
INTERNO	ICSPC-QXN-Specificarealizzazione-1.3.Docx	

Infrastrutture Condivise SPC




Specifica Realizzazione QXN

IDENTIFICATIVO

ICSPC-QXN-SpecificaRealizzazione-1.3.docx




STORIA DEL DOCUMENTO

Rev.	Data	Redatto	Approvato	Descrizione modifica
1.0	26/09/2016	A. Marcandalli, V. Muratore, L.Spaghetti	S.Di Bisceglie	Prima emissione
1.1	07/12/2016	A. Marcandalli, V. Muratore, L.Spaghetti	S.Di Bisceglie	Modifiche minori
1.2	30/01/2017	A. Marcandalli, L.Spaghetti	S.Di Bisceglie	Modifiche minori
1.3	15/11/2023	M. Mascagna	S. Di Bisceglie	Corretti riferimenti al piano di indirizzamento QXN (par. 4.1)

		
INTERNO	ICSPP-QXN-Specificarealizzazione-1.3.Docx	




ALLEGATI

Nome	Descrizione




		
INTERNO	ICSPC-QXN-Specificare realizzazione-1.3.Docx	

Sommario

1	GENERALITÀ	5
1.1	SCOPO DEL DOCUMENTO	5
1.2	APPLICABILITÀ	5
1.3	RIFERIMENTI	5
1.4	DEFINIZIONI ED ACRONIMI.....	5
2	CARATTERISTICHE DEL SERVIZIO	6
2.1	INFRASTRUTTURA QXN	6
2.1.1	<i>Connessioni geografiche</i>	<i>6</i>
2.2	SERVIZIO OPA.....	9
2.3	SERVIZIO OPO	9
2.4	SERVIZIO DNS	10
3	EQUIPAGGIAMENTO APPARATI.....	11
3.1	APPARATI DI CORE.....	11
3.2	APPARATI PER IL MANAGEMENT OOB	12
3.3	SONDE	13
3.4	FIREWALL	13
3.5	SERVER DNS ED NTP	13
3.6	ROUTER DI ACCESSO INTERNET.....	13
4	SPECIFICHE DI CONFIGURAZIONE	15
4.1	PIANO DI INDIRIZZAMENTO.....	15
4.1.1	<i>IPv4</i>	<i>15</i>
4.1.2	<i>IPv6</i>	<i>15</i>
4.2	CORE QXN	16
4.2.1	<i>Link aggregation</i>	<i>16</i>
4.2.2	<i>Routing IGP</i>	<i>17</i>
4.2.3	<i>Routing MP-BGP</i>	<i>18</i>
4.3	SERVIZIO OPA.....	18
4.3.1	<i>Attestazione dei soggetti interconnessi</i>	<i>19</i>
4.3.2	<i>Bilanciamento e simmetria del traffico OPA</i>	<i>19</i>
4.3.3	<i>Interconnessione QXN1.....</i>	<i>21</i>
4.3.4	<i>QoS OPA</i>	<i>22</i>
4.3.5	<i>Interconnessione dei Data Center IC-SPC.....</i>	<i>23</i>
4.4	SERVIZIO OPO	25
4.4.1	<i>Interconnessione dei QISP.....</i>	<i>25</i>
4.4.2	<i>Bilanciamento e simmetria del traffico OPO.....</i>	<i>26</i>
4.4.3	<i>QoS OPO.....</i>	<i>26</i>
4.5	SISTEMA DI MONITORAGGIO	27
4.5.1	<i>Sonde</i>	<i>27</i>
4.6	SICUREZZA DEI NODI QXN	28
4.6.1	<i>Network Firewall.....</i>	<i>29</i>
4.6.2	<i>Caratteristiche.....</i>	<i>29</i>
4.6.3	<i>Pre-Installazione e configurazione del FortiGate</i>	<i>31</i>
4.6.4	<i>Opzioni di configurazione.....</i>	<i>32</i>
4.6.5	<i>Configurazione</i>	<i>32</i>
4.6.6	<i>Sistema di logging centralizzato - FortiAnalyzer.....</i>	<i>33</i>
4.7	SERVIZIO NTP	34
4.8	SERVIZIO DNS	35

		
INTERNO	ICSPC-QXN-Specificarealizzazione-1.3.Docx	

4.9	RETE DI MANAGEMENT OOB.....	35
4.9.1	OOB Nodi QXN	36

		
INTERNO	ICSPC-QXN-Specificare realizzazione-1.3.Docx	

1 GENERALITÀ

1.1 SCOPO DEL DOCUMENTO

Il presente documento si prefigge l'obiettivo di descrivere l'infrastruttura di rete e DNS/NTP della QXN utilizzata per la fornitura dei servizi di interconnessione tra le Pubbliche Amministrazioni che aderiscono al contratto SPC in accordo con le offerte OPA e OPO.

1.2 APPLICABILITÀ




Il presente documento si applica all'intero Contratto [CIG 6049538CAC] stipulato in data 5/8/2016 tra AgID e l'RTI Fastweb spa-Finmeccanica spa-Sistemi Informativi srl, per l'affidamento della progettazione, realizzazione, fornitura, manutenzione e gestione delle Infrastrutture Condivise del Sistema Pubblico di Connettività d'ora in avanti ICSPC.

1.3 RIFERIMENTI

	Codice	Titolo
[1]	ID SIGEF 1366	Allegato 5 – capitolato tecnico
[2]	ID SIGEF 1366	Appendice 1 al capitolato tecnico SLA e penali
[3]	ID SIGEF 1366	Procedura aperta per l'affidamento della progettazione, realizzazione, fornitura, manutenzione e gestione delle infrastrutture condivise del sistema pubblico di connettività (id 1366) – Offerta Tecnica
[4]	ICSPC-GE-Acronimi.x.y	Acronimi

1.4 DEFINIZIONI ED ACRONIMI

Si faccia riferimento al documento [4].

		
INTERNO	ICSPC-QXN-Specificare realizzazione-1.3.Docx	

2 Caratteristiche del servizio

Nell'ambito del Progetto SPC (Sistema Pubblico di Connettività), è prevista la realizzazione di una rete, denominata QXN, di transito tra le reti dei soggetti interconnessi per erogare servizi di connettività alle Pubbliche Amministrazioni aderenti alla convenzione SPC (PA SPC).

La rete del QXN svolge quindi la funzione di Internet eXchange Point per il solo traffico dati scambiato tra le Pubbliche Amministrazioni che aderiscono al contratto SPC non permettendo l'attraversamento del traffico da e per i soggetti non attestati ad SPC. In particolare, le tipologie di traffico che attraversano il nodo QXN sono:

- Infranet (OPA): costituito dal traffico generato da due o più sedi di PA distinte che aderiscono al contratto SPC, le quali sono connesse a QISP differenti in accordo con l'Offerta Per le Amministrazioni (OPA).
- Intranet in modalità OPO: costituito dal traffico scambiato tra due o più sedi della stessa PA SPC connessa in parte ad un QISP assegnatario ed in parte alla rete del QISP aggiudicatario in accordo con l'Offerta Per gli altri Operatori (OPO).
- da/verso Infranet SPC1: costituito dal traffico generato da e verso le Pubbliche Amministrazioni ancora attestate sulla Infranet SPC1, attraverso la QXN1, durante la fase di migrazioni delle stesse PA alla nuova convenzione.




2.1 INFRASTRUTTURA QXN

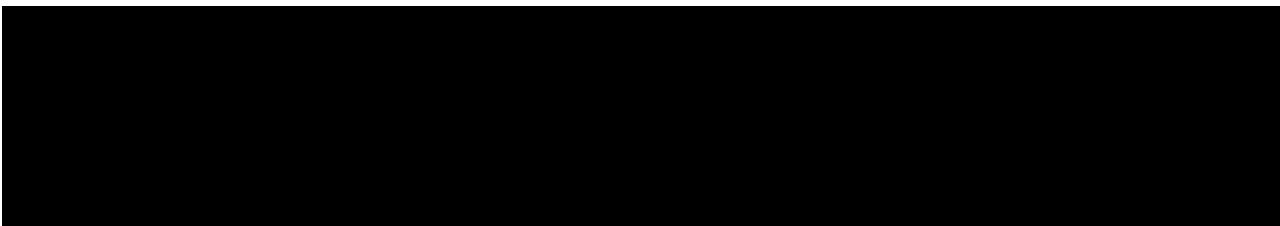
L'impiego di quattro apparati Cisco 6509E (BRqxn) di uguale equipaggiamento, interconnessi tra loro tramite collegamenti geografici ridondati, costituisce il backbone della rete QXN. Gli apparati scelti offrono prestazioni in linea con i requisiti della rete QXN, sia dal punto di vista della capacità di routing e switching, sia a livello di disponibilità d'interfacce fisiche di rete.

I suddetti apparati sono collocati in due spazi geograficamente distinti quali il NAP pubblico di Milano (MIX) e il NAP pubblico di Roma (NaMeX). La tecnologia utilizzata per i collegamenti dei due apparati all'interno dello stesso nodo è di tipo 10 GigabitEthernet. In particolare saranno utilizzate due coppie di link 10GE tra i due apparati dello stesso nodo ed è prevista l'aggregazione di ciascuna coppia di link fisici per formare due link logici ciascuno con capacità di 20Gbps. I due link logici avranno funzioni diverse: uno sarà dedicato al trasporto dei servizi L3 (OPA) e l'altro al trasporto del traffico L2 (trunk 802.1q) all'interno del nodo.

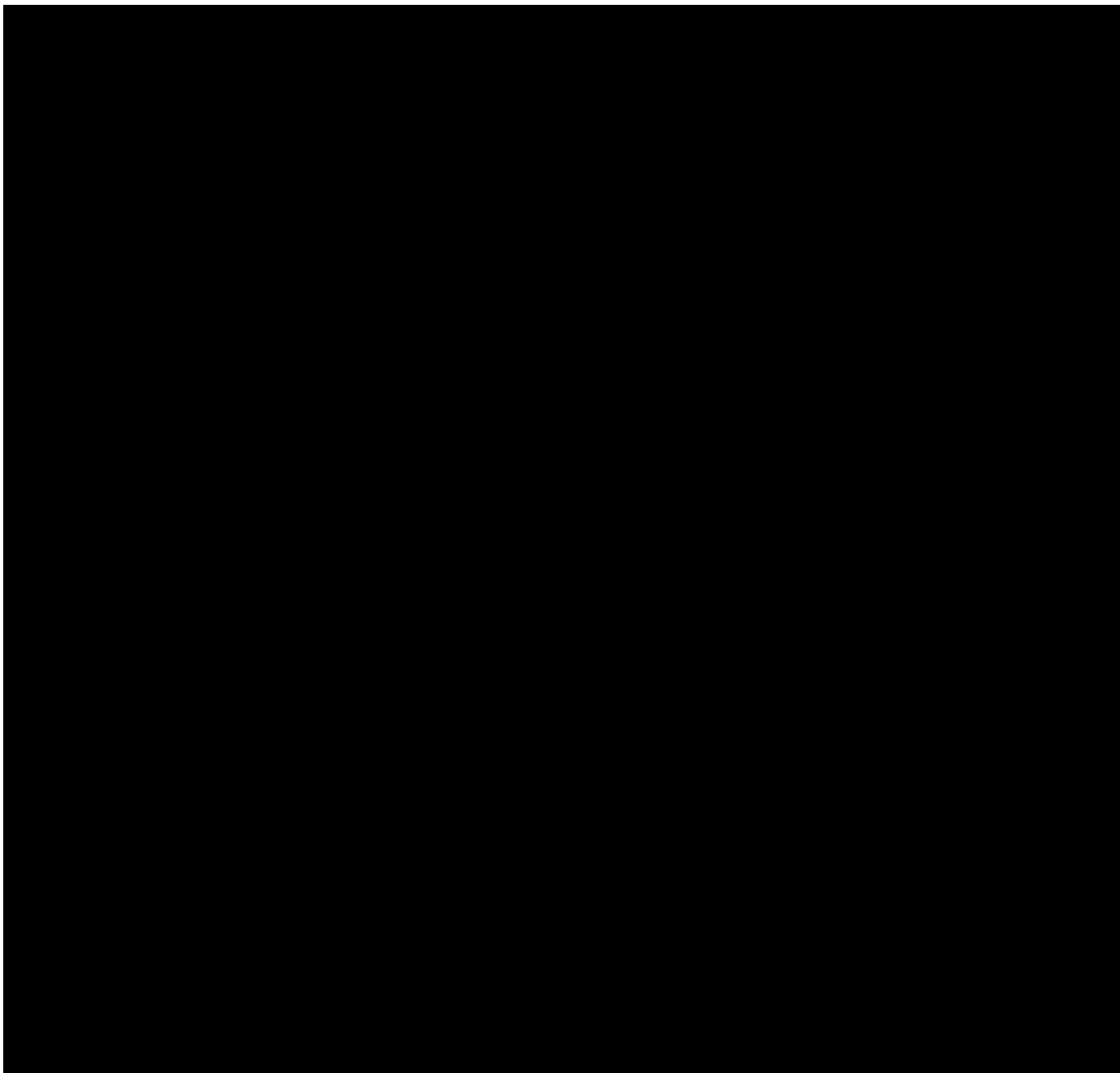
2.1.1 CONNESSIONI GEOGRAFICHE

L'architettura del layer di trasporto prevede la realizzazione di multiple connettività in tecnologia WDM a banda 1GEthernet tra le diverse sedi conformi ai requisiti e ai criteri di diversificazione richiesti. Si noti che la banda offerta è superiore a quella massima prevista dal capitolato e pertanto non si rende necessario utilizzare il processo di capacity planning. Fastweb monitorerà comunque l'utilizzo di tali collegamenti e proporrà ad AgID, qualora lo ritenesse necessario, un upgrade di banda a 10G.

		
INTERNO	ICS-PC-QXN-Specificare realizzazione-1.3.Docx	

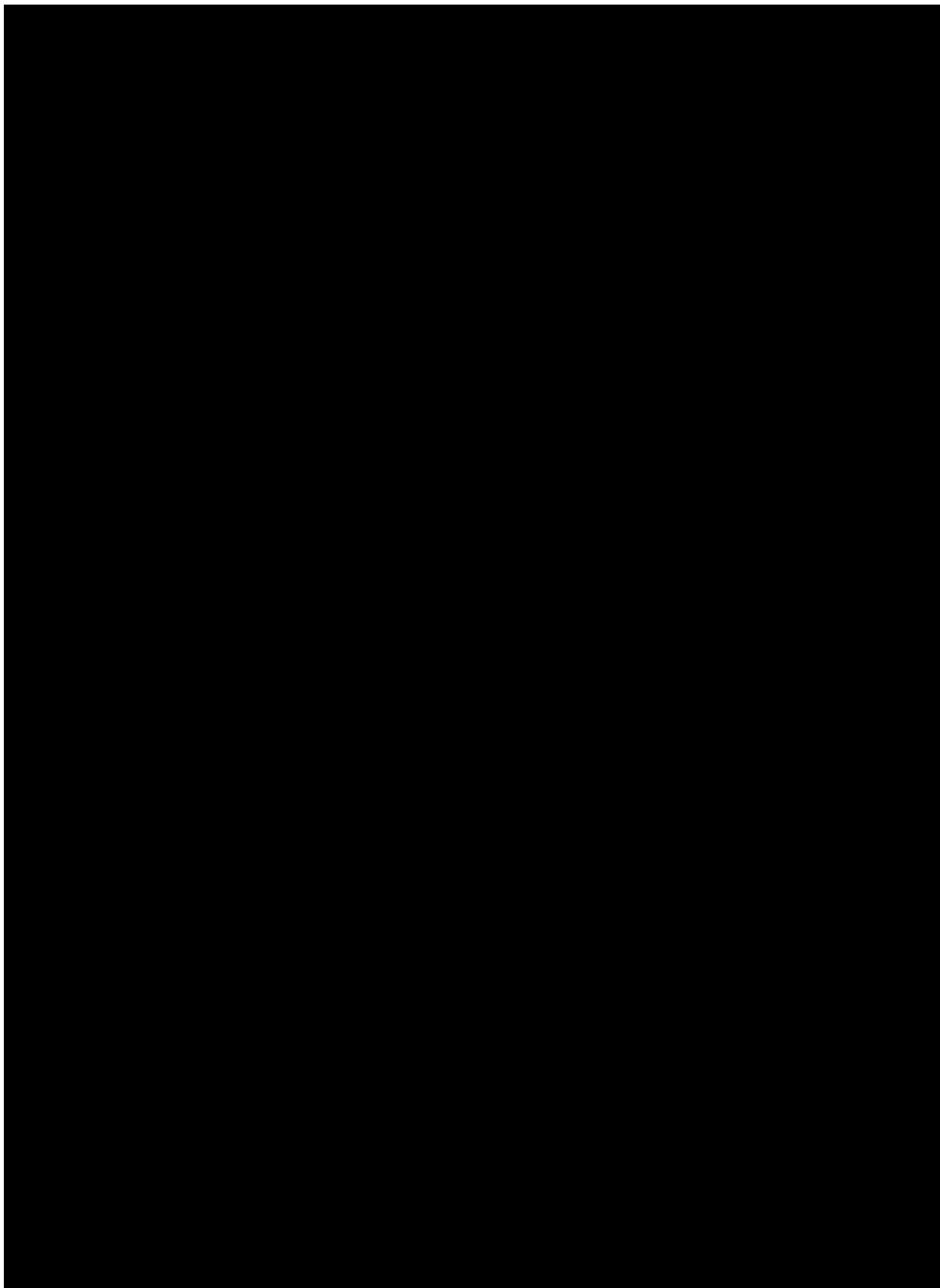





2. La Dorsale DWDM LD di FASTWEB



INTERNO

ICSPC-QXN-Specificarealizzazione-1.3.Docx



		
INTERNO	ICSPC-QXN-Specificarealizzazione-1.3.Docx	

2.2 SERVIZIO OPA

All'architettura descritta nel precedente paragrafo si aggiungeranno i nodi di rete dei diversi fornitori SPC che costituiscono il punto di accesso alla rete QXN per la gestione del traffico Infranet tra le PA SPC, in accordo con l'offerta OPA.

Anche questi apparati, definiti nel seguito come Border Router dei Q-ISP (BRqx), sono collocati in housing presso le infrastrutture (rack) della QXN ospitate al MIX e al NaMeX. L'installazione, la gestione e la manutenzione di tali apparati è a carico dei rispettivi Q-ISP. Per il collegamento di questi apparati con funzione di livello di accesso della rete QXN è previsto inizialmente l'utilizzo di tecnologia GE in fibra ottica (1000Base-SX) o rame (10/100/1000) ma sarà possibile in futuro, previa fattibilità tecnica ed economica congiunta da parte di Fastweb ed AgID, prevedere anche connettività 10GE per la connessione dei soggetti interconnessioni.

Ai fini dell'interconnessione per il trasporto di servizi Infranet nativi OPA, i nodi del QXN (BRqxn) agiscono a livello di routing (Livello 3 del modello ISO/OSI).

Nella seguente figura è riportato lo schema di collegamento di due Q-ISP generici ai due nodi dell'architettura QXN di Milano e Roma.

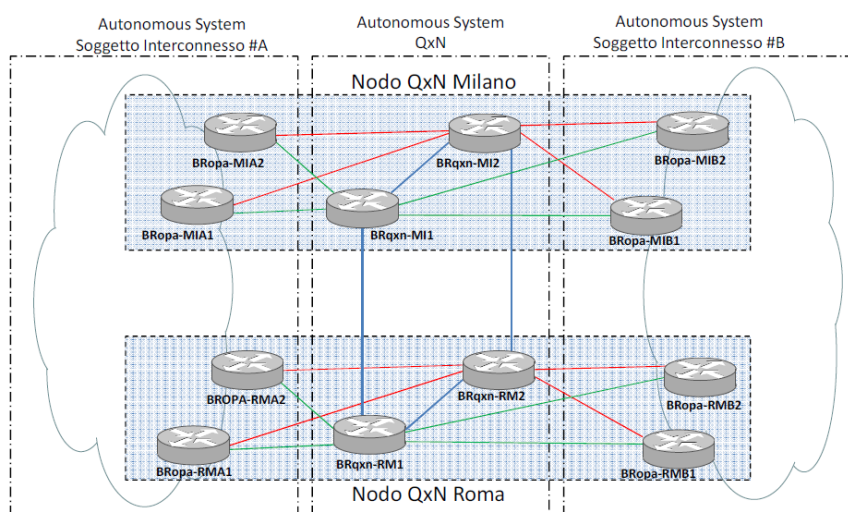





Figura 3 - Schema di connessione dei Q-ISP per il servizio OPA

2.3 SERVIZIO OPO

Il servizio OPO permette l'interconnessione a livello 2 tra il Fornitore aggiudicatario SPC ed ogni Fornitore assegnatario SPC che abbiano sottoscritto un contratto esecutivo OPO della gara SPC. I soggetti coinvolti che richiedono il profilo di servizio OPO attestano gli apparati BRopo (al più due per ciascun nodo QXN) collocandoli fisicamente in housing presso i due nodi QXN e collegandoli come previsto dal Capitolato Tecnico. Il Fornitore aggiudicatario SPC2 collega invece, per ciascun nodo, due apparati BRopo sempre co-locati in housing presso il NaMeX e il MiX. Per ciascun soggetto richiedente l'attivazione del servizio viene stabilito il nodo principale di scambio del traffico mentre l'altro ha la funzione di Backup. Sebbene ciascun BRqxn sia dimensionato in modo di poter gestire tutto il carico di lavoro, le interconnessioni con la QXN devono essere realizzate in modo che il traffico scambiato transiti in via prioritaria sul nodo QXN di Roma ed in via secondaria su quello di Milano salvo specifiche esigenze delle PA o dei soggetti richiedenti il servizio.

		
INTERNO	ICS-PC-QXN-Specificare realizzazione-1.3.Docx	




Per l'attestazione fisica dei B-Ropo dei Q-ISP alla QXN, saranno disponibili le medesime tipologie di connettività già descritte per il servizio OPA.

2.4 SERVIZIO DNS

Al fine di consentire l'interscambio dei dati tra le Pubbliche Amministrazioni, nell'ambito del traffico OPA, è reso disponibile un servizio centralizzato di risoluzione nomi all'interno della rete QXN utilizzabile sia per connettività IPv4 che IPv6.

Il servizio è erogato esclusivamente ai soggetti direttamente interconnessi che, a loro volta, lo renderanno disponibile alle Pubbliche Amministrazioni.

Presso il NAP pubblico di Milano (MIX) ed il NAP pubblico di Roma (NaMeX) sono installati in modalità ridondata 5 server di ultima generazione (per un totale di 10) atti a svolgere la funzione di server DNS.

 un passo avanti	 An IBM Company	 SISTEMI PER LA SICUREZZA E LE INFORMAZIONI
INTERNO	ICSPC-QXN-Specificare realizzazione-1.3.Docx	

3 Equipaggiamento apparati

Nel presente capitolo sono indicati gli equipaggiamenti dei vari dispositivi necessari alla realizzazione della QXN.

Tutti i dispositivi costituenti l'infrastruttura di rete QXN che saranno collocati presso i due NAP inclusi i dispositivi di sicurezza perimetrale ed i dispositivi per l'erogazione del servizio DNS e NTP, saranno ad uso esclusivo del servizio QXN.

Si conferma che per tutti i dispositivi hardware previsti per l'erogazione dei servizi non sia stata annunciata, all'atto della consegna del Progetto Esecutivo, dal vendor tecnologico di riferimento una data di "End of Sale" e/o "End of Support".

Ciascun nodo è così composto:

- n° 2 x BRqxn – Cisco WS-C6509-E
- n° 1 x terminal server per la gestione OOB dei dispositivi di rete - Cisco 2911
- n° 1 x switch per l'attestazione delle interfacce OOB di dispositivi di rete, di sicurezza e server. - Cisco Catalyst WS-C2960X-48TS-L
- n° 4 x sonde per la misurazione degli SLA – Cisco C891F
- n° 2 x Network Intrusion Detection System & Firewall – Fortinet FG-1000D
- n° 5 x Server DELL PowerEdge R430
- n° 2 x router Internet – Cisco 2911




Si aggiunge che, esclusivamente presso il Namex, sono disponibili due ulteriori apparati con la medesima configurazione prevista per i BRqxn che potranno essere utilizzati a scopo di test per la durata del progetto.

Infine, si noti che tutti gli apparati previsti sono alimentati in corrente alternata (AC 220V) e che questo costituirà un vincolo anche per gli apparati dei soggetti interconnessi che verranno ospitati in housing presso i nodi QXN del NAMEX e del MIX.

3.1 APPARATI DI CORE

Gli apparati Cisco Catalyst 6509E di core, una coppia per ciascun nodo QXN (più una coppia di test presso il Namex), sono equipaggiati singolarmente come segue:

PRODOTTO	DESCRIZIONE	Q.tà
WS-C6509-E	Catalyst 6500 Enhanced 9-slot chassis, 14RU, no PS, no Fan Tray	1
WS-C6509-E-FAN	Catalyst 6509-E Chassis Fan Tray	1
WS-X6K-SLOT-CVR	Catalyst 6000 Blank Line Card Slot Cover	5
VS-S2T-10G-XL	Cat 6500 Sup 2T with 2x10GbE and 3 x 1GbE with MSFC5 PFC4XL	1
MEM-C6K-INTFL1GB	Internal 1G Compact Flash	1
MEM-SUP2T-2GB	Catalyst 6500 2GB memory for Sup2T and Sup2TXL	1
VS-F6K-PFC4XL	Cat 6k 80G Sys Daughter Board Sup2T PFC4XL	1
VS-SUP2T-10G	Catalyst 6500 Supervisor Engine 2T Baseboard	1
S2TAK9-152015Y	Cisco CAT6000-VS-S2T IOS ADVANCED IP SERVICES FULL ENCRYPT	1
X2-10GB-SR	10GBASE-SR X2 Module	2
WS-X6848-SFP-2TXL	Catalyst 6500 48-port GigE Mod: fabric-enabled with DFC4XL	1
WS-F6K-DFC4-AXL	Cat 6k 80G Sys Daughter Board DFC4AXL for ABA Cards	1
WS-X6848-SFP	Catalyst 6500 48 Port 1G SFP Baseboard	1
GLC-SX-MMD	1000BASE-SX SFP transceiver module, MMF, 850nm, DOM	48
WS-X6848-TX-2TXL	C6k 48-port 10/100/1000 GE Mod: fabric enabled, RJ-45 DFC4XL	1
VS-S2T-10G-XL	Cat 6500 Sup 2T with 2x10GbE and 3 x 1GbE with MSFC5 PFC4XL	1
MEM-C6K-INTFL1GB	Internal 1G Compact Flash	1

 un passo avanti	 An IBM Company	 SISTEMI PER LA SICUREZZA E LE INFORMAZIONI
INTERNO	ICSPC-QXN-Specificarealizzazione-1.3.Docx	

MEM-SUP2T-2GB	Catalyst 6500 2GB memory for Sup2T and Sup2TXL	1
VS-F6K-PFC4XL	Cat 6k 80G Sys Daughter Board Sup2T PFC4XL	1
VS-SUP2T-10G	Catalyst 6500 Supervisor Engine 2T Baseboard	1
X2-10GB-SR	10GBASE-SR X2 Module	2
WS-CAC-6000W	Cat6500 6000W AC Power Supply	2
CAB-AC-2500W-EU	Power Cord, 250Vac 16A, Europe	4

Tabella 1. Configurazione HW e SW dei BRqxn

I Cisco Catalyst 6509E, nella configurazione hardware e software descritta in Tabella 1, rappresentano una evoluzione degli apparati già utilizzati con successo nella precedente infrastruttura QXN1. A livello di performance, disponibilità porte e possibilità di espansione soddisfano o superano i requisiti di capitolato. In particolare offrono:

- disponibilità di 48 porte Gigabit Ethernet rame (10/100/1000)
- disponibilità di 54 porte Gigabit Ethernet ottiche (SFP)
- disponibilità di 5 slot di espansione da utilizzare, previa richiesta di AgID, per l'aggiunta su singolo slot di espansione, di una delle tipologie di upgrade richieste dal capitolato.
- la piattaforma scelta è potenzialmente in grado di supportare fino a 16K bridge domains (concetto introdotto da Cisco per scalare il numero di VLAN).

