (COM) sezione LOG	208 g	lun 01.06.20	ven 26.03.21																								
5		Installazione nuovi firewall interfacciamento backbone IP-Netz BSA	208 g	lun 01.06.20	ven 26.03.21																								
6		Attività preliminari rete IP BSA	80 g	lun 01.02.21	ven 21.05.21																								
7		Integrazione rete COM in IPAM	80 g	lun 01.02.21	ven 21.05.21																								
8		Integrazione rete COM nel backbone IP-Netz BSA	80 g	lun 01.02.21	ven 21.05.21																								
9																													
10		Tappa 2 - Pianificazione migrazione	1947 g	gio 01.10.20	ven 02.06.28																								
11		Avvio attività di migrazione	0 g	gio 01.10.20	gio 01.10.20																								
12		Incarico accompagnamento committente (BHU)	57 g	gio 01.10.20	ven 18.12.20																								
13		Accompagnamento committente (BHU)	1887 g	lun 04.01.21	ven 02.06.28																								
14		Attività preliminari rete IP BSA	312 g	gio 01.10.20	mar 21.12.21																								
15		Incarico attività preliminari	57 g	gio 01.10.20	ven 18.12.20																								
16		Allestimento documenti di riferimento	255 g	lun 21.12.20	mar 21.12.21																								
17		Adattamento sistemi di sicurezza/gestione secondo direttive	80 g	lun 01.02.21	ven 21.05.21																								
18		Progettazione core UT IV rete IP BSA	509 g	lun 04.01.21	ven 23.12.22																								
19		Incarico progettazione, appalti e direzione lavori core UT IV rete IP BSA	120 g	lun 04.01.21	ven 18.06.21																								
20		Progettazione core UT IV rete IP BSA	130 g	lun 21.06.21	ven 17.12.21																								
21		Appalti e aggiudicazione rinnovo rete COM vs. rete IP BSA	255 g	lun 03.01.22	ven 23.12.22																								
22		Progettazione reti di campo UT IV	643 g	lun 21.06.21	ven 22.12.23																								
23		Incarico progettazione, appalti e direzione lavori reti di campo UT IV	130 g	lun 21.06.21	ven 17.12.21																								
24		Progettazione reti di campo UT IV	255 g	lun 03.01.22	ven 23.12.22																								
25		Appalti e aggiudicazione reti di campo UT IV	254 g	mar 03.01.23	ven 22.12.23																								
26																													
27		Tappa 3 - Realizzazione migrazione COM vs. rete IP BSA	1124 g	mer 03.01.24	ven 02.06.28																								
28		Sostituzione core, access e reti di campo PIU-CAS-PAR-PIO (EP08)	173 g	mer 03.01.24	ven 30.08.24																								
29		Sostituzione core, access e reti di campo GEG-CML (EP28)	122 g	lun 02.09.24	ven 28.02.25																								
30		Sostituzione core, access e reti di campo BRO (EP18)	95 g	lun 03.03.25	ven 11.07.25																								
31		Sostituzione core MEN-MRG-TAG-CEN-CMB-BSC-BIA-GRI-CMF-QUI-STA-CMA-SFE-LOG	115 g	lun 14.07.25	ven 19.12.25																								
32		Sostituzione access e reti di campo MEN-MRG-TAG-CEN-CMB-BSC-BIA-GRI-CMF-QUI-STA-CMA-SFE-LOG	617 g	lun 05.01.26	ven 02.06.28																								
33																													
34		Fine migrazione COM UT IV vs. rete IP BSA UT IV	0 g	ven 02.06.28	ven 02.06.28																								
35																													
36		Termini esterni	2032 g	gio 31.12.20	dom 31.12.28																								
37		MS1 - Backbone IP-Netz BSA (USTRÄ)	256 g	gio 31.12.20	ven 31.12.21																								
38		MS1.1 - Smantellamento VDV	384 g	gio 31.12.20	gio 30.06.22																								
39		MS2 - Messa a disposizione e integrazione tool IPAM (USTRÄ)	511 g	gio 31.12.20	sab 31.12.22																								
40		MS3 - Messa a disposizione e integrazione tool NAC (USTRÄ)	511 g	ven 31.12.21	dom 31.12.23																								

ID		Attività	Durata	Inizio	Fine	2020		2021		2022		2023		2024		2025		2026		2027		2028		2029	
						S1	S2	S1	S2	S1	S2	S1	S2	S1	S2	S1	S2	S1	S2	S1	S2	S1	S2	S1	S2
41		MS4 - Rete IP BSA completa (core) disponibile	0 g	lun 30.06.25	lun 30.06.25													30.06							
42		MS5 - Rete IP BSA completa (access) disponibile	0 g	dom 31.12.28	dom 31.12.28																				31.12
43		EP08 Faido - Varenzo	763 g	dom 01.01.23	mer 31.12.25																				
44		EP28 Gentilino - Lamone	1271 g	sab 01.01.22	gio 31.12.26																				
45		EP18 Chiasso - Balerna	1270 g	dom 01.01.23	ven 31.12.27																				
46																									