Inoltre gli apparati supportano tutte le funzionalità esplicitamente richieste dal capitolato (BGPv4, OSPF, SNMP v2/v3, funzionalità di mirroring (SPAN Port), 802.1p, VLAN, Inter-Vlan routing).

3.2 APPARATI PER IL MANAGEMENT OOB




Ciascun nodo è così composto:

- n° 1 x terminal server per la gestione OOB dei dispositivi di rete - Cisco 2911
- n° 1 x Catalyst per la gestione OOB IP dei dispositivi di rete - WS-C2960X-48TS-L

di seguito il dettaglio dei singoli apparati:

PRODOTTO	DESCRIZIONE	Q.tà
CISCO2911/K9	Cisco 2911 w/3 GE,4 EHWIC,2 DSP,1 SM,256MB CF,512MB DRAM,IPB	1
PWR-2911-AC	Cisco 2911 AC Power Supply	1
CAB-ACE	AC Power Cord (Europe), C13, CEE 7, 1.5M	1
SM-S-BLANK	Removable faceplate for SM slot on Cisco 2900,3900,4400 ISR	1
HWIC-BLANK	Blank faceplate for HWIC slot on Cisco ISR	3
ISR-CCP-EXP	Cisco Config Pro Express on Router Flash	1
MEM-2900-512MB-DEF	512MB DRAM for Cisco 2901-2921 ISR (Default)	1
MEM-CF-256MB	256MB Compact Flash for Cisco 1900, 2900, 3900 ISR	1
SL-29-IPB-K9	IP Base License for Cisco 2901-2951	1
S29UK9-15501T	Cisco 2901-2921 IOS UNIVERSAL	1
CAB-HD8-ASYNC	High Density 8-port EIA-232 Async Cable	2
HWIC-16A	16-Port Async HWIC	1
WS-C2960X-48TS-L	Catalyst 2960-X 48 GigE, 4 x 1G SFP, LAN Base	1
CAB-ACI-RA	Power Cord, Italian, Right Angle	1
PWR-CLP	Power Retainer Clip For Cisco 3560-C and 2960-C Compact Swit	1

Tabella 2. Configurazione hardware e software apparati per il management OOB

 un passo avanti	 An IBM Company	 SISTEMI PER LA SICUREZZA E LE INFORMAZIONI
INTERNO	ICSPC-QXN-Specificare realizzazione-1.3.Docx	

3.3 SONDE

Ciascun nodo è così composto:

- n° 4 x sonde per la misurazione degli SLA – Cisco C891F

Di seguito il dettaglio dei singoli apparati:

PRODOTTO	DESCRIZIONE	Q.tà
C891F-K9	Cisco 890 Series Integrated Services Routers	1
ACS-890-RM-19	Rackmount kit for 890	1
CAB-ETH-S-RJ45	Yellow Cable for Ethernet, Straight-through, RJ-45, 6 feet	1
PACK-800	Packaging PIDs for 800 with no 3G and POE	1
PWR-60W-AC-V2	Power Supply 60 Watt AC version 2 for some platforms	1
SL-890-AIS	Cisco 890 Advanced IP Services License	1
S89UK9-15403M	Cisco 890 Series IOS UNIVERSAL	1
CAB-ACE	AC Power Cord (Europe), C13, CEE 7, 1.5M	1

Tabella 3. Configurazione hardware e software sonde IP SLA

3.4 FIREWALL

Ciascun nodo è così composto:

- n° 2 x Next Generation Firewall FortiGate 1000D

PRODOTTO	DESCRIZIONE	Q.tà
FortiGate 1000D	2 x 10GE SFP+ slots, 16 x GE SFP Slots, 16 x GE RJ45 ports, 2 x GE RJ45 Management ports, FortiASIC NP6 and CP8 hardware accelerated, 1 x 120GB SSD onboard storage, dual AC power supplies	2

Tabella 4: Configurazione hardware e software Firewall

3.5 SERVER DNS ED NTP

Ciascun nodo è così composto:

- n° 5 x Server DELL PowerEdge R430

Rif.	PRODOTTO	DESCRIZIONE	Q.tà
1	Dell PowerEdge R430	Processore Intel Xeon E5 Core E52620 v3 2.4GHz	2
		S. O. Centos Linux 64 bit	1
		16GB RAM	1
		300GB 15K RPM SAS 12Gbps	2
		porte Ethernet 10/100/1000	4
		interfaccia per management remoto	1
		Alimentatore 550 W doppia via ridondata	1

Tabella 5. Configurazione hardware server DNS/NTP




3.6 ROUTER DI ACCESSO INTERNET

Ciascun nodo è così composto:

- n° 2 x router Internet – Cisco 2911




di seguito il dettaglio dei singoli apparati:

PRODOTTO	DESCRIZIONE	Q.tà
CISCO2911/K9	Cisco 2911 w/3 GE,4 EHWIC,2 DSP,1 SM,256MB CF,512MB DRAM,IPB	1
PWR-2911-AC	Cisco 2911 AC Power Supply	1

 un passo avanti	 An IBM Company	 SISTEMI PER LA SICUREZZA E LE INFORMAZIONI
INTERNO	ICSPP-QXN-Specificarealizzazione-1.3.Docx	

CAB-ACE	AC Power Cord (Europe), C13, CEE 7, 1.5M	1
SM-S-BLANK	Removable faceplate for SM slot on Cisco 2900,3900,4400 ISR	1
HWIC-BLANK	Blank faceplate for HWIC slot on Cisco ISR	4
ISR-CCP-EXP	Cisco Config Pro Express on Router Flash	1
MEM-2900-512MB-DEF	512MB DRAM for Cisco 2901-2921 ISR (Default)	1
MEM-CF-256MB	256MB Compact Flash for Cisco 1900, 2900, 3900 ISR	1
SL-29-IPB-K9	IP Base License for Cisco 2901-2951	1
S29UK9-15501T	Cisco 2901-2921 IOS UNIVERSAL	1

Tabella 6. Configurazione hardware router per l'accesso Internet

 un passo avanti	 An IBM Company	 SISTEMI PER LA SICUREZZA E LE INFORMAZIONI
INTERNO	ICSPC-QXN-Specificare realizzazione-1.3.Docx	

4 Specifiche di configurazione

Di seguito sono descritte le specifiche di configurazione degli apparati di rete, sicurezza e server dell'infrastruttura QXN.

Come previsto da capitolato, in qualsiasi momento dell'esecuzione contrattuale la configurazione degli apparati QXN (Router, Switch, Firewall e DNS), su richiesta di AgID, sarà trasmessa ad AgID stessa in apposito formato da concordare tra le parti e su idoneo supporto informatico.

Qualora lo ritenga opportuno, AgID potrà utilizzare tali configurazioni senza alcuna limitazione.

4.1 PIANO DI INDIRIZZAMENTO

La rete QXN sarà dotata di un proprio range di IP pubblici IPv4/IPv6 assegnati ad AgID in qualità di LIR (IPv4: **185.182.140.0/22** – IPv6: **2a0a:ee80::/29**) e di un proprio ASN a 32 bit (**ASN 43988**), entrambi assegnati da RIPE. Le network di IP pubblici assegnate alla QXN verranno suddivise ed utilizzate sia per numerare le interfacce di gestione (es. Loopback) e di collegamento (es. point-to-point) degli apparati che compongono la rete QXN, sia per l'erogazione dei servizi esposti dai nodi QXN in ambito Infranet e dal Data Center in ambito Infranet ed Internet. Alle Pubbliche Amministrazioni saranno invece allocati dai rispettivi fornitori SPC di riferimento blocchi di indirizzi IP prelevati dal piano di indirizzamento assegnato dal RIPE al ASN del Fornitore.

4.1.1 IPv4

La subnet IPv4 rilasciata dal RIPE ad AgID per la realizzazione della QXN è la seguente:

- 185.182.140.0/22

Gli indirizzamenti pubblici sono utilizzati sia per la realizzazione dell'infrastruttura che per l'esposizione dei servizi (DNS\NTP\DC). Per questo scopo gli indirizzamenti rilasciati saranno così ripartiti:

Network	Destinazione	Ruotati DC ICSPC	Ruotati QXN1	Ruotati Infranet	Ruotati Internet
185.182.140.0/26	QXN2 - Infrastruttura Core	SI	NO	NO	NO
185.182.140.64/26	QXN2 - Sonde	SI	SI	NO	NO
185.182.140.128/25	RISERVATA PER USI FUTURI	-	-	-	-
185.182.141.0/24	QXN2 - Connessioni OPA, DNS e NTP	SI	SI	SI	NO
185.182.142.0/24	ICSPC – Servizi Data Center	-	SI	SI (2x /25)	SI (1x /24)
185.182.143.0/24	RISERVATA PER USI FUTURI	-	-	-	-

Tabella 7. Piano di indirizzamento IPv4

Allo scopo di ottimizzare l'utilizzo dell'indirizzamento pubblico IPv4, per le connessioni punto-punto, ove possibile, saranno utilizzate subnet /31 (RFC 3021).

4.1.2 IPv6

La subnet IPv6 rilasciata dal RIPE ad AgID per la realizzazione della QXN è:

- 2a0a:ee80::/29

FASTWEB un passo avanti	SISTEMI INFORMATIVI An IBM Company	LEONARDO SISTEMI PER LA SICUREZZA E LE INFORMAZIONI
INTERNO	ICSPC-QXN-Specificare realizzazione-1.3.Docx	

Gli indirizzamenti pubblici sono utilizzati sia per la realizzazione dell'infrastruttura che per l'esposizione dei servizi (DNS\NTP\DC). Per questo scopo gli indirizzamenti rilasciati saranno così ripartiti:

Network IPv6	Destinazione	Ruotati DC ICSPC	Ruotati QXN1	Ruotati Infranet	Ruotati Internet
2a0a:ee80::/48	QXN2 - Connessioni OPA	SI	SI	SI	NO
2a0a:ee80:1::/48	QXN2 - Servizi DNS ed NTP	SI	SI	SI	NO
2a0a:ee80:8::/47	ICSPC – Servizi Data Center	-	SI	SI (2x /48)	SI (1x /47)
....	RISERVATE PER USI FUTURI	-	-	-	-

Tabella 8. Piano di indirizzamento IPv6

4.2 CORE QXN

Il livello di Core dell'infrastruttura QXN è composto da due nodi realizzati presso il NaMeX di Roma ed il MIX di Milano interconnessi fra loro tramite quattro circuiti geografici di capacità pari a 1 Gbps ciascuno.

Ciascun nodo è composto da una coppia di apparati Cisco Catalyst 6509E (Sup 2T), denominati BRqxn fra loro connessi localmente mediante 4 link 10GE come rappresentato in Figura 4.

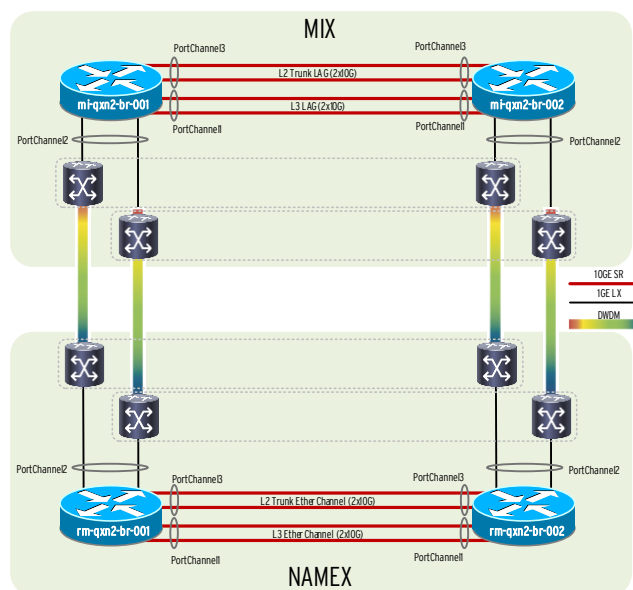


Figura 4 - Core QXN




Per ulteriori dettagli circa l'architettura dei link di trasporto si faccia riferimento al par. 2.1.1.

4.2.1 LINK AGGREGATION

I BRqxn all'interno dello stesso nodo saranno connessi mediante 4 link 10Gbps aggregati a coppie mediante protocollo LACP per ottenere:

- Un link logico L3 (2 x 10G) dedicato al trasporto del traffico MPLS (OPA)
- Un link logico L2 (2 x 10G) dedicato al trasporto delle VLAN interne al nodo

Sfruttando la disponibilità di due moduli supervisor Sup2T all'interno dello stesso chassis, i link appartenenti a ciascuna coppia saranno attestati su moduli differenti per evitare single point of failure.

		
INTERNO	ICSPC-QXN-Specificarealizzazione-1.3.Docx	

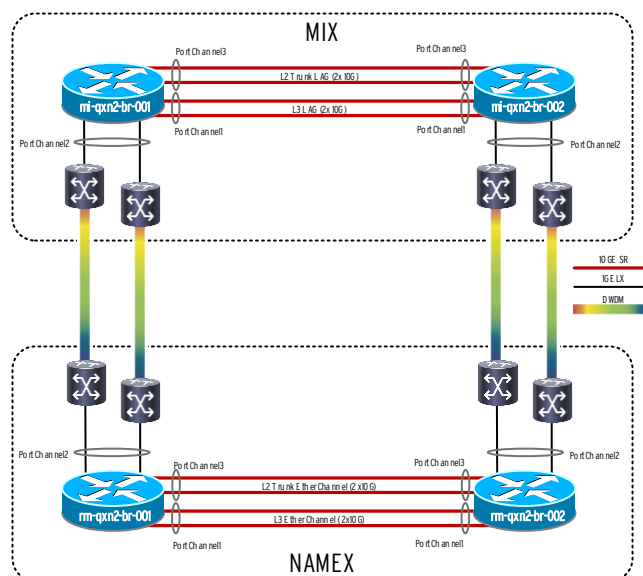


Figura 5 - Collegamenti CORE

Analogamente, i link geografici ad 1Gbps attestati sullo stesso apparato BRqxn saranno anch'essi aggregati a formare un unico link logico L3 con capacità complessiva di 2 Gbps ed attestati su moduli supervisor differenti.

4.2.2 ROUTING IGP

Come protocollo di routing IGP è stato previsto l'utilizzo di OSPFv2 in global routing table per la distribuzione delle loopback e delle punto-punto necessarie al management del core ed all'implementazione del MP-BGP.

Verrà utilizzata la sola area 0 estesa a tutti i link fra i BRqxn ed alle loopback. Per maggiore sicurezza, come richiesto dal capitolato, è prevista l'autenticazione delle adiacenze OSPF mediante MD5. Gli indirizzi di loopback verranno utilizzati come router-id OSPF.

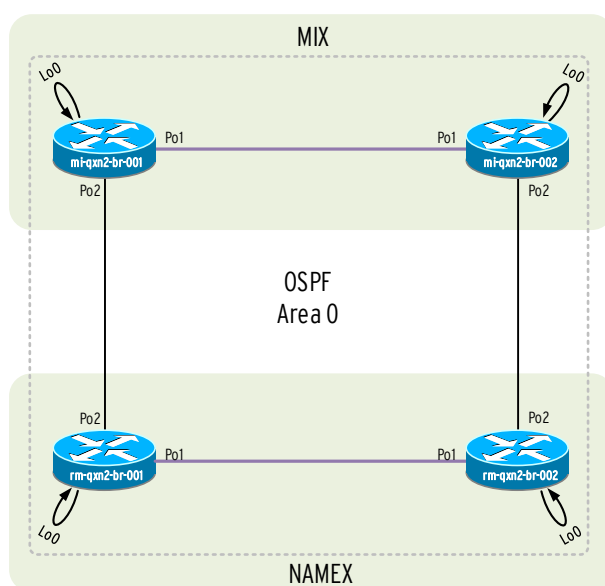




Figura 6 – Topologia IGP

Allo scopo di migliorare i tempi di riconvergenza dell'OSPF sono previste le seguenti ottimizzazioni:

FASTWEB un passo avanti	 SISTEMI INFORMATIVI An IBM Company	 LEONARDO SISTEMI PER LA SICUREZZA E LE INFORMAZIONI
INTERNO	ICSPC-QXN-Specificarealizzazione-1.3.Docx	

- impostazione del network type point-to-point su tutti i link layer3 tra i BR per minimizzare la complessità della topologia OSPF
- tuning dei timer OSPF relativi alla generazione degli LSA e trigger dello SPF per ottimizzare i tempi di riconvergenza in caso di failure
- abilitazione della funzionalità di Loop Free Alternative Fast ReRoute
- abilitazione del protocollo BFD sui link tra i BRqxn per ridurre i tempi di rilevazione dei guasti non rilevati a livello 1/2.

Su tutti i link tra i BRqxn sarà abilitato contestualmente all'OSPF, il protocollo LDP per lo scambio delle label funzionale al servizio MPLS VPN.

4.2.3 ROUTING MP-BGP

Nella soluzione adottata i BR della QXN utilizzano i protocolli MPLS ed MP-BGP per l'implementazione del servizio L3VPN. Tutto il traffico OPA IPv4/IPv6 transiterà in un VRF dedicato. L'infrastruttura di core non sarà quindi visibile in ambito Infranet (altri soggetti interconnessi SPC1/SPC, PA, ecc.).

I BRQxn saranno configurati con l'AS pubblico assegnato alla QXN e formeranno fra loro un full mesh di peering MP-iBGP su trasporto IPv4. Come terminazione dei peering sarà utilizzata la loopback 0 di ciascun BRqxn.

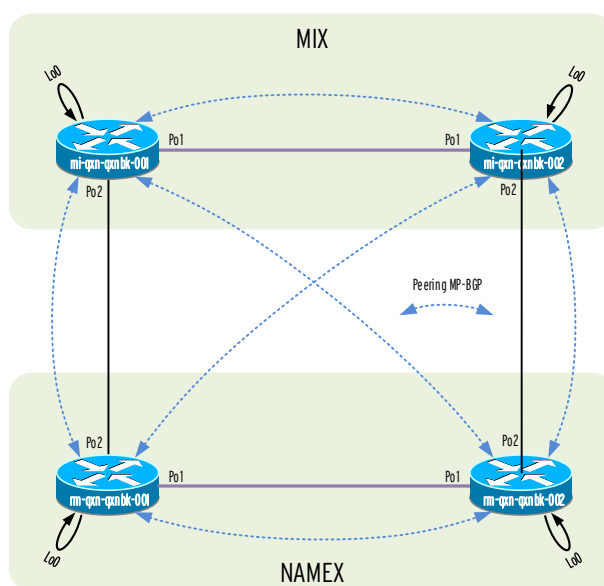


Figura 7 – Peering MP iBGP




I peering MP-iBGP trasporteranno le seguenti address-family:

- IPv4 Unicast utilizzato per i soli prefissi di gestione (loopback)
- VPNv4 e VPNv6 per l'annuncio rispettivamente dei prefissi IPv4 ed IPv6 utilizzati all'interno delle diverse VRF che costituiranno l'ambito Infranet (DC, OPA, ...)

Sui peering MP-iBGP sarà inoltre attiva l'autenticazione MD5 come richiesto dal capitolato.

4.3 SERVIZIO OPA

Sfruttando l'infrastruttura MPLS/MP-BGP precedentemente descritta, verrà creata sui BRqxn una VPN MPLS dedicata al traffico OPA. In tale VPN saranno terminati i peering eBGP dei Soggetti Interconnessi oltre ai peering verso l'infrastruttura QXN1 come descritto più in dettaglio nei paragrafi seguenti.

		
INTERNO	ICSPC-QXN-Specificare realizzazione-1.3.Docx	

4.3.1 ATTESTAZIONE DEI SOGGETTI INTERCONNESSI

Per quanto riguarda le connessioni dei soggetti interconnessi con la QXN, e per il traffico di tipo Infranet (OPA), i BRqxn agiscono a livello 3 della pila ISO/OSI.

I BRqxn avranno una sessione eBGP IPv4 ed una IPV6 distinta con i BRqx dei vari soggetti interconnessi. Ciascun Soggetto interconnesso si presenterà al QXN con il proprio ASN. L'ASN della rete QXN appare quindi come AS di transito per il traffico tra PA SPC connesse a due Q-ISP SPC differenti.

Per garantire la sicurezza e l'autenticità degli annunci scambiati tra i 4 BRqxn e tra questi e i BRqx dei soggetti interconnessi, è previsto l'impiego della funzione di hash MD-5 per l'autenticazione dei pacchetti, attivata sui protocolli di routing di interconnessione.

Previa verifica della disponibilità della funzionalità sui BRqx dei Q-ISP interconnessi, verrà attivata anche la funzione di protezione dei peering eBGP basata sul TTL (GTSM). Nel momento in cui tale funzione è attiva, il traffico BGP viene inviato con TTL pari a 255 ed accettato esclusivamente se ricevuto con tale TTL. Questo semplice meccanismo evita di esporre il control-plane del router ad attacchi (generati da host non direttamente connessi) che mirino a sovraccaricare la CPU.

Inoltre, gli annunci dei soggetti interconnessi verso la QXN saranno accettati dai BRqxn solo se con mask pari o inferiore a 24 bit per IPv4 come richiesto da capitolato. Per IPv6, non essendo presenti indicazioni da capitolato, potrà essere eventualmente applicato un analogo limite a 48bit che costituisce la granularità minima degli annunci IPv6 tipicamente distribuiti in Internet.

4.3.2 BILANCIAMENTO E SIMMETRIA DEL TRAFFICO OPA

All'interno del nodo QXN il singolo BRqx, deve propagare le informazioni di raggiungibilità relative alle PA SPC di propria pertinenza in maniera identica (medesimi attributi BGP) verso la coppia di BRqxn. Per determinare univocamente verso quale BRqx debba essere instradato il traffico proveniente dalla rete QXN (originato dalle PA SPC afferenti agli altri soggetti interconnessi), i BRqx di ciascun soggetto interconnesso devono invece annunciare i propri aggregati con communities diverse.

Al fine di rispettare anche requisito di simmetria del traffico OPA, ciascun soggetto interconnesso garantisce che il traffico da/ verso una PA SPC (o gruppo di PA SPC) attestata sulla propria rete sia consegnato/ricevuto sempre presso un unico nodo della QXN (es. Roma o Milano), come rappresentato nella figura seguente.

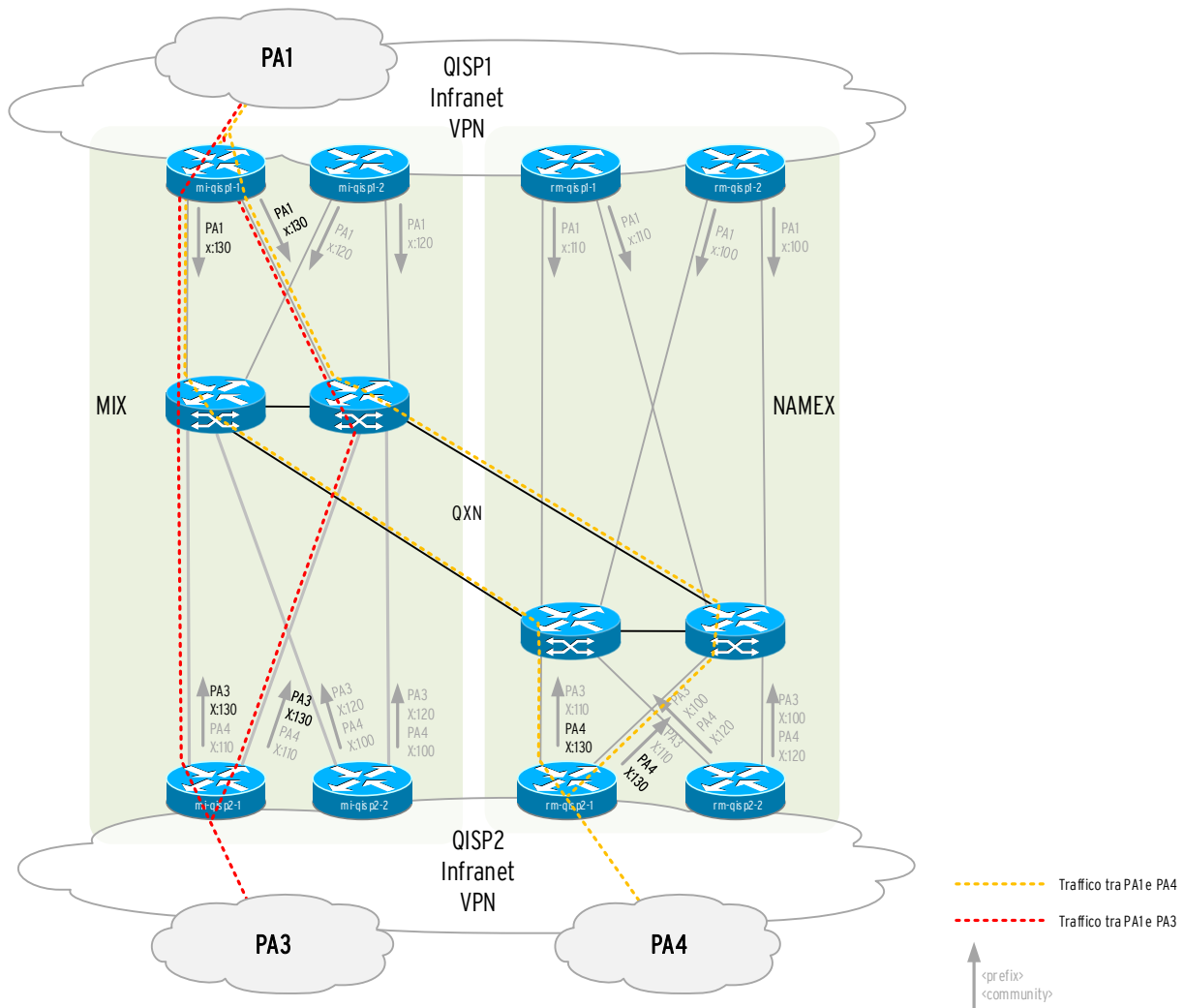





Figura 8 – Annunci BGP e conseguente instradamento simmetrico del traffico OPA sul QISP2, QXN e QISP1

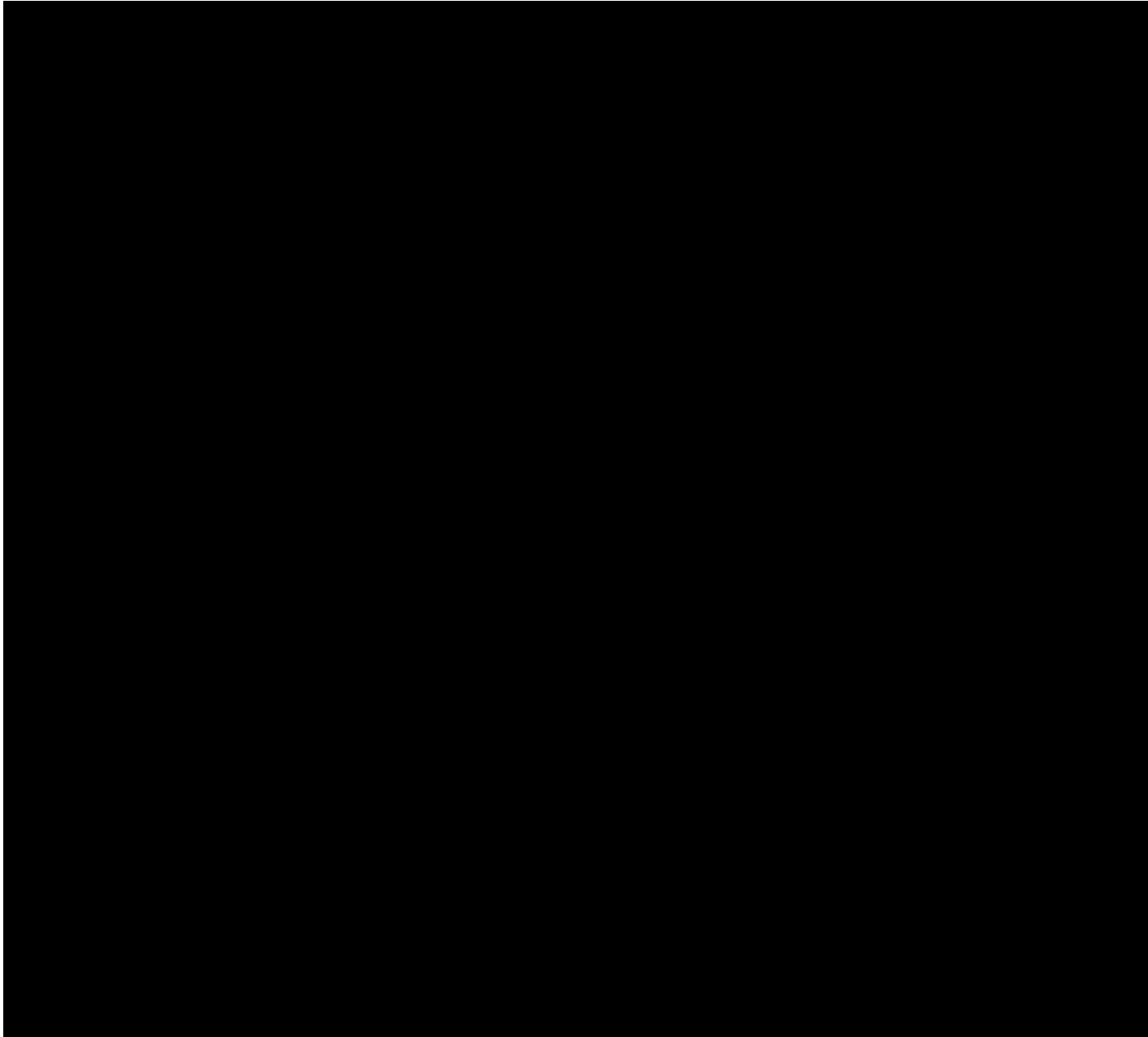
In definitiva per realizzare i requisiti di bilanciamento e simmetria occorre:




- Traffico dalla QXN verso il QISP(o soggetto interconnesso):
 - I QISP assegneranno a ciascuno dei propri BRqx una preferenza di ingresso mediante l'applicazione di una community decisionale che influenzerà l'uscita del traffico dalla QXN. A ciascuna community decisionale corrisponderà l'applicazione di una local-preference da parte dei BRQXN.
 - community x:130 = Setta la LP a 130 all'interno del QXN
 - community x:120 = Setta la LP a 120 all'interno del QXN
 - community x:110 = Setta la LP a 110 all'interno del QXN
 - community x:100 = Setta la LP a 100 all'interno del QXN
 - no community = no import: DROP dell'annuncio
 - Affinché il traffico sia bilanciato su entrambi i link del BRqx preferito, la community dovrà essere applicata in modo identico su entrambi i peering.

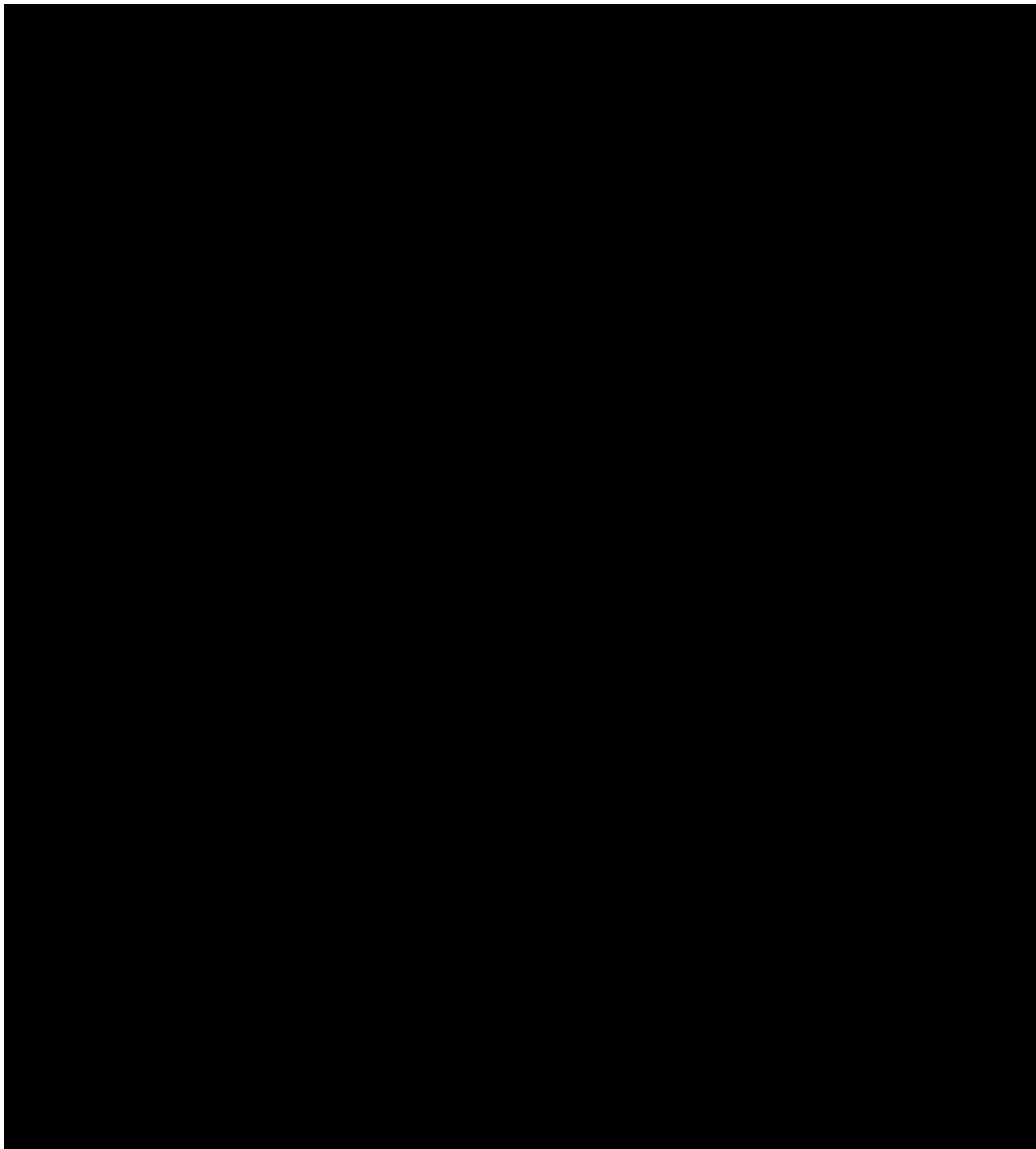
		
INTERNO	ICSPC-QXN-Specificare realizzazione-1.3.Docx	

- L'annuncio sarà propagato da entrambi i BRqxn verso i nodi adiacenti rendendo possibile il bilanciamento del traffico di uscita sui due percorsi disponibili. Per ottenere questo tipo di bilanciamento non è necessario l'uso di eBGP multipath all'interno della rete QXN.
- Traffico dal QISP(o soggetto interconnesso) verso la QXN:
 - Per ottenere la simmetria del traffico, sarà compito del QISP garantire che il BRqx preferenziale per l'ingresso sia utilizzato anche per l'uscita del traffico.
 - Il bilanciamento potrà essere ottenuto utilizzando la funzione di eBGP multipath sul BRqx. Il BRqx riceverà infatti, in condizioni normali, annunci con attributi equivalenti (ASPATH) da entrambi i BRqxn cui sarà attestato.

Si noti che la logica appena descritta è applicabile sia agli annunci IPv4 che a quelli IPv6 in modo indipendente (es. i punto di ingresso/uscita preferiti di un QISP potrebbero essere distinti per IPv4 ed IPv6).






		
INTERNO	ICSPC-QXN-Specificarealizzazione-1.3.Docx	



4.3.4 QoS OPA

Il traffico OPA, a livello di QoS, sarà trattato dalla QXN nel modo seguente:

		
INTERNO	ICSPC-QXN-Specificare realizzazione-1.3.Docx	




- Il traffico in ingresso proveniente dai Q-ISP, dovrà avere la marcatura DSCP in linea con i valori richiesti da capitolato e riportati in Tabella 9. Nel caso il traffico sia marcato con valori ammessi la marcatura sarà lasciata inalterata mentre nel caso di valori non ammessi i BRqxn rimarcheranno il traffico come BestEffort (DSCP 0).

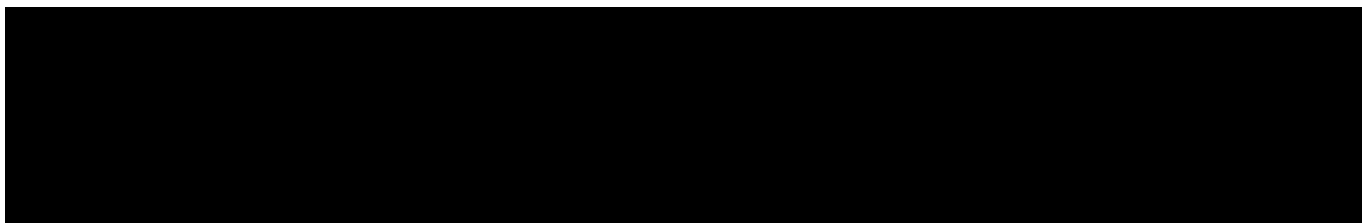
Classe di Servizio	DSCP PHB	DSCP Valore Decimale
Real Time	AF41	34
Mission Critical	AF31	26
Streaming	AF21	18
Multimedia	AF11	10
Best Effort	DF	0

Tabella 9 - Classificazione del traffico OPA

INTERNO

ICSPC-QXN-Specificarealizzazione-1.3.Docx

		
INTERNO	ICSPC-QXN-Specificare realizzazione-1.3.Docx	



4.4 SERVIZIO OPO

In accordo con l'offerta OPO, ogni fornitore assegnatario della gara multi fornitore SPC, purché abbia sottoscritto un contratto esecutivo OPO con il fornitore aggiudicatario, deve prevedere l'interconnessione con la rete QXN mediante apparati dedicati, nel seguito denominati BRopo o, in alternativa, utilizzando gli stessi apparati (BRqx) già previsti per l'interconnessione OPA.

Nel caso di singolo apparato usato dal QISP per entrambi i servizi di interconnessione OPA e OPO, le interfacce per il collegamento OPO saranno fisicamente distinte da quelle previste per l'interconnessione OPA. In caso di apparato dedicato al servizio OPO, il BRopo potrà essere un apparato con il ruolo di PE o un CE Multi-VRF.

La scelta del livello di affidabilità e ridondanza, in termini di numero di BRopo che ciascun Q-ISP può installare presso un nodo QXN, è demandato al QISP stesso nel caso di fornitore assegnatario (fermo restando il limite massimo di due apparati BRopo per ciascun nodo QXN) mentre il fornitore aggiudicatario dovrà comunque prevedere il massimo livello di affidabilità con una coppia di apparati presso ciascuno nodo QXN.

4.4.1 INTERCONNESSIONE DEI QISP

La soluzione prevede da parte dei QISP l'utilizzo di apparati BRopo collegati in trunk inizialmente con singolo link GE a ciascuno dei BRqxn. Su tali trunk sarà veicolato un numero di VLAN pari al numero di PA SPC che richiedono connettività Intranet in accordo con l'offerta OPO. All'interno del backbone dei due QISP le varie PA SPC saranno trattate come singole VPN.

Il collegamento è configurato in modalità trunk (IEEE 802.1q) per il trasporto di un numero di VLAN pari al numero di PA SPC che richiedono connettività Intranet in accordo con l'offerta OPO. L'identificativo di ciascuna VLAN (VLAN ID) viene assegnato da Fastweb e sarà univoco a livello di nodo QXN. Tale modalità di interconnessione, offre la possibilità di monitoraggio e visibilità del traffico OPO da parte AgID, oltre a delimitare univocamente il confine di ciascun operatore alla porta del BRqxn.

Le porte tra QISP aggiudicatario e ciascun assegnatario, dovranno essere dedicate. Inizialmente quindi, per ogni assegnatario che sottoscriva l'offerta OPO e richieda una porta 1GE, l'aggiudicatario dovrà prevedere una corrispondente porta 1GE. Questo vincolo ha l'obiettivo di garantire la disponibilità di una banda coerente sulla tratta QISPass-QXN-QISPagg ed evitare che la rete QXN possa costituire un potenziale collo di bottiglia per il traffico OPO.

Nel caso l'utilizzo di una interconnessione OPO tra una coppia di QISP renda necessario un incremento di banda, potrà essere valutata sia la realizzazione di una ulteriore connessione indipendente 1GE (per il trasporto di altre vlan), sia l'aggregazione di più link GE mediante protocollo LACP. In ogni caso l'upgrade di banda dovrà essere effettuato coerentemente sia dall'aggiudicatario che dall'assegnatario. Un eventuale upgrade a link a 10GE potrà essere considerato a valle di una fattibilità tecnico/economica congiunta tra AgID e Fastweb.

Lo schema in Figura 13 riporta, a titolo di esempio, le connessioni OPO di due QISP assegnatari (QISP2 e QISP3) al QISP aggiudicatario, in uno scenario in cui si siano dotati rispettivamente di un link singolo GE e due link GE.

FASTWEB un passo avanti	SISTEMI INFORMATIVI An IBM Company	LEONARDO SISTEMI PER LA SICUREZZA E LE INFORMAZIONI
INTERNO	ICSPC-QXN-Specificare realizzazione-1.3.Docx	

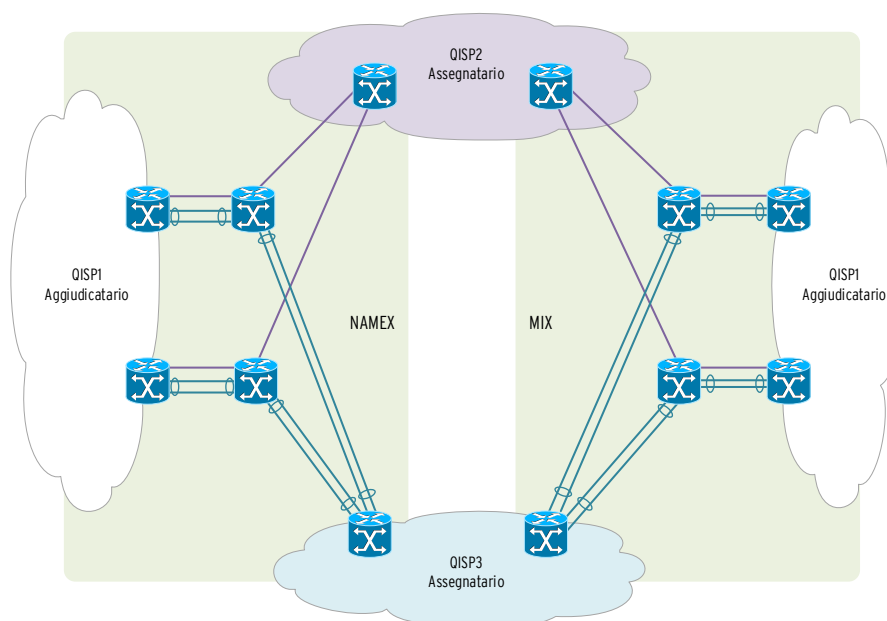


Figura 13 - Esempio di interconnessioni OPO tra QISP aggiudicatario e assegnatari.

4.4.2 BILANCIAMENTO E SIMMETRIA DEL TRAFFICO OPO

L'interconnessione OPO attraverso il QXN deve essere configurata in modo tale che il traffico OPO scambiato tra la rete del Q-ISP assegnatario e quella dell'aggiudicatario, a meno di diversa indicazione, transiti in via prioritaria sul nodo QXN di Roma ed, in via secondaria, su quello di Milano in caso di indisponibilità totale del nodo QXN di Roma. E' lasciato ai Q-ISP concordare le politiche di routing più opportune al fine di garantire la simmetria del traffico OPO entrante ed uscente dal BRopo per una determinata PA SPC, essendo, tuttavia, raccomandato l'uso delle stesse communities definite per il traffico Infranet nativo OPA sul QXN o tramite meccanismi di "AS-path prepending".




4.4.3 QoS OPO

Il traffico OPO generato dai Q-ISP in ingresso sui BRqxn, dovrà avere una marcatura DSCP in linea con i valori riportati in Tabella 10 per ciascuna classe di servizio. Nel caso il traffico sia marcato con valori ammessi la marcatura sarà lasciata inalterata (DSCP trust) mentre nel caso di valori non ammessi, i BRqxn rimarcheranno il traffico come BestEffort (DSCP 0).

Classe di Servizio	DSCP PHB	DSCP Valore Decimale
Real Time	AF41	34
Mission Critical	AF31	26
Streaming	AF21	18
Multicast	AF23	22
Multimedia	AF11	10
Best Effort	DF	0

Tabella 10 - Classificazione del traffico OPO

Si noti che, il traffico Multicast, se presente, dovrà essere marcato coerentemente dagli operatori con il DSCP 23, non corrispondente ad alcun servizio standardizzato dalla RFC 4594 ma con validità locale alla QXN.

 un passo avanti	 SISTEMI INFORMATIVI An IBM Company	 SISTEMI PER LA SICUREZZA E LE INFORMAZIONI
INTERNO	ICSPC-QXN-Specificarealizzazione-1.3.Docx	

4.5 SISTEMA DI MONITORAGGIO

Per la rete QXN è previsto un sistema di sonde, connesse a ciascun nodo QXN, al fine di monitorare i livelli di servizio previsti per il QXN per le due tipologie di traffico OPA e OPO. Il sistema di performance monitoring si basa sullo scambio di pacchetti tra due apparati, le sonde appunto, le quali espletano sia la funzionalità di *querier* (generatore di pacchetti di misura), sia quella di *responder* (target dei pacchetti di misura). In particolare ad ogni BRqxn sarà attestata una sonda con funzionalità di *querier* ed una sonda con funzionalità di *responder*. Questa modalità di attestazione delle sonde è tale da consentire che le sorgenti e le destinazioni delle misure siano rappresentativi di tutti i possibili percorsi tra punto di ingresso e di uscita alla QXN. Per i dettagli implementativi del sistema di performance monitoring si rimanda alla Specifica di Controllo.

4.5.1 SONDE

Come precedentemente indicato ogni BRqxn avrà collegate una coppia di sonde, un *querier* ed un *responder*. Le Sonde generano il traffico di controllo tramite opportuni flussi di misura tra Querier e Responder: per ciascuna direttrice di misura, mediante acquisizione delle variabili MIB ai Querier, si ricavano i valori delle metriche Round Trip Delay, Packet Loss e Packet Delay Variation riferite alla tratta Querier-Responder-Querier. Tale architettura permette il corretto monitoraggio di tutte le direttrici di traffico della QXN.

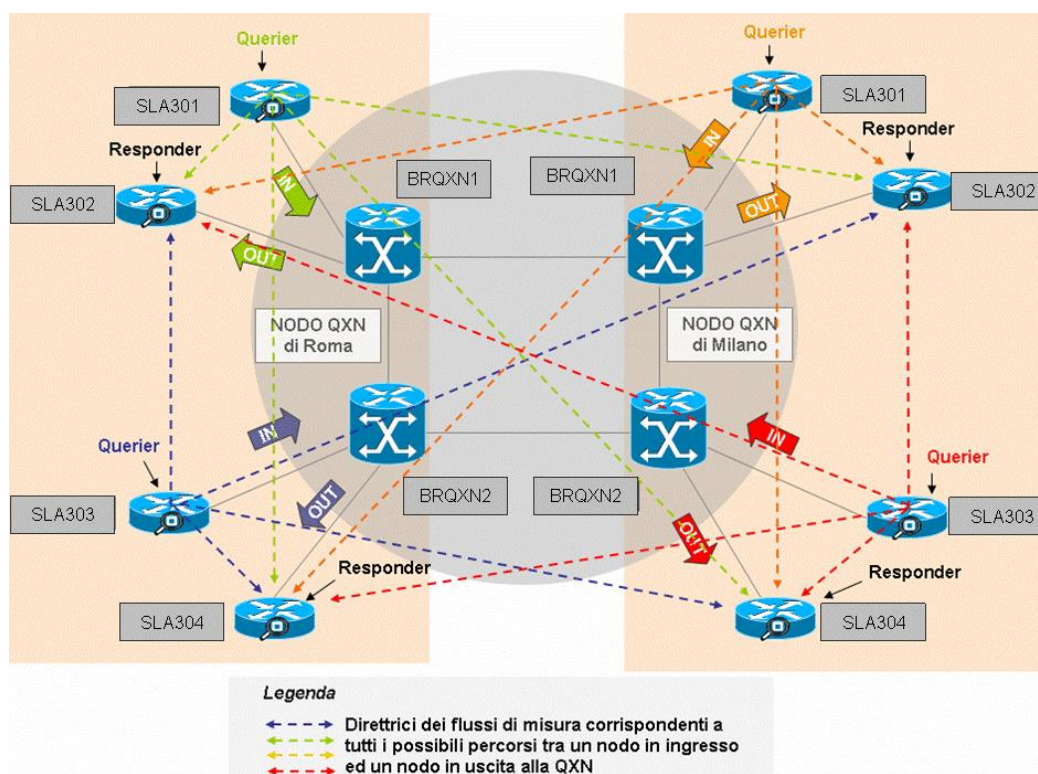





Figura 14 - Direttrici di traffico OPA

		
INTERNO	ICSPC-QXN-Specificarealizzazione-1.3.Docx	

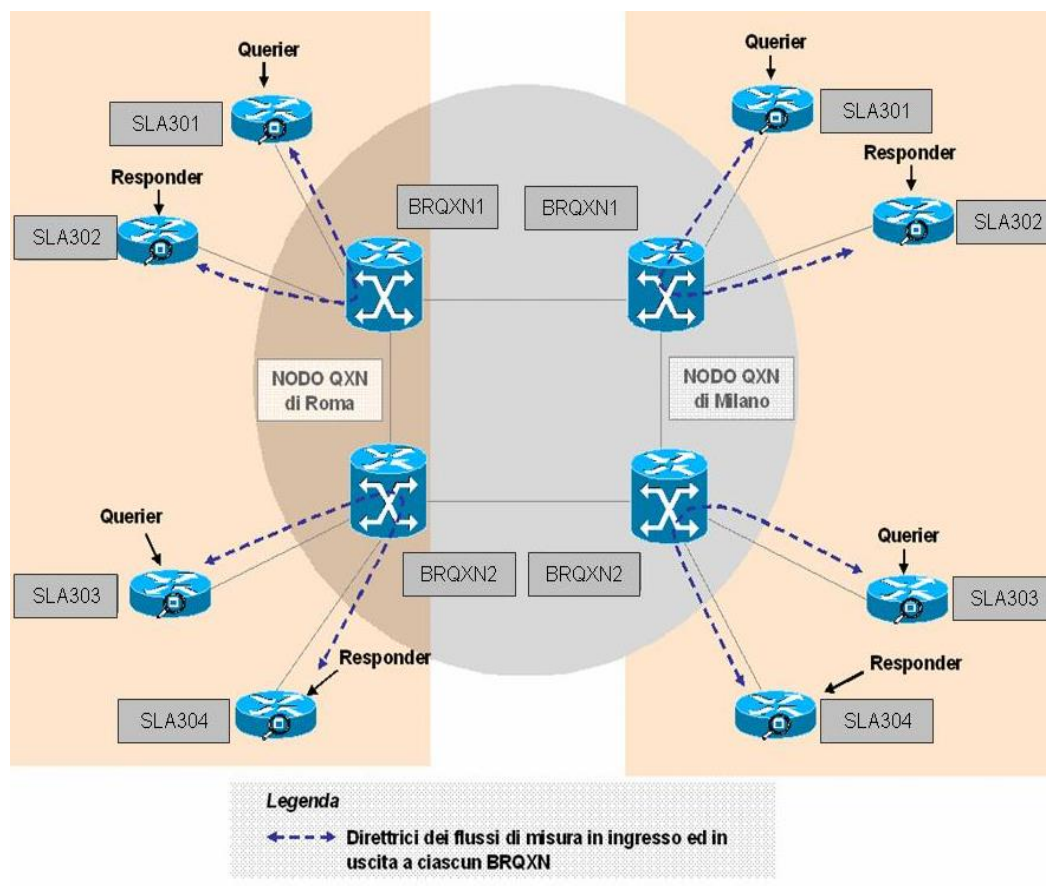


Figura 15 - Direttrici di traffico OPA

4.6 SICUREZZA DEI NODI QXN

L'infrastruttura di sicurezza di QXN prevede una coppia di firewall in alta affidabilità presso il MIX e presso il NAMEX..




I firewall svolgono le seguenti funzioni:

- Proteggono gli accessi amministrativi da remoto agli apparati di rete.
- Proteggono l'accesso ai servizi DNS e NTP dalla Infranet
- Inibiscono l'accesso ai servizi DNS e NTP da internet.
- Consentono il traffico DNS e NTP in uscita verso internet per la risoluzione delle query ricorsive e la sincronizzazione NTP l'INRIM

Al fine di prevenire eventuali tentativi di intrusione, aumentando la capacità di reazione a fronte di attacchi, i firewall hanno integrate le funzionalità di Intrusion Prevention System nella medesima coppia di macchine.

Al fine di proteggere il traffico di gestione remota degli apparati, i collegamenti tra SOC\NOC e la QXN sono realizzati tramite collegamento MPLS con indirizzamento Fastweb non visibile all'esterno.

L'autenticazione per gli apparati di rete e per gli apparati di sicurezza viene effettuata tramite un cluster di server radius collocato all'interno della rete Fastweb garantendo la gestione centralizzata e la profilatura delle utenze.

		
INTERNO	ICSPC-QXN-Specificare realizzazione-1.3.Docx	

4.6.1 NETWORK FIREWALL

Il presente paragrafo si prefigge l'obiettivo di definire le caratteristiche tecniche e quantitative delle risorse hardware e software che saranno necessarie all'implementazione della componente firewall.

Data l'elevata criticità del servizio, ogni elemento è stato previsto e realizzato con una coppia di dispositivi in alta affidabilità con meccanismo di hot standby.

La soluzione tecnologica adottata è stata selezionata in base ai seguenti criteri:

- Performance
- Scalabilità
- Efficacia del processo di gestione e monitoraggio

La soluzione tecnica che è stata individuata e che soddisfa al meglio i criteri succitati, è realizzata attraverso la tecnologia UTM di Fortinet.

Gli apparati FortiGate Firewall sono dispositivi hardware dedicati che forniscono protezione completa in real-time al perimetro di rete. Basati sul processore FortiASIC, la piattaforma FortiGate è un sistema che identifica minacce basate sui contenuti senza ridurre le performance di rete. I sistemi FortiGate includono un firewall, un motore di content filtering, VPN, un sistema IDS/IPS e un motore di gestione della banda. Queste funzionalità integrate fanno dei FortiGate una soluzione di protezione di rete potente e conveniente dal punto di vista dei costi.

Gli appliance FortiGate sono fisicamente localizzati presso i NAP di MIX e NAMEX. Il modello scelto per implementare il Servizio firewall è il FORFG-1000D.

La configurazione degli apparati, prima dell'installazione presso la sede dei NAP, è eseguita dal SOC-QXN in modo da preimpostare i parametri di connettività e politiche di sicurezza che regolamentino tutto il traffico in transito tra le interfacce del firewall.

I log generati, sono inviati ad un'altra soluzione centralizzata Fortinet identificata nell'apparato FortiAnalyzer 1000D collocato presso il DC IC-SPC.




4.6.2 CARATTERISTICHE

Le caratteristiche di base del servizio Firewall comprendono:

- Filtraggio di traffico IP: attraverso filtri (drop o accept) di indirizzi, porte e protocolli.
- Stateful Inspection: attraverso l'ispezione dei datagrammi IP e filtraggio sulla base delle regole implementate.
- Auditing e Logging: attraverso memorizzazione dei Log del traffico che attraversa il firewall e successiva analisi in accordo con le specifiche politiche di sicurezza implementate.

La gestione da remoto dei firewall, sarà garantita tramite le attività di configurazione e monitoraggio da parte del SOC-QXN. Il supporto di funzionalità di High Availability consente un failover trasparente per applicazioni mission-critical. Riduce l'esposizione alle minacce individuando e prevenendo intrusioni basandosi su signature e su anomalie di rete. Il supporto di più zone consente una segmentazione granulare in zone con politiche e livelli di sicurezza indipendenti. Garantisce performance superiori e affidabilità grazie all'architettura hardware accelerata ASIC e alimentazione hot-swap ridondata. Il sistema di download automatico delle ultime definizioni di attacchi può accettare aggiornamenti "push" dal network FortiResponse.

I dispositivi FortiGate consentono attraverso un agent SNMP il supporto, sia del MIB proprietario sia del MIB standard definito nel RFC 1213 e RFC 2665.




 un passo avanti	 An IBM Company	 SISTEMI PER LA SICUREZZA E LE INFORMAZIONI
INTERNO	ICSPC-QXN-Specificare realizzazione-1.3.Docx	




E' possibile configurare inoltre SNMP sugli apparati di protezione al fine di ottenere le informazioni sul funzionamento degli apparati o di ricevere trap asincrone come allarmi di sistema oppure allarmi relativi ai moduli di protezione come ad esempio VPN, NIDS e AntiVirus.

Il sistema operativo FortiOS™ è certificato ICSA per le funzionalità di Firewall, IPSec e NIDS.

I Virtual Domain di FortiGate consentono di configurare firewall logici multipli e routers in una singola unità FortiGate.

Nella tabella seguente sono state riassunte le principali caratteristiche degli appliance FortiGate, i benefici ad esse associati e le eventuali certificazioni ottenute.

Firewall 	Industry Standard Firewall Stateful inspection, ispeziona i pacchetti IP verificando sorgente, destinazione, porte sorgente e destinazione, mantiene lo stato delle connessioni, consentendo o negando ai pacchetti il transito attraverso il firewall. Supporta il VLAN tagging 802.1q. Consente di configurare autenticazione basata su gruppi sulle regole di firewall. Protezione certificata, massima performance e scalabilità. Previene IP spoofing con le funzionalità di IP/MAC binding.
Transparent or bridge mode	Connette due reti in bridge senza dover realizzare due diverse subnet. Il FortiGate opera senza IP address assegnato sulle interfacce. Supporta tutte le funzionalità del Firewall e dell'analisi dei contenuti.
VPN 	Industry standard supporto di PPTP, L2TP, e IPSec VPN. Una rete private virtuale (VPN) è una estensione di una rete privata che si appoggia su link su reti pubbliche come InterNet. E' possibile fornire una connessione sicura tra reti geograficamente connesse o fornire accesso ad utenti remoti verso una rete privata. Abbattimento dei costi utilizzando una rete pubblica (Internet) per comunicazioni di reti site-to-site e utenti remoti. L'implementazione della VPN IPSEC supporta algoritmi di cifratura 3DES, DES, AES e algoritmi di autenticazione MD5, SHA-1, autenticazione XAUTH, IPSEC Nat Traversal, architetture a stella (Hub and Spoke).
Network Intrusion Detection and Prevention System 	Sistema NIDS in real-time che identifica e previene una vasta varietà di attività di rete sospette. L'IPS usa signatures di attacchi e anomalie per identificare migliaia di attacchi. Sia le signatures predefinite dell'IPS che il motore IPS sono aggiornabili tramite la rete FortiResponse Distribution Network (FDN). E' inoltre possibile creare signatures personali custom.
VLAN	Supporta il protocollo di Virtual LAN IEEE 802.1q. Utilizzando la tecnologia delle VLAN un singolo apparato FortiGate può fornire servizi di sicurezza e controllare connessioni tra domini multipli utilizzando il tag di VLAN in ogni pacchetto. Il FortiGate può identificare l'ID della VLAN ed applicare policy di sicurezza al traffico tra le diverse VLAN. Può inoltre richiedere autenticazione ed effettuare operazioni di content filtering e protezione antivirus a reti su diverse VLAN.
Virtual Domain	I virtual domains di FortiGate forniscono firewall logici multipli e routers in una singola unità FortiGate. Utilizzando i virtual domain, un singolo apparato FortiGate può fornire servizi di firewalling e routing a reti diverse mantenendo effettivamente separato il traffico che attraversa i diversi virtual domain.

 un passo avanti	 An IBM Company	 SISTEMI PER LA SICUREZZA E LE INFORMAZIONI
INTERNO	ICSPC-QXN-Specificare realizzazione-1.3.Docx	

High Availability	Consente il failover tra due o più unità FortiGate. Il FortiGate realizza HA usando più apparati e il protocollo FGCP (FortiGate Clustering Protocol). E' possibile configurare le unità FortiGate sia per la modalità active-passive (A-P Hot standby) che active-active. Il software di HA garantisce che in caso di indisponibilità di una delle unità del cluster tutte le funzioni, la tabella delle sessioni, e i tunnel VPN rimangono attivi.
Traffic Shaping	Controlla la quantità di banda disponibile e stabilisce la priorità del traffico processato dalle policy. Consente di controllare quale policy ha più alta priorità quando grandi quantità di dati si muovono attraverso il FortiGate.
IP/MAC binding	L'associazione IP/MAC protegge l'apparato FortiGate e la rete da IP spoofing.
User Authentication	Gli apparati FortiGate supportano l'autenticazione di utenti con il database di utenti dell'apparato, o con un server RADIUS o LDAP.
Logging and Reporting	I log possono essere inviati ad un server syslog remoto o a WebTrends NetIQ Security reporting center e Firewall Suite server usando il formato avanzato di WebTrends. Alcuni modelli sono dotati di hard disk e possono registrare i log in locale. Gli apparati che non sono dotati di disco fisso possono comunque registrare gli ultimi eventi ed attacchi individuati dall'IDS su memoria condivisa con il sistema.

Technology Program	Vendor	Product Testing Reports ▲	Certification	Product Version	Date	Certification Type	Operating System
Advanced Threat Defense (ATD)	Fortinet, Inc.	Advanced Threat Protection Solution	Advanced Threat Defense (ATD)	see report	12/08/2015	Not Specified	N/A
Anti-Virus	Fortinet, Inc.	FortiGate® Consolidated Security Platforms	Gateway Anti-Virus Detection	current		Corporate	FortiOS™
IPSec	Fortinet, Inc.	FortiGate® Consolidated Security Platforms	IPSec IKEv2	current	12/03/2015	Enhanced	FortiOS™
Network Firewalls	Fortinet, Inc.	FortiGate® Consolidated Security Platforms	Network Firewalls	current	07/12/2016	Corporate	FortiOS™
Network IPS	Fortinet, Inc.	FortiGate® Consolidated Security Platforms	Network IPS	current	03/30/2016	Enterprise	FortiOS™
SSL-TLS	Fortinet, Inc.	FortiGate® Consolidated Security Platforms	SSL-TLS VPN 4.0	current	12/15/2015	Not Specified	FortiOS™
Web Application Firewalls	Fortinet, Inc.	FortiWeb-1000D	Web Application Firewalls	current	08/05/2016	Not Specified	Proprietary

Tabella 11 - Caratteristiche e certificazioni FortiGate

4.6.3 PRE-INSTALLAZIONE E CONFIGURAZIONE DEL FORTIGATE

Prima di procedere alla configurazione di una unità FortiGate, è necessario pianificare quale dei due modi operativi si intende utilizzare: NAT/Route o Transparent mode.




4.6.3.1 NAT/Route mode

In modo NAT/Route, l'apparato è visibile alla rete. Come un router, tutte le sue interfacce sono su subnet differenti. Le interfacce disponibili in NAT/Route mode:

- Interfaccia esterna (ad es.: Internet)
- Interfaccia interna
- Una o più DMZ, in base al profilo scelto.

E' possibile aggiungere policy per controllare qualsiasi comunicazione che passi attraverso il FortiGate. Le policy controllano il traffico basandosi sull'indirizzo sorgente, destinazione, e servizio di ogni singolo pacchetto. In modalità NAT il FortiGate esegue la traduzione degli indirizzi (NAT) prima che il pacchetto sia spedito alla rete di destinazione.

Il FortiGate ha una policy predefinita in modalità NAT, che consente agli utenti sulla rete interna di accedere in maniera sicura ai contenuti sulla rete esterna. Nessun altro tipo di traffico è possibile se non si configurano ulteriori policy.

		
INTERNO	ICSPC-QXN-Specificare realizzazione-1.3.Docx	

Tipicamente si utilizza la modalità NAT/Route, quando il FortiGate è usato come gateway tra reti private e pubbliche. In questa configurazione si creano policy NAT per controllare il traffico tra le reti interne private e quelle esterne pubbliche. Se sono disponibili più reti interne, come ad esempio una DMZ, è possibile creare policy e regole di routing per il traffico che si muove tra le varie zone.

4.6.3.2 *Transparent mode*

In modalità transparent, il FortiGate è invisibile alla rete. Simile ad un bridge di rete, tutte le interfacce FortiGate appartengono alla stessa subnet. Sull'apparato si configura un singolo indirizzo IP per il management.

L'indirizzo IP di management è anche usato per il download delle definizioni degli attacchi e dei virus. Tipicamente questa modalità si usa su reti private dietro un firewall già installato o dietro un router. L'apparato funziona sia come firewall che come antivirus.

4.6.4 OPZIONI DI CONFIGURAZIONE

Selezionata la modalità di funzionamento, si può completare il piano di configurazione e iniziare a configurare l'apparato. E' possibile usare l'interfaccia web, l'interfaccia a linea di comando, per tutte le operazioni di configurazione di base dell'apparato.

La modalità utilizzata per erogare i servizi descritti nel presente documento è NAT/Route mode

4.6.5 CONFIGURAZIONE

La configurazione dei firewall permette l'erogazione dei servizi DNS ed NTP in ambito Infranet su ciascun nodo QXN mediante IP virtuali IPv4/IPv6. L'indirizzamento della rete DMZ è pubblico IPv4/IPv6 ma non annunciato su Internet.




Per consentire il browsing Internet, necessario al corretto funzionamento dei servizi, il firewall effettuerà dinamicamente il NAT degli indirizzi IP posti in DMZ utilizzando indirizzi IP pubblici Fastweb.

Per quanto concerne la connettività Internet sono previsti i seguenti flussi:

- I server NTP utilizzeranno la connettività Internet per contattare il servizio NTP stratum 1 dell'INRiM.
- I server DNS per la risoluzione delle query ricorsive.

Il routing del firewall sarà infine configurato come segue:

- Lato Infranet per apprendere dinamicamente, via protocollo di routing dinamico le rotte Infranet ed annunciare la propria DMZ ed i VIP.
- Lato Internet con una default statica verso l'indirizzo HSRP dei CPE Internet Fastweb.

		
INTERNO	ICSPC-QXN-Specificarealizzazione-1.3.Docx	

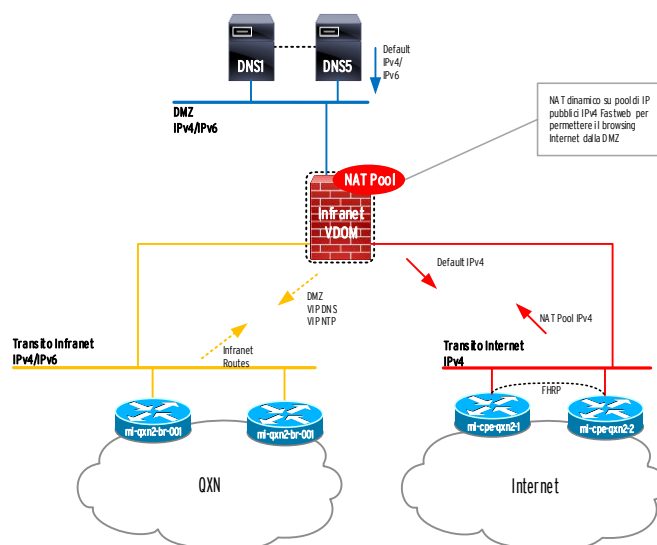


Figura 16 - Routing Firewall

4.6.6 SISTEMA DI LOGGING CENTRALIZZATO - FORTIANALYZER

L'unità di logging è un appliance di rete posizionato nel Data Center IC-SPC che effettua un'analisi e colleziona i dati spediti dai dispositivi di protezione. L'unità riceve i log da dispositivi multipli di protezione, e li utilizza per fornire dei report sui quali verrà successivamente fatta l'analisi definitiva del traffico e degli attacchi.

Tali dati saranno disponibili su richiesta di CERT PA e trasmesse via e-mail.

Le unità di log sono dedicate alla raccolta dei log e alla generazione della reportistica e possono raccogliere e aggregare i log di differenti apparati o di apparati di terze parti.

Il sistema di log centralizzato è composto da hardware dedicato che riceve e analizza in modo sicuro i log provenienti dagli apparati per la sicurezza.

Tali prodotti assicurano agli amministratori di reti un quadro completo delle informazioni relative all'uso e alla sicurezza delle stesse.

Le apparecchiature in questione accettano ed elaborano una gamma completa di registrazioni dei log forniti dai sistemi di protezione, compresi i dati riguardanti il traffico, gli eventi, i virus e gli attacchi.




L'analisi integrata dei log costituisce un punto fermo per una valutazione coerente dell'utilizzo delle reti, delle attività su Web e delle attività d'attacco ai sistemi

Il sistema fornisce informazioni di sicurezza e relative all'utilizzo della rete facilitando l'individuazione di eventuali vulnerabilità. I log sono trasmessi tramite un canale crittografato per assicurare la sicurezza della trasmissione delle informazioni. Il sistema fornisce la possibilità di scaricare i file di log su un FTP server per scopi di archiviazione.

L'unità di raccolta consente di ottenere un elevato livello di logging sia per il traffico che per tutte le altre funzioni di protezione e fornisce in forma dettagliata dei report per una ulteriore analisi ed aiuta in questo modo ad identificare i problemi di sicurezza.

La tipologia di log nei dispositivi di protezione sono i seguenti:

- Log relative al traffico;
- Eventi relativi al sistema (system restarts, HA e VPN);
- Signature e anomaly attack Logging;

 un passo avanti	 An IBM Company	 SISTEMI PER LA SICUREZZA E LE INFORMAZIONI
INTERNO	ICSPC-QXN-Specificare realizzazione-1.3.Docx	

- Instant Messaging e traffico Peer-to-peer

Per ognuna di queste tipologie è possibile avere i seguenti livelli di priorità o severity:

- 0 - Emergency: Il sistema è diventato instabile
- 1 - Alert: È richiesta un'azione immediata.
- 2 - Critical: Influenzate le funzionalità
- 3 - Error: Esistenza di una condizione di errore o di funzionalità

Le principali funzionalità dell'unità FortiAnalyzer sono:

- Reporting: Analisi del log e Reportistica consente di generare una varietà di report (HTML) che consentono di intervenire in maniera proattiva. Attraverso i report è possibile analizzare le informazioni relative ai tentativi di intrusione, così come identificare alti volumi di traffico o attacchi che possono rallentare la rete;
- Log viewer: Il Log viewer consente di visualizzare i messaggi spediti dai dispositivi remoti verso l'unità di logging. Con il viewer è possibile visualizzare qualsiasi file di log memorizzato sull'unità di logging. A tutti i file di log e i messaggi è possibile applicare dei filtri per effettuare delle ricerche mirate per localizzare informazioni specifiche;
- Real-time log viewing: L'unità di logging effettua un content logging in real-time per il traffico di tipo WEB, EMAIL e FTP. È possibile visualizzare in tempo reale il contenuto per i dispositivi remoti amministrati. Nel content logging sono incluse le informazioni relative al traffico. Ad esempio un log relativi al protocollo http, include l'indirizzo sorgente e l'indirizzo di destinazione per la URL specificata;
- Aggregazione dei log: L'aggregazione del log è un metodo che consente di collezionare i log provenienti dalle unità di log oppure da dispositivi di terze parti che supportano il formato syslog.




Il FortiAnalyzer svolge la funzione di collettore di Eventi e Log e quella di generatore di Report.

Questa soluzione è in grado di ricevere i file di log dai dispositivi locali (Fortigate e Syslog Devices), memorizzarli, analizzarli e produrre dei report aggregando i dati grezzi o viste logiche derivate dai dati stessi.

- FortiAnalyzer è costituito dai moduli di seguito elencati:
- Reporting: è la funzione preposta alla generazione di report e analisi dei log;
- Alerting: è la funzione preposta all'invio degli Alert al verificarsi di determinati eventi critici;
- Content Archiving: implementa la possibilità di consultare i log in tempo-reale o quelli vecchi archiviati anche attraverso l'applicazione di filtri personalizzati in base all'utente;
- Event Correlation: permette di verificare le eventuali correlazioni esistenti tra eventi diversi attraverso l'analisi dei log;
- Vulnerability Scanner: attraverso questa funzione è possibile verificare le vulnerabilità di un appliance;
- Network Analyzer: questa funzione viene utilizzata in quelle aree della rete dove gli appliance FortiGate non sono impiegati e permette di controllare il traffico in real-time su una porta dedicata dello stesso FL;
- Network Attached Storage (NAS): implementa a tutti gli effetti un sistema NAS utile nel caso in cui un sistema esterno debba condividere log o report del FL.

4.7 SERVIZIO NTP

L'infrastruttura QXN include un servizio NTP per la generazione del tempo ufficiale di rete in ambito Infranet. Tale funzionalità sarà erogata su entrambi i nodi QXN, da un cluster di server (i medesimi utilizzati per erogare il servizio DNS). Tali server acquisiranno a loro volta il tempo ufficiale dai server dell'Istituto Galileo Ferraris in modalità NTPv3 autenticata, attraverso la connettività Internet ridondata e protetta da Firewall. La scelta

		
INTERNO	ICSPP-QXN-Specificare realizzazione-1.3.Docx	

di introdurre i Firewall ha lo scopo di isolare e proteggere l'ambiente QXN, ritenuto di per sé affidabile, da una rete intrinsecamente "non trusted" qual è Internet.

Al fine di garantire la massima affidabilità del servizio, ciascun cluster di server renderà disponibile il Tempo Ufficiale di Rete (TUR) in modalità NTPv3 non autenticata, attraverso un Virtual IP address (VIP) appartenente allo spazio di indirizzamento di una DMZ annunciata in ambito Infranet. In questo modo viene reso disponibile un servizio NTP distribuito sui due nodi QXN (ciascuno in alta affidabilità). Sarà discrezione della singola PA decidere quale dei due nodi QXN disponibili tra Milano e Roma verrà utilizzato come NTP server primario e secondario sui propri apparati di rete che fungeranno da client del servizio.

Il servizio NTP sarà disponibile sia in IPv4 che IPv6.

4.8 SERVIZIO DNS

L'architettura QXN prevede l'introduzione di un sistema DNS mediante il quale garantire la risoluzione di tutti i domini appartenenti alle Pubbliche Amministrazioni che aderiscono all'SPC. Il medesimo sistema fungerà da resolver per i domini extra SPC, la cui risoluzione è demandata ai root server presenti su Internet. Per consentire al sistema DNS di assolvere a tale funzione è necessario garantirne l'accesso ad Internet protetto anch'esso dal sistema di firewalling.

Al fine di garantire la massima affidabilità del servizio, il sistema DNS è costituito da due cluster distribuiti sugli altrettanti nodi della QXN di Roma e Milano. Ciascun cluster è formato da 5 server che erogheranno il servizio mediante un Virtual IP address (VIP). Sarà facoltà di ciascun Q-ISP della SPC scegliere il cluster primario e quello secondario (instradando verso il VIP preferito le richieste DNS).

La comunicazione tra il generico DNS dedicato alle Pubbliche Amministrazioni SPC di ciascun Q-ISP e il sistema DNS presso il QXN attraverserà l'ambito Infranet di ciascun Q-ISP e, passando per l'infrastruttura di accesso OPA realizzata tra BRqxn e BRqxn, sarà instradato da questi ultimi verso la coppia di firewall in HA mediante la LAN di servizio.

La connessione verso Internet consente solamente l'invio delle query ricorsive DNS relative a richieste di risoluzione di nomi/domini non SPC. Il servizio è realizzato mediante la medesima architettura di rete/sicurezza già indicata per il servizio NTP. In caso di indisponibilità della connettività Internet, il cluster smetterà di rispondere alle query provenienti da ciascun Q-ISP.

Il servizio sarà erogato in rispetto delle normative vigenti legate alla gestione di servizi DNS pubblici, come ad esempio: il filtraggio nomi, domini ed indirizzi IP dei siti segnalati dal Centro Nazionale per il contrasto della pedopornografia sulla rete Internet (c.d. Decreto Gentiloni); blocco dei domini secondo quanto richiesto dalla Autorità Giudiziaria e dalla Polizia Postale; blocco della risoluzione ai siti indicati da AAMS.



Il servizio sarà disponibile sia in IPv4 che IPv6.

Durante la fase di migrazione da vecchia a nuova QXN, sarà garantita la risoluzione dei domini pubblicati sulla SPC1 anche alle PA già presenti in SPC mediante comunicazione tra i DNS della QXN con quelli della QXN1.

4.9 RETE DI MANAGEMENT OOB

Il progetto prevede una infrastruttura che consente il management out-of-band di apparati di rete, sicurezza e dei server in **due modalità**:

- **Console** – Dedicata esclusivamente ad apparati di rete e firewall, consente l'accesso remoto, mediante terminal server, alle porte console degli apparati. Questa modalità è indispensabile per eseguire la **prima configurazione degli apparati ed operazioni di manutenzione straordinarie**.
- **IP OOB** – Utilizzata su apparati di rete, firewall e server, consente un accesso IP alle macchine utilizzando un **percorso fisico e logico distinto da quello utilizzato per l'erogazione dei servizi**. Il NOC

FASTWEB un passo avanti	 SISTEMI INFORMATIVI An IBM Company	 LEONARDO SISTEMI PER LA SICUREZZA E LE INFORMAZIONI
INTERNO	ICSPC-QXN-Specificarealizzazione-1.3.Docx	

ed il SOC Fastweb utilizzeranno di norma questo accesso per la gestione degli apparati/server. In ambito IP OOB verranno utilizzati indirizzi IPv4 non annunciati.

Gli apparati saranno gestiti anche in modalità IB attraverso l'infrastruttura QXN. In questo ambito verrà utilizzato indirizzamento pubblico IPv4 assegnato ad AgID.

Questa modalità verrà utilizzata dal sistema TNMS per il monitoraggio e l'inventary degli apparati oltre che dal FortiAnalyzer per raccogliere i log dei Firewall. Entrambi questi sistemi saranno posizionati all'interno del DC IC-SPC. Sarà inoltre utilizzata come backup per accedere agli apparati dal NOC Fastweb nel caso di indisponibilità dell'infrastruttura OOB su uno dei nodi (utilizzando come jump-host il TNMS o un altro apparato).

4.9.1 OOB Nodi QXN

Le interfacce OOB di server e apparati di rete si attesteranno su due vlan/subnet distinte («Inside OOB Net» e «Inside OOB DNS») entrambe con indirizzamento privato ridistribuite dal Firewall ed annunciate al CPE di management Fastweb come rappresentato in Figura 17

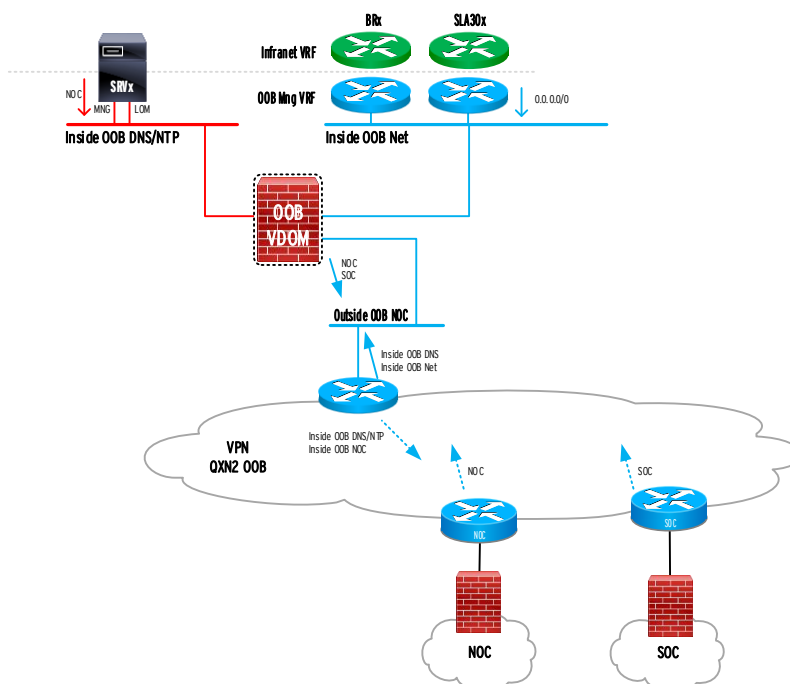


Figura 17 - Out Of Band Management dei nodi QXN




I server saranno attestati con due interfacce alla rete OOB:




- Una interfaccia di “management” che garantirà l’accesso al sistema operativo
- Una interfaccia LOM che permetterà di eseguire operazioni di manutenzione straordinaria sul server (console remota)

Entrambe le interfacce ruoteranno verso il firewall, sul quale verrà realizzato un VDOM dedicato al management OOB, tutto l’indirizzamento di management e la rete del NOC.




L’interfaccia di management degli apparati di rete Cisco sarà configurata all’interno di un VRF dedicato al management OOB ed in questo contesto verrà utilizzato il firewall come default gateway.

Il firewall sarà gestito attraverso l’interfaccia logica «Inside OOB Net». Attraverso di esso saranno raggiungibili il NOC, il SOC attraverso la VPN di management.

		
INTERNO	ICSPC-QXN-Specificarealizzazione-1.3.Docx	

		
INTERNO	ICSPC-QXN-Specificarealizzazione-1.3.Docx	

Fine del Documento

		
INTERNO	ICSPC-QXN-Specificacontrollo-1.2.Docx	

Infrastrutture Condivise SPC




Specifica di controllo IQXN

IDENTIFICATIVO

ICSPC-QXN-SpecificaControllo-1.2




STORIA DEL DOCUMENTO

Rev.	Data	Redatto	Approvato	Descrizione modifica
1.0	28/10/2016	A. Marcandalli	S. DI Bisceglie	Prima emissione
1.1	13/01/2017	A. Marcandalli	S. DI Bisceglie	Rimosso par. aggregazione oraria, modificata formula calcolo PL.
1.2	31/01/2017	A. Marcandalli T. Petrino	S. DI Bisceglie	Par. 5.1.4: Precisata modalità gestione della casistica di assenza completa di misurazioni PL, RTD, PDV in un intervallo di riferimento

 un passo avanti	 SISTEMI INFORMATIVI An IBM Company	 LEONARDO SISTEMI PER LA SICUREZZA E LE INFORMAZIONI
INTERNO	ICSPC-QXN-Specificacontrollo-1.2.Docx	




ALLEGATI

Nome	Descrizione

 un passo avanti	 An IBM Company	 SISTEMI PER LA SICUREZZA E LE INFORMAZIONI
INTERNO	ICSPC-QXN-Specificacontrollo-1.2.Docx	

Sommario

1	GENERALITÀ	4
1.1	SCOPO DEL DOCUMENTO	4
1.2	APPLICABILITÀ	4
1.3	RIFERIMENTI	4
1.4	DEFINIZIONI ED ACRONIMI.....	5
2	INTRODUZIONE	6
3	ARCHITETTURA DEL SISTEMA DI MONITORAGGIO DELLE PRESTAZIONI	7
3.1	SERVIZIO OPA.....	7
3.2	SERVIZIO OPO	7
3.3	SPECIFICHE DEI FLUSSI DI MISURA.....	8
3.4	ACQUISIZIONE DELLE MISURE	8
4	DEFINIZIONI E METODI DI CALCOLO DELLE METRICHE.....	9
4.1	ROUND TRIP DELAY	9
4.2	PACKET LOSS.....	10
4.2.1	<i>Esempio in caso di perdita di pacchetti.....</i>	<i>10</i>
4.3	PACKET DELAY VARIATION	11
5	ACQUISIZIONE ED ELABORAZIONE DEI DATI SUL TNMS.....	13
5.1	MODALITÀ DI ESTRAZIONE DELLE VARIABILI MIB	13
5.1.1	<i>Tasso di perdita dei pacchetti (Packet Loss)</i>	<i>13</i>
5.1.2	<i>Round Trip Delay.....</i>	<i>13</i>
5.1.3	<i>Packet delay variation.....</i>	<i>14</i>
5.1.4	<i>Consolidamento dei dati</i>	<i>14</i>
5.2	MODALITÀ DI ESPORTAZIONE DEI DATI AL SIRF	14

 un passo avanti	 An IBM Company	 SISTEMI PER LA SICUREZZA E LE INFORMAZIONI
INTERNO	ICSPC-QXN-Specificacontrollo-1.2.Docx	

1 GENERALITÀ

1.1 SCOPO DEL DOCUMENTO

Il presente documento si prefigge di descrivere la soluzione per il controllo dei parametri prestazionali della rete QXN.

Diversamente per gli SLA di disponibilità e Provisioning: SLA 2.2.2, SLA 2.2.3, SLA 2.2.4, SLA 2.2.5, SLA 2.2.6, SLA 2.2.7 e SLA 2.2.8 il sistema di rilevamento dei fault è TNMS, il sistema di tracking delle attività è Remedy. Entrambi i sistemi TNMS e Remedy sono descritti nel documento ICSPC-SSOP-Specifica Realizzazione-x.y




In aggiunta per lo SLA SLA 2.2.1 trattandosi di SLA relativo ad attività implementative è necessario far riferimento al Service Manager e nella fattispecie alla fonte alimentante FA SERVICE_MANAGER.

1.2 APPLICABILITÀ

Il presente documento si applica all'intero Contratto [CIG 6049538CAC] stipulato in data 5/8/2016 tra AgID e l'RTI Fastweb spa-Finmeccanica spa-Sistemi Informativi srl, per l'affidamento della progettazione, realizzazione, fornitura, manutenzione e gestione delle Infrastrutture Condivise del Sistema Pubblico di Connettività d'ora in avanti ICSPC.

1.3 RIFERIMENTI




Rif.	Codice	Titolo
DA-1.		"SPC-IC – Allegato 5 – Capitolato Tecnico" relativo alla "Gara a procedura aperta per l'affidamento della progettazione, realizzazione, fornitura, manutenzione e gestione delle infrastrutture condivise del sistema pubblico di connettività (ID SIGEF 1366)"
DA-2.		Appendice 1 al Capitolato Tecnico "SLA e Penali" relativo alla "Gara a procedura aperta per l'affidamento della progettazione, realizzazione, fornitura, manutenzione e gestione delle infrastrutture condivise del sistema pubblico di connettività (ID SIGEF 1366)"
DA-3.	CIG 6049538CAC	Contratto per l'affidamento della progettazione, realizzazione, fornitura, manutenzione e gestione delle Infrastrutture Condivise del Sistema Pubblico di Connettività stipulato in data 5/8/2016 tra AgID e l'RTI Fastweb spa-Finmeccanica spa-Sistemi Informativi srl
DA-4.		"IC-SPC Relazione tecnica FW-SES-SI" relativo alla "Gara a procedura aperta per l'affidamento della progettazione, realizzazione, fornitura, manutenzione e gestione delle infrastrutture condivise del sistema pubblico di connettività (ID SIGEF 1366)"
DA-5.		ICSPC-SSOP-Specifica Realizzazione-x.y
DA-6.		ICSPC-GE-Raccoglitore_Requisiti_x.y

		
INTERNO	ICSPC-QXN-Specificacontrollo-1.2.Docx	

Rif.	Codice	Titolo
DA-7.		ICSPC-GE-Acronimi-x.y

1.4 DEFINIZIONI ED ACRONIMI

Definizione/Acronimo	Descrizione
PL	Packet Loss
PDV	Packet Delay Variation
RTD	Round Trip Delay
SLA	Service Level Agreement
MIB	Management Information Base
SNMP	Simple Network Management Protocol
DC	Data Center
QXN	Qualified Exchange Network
QXN1	Vecchia infrastruttura QXN

		
INTERNO	ICSPC-QXN-Specificacontrollo-1.2.Docx	

2 Introduzione

Il sistema di monitoraggio dei livelli di servizio della QXN ha l'obiettivo di misurare i KPI prestazionali della rete QXN e permettere la verifica della rispondenza degli stessi agli SLA Target previsti da capitolato oltre che raccogliere e presentare dati utili a fini di analisi e troubleshooting della rete.

Il sistema si compone di due elementi principali:

- Le sonde di misura - realizzate con sonde Cisco IP SLA, mediante la generazione di traffico, misurano le prestazioni della QXN in termini di PL, RTD e PDV.
- Il sistema di monitoraggio – basato piattaforma TNMS, collocata nel DC IC-SPC, si occupa di acquisire via SNMP i risultati delle misure eseguite dalle sonde. Il sistema si occupa anche di calcolare ed aggregare temporalmente i valori di PL, RTD e PDV sulla base dei dati esposti dalle sonde attraverso le MIB.

I dati raccolti ed aggregati dal TNMS costituiscono inoltre una delle fonti alimentanti del sistema di rendicontazione e calcolo delle penali.

Nel seguito del documento verranno descritti:

- L'architettura del sistema di monitoraggio dei livelli di servizio
- Le modalità di calcolo delle prestazioni come eseguite dalle sonde IP SLA
- La modalità di acquisizione dei dati da parte del sistema di monitoraggio
- Le elaborazioni eseguite dal sistema di monitoraggio sui dati grezzi acquisiti dalle sonde per il calcolo dei KPI grezzi
- Le modalità di esportazione dei dati verso il SIRF

FASTWEB un passo avanti	SISTEMI INFORMATIVI An IBM Company	LEONARDO SISTEMI PER LA SICUREZZA E LE INFORMAZIONI
INTERNO	ICSPC-QXN-Specificacontrollo-1.2.Docx	

3 Architettura del sistema di monitoraggio delle prestazioni

La misurazione delle prestazioni si basa sullo scambio di pacchetti tra coppie di apparati (sonde Cisco IP SLA) che svolgono l'una il ruolo di *querier* (sorgente di pacchetti di misura) e l'altra quello di *responder* (destinazione dei pacchetti di misura). A questo livello, l'architettura prevista, è simile a quella prevista per la QXN1.

I punti di attestazione delle sonde sono tali da consentire che le sorgenti e le destinazioni delle misure siano rappresentativi di tutti i possibili percorsi tra punto di ingresso e di uscita dalla QXN.

Per ciascun tipo di servizio di interconnessione (OPA/OPO), le sonde generano il traffico di controllo, in modo da simulare il reale instradamento sul QXN, in relazione al tipo di funzionalità richiesto ai BRqxn.

3.1 SERVIZIO OPA

Per servizi OPA (BRqxn con funzionalità di routing): i flussi di misura sono generati da ciascuna sonda *querier* verso tutte le altre sonde *responder*, attraversando i vari BRqxn a livello 3 (simulano il traffico tra due BRqx di Q-ISP differenti).

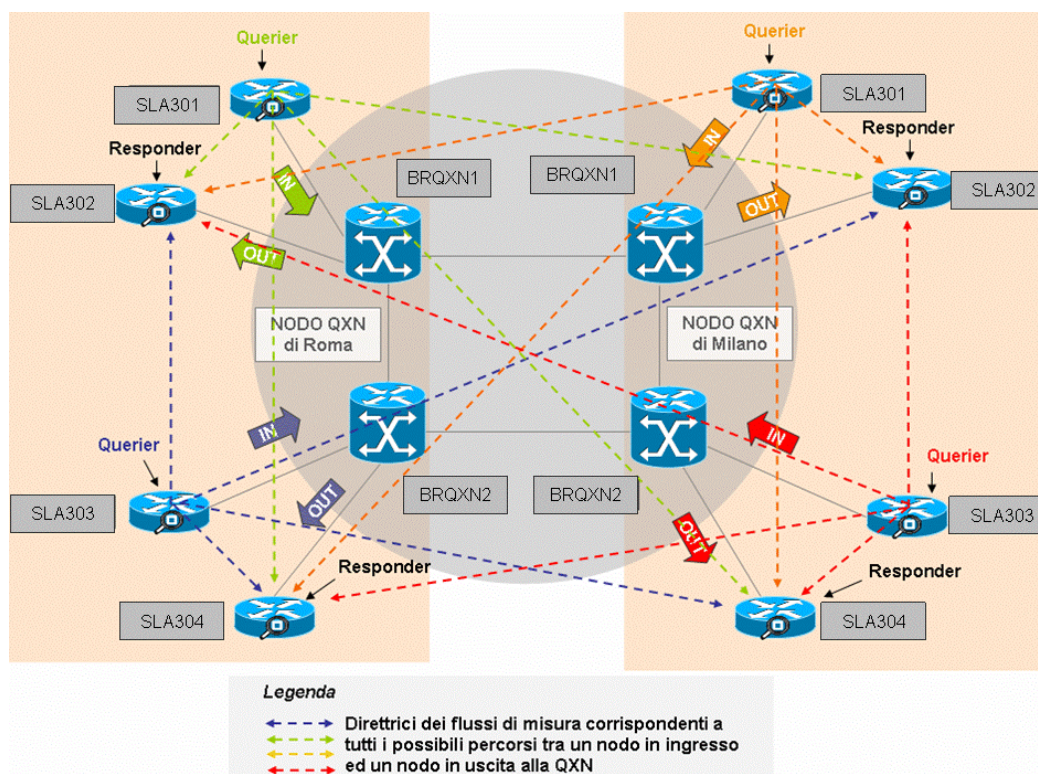





Figura 1 – Architettura di riferimento del sistema di monitoraggio per il servizio di tipo OPA

Al fine di garantire un monitoraggio completo del servizio OPA anche in fase di migrazione da SPC1 alla nuova convenzione SPC2, sono stati previsti degli ulteriori flussi di misura fra ciascuno dei querier QXN verso ciascuno dei responder già presenti nella QXN1 per un totale di 16 ulteriori direttrici di traffico. Tali flussi verranno tuttavia utilizzati esclusivamente a fini di monitoraggio delle interconnessioni QXN1-QXN e non al fine della rendicontazione e del calcolo delle penali.

3.2 SERVIZIO OPO

Per i servizi OPO (BRqxn con funzionalità di switching), i flussi di misura sono confinati tra le due sonde attestare al medesimo BRqxn e attraversano quest'ultimo solo a livello 2. Ogni collegamento tra due sonde

	 SISTEMI INFORMATIVI <small>An IBM Company</small>	
INTERNO	ICSPC-QXN-Specificacontrollo-1.2.Docx	

è realizzato mediante una subnet terminata a livello IP dalle sonde medesime. In tale scenario, il BRqxn offre solo le porte e la VLAN di interconnessione per le sonde.

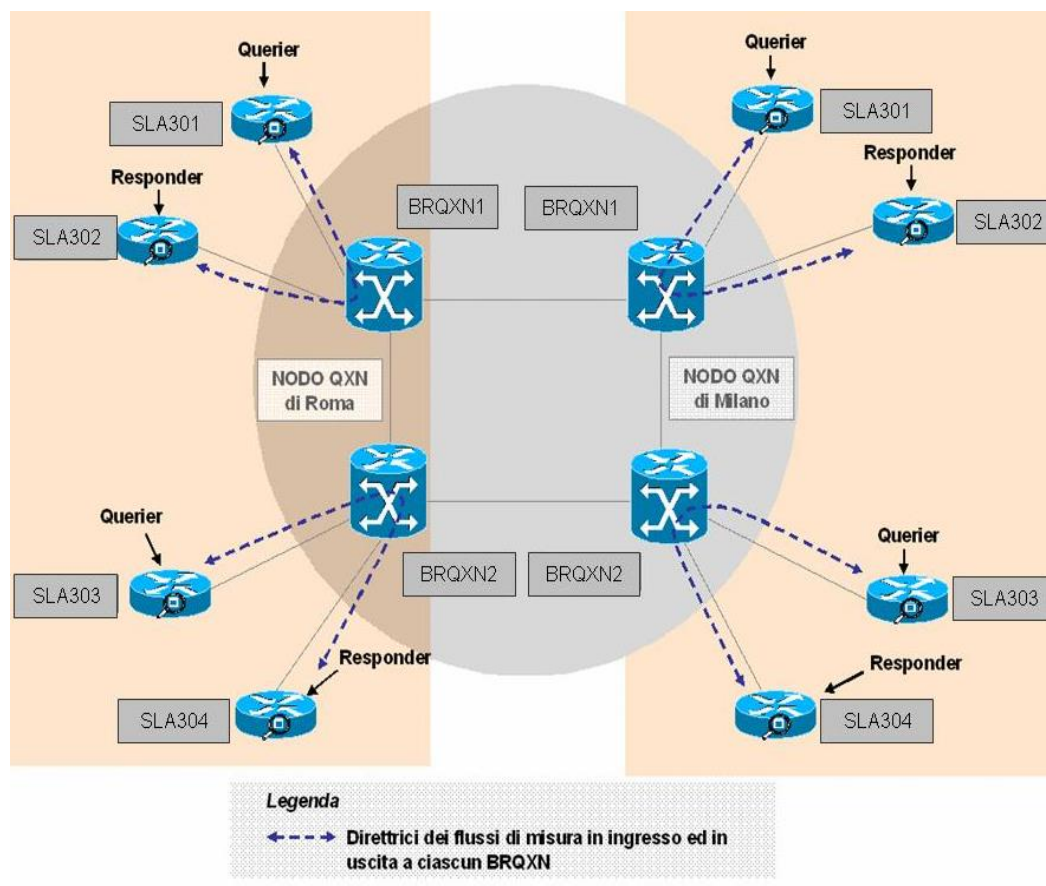


Figura 2 - Architettura di riferimento del sistema di monitoraggio per il servizio di tipo OPO

3.3 SPECIFICHE DEI FLUSSI DI MISURA

Il flusso di misura utilizzato per la verifica della prestazione della QXN è composto da pacchetti IPv4 marcati con DSCP pari a zero (Best Effort). I pacchetti hanno una dimensione pari a 200 Byte (a livello IP) e sono trasmessi in un numero pari a 10 ogni minuto e con 200 msec come intervallo di tempo tra la trasmissione di due pacchetti consecutivi.

3.4 ACQUISIZIONE DELLE MISURE

I risultati delle misure raccolte dalle sonde IP SLA vengono esposti attraverso MIB SNMP dai Querier. Il sistema di monitoraggio TNMS accede periodicamente (ogni minuto) in lettura alle MIB e raccoglie i risultati in un DB dopo avere eseguito una prima elaborazione sui dati.

Tale elaborazione è necessaria al fine di:

1. calcolare i parametri non esportati direttamente nelle MIB ma comunque derivabili da essi
2. gestire la presenza di misure incomplete o errori in fase di acquisizione.
3. eseguire un primo consolidamento su intervalli di 5 minuti.

FASTWEB un passo avanti	SISTEMI INFORMATIVI An IBM Company	LEONARDO SISTEMI PER LA SICUREZZA E LE INFORMAZIONI
INTERNO	ICSPC-QXN-Specificacontrollo-1.2.Docx	

4 Definizioni e metodi di calcolo delle metriche

Di seguito vengono descritte le modalità con le quali le sonde calcolano le misure di RTD, PL e PDV ed espongono i risultati via MIB.

Tutte le misure si basano sull'utilizzo di un unico tipo di probe IP SLA, l'UDPJitter in grado di stimare tutti i parametri di interesse con la medesima sequenza di pacchetti di misura.

4.1 ROUND TRIP DELAY

Il round trip delay è calcolato dal querier sulla base dei sequence number e dei timestamp di trasmissione inseriti all'interno dei pacchetti di misura del probe UDPJitter.

Nella figura di seguito si riportano le formule utilizzate per il calcolo dei ritardi di trasferimento Round Trip Delay e One-Way Delay nelle direzioni dal *Querier* al *Responder* e dal *Responder* al *Querier* sulla base dei timestamp raccolti dalla sonda IP SLA per ciascuna misura.

Ai fini del presente documento risulta di interesse solo la misura di RTD.

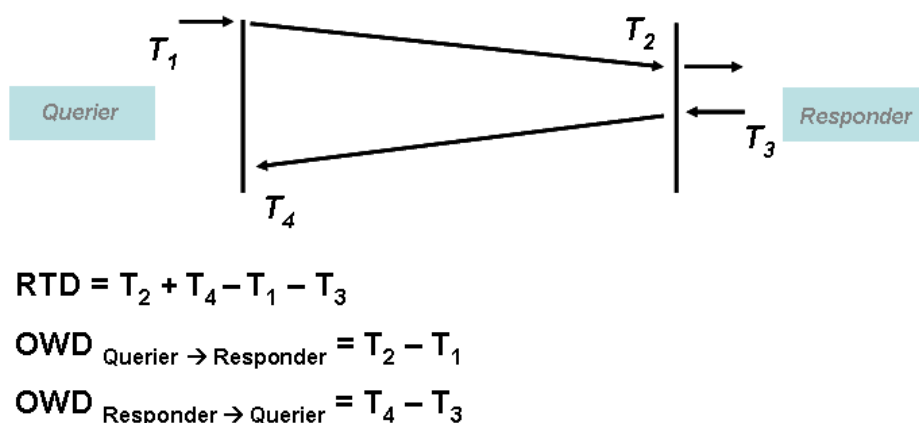


Figura 3 – Metodo di calcolo impiegato nella misurazione del RTD

Al termine di ogni istanza del probe (corrispondente all'esecuzione di una sequenza di misure) il *Querier* aggiorna le seguenti MIB SNMP utili ai fini del calcolo del RTD.




Variabile MIB	Descrizione
RTTSum	La somma dei valori di Round Trip Delay misurati
NumOfRTT	Il numero dei campioni di misura di Round Trip Delay computati con successo

Tabella 1 – Elenco variabili MIB utili al calcolo del RTD

Qualora durante l'esecuzione della misura avvenga una perdita di pacchetti, il numero di campioni considerato per il calcolo della media per la valorizzazione del campione di misura è modificato in accordo con la perdita di pacchetti rilevata. Tale informazione viene mantenuta dalla sonda nella MIB NumOfRTT che sarà quindi pari o inferiore al numero di pacchetti effettivamente inviati dal Querier (vedi esempio al par. 4.2.1). In assenza di packet loss la variabile NumOfRTT sarà pari a 10.

Il valore di RTD sarà derivabile con la seguente formula:

$$RTD = \frac{RTTsum}{NumOfRTT}$$

 un passo avanti	 An IBM Company	 SISTEMI PER LA SICUREZZA E LE INFORMAZIONI
INTERNO	ICSPC-QXN-Specificacontrollo-1.2.Docx	

che corrisponde alla media aritmetica delle misure di RTD eseguite con successo dall'istanza IP SLA.

4.2 PACKET LOSS

La misura del parametro Packet Loss è ottenuta dall'elaborazione dei sequence number inseriti a tale scopo nei pacchetti di misura da querier e responder; nota la sequenza d'invio è possibile calcolare al momento della ricezione il numero dei pacchetti persi nella tratta sotto osservazione.

La lettura del valore del numero di pacchetti persi per entrambe le direzioni di comunicazione sul *Querier* che espone via SNMP le informazioni descritte in Tabella 2.

Parametro	Descrizione
PacketLossSD	Il numero di pacchetti persi nel tragitto dal Querier al Responder
PacketLossDS	Il numero di pacchetti persi nel tragitto dal Responder al Querier
PacketMIA	Il numero di pacchetti persi per i quali non è possibile stabilire se la perdita sia avvenuta nella direzione dal Querier al Responder o nella direzione opposta
PacketLateArrival	Il numero di pacchetti che arrivano dopo il timeout
PacketOutOfSequence	Il numero di pacchetti che sono ritornati fuori sequenza
NumOfRTT	Il numero dei campioni di misura di Round Trip Delay computati con successo.

Tabella 2. MIB utili ai fini del calcolo del RTD.

Il time-out per la valorizzazione del parametro *PacketLateArrival* è configurabile e pari a 5 secondi per default.

Il sistema di misura consente di individuare anche la direzione dove si è verificata la perdita del pacchetto, grazie all'utilizzo di due Sequence Number distinti nelle due direzioni di trasmissione, a patto che la perdita del pacchetto, o di un treno consecutivo di pacchetti, non includa l'ultimo pacchetto della sessione di misura. In questo caso non è possibile discriminare se la perdita del pacchetto sia avvenuta nella direzione *Querier-Responder* o viceversa, e il pacchetto perso viene classificato come MIA (Missing In Action, alternativamente definiti come Tail-Drop).

A partire dai valori delle MIB è possibile calcolare il numero totale di pacchetti persi lungo la tratta (querier-responder-querier) ed il numero totale di pacchetti trasmessi dal *Querier* (*TotalPacketSent*) in accordo con le seguenti formule:

$$LostPackets = PacketMIA + PacketLossDS + PacketLossSD$$

$$TotalPacketsSent = NumOfRTT + PacketOutOfSequence + PacketLateArrival + LostPackets$$

4.2.1 ESEMPIO IN CASO DI PERDITA DI PACCHETTI

Nell'esempio rappresentato nella figura seguente, la sonda invia 5 pacchetti ma vengono persi due pacchetti relativi a due differenti misure di RTT.

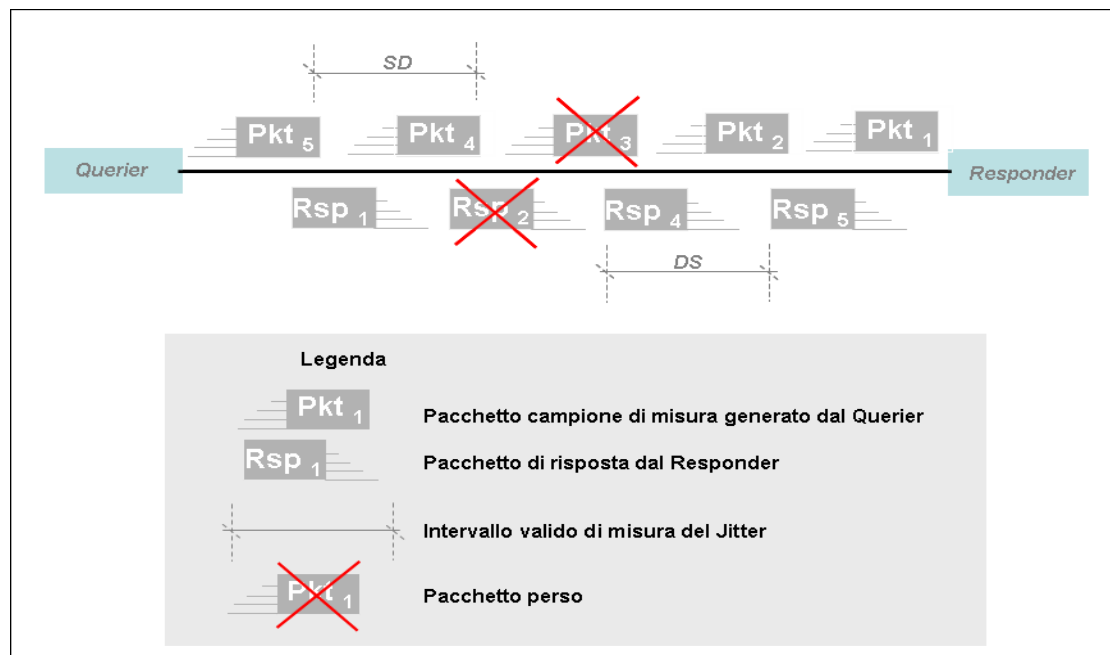


Figura 4 – Effetto della Packet Loss sul calcolo dei parametri prestazionali

In questo scenario si otterrebbe:

$$NumOfRTT = 3$$

$$PacketLossSD = 1$$

$$PacketLossDS = 1$$

$$PacketMIA = 0$$

$$PacketOutOfSequence = 0$$

$$PacketLateArrival = 0$$

Il numero totale dei pacchetti persi sarebbe quindi:

$$LostPackets = PacketMIA + PacketLossDS + PacketLossSD = 2$$

e di conseguenza, il numero di pacchetti totali inviati dal querier sarebbe correttamente calcolato come:

$$TotalPacketsSent = NumOfRTT + PacketOutOfSequence + PacketLateArrival + LostPackets = 5$$

4.3 PACKET DELAY VARIATION




La stima del PDV si basa sull'invio di una sequenza di pacchetti ad intervalli regolari e configurabili. Sulla base della conoscenza a priori dell'intervallo di invio e dell'osservazione della variazione dei tempi di arrivo, il querier è in grado di stimare il PDV introdotto dalla rete sulla tratta querier-responder-querier.

La sonda esporta il valore medio di PDV (Jitter) calcolato nell'intervallo di osservazione attraverso la seguente MIB:

Parametro	Descrizione
avgJitter	Media dei valori di Jitter positivi e negativi osservati sulla tratta querier-responder-querier in millisecondi.




Il valore è a sua volta internamente calcolato dall'apparato come:

$$avgJitter = \left\lfloor \frac{jitterSum}{jitterNum} \right\rfloor$$

		
INTERNO	ICSPC-QXN-Specificacontrollo-1.2.Docx	

dove jitterSum è la somma dei valori di jitter positivi e negativi (in valore assoluto) osservati dalla sonda e jitterNum è il numero di campioni di jitter misurati con successo nelle tratte querier-responder e responder-querier. Il valore jitterNum non è esposto nelle MIB dalle sonde.

In caso non sia stato possibile eseguire alcuna misura di Jitter, la variabile avgJitter sarà pari a zero.

 un passo avanti	 An IBM Company	 SISTEMI PER LA SICUREZZA E LE INFORMAZIONI
INTERNO	ICSPC-QXN-Specificacontrollo-1.2.Docx	

5 Acquisizione ed elaborazione dei dati sul TNMS

In questo capitolo vengono descritte le modalità di estrazione dei dati dalle sonde Cisco IP SLA da parte del sistema di monitoraggio TNMS e le successive elaborazioni applicate dallo stesso ai dati prima dell'esportazione verso il sistema di rendicontazione e calcolo delle penali.

5.1 MODALITÀ DI ESTRAZIONE DELLE VARIABILI MIB

L'acquisizione delle metriche è eseguita mediante operazioni get SNMP delle variabili MIB esposte dai *querier*. Le MIB di interesse sono di tipo Gauge32 ed il sistema ne legge il valore con una frequenza pari a 1 minuto. I valori sono successivamente elaborati al fine di ricavare i valori di RTD, PL e PDV con le formule descritte al Cap. 4.

I dati letti sono considerati non validi nei seguenti casi:

- La sonda non è riuscita a effettuare la misura (es. responder down).
- Non è stato possibile recuperare le informazioni attraverso le get SNMP.

Qualora i dati per un certo intervallo temporale e direttrice di traffico non siano disponibili a causa di errori nell'esecuzione della misura o nell'acquisizione dei risultati, i dati risulteranno indefiniti e non considerati ai fini della successiva aggregazione e di conseguenza ai fini della rendicontazione e del calcolo delle penali.

Di seguito vengono descritte le ulteriori elaborazioni applicate ai dati acquisiti al fine di scartare misure non valide ed agevolarne il successivo consolidamento.

5.1.1 TASSO DI PERDITA DEI PACCHETTI (PACKET LOSS)

Per calcolare correttamente la percentuale di pacchetti persi che viene considerata ai fini della misura del PL è necessario fare riferimento alle variabili *TotalPacketSent* e *LostPacket* come definite al par. 4.1.

Tali valori permettono di calcolare il numero di pacchetti spediti dall'apparato in caso di risposta di almeno uno dei pacchetti presenti nel treno. Nel caso siano persi tutti i pacchetti di un treno, allora *TotalPacketSent* risulterà pari a zero. Per gestire questa situazione e agevolare il calcolo del PL sull'intervallo aggregato di 5 minuti (come descritto al par. 5.1.4) vengono calcolate per ogni campagna di misura le seguenti variabili intermedie a partire dalle MIB:

$$LP = \begin{cases} \text{LostPackets} & \text{TotalPacketsSent} > 0 \\ N & \text{TotalPacketsSent} = 0 \end{cases}$$

$$TPS = \begin{cases} \text{TotalPacketsSent} & \text{TotalPacketsSent} > 0 \\ N & \text{TotalPacketsSent} = 0 \end{cases}$$




Dove N è pari al numero di pacchetti del treno di misura che nella configurazione prevista è pari a 10.

Il rapporto LP/TPS rappresenterà di conseguenza il PL anche nel caso di perdita di tutto il treno di pacchetti (LP/TPS = N/N = 1) permettendo quindi un trattamento omogeneo dei dati in fase di consolidamento.

5.1.2 ROUND TRIP DELAY

Nel caso del RTD la condizione per cui i dati raccolti siano utili ai fini del RTD è che la variabile *NumOfRTT* sia maggiore di zero, ovvero che la sonda abbia eseguito almeno una misura.

$$RTD = \begin{cases} \frac{RTTsum}{NumOfRTT} & NumOfRTT > 0 \\ \text{null} & NumOfRTT = 0 \end{cases}$$

 un passo avanti	 An IBM Company	 SISTEMI PER LA SICUREZZA E LE INFORMAZIONI
INTERNO	ICSPC-QXN-Specificacontrollo-1.2.Docx	

5.1.3 PACKET DELAY VARIATION

La misura di PDV è considerata non nulla se vale la seguente condizione:

$$PDV = \begin{cases} AvgJitter & AvgJitter > 0 \text{ or } NumOfRTT \geq \frac{N}{2} + 1 \\ null & AvgJitter = 0 \text{ and } NumOfRTT < \frac{N}{2} + 1 \end{cases}$$

Dove N è pari al numero di pacchetti del treno di misura che nella configurazione prevista è pari a 10.

Tali formule si basano sull'osservazione che devono essere ricevuti almeno due pacchetti consecutivi affinché sia possibile per il querier stimare un valore di Jitter. La condizione $NumOfRTT \geq \frac{N}{2} + 1$ è sufficiente quindi (pur non essendo necessaria) per garantire la validità della misura nei casi in cui avgJitter sia pari a zero.

5.1.4 CONSOLIDAMENTO DEI DATI

Tutte le misure non nulle raccolte dalle sonde con frequenza di 1 minuto, vengono consolidate in intervalli di 5 minuti per l'archiviazione locale sul TNMS applicando le seguenti funzioni per i diversi KPI:

$$PL_{5m} = \frac{\sum_i LP_i}{\sum_i TPS_i} * 100$$

$$RTD_{5m} = avg(RTD_i)$$

$$PDV_{5m} = avg(PDV_i)$$

Dove avg rappresenta la media aritmetica.

Per i KPI PL, RTD e PDV nel caso sia disponibile almeno una misura nell'intervallo di riferimento quest'ultima sarà utilizzata ai fini della rendicontazione.

Nel caso di indisponibilità totale delle misure relative al Servizio di Interconnessione OPA in un intervallo di riferimento, causate da un disservizio del TNMS – rilevabile da Nagios - e/o da un fault delle sonde querier e responder – rilevabile da TNMS, il SEDE aprirà in proattività un TT sul Cliente AGID (in modo da corrispondere l'eventuale penale a tutti i soggetti interconnessi) per disservizio non bloccante sull'interconnessione OPA di Roma e Milano.

In maniera del tutto analoga nel caso si rilevi un'assenza completa in un intervallo d'osservazione delle misure relative al servizio di Interconnessione OPO, il SEDE aprirà un TT in proattività sul cliente AGID per disservizio non bloccante sul servizio di interconnessione OPO.

In entrambi i casi il tempo di ripristino (SLA 2.2.7) sarà oggetto di misurazione ai fini del calcolo delle eventuali penali.




5.2 MODALITÀ DI ESPORTAZIONE DEI DATI AL SIRF

Le informazioni che saranno esportate al SIRF conterranno: il timestamp della misura, il valore di PL, il valore di RTD, il valore di PDV.




Il TNMS renderà disponibili 12 misurazioni l'ora nell'arco di una giornata a partire dalle ore 0.00 fino alle ore 23.55; per un totale di 12*24 misurazioni giornaliere, pari a 288, per ciascuna delle direttrici di traffico previste. Le misure saranno consolidate come descritto al paragrafo 5.1.4; ad esempio la misura con timestamp 0.00 rappresenterà la media dei campioni da 00:00 a 00:04 e così via, fino alla misura con timestamp 23:55 che sarà il risultato dei campioni da 23:55 a 23:59.

Nel caso di misurazioni non valide, sarà valorizzata una riga di campi vuoti al fine di mantenere sempre costante il numero di campioni esportati.




Il file utilizzato per l'esportazione è in formato csv, si riporta di seguito un estratto a titolo di esempio:

 un passo avanti	 An IBM Company	 SISTEMI PER LA SICUREZZA E LE INFORMAZIONI
INTERNO	ICSPC-QXN-Specificacontrollo-1.2.Docx	

Timestamp	PL	RTD	PDV
2016-09-12 00:00:00.000	0	5	2
.	.	.	.
.	.	.	.
2016-09-12 01:05:00.000	0	5	1
2016-09-12 01:10:00.000	0	6	2
2016-09-12 01:15:00.000	0	5	1
2016-09-12 01:20:00.000	NOVALUE	NOVALUE	NOVALUE
2016-09-12 01:25:00.000	NOVALUE	NOVALUE	NOVALUE
.	.	.	.
.	.	.	.
2016-09-12 23:55:00.000	0	5	1

		
INTERNO	ICSPC-QXN-Specificacontrollo-1.2.Docx	

Fine del Documento

 un passo avanti	 An IBM Company	 SISTEMI PER LA SICUREZZA E LE INFORMAZIONI
INTERNO	ICSPC-QXN-Regole Tecniche Per Interconnessione A QXN-1.4.Docx	

Regole Tecniche per interconnessione a QXN Infrastrutture Condivise SPC




Regole Tecniche per interconnessione a QXN

IDENTIFICATIVO

ICSPC-QXN-Regole Tecniche per interconnessione a QXN-1.4.docx




STORIA DEL DOCUMENTO

Rev.	Data	Redatto	Approvato	Descrizione modifica
1.0	15/10/2016	A. Marcandalli L. Spaghetti T. Petrino	M. Mascagna	Prima emissione
1.1	07/12/2016	A. Marcandalli L. Spaghetti T. Petrino	M. Mascagna	Modifiche minori
1.2	20/01/2017	A. Marcandalli L. Spaghetti T. Petrino	M. Mascagna	Modifiche minori
1.3	04/05/2017	A. Marcandalli L. Spaghetti	M. Mascagna	Par. 2.2: modificata profondità massima AS-Path da 2 a 3
1.4	25/07/2018	A. Marcandalli	M. Mascagna	Introdotta scenario di attestazione QCN con doppio operatore.

		
INTERNO	ICSPC-QXN-Regole Tecniche Per Interconnessione A QXN-1.4.Docx	




ALLEGATI

Nome	Descrizione

		
INTERNO	ICSPC-QXN-Regole Tecniche Per Interconnessione A QXN-1.4.Docx	

Sommario

1	GENERALITÀ	4
1.1	SCOPO DEL DOCUMENTO	4
1.2	APPLICABILITÀ	4
1.3	RIFERIMENTI	4
1.4	DEFINIZIONI ED ACRONIMI.....	4
2	REGOLE TECNICHE PER L'INTERCONNESSIONE ALLA QXN	6
2.1	PREMESSA	6
2.2	PROFILO DI SERVIZIO "INTERCONNESSIONE OPA"	6
2.3	PROFILO DI SERVIZIO "INTERCONNESSIONE OPO"	9
2.4	MODALITÀ DI CONNESSIONE ALLA QXN.....	10
2.5	INTERCONNESSIONE DELLE QUALIFIED COMMUNITY NETWORK.....	11
3	VERIFICHE TECNICHE DI INTERCONNESSIONE AL QXN	11
4	SERVICE LEVEL AGREEMENT	12
5	ANNESSO A: SPECIFICHE TECNICHE DEL SERVIZIO QXN	13
5.1	CARATTERISTICHE DEL SERVIZIO	13
5.2	INFRASTRUTTURA DELLA RETE QXN	13
5.3	INTERCONNESSIONE OPA TRAMITE RETE QXN (PROFILO DI SERVIZIO "INTERCONNESSIONE OPA")	14
5.4	INTERCONNESSIONE OPO TRAMITE RETE QXN (PROFILO DI SERVIZIO "INTERCONNESSIONE OPO")	16
5.5	SERVIZIO DI EROGAZIONE DEL TEMPO UFFICIALE DI RETE (NTP)	18
5.6	SERVIZIO DNS	18
5.7	ASSISTENZA TECNICA SUI SERVIZI QXN	18
6	ANNESSO B: REGOLE TECNICHE PER L'INTERCONNESSIONE ALLA QXN CON PIU' FORNITORI SPC	19
6.1	PREMESSA	19
6.2	VINCOLI E PRECONDIZIONI	19
6.3	REGOLE DI INTERCONNESSIONE	19
6.4	LINEE GUIDA DI IMPLEMENTAZIONE PER LA QCN	20
6.4.1	Policy per la manipolazione del traffico in downstream	20
6.4.2	Policy per la manipolazione del traffico in upstream.....	21
6.5	INTERFACCIAMENTO TRA FSPC E QCN	22

 un passo avanti	 An IBM Company	 SISTEMI PER LA SICUREZZA E LE INFORMAZIONI
INTERNO	ICSPC-QXN-Regole Tecniche Per Interconnessione A QXN-1.4.Docx	

1 GENERALITÀ

1.1 SCOPO DEL DOCUMENTO

Il presente documento ha l'obiettivo di dettagliare le regole tecniche che devono essere osservate da tutti i Soggetti che intendano connettersi alla rete QXN per usufruire del profilo di servizio "Interconnessione OPA" e da i soli Soggetti della Gara Multifornitore per i Servizi di Connettività SPC [3] che intendano avvalersi del profilo di servizio "Interconnessione OPO"

1.2 APPLICABILITÀ




Il documento si applica al progetto IC-SPC, in esecuzione del Contratto[1] stipulato tra AgID e l'RTI Fastweb spa-Finmeccanica spa-Sistemi Informativi srl.

1.3 RIFERIMENTI




Codice	Titolo
[1]	Contratto per l'Affidamento della progettazione, realizzazione, fornitura, manutenzione e gestione delle Infrastrutture Condivise del Sistema Pubblico di Connettività (IC-SPC) del 5/8/2016 [CIG 6049538CAC]
[2]	Gara a procedura aperta per l'affidamento della progettazione, realizzazione, fornitura, manutenzione e gestione delle Infrastrutture Condivise del Sistema Pubblico di Connettività (IC-SPC) – ID1366 (di seguito indicata per brevità come <i>Gara IC-SPC</i>)
[3]	Procedura ristretta per l'affidamento dei servizi di connettività nell'ambito del Sistema Pubblico di Connettività (SPC) - ID 1367 (Gara Multifornitore per i servizi di connettività SPC2 – di seguito indicata per brevità come <i>Gara MF SPC2</i>)
[4]	All. D al contratto [1] - Schema di Contratto Attuativo per l'adesione ai servizi IC-SPC

1.4 DEFINIZIONI ED ACRONIMI

Definizione/Acronimo	Descrizione
ASN	Autonomous System Number
QCN	Qualified Community Network
QXN	Qualified Exchange Network
QXN1	Infrastruttura QXN collaudata nel 2007 nell'ambito della Gara Multifornitore SPC 2005.
IQXN	Servizio di Interconnessione erogati dalla QXN
Fornitore IQXN	Soggetto, aggiudicatario della Gara [2], che eroga i servizi IQXN
FSPC	Fornitore SPC

		
INTERNO	ICSPC-QXN-Regole Tecniche Per Interconnessione A QXN-1.4.Docx	

Definizione/Acronimo	Descrizione
Utente IQXN	Soggetto titolato che utilizza i servizi IQXN
OPA	Offerta per le Amministrazioni
OPO	Offerta per gli Operatori

 un passo avanti	 SISTEMI INFORMATIVI An IBM Company	 LEONARDO SISTEMI PER LA SICUREZZA E LE INFORMAZIONI
INTERNO	ICSPC-QXN-Regole Tecniche Per Interconnessione A QXN-1.4.Docx	

2 REGOLE TECNICHE PER L'INTERCONNESSIONE ALLA QXN

2.1 PREMESSA

Nel presente documento vengono descritte le regole tecniche che devono essere osservate dal Soggetto (qui definito come Utente IQXN) che intenda connettersi alla rete QXN per usufruire dei profili di servizio "Interconnessione OPA" ed "Interconnessione OPO".

La infrastruttura QXN ed i servizi da essa erogati sono forniti dal RTI Fastweb-Finmeccanica-Sistemi Informativi (di seguito indicato come "Fornitore IQXN") che è risultato aggiudicatario della Gara IC-SPC [2].

Nell'Annesso A al presente documento viene fornito un quadro complessivo dell'infrastruttura QXN, dei servizi da essa erogati.

Vengono, infine, fornite informazioni utili ai fini di una semplice gestione della connessione alla rete QXN.

Gli apparati di rete dei Soggetti che si interconnettono alla rete QXN devono supportare le funzionalità descritte all'interno del presente documento.

Tali apparati sono convenzionalmente denominati Border Router OPA (BRopa), qualora coinvolti nel Profilo di Servizio "Interconnessione QXN OPA", e Border Router OPO (BRopo) qualora coinvolti nel Profilo di Servizio "Interconnessione QXN OPO".

Il Fornitore IQXN e gli Utenti IQXN sono rispettivamente responsabili della manutenzione di ogni componente del proprio dominio di competenza e sono abilitati ad operare esclusivamente su tali componenti.

In particolare, il dominio di competenza del Fornitore IQXN è rappresentato:

- dagli apparati dedicati all'erogazione del Servizio IQXN (router, switch, server, firewall, etc.) e dai rack che li ospitano;
- dalle interconnessioni locali tra tali apparati;
- dalle interconnessioni geografiche tra i due nodi della QXN di Roma e Milano;
- dalle infrastrutture (rack) predisposte per il servizio di housing in cui vengono alloggiate le apparecchiature degli Utenti IQXN.

Il confine del dominio di competenza del Fornitore IQXN è individuato nel cassetto ottico e/o dal patch panel UTP installato e mantenuto dal Fornitore IQXN stesso all'interno di ciascun rack coinvolto nel servizio di housing offerto all'Utente IQXN.




Relativamente al profilo di servizio "Interconnessione OPA", il Fornitore IQXN deve comunicare agli Utenti IQXN gli spazi di indirizzamento IP gestiti ed i relativi AS Number, aggiornando contestualmente l'Area informativa QXN.

Per poter fruire dei Servizi di Interconnessione QXN, l'Utente IQXN deve aver aderito alle norme tecniche del SPC, deve essere aggiudicatario o assegnatario della gara MF SPC2 [3], oppure aggiudicatario della gara S-RIPA oppure essere soggetto abilitato da AgID alla fruizione di servizi nell'ambito Infranet.

Deve, inoltre, aver stipulato un apposito Contratto Attuativo [4] con il Fornitore IQXN per la sottoscrizione dei profili di servizio "Interconnessione OPA" e/o "Interconnessione OPO"




2.2 PROFILO DI SERVIZIO "INTERCONNESSIONE OPA"

- a) L'Utente IQXN deve interconnettersi ad un nodo QXN, di Roma o di Milano, mediante al più una coppia di apparati (denominati Border Router – BR) internessi agli apparati QXN (denominati BRqxn) mediante la sottoscrizione di un Profilo di Servizio di "Interconnessione OPA", come definito

		
INTERNO	ICSPC-QXN-Regole Tecniche Per Interconnessione A QXN-1.4.Docx	

in Annesso A, stipulando un apposito Contratto Attuativo con il Fornitore IQXN. Per i fornitori aggiudicatari o assegnatari della Gara MF SPC2 [3] è obbligatoria l'interconnessione a ciascun nodo QXN mediante l'utilizzo di una coppia di apparati BR per nodo;

- b) per ottenere una maggiore affidabilità complessiva, l'Utente IQXN può richiedere che l'interconnessione OPA avvenga sui due nodi QXN di Roma e Milano, ridondando geograficamente l'accesso. A tale scopo, l'Utente IQXN deve sottoscrivere un ulteriore profilo di Servizio di "Interconnessione OPA" sull'altro nodo QXN di Roma o Milano. Questa modalità di interconnessione è obbligatoria per i fornitori aggiudicatari e assegnatari della Gara MF SPC2 [3].
- c) gli apparati BR dell'Utente IQXN devono essere collocati in housing presso i nodi QXN, all'interno delle infrastrutture (rack) appositamente predisposte ed individuate dal Fornitore IQXN;
- d) l'installazione, gestione e manutenzione degli apparati BR è a cura e spese dell'Utente IQXN;
- e) la realizzazione, gestione e manutenzione dei link necessari al collegamento dei BR dell'Utente IQXN alla propria rete sono a cura e spese dell'Utente IQXN, in coerenza con le regole previste dal NAP ospitante;
- f) la realizzazione, gestione e manutenzione dei cablaggi di collegamento tra i BR dell'Utente IQXN ed il cassetto ottico e/o patch panel UTP di sezionamento, predisposti e mantenuti da Fornitore IQXN all'interno del rack riservato all'Utente IQXN, sono a cura e spese dell'Utente IQXN;
- g) la realizzazione, gestione e manutenzione dei cablaggi di collegamento tra i BRqxN ed il cassetto ottico e/o patch panel UTP di sezionamento, predisposti e mantenuti da Fornitore IQXN all'interno del rack riservato all'Utente IQXN, sono a cura e spese di Fornitore IQXN;
- h) i BR dell'Utente IQXN devono operare a livello di routing (Livello 3 OSI) e comunicare con i BRqxN mediante sessioni E-BGP v.4. Non sono ammesse configurazioni di altri protocolli di routing aggiuntivi sull'interfaccia di interconnessione OPA;
- i) Ciascun soggetto interconnesso alla rete QXN annuncerà ai BRqxN il proprio AS number e lo spazio di indirizzamento (riservato all'interno del suo AS) abilitato a scambiare traffico IP per il tramite della QXN. All'interno dell'infrastruttura QXN il suddetto traffico deve essere bilanciato sui BRqxN che attraversa;
- j) l'Utente IQXN, attraverso i propri BR, può:
 - annunciare ai BRqxN il proprio ASN pubblico ed esclusivamente i prefissi IP pubblici, assegnatigli dal RIPE o altro Registro equivalente, che vengono utilizzati per l'erogazione dei servizi di connettività in ambito Infranet alle PA connesse alla propria rete;
 - annunciare ai BRqxN, utilizzando il proprio ASN pubblico come AS di transito, gli ASN pubblici ed i prefissi IP pubblici appartenenti ad altri Soggetti, afferenti al SPC ma non interconnessi direttamente alla QXN, i quali impieghino tali ASN e tali prefissi IP per erogare e/o utilizzare servizi di connettività Infranet. È responsabilità dell'Utente IQXN verificare la correttezza degli annunci BGP (prefissi e AS pubblici) dei Soggetti ad esso interconnessi prima che l'Utente IQXN stesso li annunci su QXN;
 - annunciare ai BRqxN utilizzando il proprio ASN pubblico i prefissi IP della rete STESTA assegnati alle amministrazioni di propria competenza;
- k) allo scopo di assicurare il mantenimento dei livelli di sicurezza previsti dal SPC per la Infranet (rete trusted), l'Utente IQXN deve garantire che il traffico scambiato con la QXN non sia proveniente da Internet o da altre reti non trusted;
- l) Per garantire la sicurezza ed autenticità degli annunci scambiati con i BRqxN, i BR dell'Utente IQXN devono attivare la funzione di hash MD5 sul protocollo E-BGP;
- m) Sui BRqx dei Soggetti interconnessi verrà attivata, se disponibile, la funzione di protezione dei peering eBGP basata sul TTL (GTSM);
- n) i prefissi IP di cui al punto j) devono essere annunciati dai BR dell'Utente IQXN verso i BRqxN:
 - utilizzando AS di tipo pubblico (non sono ammessi AS privati);

 un passo avanti	 An IBM Company	 SISTEMI PER LA SICUREZZA E LE INFORMAZIONI
INTERNO	ICSPC-QXN-Regole Tecniche Per Interconnessione A QXN-1.4.Docx	

- assicurando che la profondità dell'AS-path degli annunci visibili sulla QXN non sia superiore a 3;
 - garantendo il massimo grado di aggregazione e, comunque, con netmask uguale o inferiore a 24 bit (subnet /24 o meno specifiche) per indirizzamenti IPv4 e 48 bit (subnet /48 o meno specifiche) per indirizzamenti IPv6. Tale vincolo non si applica ai prefissi relativi alla rete S-TESTA che potranno essere annunciati con mask di lunghezza superiore;
- o) l'Utente IQXN, qualora utilizzi uno o più prefissi IP pubblici per l'erogazione dei servizi di connettività sia in ambito Infranet che Internet, dovrà farsi carico di annunciare la/le relativa/e subnet in modo più specifico su Infranet rispetto alla/alle medesime annunciata/e su Internet. Tutto ciò è valido sia nel caso in cui l'Utente IQXN si attesti direttamente alla QXN, sia che faccia da transito per altri AS (v. par j);
- p) i prefissi di cui al punto j) precedente debbono essere annunciati utilizzando le seguenti communities BGP:
- **Community di tipo "decisionale"**: che determina la priorità dei collegamenti dell'Utente IQXN per dare indicazione del percorso preferenziale del traffico di una specifica PA attraverso il QXN. La community ha il seguente formato: <ASQXN>: LP, dove:
 - LP identifica il valore della Local Preference settata all'interno del QXN per l'annuncio specifico (LP = 130; LP = 120; LP = 110; LP=100). La priorità dell'annuncio è direttamente proporzionale al valore di LP assegnato;




Nel caso la Community non sia indicata, il relativo traffico viene scartato dai nodi QXN.

- q) Il traffico generato dai prefissi annunciati dall'Utente IQXN verso la QXN, di cui al punto j) precedente, deve essere inviato dai BR dell'Utente IQXN verso i BRqxn secondo le stesse priorità definite dalle Communities BGP ed in modo bilanciato per sessione (identificata dalla coppia IP sorgente-IP destinazione);
- r) ai fini della corretta gestione della QoS, l'Utente IQXN, prima di consegnare il traffico ai BRqxn, dovrà marcare i pacchetti relativi a ciascuna tipologia di traffico OPA per associarli alla rispettiva Classe di Servizio (CdS) utilizzando i seguenti valori di DSCP:

Classe di Servizio	DSCP PHB	DSCP Valore Decimale
Real Time	AF41	34
Mission Critical	AF3	26
Streaming	AF21	18
Multimedia	AF11	10
Best Effort	DF	0

I BRqxn, rimarcheranno a DSCP 0 eventuale traffico ricevuto con una marcatura DSCP non inclusa nella tabella precedente.




- s) L'Utente IQXN deve garantire che il traffico Infranet nativo OPA tra sedi di due PA attestata alla propria infrastruttura non transiti in alcun caso sugli apparati del QXN
- t) il DNS SPC dell'Utente IQXN devono essere collegati ai server DNS della QXN ed essere configurati in modo da annunciare automaticamente a questi ultimi il cambiamento di una zona di propria competenza tramite i meccanismi di DNS Notify (RFC1996).
- u) il DNS SPC dell'Utente IQXN deve essere configurato in modo tale da accettare le richieste di AXFR (Full Zone Transfer) e IXFR (Incremental Zone Transfer RFC1995), provenienti dai Name Server della QXN.

		
INTERNO	ICSPC-QXN-Regole Tecniche Per Interconnessione A QXN-1.4.Docx	

- v) Il DNS della QXN è configurato in modo tale da:
- ricevere le DNS Notify da parte del DNS SPC dell'Utente IQXN,
 - verificare che la notifica provenga da un DNS SPC autorizzato dell'Utente IQXN,
 - effettuare lo zone transfer delle zone delle Amministrazioni dai server DNS SPC dell'Utente IQXN, al fine di esporle in ambito SPC.
- w) il DNS della QXN dovrà replicare esclusivamente le "zone SPC" presenti sul DNS SPC di ciascun soggetto interconnesso. Tali zone potrebbero coincidere con le "zone pubbliche" qualora l'amministrazione non abbia necessità di distinguere tra "host pubblici" ed "host infranet"
- x) I meccanismi di Zone Transfer dai Name Server della PA verso i Name Server del DNS SPC dell'Utente IQXN sono di pertinenza di quest'ultimo. La distinzione tra "zone pubbliche" e "zone SPC" della PA, è invece di pertinenza di ciascuna PA e sotto la sua diretta responsabilità.

2.3 PROFILO DI SERVIZIO "INTERCONNESSIONE OPO"

- Questa modalità di interconnessione alla QXN è riservata esclusivamente a Soggetti che risultino fornitori aggiudicatari o assegnatari della Gara MF SPC2 [3];
- in accordo con l'offerta OPO, il Fornitore assegnatario della Gara MF SPC2 [3] ed il Fornitore aggiudicatario della Gara MF SPC2 [3] che abbiano sottoscritto tra loro un contratto esecutivo OPO, devono prevedere l'interconnessione con la rete QXN mediante apparati dedicati (denominati BRopo) o, in alternativa, utilizzando gli stessi apparati BRqx già previsti per la connettività OPA. Ciò allo scopo di consentire lo scambio del traffico tra la rete del *Fornitore aggiudicatario*, che eroga i servizi in modalità OPO (di seguito indicato come **Utente IQXN- Fornitore OPO**), ed il *Fornitore assegnatario* che usufruisce di tali servizi (di seguito indicato come **Utente IQXN- Cliente OPO**). Per ciascun contratto Esecutivo OPO stipulato tra due Fornitori (aggiudicatario ed assegnatario), l'Utente IQXN-Fornitore OPO e l'Utente IQXN-Cliente OPO devono sottoscrivere, ciascuno per proprio conto, due Profili di Servizio di "Interconnessione OPO", uno per il nodo QXN di Roma, l'altro per il nodo QXN di Milano;
- l'Utente IQXN Fornitore OPO deve interconnettersi ad entrambi i nodi QXN di Roma e di Milano mediante una coppia di apparati dedicati (Border Router OPO – BRopo) in ciascun nodo;
- l'utente IQXN Cliente OPO deve interconnettersi ad entrambi i nodi QXN di Roma e di Milano mediante almeno un apparato dedicato (Border Router OPO – BRopo) in ciascun nodo;
- La funzionalità di BRopo può essere implementata dall'Utente IQXN, a sua discrezione, sugli stessi apparati BR già utilizzati per l'interconnessione al QXN per il profilo di Servizio Interconnessione OPA;
- Ciascun BRopo dell'Utente IQXN deve essere interconnesso alla coppia di BRqx del nodo QXN di attestazione mediante un profilo di servizio "Interconnessione OPO" con banda nominale 1 Gbps secondo le modalità descritte nell' Annesso A;
- Come opzione aggiuntiva del servizio, per ottenere una banda complessiva OPO superiore ad 1Gbps, l'Utente IQXN-Fornitore OPO può richiedere ulteriori porte 1GE da utilizzare in modo aggregato mediante protocollo LACP, secondo le modalità descritte in Annesso A. In tal caso, uguale ampliamento dovrà essere necessariamente realizzato anche sul profilo di Interconnessione OPO dell'Utente IQXN-Cliente OPO allo scopo di assicurare che la banda disponibile per la relazione del traffico OPO tra i due Utenti IQXN (Fornitore OPO e Cliente OPO) abbia sempre uguale dimensionamento su entrambi i lati dell'interconnessione IQXN;
- gli apparati BRopo dell'Utente IQXN devono essere collocati in housing presso i nodi QXN, all'interno delle infrastrutture (telai) appositamente predisposte ed individuate da Fornitore IQXN;
- l'installazione, gestione e manutenzione degli apparati BRopo è a cura e spese dell'Utente IQXN;
- la realizzazione, gestione e manutenzione dei cablaggi di collegamento tra i BRopo dell'Utente IQXN ed il cassetto ottico e/o patch panel UTP di sezionamento, predisposti e mantenuti da Fornitore IQXN all'interno del rack riservato all'Utente IQXN, sono a cura e spese dell'Utente IQXN;

 un passo avanti	 An IBM Company	 SISTEMI PER LA SICUREZZA E LE INFORMAZIONI
INTERNO	ICSPC-QXN-Regole Tecniche Per Interconnessione A QXN-1.4.Docx	

- k. la realizzazione, gestione e manutenzione dei cablaggi di collegamento tra i BRqxn ed il cassetto ottico e/o patch panel UTP di sezionamento, predisposti e mantenuti da Fornitore IQXN all'interno del rack riservato all'Utente IQXN, sono a cura e spese di Fornitore IQXN;
- l. i collegamenti tra i BRopo dell'Utente IQXN-Fornitore OPO, i BRqxn ed i BRopo dell'Utente IQXN-Cliente OPO devono essere realizzati in modalità bridged (Liv. 2 OSI) in configurazione trunk (IEEE 802.1q) su ciascuna porta di interconnessione al QXN;
- m. ciascun VLAN configurata in trunk deve trasportare il traffico relativo ad una VPN di una PA, realizzata in modalità OPO in parte sulla rete dell'Utente IQXN-Fornitore OPO ed in parte su quella del Utente IQXN-Cliente OPO. L'identificativo di ciascuna VLAN (VLAN ID) viene assegnato da Fornitore IQXN;
- n. il traffico inviato dal BRopo dell'Utente IQXN verso i due BRqxn di attestazione deve essere bilanciato a livello di sessione BGP su entrambi i link di interconnessione;
- o. ad ogni porta del BRqxn utilizzata dall'Utente IQXN deve corrispondere, lato BRopo, un solo MAC address;
- p. l'interconnessione attraverso il QXN deve essere configurata in modo che il traffico scambiato tra la rete dell'Utente IQXN-Fornitore OPO e quella del Utente IQXN-Cliente OPO transiti in via prioritaria sul nodo QXN di Roma ed in via secondaria su quello di Milano, in caso di indisponibilità totale del nodo QXN di Roma. E' lasciato all'Utente IQXN-Fornitore OPO ed al Utente IQXN- Cliente OPO concordare le politiche di routing più opportune al fine di garantire la simmetria del traffico OPO sulla QXN;
- q. ai fini della corretta gestione della QoS, l'Utente IQXN prima di consegnare il traffico ai BRqxn dovrà marcare i pacchetti relativi a ciascuna tipologia di traffico nativo OPA per associarli alla rispettiva Classe di Servizio (CdS) utilizzando i seguenti parametri TOS/DSCP.

Classe di Servizio	DSCP PHB	DSCP Valore Decimale
Real Time	AF41	34
Mission Critical	AF31	26
Streaming	AF21	18
Multicast	AF23	22
Multimedia	AF11	10
Best Effort	DF	0

2.4 MODALITÀ DI CONNESSIONE ALLA QXN




La connessione all'infrastruttura del QXN da parte dell'Utente IQXN deve essere realizzata attraverso degli apparati di "confine che devono essere posizionati in housing presso i nodi del QXN.

Il servizio di housing è compreso nel profilo di Servizio "Interconnessione OPA" e prevede la messa a disposizione dell'Utente IQXN di **max n. 1 telaio rack 19" 600x800 (42 unità) con alimentazione 220 AC su linee ridondate e con servizi di condizionamento, vigilanza, logistica e pulizia.**

Ciascun telaio dispone di una doppia alimentazione 220V AC, su barre ridondate attestate a quadri elettrici con interruttori magnetotermici a 16A.

Ciascun telaio, inoltre, è precablato – a cura di Fornitore IQXN, verso i rack che ospitano i nodi del QXN mediante le seguenti tipologia di cablaggi:

- cablaggi in fibra ottica multimodale di tipo 50/125 con connettorizzazione SC su cassette ottici 24fo

		
INTERNO	ICSPC-QXN-Regole Tecniche Per Interconnessione A QXN-1.4.Docx	

- cablaggi in rame UTP (cat 6), con connettorizzazione RJ45, su patch panel 24 porte UTP.

L'Utente IQXN deve prevedere il cablaggio delle porte dei propri apparati attivi sui cassette ottici/patch panel predisposti dal Fornitore IQXN all'interno del rack assegnato all'Utente IQXN. La realizzazione e la manutenzione del cablaggio da questo punto di sezionamento fino alle porte dei nodi QXN è a cura di Fornitore IQXN.

L'assegnazione del/i rack che ospitano gli apparati attivi BR dell'Utente IQXN è effettuata da Fornitore IQXN.

L'attestazione dei BR dell'Utente IQXN agli apparati del QXN può essere realizzata mediante le seguenti porte:

- 1 GigabitEthernet ottiche multimodali 1000 base SX – 850 nm – distanza max 550m
- 10/100/1000 GigabitEthernet elettriche con connettori RJ-45 cat 6.

Nel caso l'Utente IQXN richieda altre tipologie di porte (es. 10GE SR), il Fornitore IQXN si riserva di darne una valutazione di fattibilità tecnica, previa verifica con Agid.

I materiali da procurarsi a cura dell'Utente IQXN per l'installazione del/i proprio/i apparato/i sono i seguenti:

- Cavi di alimentazione con spina italiana o shuko della lunghezza di almeno 2,5 mt;
- Dadi a gabbia completi di viti
- Fascette per il fissaggio dei cavi
- Per le connessioni in GigaEthernet elettrica, una patch-cord (per interfaccia) UTP cat. 6 con connettori RJ-45 di lunghezza 2 mt (ad uso bretella di rilancio dall'apparato dell'Utente IQXN fino al patch panel interno al rack)
- Per le connessioni in GigabitEthernet, una bretella (per interfaccia) in fibra ottica multimodale (50/125) con connettori lato QXN di tipo SC di lunghezza 2 mt (ad uso di bretella di rilancio dell'apparato dell'Utente IQXN fino al cassetto ottico interno al rack);

Per ogni altro non contemplato nel presente documento, si può fare riferimento al Fornitore IQXN.

2.5 INTERCONNESSIONE DELLE QUALIFIED COMMUNITY NETWORK

L'interconnessione delle QCN a SPC, in ottemperanza al dettato dell'articolo 17 comma 5 del DPCM 1° aprile 2008 "Regole tecniche e di sicurezza del Sistema Pubblico di Connettività", può essere realizzata mediante:




- a) l'acquisizione di uno o più profili di servizio "Interconnessione OPA" (lettera "a" del sopra citato articolo del DPCM 1° aprile 2018) come descritto nel paragrafo 2.2;
- b) l'acquisizione di connettività Infranet (lettera "b" del sopra citato articolo del DPCM 1° aprile 2018) secondo una delle seguenti modalità:
 - la sottoscrizione di un Contratto SPC con un unico Fornitore di Connettività SPC;
 - la sottoscrizione di un Contratto SPC con più Fornitori di Connettività SPC in modalità peering BGP come descritto nell'Annesso B;

3 Verifiche tecniche di interconnessione al QXN

Questa sezione descrive i collaudi tecnici preliminari che devono essere condotti dal Soggetto che intenda interconnettersi alla QXN per aderire al profilo di servizio Interconnessione OPA.

Il Fornitore IQXN fornirà supporto all'Utente IQXN per l'esecuzione dei collaudi.

Lo scopo dei collaudi è quello di verificare che l'Utente IQXN risulti conforme alle Regole Tecniche di Interconnessione alla QXN, descritte nel presente documento.

		
INTERNO	ICSPC-QXN-Regole Tecniche Per Interconnessione A QXN-1.4.Docx	

Per l'esecuzione dei collaudi verrà richiesto al Utente IQXN di portare i propri apparati di interconnessione (Border Router – BR) e le relative connessioni alla propria rete presso i siti QXN di Roma – Via dei Tizii 2 (c/o NAMEX) e/o di Milano – Via Caldera 21 (c/o MIX).

Gli apparati BR del Utente IQXN verranno di norma ospitati per la durata dei collaudi all'interno dello stesso rack dove sono installati gli apparati del test-bed QXN, laddove ciò sia tecnicamente possibile. Viceversa, il Fornitore IQXN individuerà una soluzione alternativa. Al termine del collaudo verrà prodotto un verbale conclusivo che deve essere sottoscritto congiuntamente da Fornitore IQXN e dal Utente IQXN.




I collaudi che l'Utente IQXN dovrà sostenere sono finalizzati alla verifica dei seguenti aspetti:

- a. caratteristiche tecniche generali degli apparati BR del Utente IQXN preposti all'interconnessione con la QXN (ingombro, tipologia di porte di interconnessione, alimentazione elettrica etc...);
- b. corretto scambio tra QXN e la rete del Utente IQXN dei prefissi BGP in accordo con le politiche di routing definite nelle regole tecniche di interconnessione al QXN;
- c. corretto instradamento da parte della rete del Utente IQXN del traffico Infranet nativo OPA in accordo con le regole tecniche di interconnessione alla QXN ed in particolare:
 - verifica che il traffico Infranet nativo OPA tra sedi di due PA attestata alla rete del Utente IQXN non transiti in alcun caso sugli apparati del QXN;
 - verifica che il traffico scambiato da/verso Internet da una generica PA attestata sulla rete del Utente IQXN non transiti in alcun caso sugli apparati del QXN;
 - verifica che il traffico Infranet nativo OPA scambiato tra la rete di una PA attestata sulla rete del Utente IQXN e quella di un'altra PA attestata sulla rete di un altro Utente IQXN, connesso alla QXN transiti sempre attraverso quest'ultima;
 - verifica che il comportamento della rete del Utente IQXN sia conforme a quanto indicato nelle Regole Tecniche di Interconnessione alla QXN rispetto alle modalità di gestione del traffico (ridondanza, bilanciamento, simmetria) scambiato con la QXN;
- d. applicazione delle misure di sicurezza ed autenticità degli annunci BGP scambiati tra gli apparati BR del Utente IQXN e quelli della QXN;
- e. corretta marcatura ai fini della QoS, da parte del Utente IQXN, delle varie tipologie di traffico OPA scambiato con la QXN per associarle alla rispettiva Classe di Servizio (CdS);
- f. verifica della corretta implementazione dei meccanismi di risoluzione domini, Zone Transfer e DNS Notify nei confronti del DNS QXN.

I punti suddetti vengono verificati attraverso test eseguiti dall' Utente IQXN con il supporto del Fornitore IQXN: la descrizione e l'evidenza dell'esecuzione (report) di tali test verrà fornita dall' Utente IQXN interessato ed approvata dal Fornitore IQXN.

4 Service Level Agreement

I Livelli di Servizio (SLA) che regolano il servizio IQXN sono descritti nell'Appendice 1 del Capitolato Tecnico della Gara IC-SPC [2]. Tale documento costituisce parte integrante e sostanziale del Contratto Attuativo [4] che deve essere sottoscritto tra il Fornitore IC-SPC ed il Soggetto che intenda interconnettersi alla QXN per usufruire dei servizi da essa erogati.

		
INTERNO	ICSPC-QXN-Regole Tecniche Per Interconnessione A QXN-1.4.Docx	

5 Annesso A: Specifiche tecniche del servizio QXN

5.1 CARATTERISTICHE DEL SERVIZIO

Il Sistema Pubblico di Connettività prevede la realizzazione di una rete – denominata QXN (Qualified Exchange Network) – di interconnessione tra le reti dei fornitori SPC nonché dei soggetti abilitati da AgID alla fruizione di servizi di interconnessione per erogare servizi di comunicazione tra le Pubbliche Amministrazioni (PA).

La progettazione, realizzazione e gestione della QXN è demandata a Fornitore IQXN, individuato in quanto aggiudicatario della Gara [2] e sottoscrittore del contratto [1] con Agid.

Gli afferenti della rete QXN sono i Fornitori SPC, ovvero i Soggetti abilitati da AgID alla fruizione di servizi di interconnessione.

La rete del QXN svolge quindi la funzione di Internet eXchange Point per il solo traffico dati scambiato tra le Pubbliche Amministrazioni che aderiscono al contratto SPC2. In particolare le tipologie di traffico che attraversano il nodo QXN sono:

- Infranet: costituito dal traffico generato da due o più sedi di PA distinte che aderiscono al contratto SPC2 e che sono connesse a fornitori SPC differenti in accordo con l’Offerta Per le Amministrazioni (OPA).
- Intranet/Infranet in modalità OPO: costituito dal traffico scambiato tra due o più sedi della stessa PA connessa in parte ad un Fornitore IQXN assegnatario della Gara [Riferimento] ed in parte alla rete del Fornitore IQXN aggiudicatario della Gara [Riferimento] in accordo con l’Offerta per gli altri Operatori (OPO).
- Da/Verso QXN1: costituito dal traffico scambiato, per il tramite della rete QXN1 gestita dalla QXN Scpa, con le pubbliche amministrazioni ancora aderenti alla convenzione SPC1 con i relativi Fornitori Qualificati SPC1 (Fastweb, Telecom Italia, Wind, British Telecom). Questa tipologia di traffico verrà a cessare una volta che sarà stata completata la migrazione a SPC di tutte le PA attualmente attestate su SPC1.

Il Fornitore IQXN, oltre al servizio appena descritto di transito per il traffico dati tra le PA, offre anche servizi di Housing per ospitare gli apparati dei Soggetti Interconnessi utilizzati esclusivamente ai fini dell’interconnessione delle reti di questi ultimi con i nodi QXN mettendo a disposizione le porte GigabitEthernet per l’interconnessione degli apparati di accesso dei Soggetti Interconnessi. Mette, inoltre, a disposizione una sorgente di Tempo Ufficiale di Rete tramite protocollo NTP, mediante servers sincronizzati al segnale temporale generato dall’IEN, ed un servizio di DNS centralizzato per la risoluzione dei nomi a dominio in ambito SPC.

5.2 INFRASTRUTTURA DELLA RETE QXN

La QXN è una infrastruttura di backbone costituita da due nodi, situati rispettivamente a Roma presso i locali del Consorzio NAMEX e a Milano presso i locali della MIX srl. Ciascun nodo si compone, essenzialmente, di due apparati Cisco 6509E (Border Router - BRqxn) di uguale equipaggiamento, interconnessi tra loro mediante link ottici 10GBE e verso la coppia di identici apparati situati nel nodo remoto attraverso collegamenti geografici ridondati. Gli apparati scelti offrono prestazioni adeguate ai requisiti della rete QXN, sia dal punto di vista della capacità di routing e switching, sia a livello di disponibilità d’interfacce fisiche di rete.

La tecnologia utilizzata per i collegamenti dei due apparati in ciascun nodo è di tipo 10GE SR. Tra i due apparati dello stesso nodo geografico è previsto l’impiego di configurazione EtherChannel per l’aggregazione

FASTWEB un passo avanti	SISTEMI INFORMATIVI An IBM Company	LEONARDO SISTEMI PER LA SICUREZZA E LE INFORMAZIONI
INTERNO	ICSPC-QXN-Regole Tecniche Per Interconnessione A QXN-1.4.Docx	

di più collegamenti fisici in un unico circuito logico. I due circuiti geografici sono realizzati per mezzo di tecnologia di trasporto DWDM, con circuiti protetti sulla coda locale (nodo PoP di lunga distanza) e con percorsi differenziati sulla lunga distanza. Il dimensionamento di ciascun circuito geografico è pari a 1Gbps. Ciascun BRqxn sarà collegato mediante connessione GigabitEthernet ad una scheda differente dell'ADM.

Nello schema di rete sotto riportato è descritto graficamente la modalità di interconnessione dei due nodi QXN.

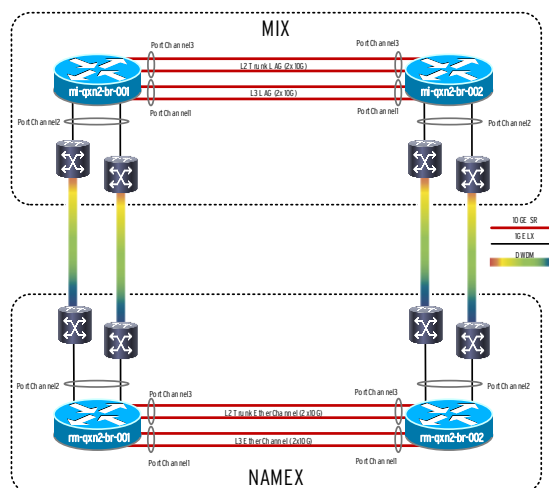





Figura 1 - Architettura di interconnessione tra i due nodi QXN

5.3 INTERCONNESSIONE OPA TRAMITE RETE QXN (PROFILO DI SERVIZIO "INTERCONNESSIONE OPA")

Allo scenario descritto in precedenza si devono aggiungere i nodi di rete dei diversi Utenti QXN che costituiscono il punto di accesso della rete QXN per la gestione del traffico Infranet tra le PA, in accordo con l'offerta OPA. Anche questi apparati, definiti come Border Router degli Utenti IQXN SPC (BRqx), sono collocati in housing presso le infrastrutture (rack) della QXN ospitate al MIX e al NaMeX. L'installazione, la gestione e la manutenzione di tali apparati è a carico dei rispettivi Utenti IQXN. Per il collegamento di questi apparati con funzione di livello di accesso della rete QXN è previsto l'utilizzo di tecnologia GigabitEthernet in fibra ottica (connessione multimodale short length) o in rame (categoria 6). Per il profilo di Servizio "Interconnessione OPA" i nodi del QXN (BRqxn) agiscono a livello di routing (Livello 3 del modello ISO/OSI).

Ciascun Utente IQXN aderente Profilo di Servizio "Interconnessione OPA", deve interconnettersi ad almeno un nodo QXN mediante una coppia di apparati BRqx interconnessi con gli apparati QXN (BRqxn) attraverso quattro porte 1 GigabitEthernet di tipo ottico o elettrico. Tale configurazione di interconnessione costituisce il **Profilo di Servizio "interconnessione OPA" con banda nominale 1 Gbps** ed è rappresentata nella figura 2 seguente.

		
INTERNO	ICSPC-QXN-Regole Tecniche Per Interconnessione A QXN-1.4.Docx	

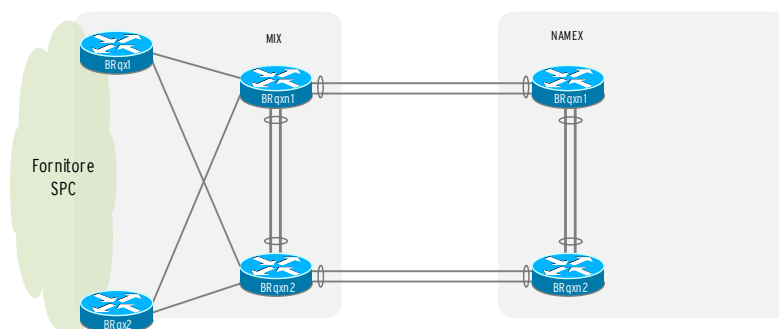


Figura 2 - ACCESSO OPA con banda nominale 1 Gbps

E' prevista per l'Utente IQXN, come opzione aggiuntiva la possibilità di replicare tale configurazione su entrambi i nodi QXN di Roma e Milano al fine di disporre di una maggiore affidabilità complessiva del servizio stesso. A tale scopo l'Utente IQXN dovrà sottoscrivere un ulteriore profilo di servizio "Interconnessione OPA" sull'altro nodo QXN dove intende interconnettersi.

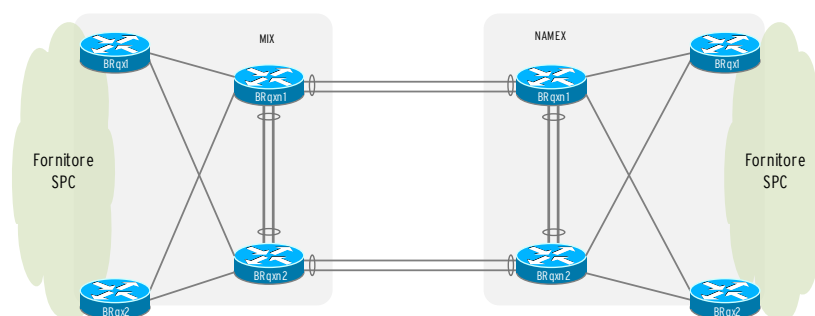


Figura 3 - RIDONDANZA GEOGRAFICA dell'ACCESSO OPA

Nella seguente figura 4 è riportato lo schema di collegamento di due Utenti IQXN generici ai due nodi dell'architettura QXN di Milano e Roma.

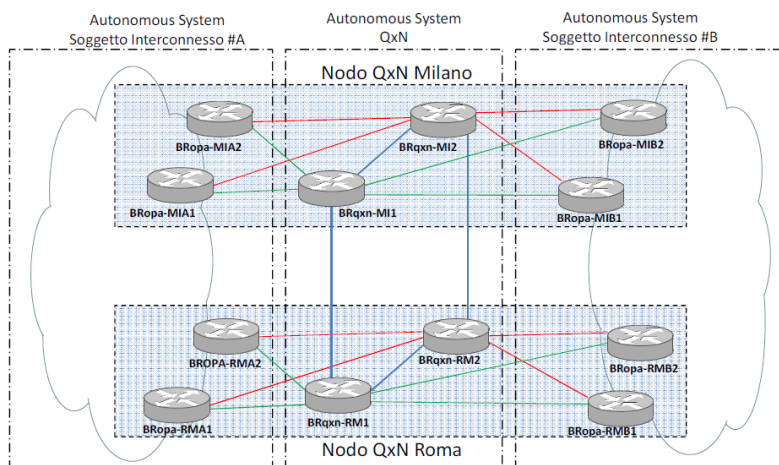


Figura 4 - Infrastruttura del backbone QXN

FASTWEB un passo avanti	SISTEMI INFORMATIVI An IBM Company	LEONARDO SISTEMI PER LA SICUREZZA E LE INFORMAZIONI
INTERNO	ICSPC-QXN-Regole Tecniche Per Interconnessione A QXN-1.4.Docx	

5.4 INTERCONNESSIONE OPO TRAMITE RETE QXN (PROFILO DI SERVIZIO “INTERCONNESSIONE OPO”)

In accordo con l’offerta OPO, il Fornitore SPC aggiudicatario della Gara MF SPC2 [3] ed il Fornitore assegnatario della medesima Gara [3] che abbia sottoscritto un contratto esecutivo OPO, devono prevedere l’interconnessione con la rete QXN mediante apparati dedicati BRopo o, in alternativa, utilizzando gli stessi apparati BRqx già previsti per la connettività OPA. Ciò allo scopo di consentire lo scambio del traffico tra le rispettive reti, ovvero:

- la rete del Fornitore SPC aggiudicatario, che eroga i servizi in modalità OPO (di seguito indicato come **Utente IQXN- Fornitore OPO**),
- la rete del Fornitore SPC assegnatario che usufruisce di tali servizi (di seguito indicato come **Utente IQXN- Cliente OPO**)

Nel caso l’Utente IQXN (Fornitore OPO o Cliente OPO) utilizzi il medesimo apparato per entrambi i servizi OPA e OPO, le interfacce per il collegamento OPO saranno distinte da quelle previste per la connettività OPA. In caso di apparato dedicato al servizio OPO, il BRopo, potrà essere un PE o un CPE “VRF aware”.

La soluzione rappresentata in Fig. 5 prevede l’utilizzo di un PE o di un CE VRF aware (BRopo) collegato in trunk ai nodi della dorsale QXN (BRqxn) per il trasporto di un numero di VLAN e sessioni E-BGP pari al numero di PA che richiedono connettività intranet in accordo con l’offerta OPO. All’interno del backbone dei due FORNITORI SPC2 le varie PA saranno trattate come singole VRF.

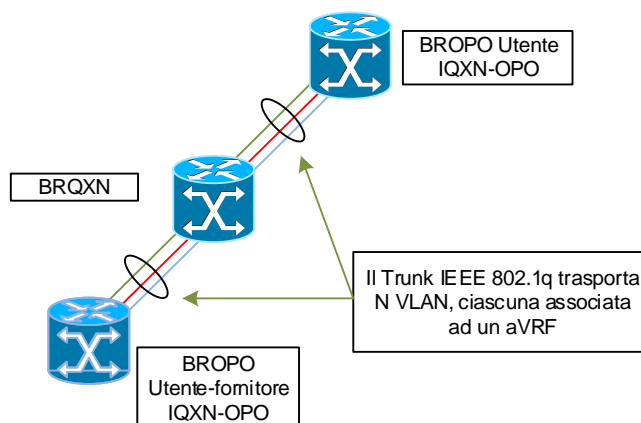


Figura 5 - Modello di interconnessione OPO PE-to-PE

L’interconnessione fisica tra i BRopo di ciascun Utente IQXN-Cliente OPO e il BRopo del Utente IQXN-Fornitore OPO non è diretta, ma realizzata tramite gli switch della rete QXN, utilizzando sempre tecnologia Ethernet. Il collegamento sopra citato deve essere configurato in modalità trunk (IEEE 802.1q) per il trasporto di un numero di VLAN pari al numero di PA che richiedono connettività Intranet in accordo con l’offerta OPO. Inoltre per l’Utente IQXN-Fornitore OPO è obbligatorio prevedere un collegamento OPO fisico dedicato e distinto per ogni Utente IQXN-Cliente OPO. **Entrambi i collegamenti OPO (lato Utente IQXN-Fornitore OPO e lato Utente IQXN-Cliente OPO) devono essere configurati con uguale capacità di banda.**

Tale modalità di interconnessione, offre la possibilità di monitoraggio e visibilità del traffico ai fini della misurazione degli SLA, oltre a delimitare univocamente il confine di ciascun operatore alla porta del BRqxn.

In definitiva, per i servizi OPO, i nodi del QXN (BRqxn) agiscono a livello di switching (Livello 2 del modello ISO/OSI).

Come per gli apparati previsti per i servizi di Interconnessione OPA, eventuali apparati dedicati al traffico OPO devono essere installati presso le infrastrutture di housing della rete QXN.

FASTWEB un passo avanti	SISTEMI INFORMATIVI An IBM Company	LEONARDO SISTEMI PER LA SICUREZZA E LE INFORMAZIONI
INTERNO	ICSPC-QXN-Regole Tecniche Per Interconnessione A QXN-1.4.Docx	

Il livello di affidabilità e ridondanza, in termini di numero di BRopo presenti presso ciascun nodo QXN, è demandato al singolo Utente IQXN. Il BRopo di interconnessione per ciascuna VPN cliente, peraltro, sarà univoco su ciascun nodo QXN, perciò ciascun Utente IQXN potrà essere autonomo nel scegliere se definire tutte le VLAN e sessioni BGP su un unico apparato o distribuire le VLAN/sessioni BGP sulla coppia di apparati a propria disposizione. Indipendentemente dalla tipologia di apparato preferita dal Utente IQXN, la modalità base di interconnessione prevede che quest'ultimo interfacci la propria rete al QXN su entrambi i nodi di Roma e Milano. Su ciascun nodo, l'interconnessione sarà realizzata mediante almeno un BRopo con due porte 1 GBE attestate alla coppia di BRqxn (sulle quali sarà bilanciato il traffico). Tale configurazione costituisce il **profilo di servizio "interconnessione OPO" con banda nominale a 1 Gbps** ed è illustrata nella figura 6 seguente.

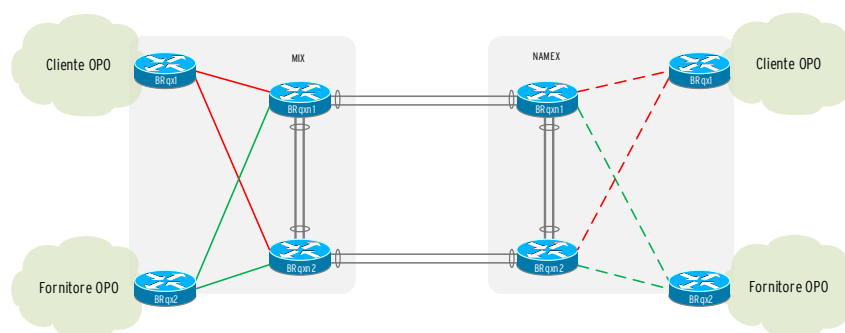





Figura 6 – Profilo di Servizio "interconnessione OPO" con banda nominale 1 Gbps

Ai fini dell'interconnessione OPO, si considera come nodo QXN principale quello di Roma e come nodo QXN di backup quello di Milano. Pertanto, tutto il traffico OPO scambiato tra il Utente IQXN-Fornitore OPO e ciascun Fornitore IQXN-Cliente OPO sarà scambiato prioritariamente su Roma, salvo passare su Milano in caso di fault completo del nodo QXN.

Qualora la banda richiesta per interconnessione tra il Utente IQXN_Fornitore OPO e l'Utente IQXN-Cliente OPO superi complessivamente la soglia di 1 Gbps, possono essere considerate le seguenti alternative (corrispondenti ad altrettante opzioni di servizio), da valutare in funzione di un'analisi di fattibilità tecnico-economica condotta dal Fornitore IQXN ed approvata da AgID:

- Realizzare la banda aggiuntiva mediante incrementi di porte a 1 GBE, sia per l'Utente IQXN-Fornitore OPO, che per l'Utente IQXN-Cliente OPO verso ciascun BRqxn di entrambi i nodi QXN. Le porte incrementalmente possono essere attestate, lato Utente IQXN, sulla stessa macchina BRopo oppure su due macchine BRopo distinte, distribuendo opportunamente il traffico delle VLAN richieste. Questa soluzione non è percorribile qualora la singola VLAN associata alla VPN della PA abbia banda superiore ad 1 Gbps.
- Come opzione alternativa alla precedente, per ottenere una banda complessiva OPO superiore ad 1Gbps, l'Utente IQXN-Fornitore OPO può richiedere ulteriori porte 1GE da utilizzare in modo aggregato mediante protocollo LACP. Anche questa modalità è realizzata mediante incrementi di porte a 1 GBE, sia per l'Utente IQXN-Fornitore OPO che per l'Utente IQXN-Cliente OPO, verso ciascun BRqxn di entrambi i nodi QXN. Questa soluzione è percorribile qualora la singola VLAN associata alla VPN della PA abbia banda superiore ad 1 Gbps.
- Realizzare la banda aggiuntiva mediante porte a 10 GBE, l'Utente IQXN-Fornitore OPO che per l'Utente IQXN-Cliente OPO attestate su ciascun BRqxn di entrambi i nodi QXN.

		
INTERNO	ICSPC-QXN-Regole Tecniche Per Interconnessione A QXN-1.4.Docx	

5.5 SERVIZIO DI EROGAZIONE DEL TEMPO UFFICIALE DI RETE (NTP)

L'architettura QXN prevede la presenza di un proprio server NTP per la generazione del tempo ufficiale di rete. Tale funzionalità sarà assolta da un cluster di server, i quali si sincronizzeranno con il server NTP dell'Istituto Galileo Ferraris, via Internet, mediante una LAN segregata e non ruotata (DMZ pubblica).

Al fine di garantire la massima affidabilità del servizio, ciascun cluster renderà disponibile il Tempo Ufficiale di Rete (TUR), fornendo, di fatto, un NTP server distribuito sui due NAP (ciascuno in alta affidabilità).

5.6 SERVIZIO DNS

Il servizio DNS erogato dalla QXN consente di centralizzare la gestione dei nomi di dominio delle PA afferenti all'SPC e di rendere disponibile questa informazione ai diversi Soggetti interconnessi alla QXN.

Il DNS della QXN, inoltre, è collegato:

- ai root server di Internet per la risoluzione dei nomi esterni allo spazio dei domini gestiti da SPC
- al DNS della QXN1 per la risoluzione dei nomi appartenenti allo spazio dei domini pubblicati su Infranet dalle PA aderenti alla vecchia SPC (limitatamente alla fase di migrazione dalla vecchia alla nuova convenzione SPC)

Questa configurazione consente ai diversi Utenti IQXN di disporre di un unico sistema DNS, in grado di risolvere in maniera centralizzata tanto i nomi interni all'ambito SPC quanto nomi internet, costituendo il riferimento primario per la risoluzione di tutti i nomi host in ambito SPC.

5.7 ASSISTENZA TECNICA SUI SERVIZI QXN

Il Fornitore IQXN attraverso il proprio Service Desk, mette a disposizione degli Utenti IQXN un servizio di assistenza tecnica volto:




- Alla gestione della infrastruttura QXN ed al monitoraggio dei servizi erogati
- Alla acquisizione delle segnalazioni di disservizi inviate dagli Utenti IQXN ed alla conseguente gestione e risoluzione dei disservizi stessi. Ciascuna segnalazione viene associata univocamente ad un corrispondente Trouble Ticket, che il Service Desk comunica all'Utente IQXN e mediante il quale viene referenziato il disservizio.
- Alla gestione delle richieste di provisioning di nuovi servizi sulla QXN (interconnessione OPO/OPA, creazione file di zona sul DNS)
- Alla gestione delle richieste di accesso presso i nodi QXN per esigenze di manutenzione ordinaria/straordinaria degli apparati dell'Utente IQXN.
- Al monitoraggio dei Livelli di Servizio (SLA) ed alla fornitura della relativa reportistica gestionale.

Per gli ambiti suddetti, il Fornitore IQXN ha predisposto apposite Procedure Operative che verranno fornite agli Utenti IQXN, contestualmente all'avvio dei Servizi di Interconnessione da essi contrattualizzati.

Il servizio è accessibile su base h. 24x365 giorni attraverso i seguenti canali:

- N.ro telefonico: **800.893.576**
- E-mail: nocpa@fastweb.it

Le richieste di accesso ai locali in cui sono ubicati i nodi QXN per esigenze di manutenzione ordinaria/straordinaria sono regolate da una apposita procedura operativa, che verrà fornita agli Utenti IQXN contestualmente all'avvio dei Servizi di Interconnessione da essi contrattualizzati.

		
INTERNO	ICSPC-QXN-Regole Tecniche Per Interconnessione A QXN-1.4.Docx	

6 ANNESSO B: REGOLE TECNICHE PER L'INTERCONNESSIONE ALLA QXN CON PIU' FORNITORI SPC

6.1 PREMESSA

Nel presente annesso vengono dettagliate le regole tecniche che devono essere osservate dalle QCN che intendano interconnettersi a SPC per il tramite di più Fornitori SPC.

6.2 VINCOLI E PRECONDIZIONI

L'unica soluzione adottabile per lo scenario del presente annesso prevede che la QCN:

- a) sia dotata di un proprio ASN e proprio indirizzamento pubblico IPv4/IPv6;
- b) intenda interconnettersi alla Infranet mediante peering BGP.

L'interconnessione a SPC può avvenire solo per il tramite di due distinti Fornitori SPC.

6.3 REGOLE DI INTERCONNESSIONE

Al fine di ottenere la simmetria del traffico e semplificare il troubleshooting sulla QXN e sulle reti dei FSPC coinvolti, la QCN dovrà eseguire l'interconnessione rispettando i seguenti vincoli:

1. a ciascuno dei FSPC la QCN si interconnetterà con un singolo link. La ridondanza della connessione alla rete Infranet sarà comunque garantita dal link verso il secondo operatore.
2. la QCN configurerà un peering BGP in modalità multi-hop verso ciascun operatore. La raggiungibilità dell'indirizzo del peer sarà ottenuta mediante routing statico¹.
3. la QCN potrà terminare entrambi i peering su un singolo apparato o su apparati distinti in funzione dei propri requisiti di disponibilità.
4. la QCN annuncerà, verso entrambi i FSPC, esclusivamente i propri prefissi come originati dal proprio ASN.
5. la QCN annuncerà i prefissi verso entrambi i FSPC con la medesima lunghezza di maschera.
6. la lunghezza massima dei prefissi annunciati dalla QCN sarà /24 per IPv4 e /48 per IPv6 in coerenza con quanto previsto sulla rete QXN.
7. la QCN dovrà indicare un FSPC primario ed uno secondario ed agire sugli annunci BGP in modo da preferire il link primario per tutto il traffico da e verso la QXN. Il traffico da e verso le destinazioni interne ai due operatori che le forniscono il servizio, seguirà invece lo shortest path e quindi non attraverserà la QXN². In particolare:
 - a. verso il FSPC secondario la QCN sfavorirà gli annunci applicando un singolo as-path prepend del proprio ASN. Annunci con un numero di prepend superiore verranno scartati.
 - b. la QCN dovrà privilegiare gli annunci ricevuti dal FSPC primario limitatamente a quelli con AS-PATH che includano l'ASN della QXN (43988) escludendo tuttavia quelli originati dal FSPC secondario.
8. ciascun FSPC dovrà garantire che il traffico scambiato tra le PA/QCN a cui eroga il servizio OPA, rimanga locale e non venga quindi consegnato alla QXN.
9. Per la pubblicazione dei nomi in ambito Infranet la QCN dovrà utilizzare i servizi del FSPC primario.

¹ Si veda il par. 6.5 per maggiori dettagli.

² Si faccia riferimento al par. 6.4 per le linee guida di configurazione.

FASTWEB un passo avanti	SISTEMI INFORMATIVI An IBM Company	LEONARDO SISTEMI PER LA SICUREZZA E LE INFORMAZIONI
INTERNO	ICSPC-QXN-Regole Tecniche Per Interconnessione A QXN-1.4.Docx	

6.4 LINEE GUIDA DI IMPLEMENTAZIONE PER LA QCN

La modalità di connessione con doppio operatore, prevede l'autonomia della QCN nell'annuncio dei propri prefissi. Ciononostante, al fine di permettere una efficace gestione del servizio da parte dei FSPC, la QCN dovrà impostare le proprie policy BGP in modo da rispettare i vincoli descritti al punto 7 del par. 6.3.

Allo scopo di agevolare in tale compito la QCN, vengono riportate di seguito delle linee guida per l'implementazione di policy BGP coerenti con le regole di interconnessione precedentemente descritte.

6.4.1 POLICY PER LA MANIPOLAZIONE DEL TRAFFICO IN DOWNSTREAM

Per privilegiare il transito del traffico in downstream³ attraverso il FSPC primario, sarà sufficiente per la QCN agire sugli annunci verso i due operatori applicando un singolo prepend verso il FSPC secondario.

Tale prepend sarà propagato dal FSPC secondario alla QXN che quindi, sulla base della lunghezza dell'AS-PATH, selezionerà come best path il percorso attraverso il FSPC primario.

Si noti che il prepend non avrà invece effetto sul traffico originato dai due FSPC con i quali fa peering la QCN in quanto, anche sul FSPC secondario, sarà preferito l'annuncio ricevuto direttamente dalla QCN (lunghezza AS-PATH 2) rispetto a quello transitato per la QXN (lunghezza AS-PATH 3).

Per maggiore chiarezza, lo schema seguente dettaglia gli AS-PATH ed i best path selezionati dagli AS coinvolti (FSPC1, FSPC2, QXN).

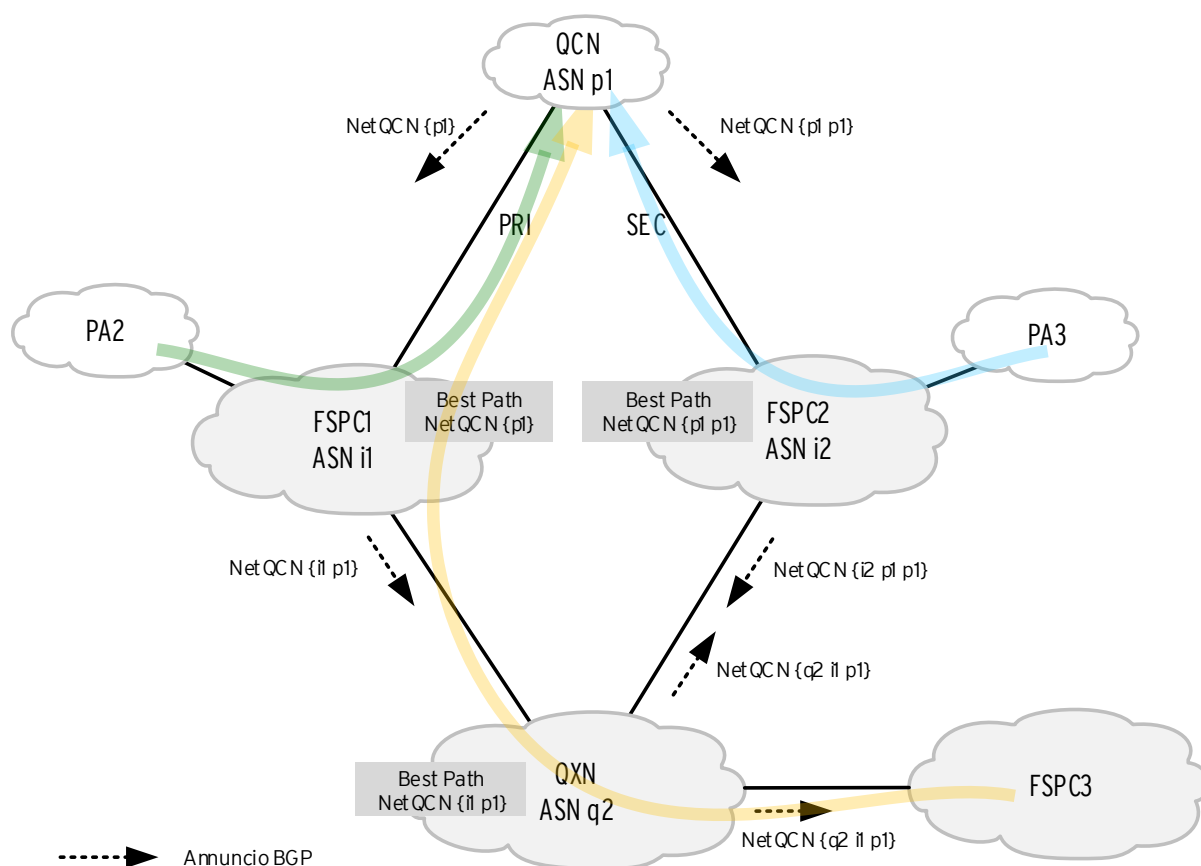


Figura 7. Annunci BGP e best path che influenzano il percorso del traffico in downstream.

³ Traffico in ingresso sulla QCN proveniente dalla QNX.

FASTWEB un passo avanti	SISTEMI INFORMATIVI An IBM Company	LEONARDO SISTEMI PER LA SICUREZZA E LE INFORMAZIONI
INTERNO	ICSPC-QXN-Regole Tecniche Per Interconnessione A QXN-1.4.Docx	

6.4.2 POLICY PER LA MANIPOLAZIONE DEL TRAFFICO IN UPSTREAM

Per privilegiare il transito del traffico in upstream⁴ attraverso il link primario sarà possibile applicare una local preference superiore a quella di default alle rotte con as-path che includano l'ASN della QXN ma non quello del FSPC secondario.

Per tutte le altre rotte, su entrambi i link, potrà essere applicata la local-preference di default demandando quindi la scelta del best path alla lunghezza dell'as-path.

A solo scopo di esempio si riporta una configurazione parziale per l'implementazione della policy appena descritta:

```
ip as-path access-list 1 deny _<ASN_FSPC_SEC>_
ip as-path access-list 1 permit _43988_
route-map SET-PRIMARY-IN permit 10
  match as-path 1
  set local-preference 200
route-map SET-PRIMARY-IN permit 20
```

Per maggiore chiarezza, lo schema seguente dettaglia gli AS-PATH e le Local Preference dal punto di vista della QCN a valle dell'applicazione delle policy precedentemente descritte.

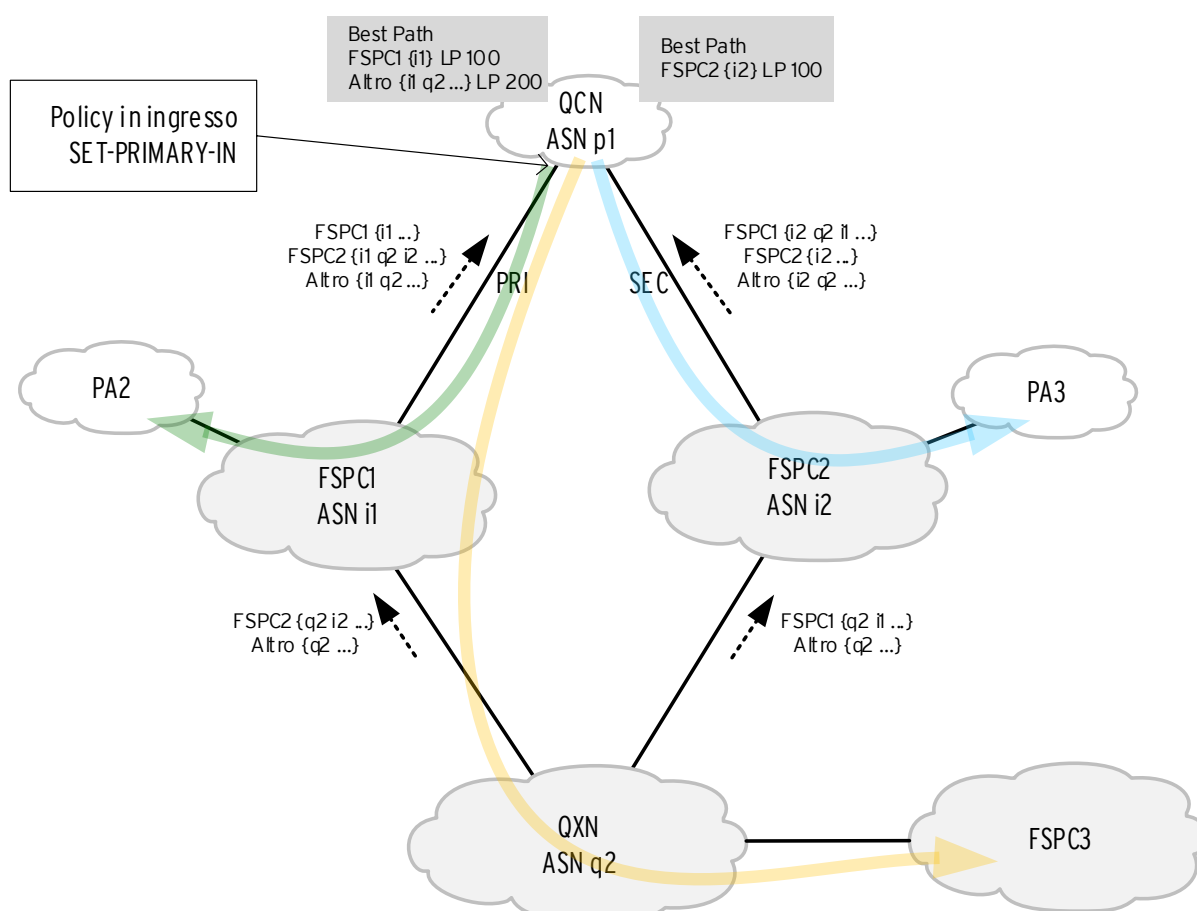





Figura 8. Annunci BGP e best path che influenzano il percorso del traffico in upstream.

⁴ Traffico in uscita dalla QCN per destinazioni conosciute attraverso la QNX2.

		
INTERNO	ICS-PC-QXN-Regole Tecniche Per Interconnessione A QXN-1.4.Docx	

6.5 INTERFACCIAMENTO TRA FSPC E QCN

Per la realizzazione del punto di accesso alla rete Infranet, ciascun operatore installerà presso i locali della QCN un CPE. Tale CPE, risulta necessario nel contesto SPC2, al fine di gestire la QoS (SBRI) ed il relativo performance monitoring.

Il CPE d'altra parte non sarà coinvolto nel routing BGP rendendo quindi la QCN indipendente nella gestione dei propri annunci mediante le sessioni eBGP multi-hop instaurate direttamente con il PE dell'operatore.

La comunicazione di base necessaria all'instaurazione delle sessioni BGP sarà realizzata mediante routing statico tra PE, CPE e router cliente.

Indirizzamento e parametri di configurazione specifici di ciascuna sessione eBGP saranno concordati direttamente tra la QCN e ciascun FSPC.

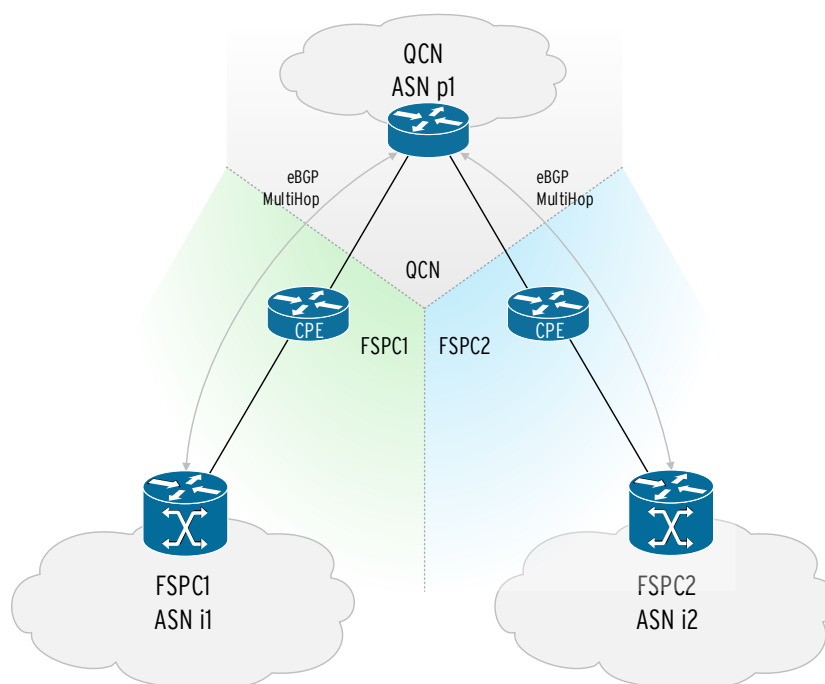





Figura 9. Interfacciamento tra QCN e FSPC.

		
INTERNO	ICSPC-QXN-Regole Tecniche Per Interconnessione A QXN-1.4.Docx	

Fine del Documento
