

	Qualified Exchange Network
Specifica di Realizzazione del servizio InterC	QXN-InterC-SpecRealizzazione

Specifica di Realizzazione del servizio

InterConnessione QXN

	Qualified Exchange Network
Specifica di Realizzazione del servizio InterC	QXN-InterC-SpecRealizzazione

Sommario

0. GENERALITÀ	4
0.1 DEFINIZIONE ED ACRONIMI.....	4
1. CARATTERISTICHE DEL SERVIZIO	6
1.1 INFRASTRUTTURA DELLA RETE DEL QXN	7
1.2 INTERCONNESSIONE PER TRASPORTO DI TRAFFICO INFRANET NATIVO OPA TRAMITE RETE QXN (OFFERTA OPA) 9	
1.3 INTERCONNESSIONE PER TRASPORTO DI TRAFFICO NATIVO OPA IN MODALITÀ OPO TRAMITE RETE QXN (OFFERTA OPO)	10
1.3.1 Interconnessione PE-to-PE.....	11
2. EQUIPAGGIAMENTO APPARATI DEL QXN	13
2.1 APPARATI DI DORSALE – BRQXN	14
2.1.1 Motivazioni della scelta tecnologica per i Cisco 7609 come BRqxn.....	15
2.2 TERMINAL SERVER PER LA GESTIONE OOB.....	16
2.3 FIREWALL	16
2.4 SONDE PER LA MISURAZIONE DEGLI SLA.....	16
2.5 FIREWALL/NETWORK INTRUSION DETECTION SYSTEM.....	16
2.6 ROUTER DI ACCESSO INTERNET.....	17
2.7 SERVER DNS	17
2.8 INDIRIZZAMENTO IP NELLA RETE QXN.....	17
2.9 INSTRADAMENTO DEL TRAFFICO INFRANET NATIVO OPA.....	18
2.10 SOLUZIONI DI ROUTING PER L'INSTRADAMENTO DEL TRAFFICO NELLA RETE QXN.....	18
2.10.1 Soluzioni di routing per il bilanciamento del traffico Infranet OPA	19
2.10.2 Soluzioni di routing per il bilanciamento del traffico OPO	20
2.10.3 Soluzioni di routing per la simmetria del traffico Infranet nativo OPA	20
2.10.4 Soluzioni di routing per la simmetria del traffico OPO	22
2.10.5 Resilienza dell'instradamento del traffico Infranet OPA a fronte di uno o più fault.....	23
2.10.6 Resilienza dell'instradamento del traffico OPO a fronte di uno o più fault.....	24
2.11 SERVIZI DI QOS	24
2.12 SERVIZIO DI EROGAZIONE DEL TEMPO UFFICIALE DI RETE (NTP)	25
2.13 SERVIZIO DNS	25
2.14 MONITORING E GESTIONE DELLA RETE QXN	26

	Qualified Exchange Network
Specifica di Realizzazione del servizio InterC	QXN-InterC-SpecRealizzazione

Indice delle Figure

Figura 6 – Architettura di interconnessione tra i due nodi QXN.....	8
Figura 7 – Infrastruttura del backbone QXN.....	9
Figura 8 – Modello di interconnessione OPO PE-to-PE	11
Figura 9 – Architettura logica dell'interconnessione OPO.....	12
Figura 11 – Soluzioni di routing sul backbone QXN	19
Figura 12 – Intradamento simmetrico del traffico sul QXN	21

Indice delle Tabelle

Tabella 1 – Apparati di dorsale di ciascun nodo QXN.....	14
Tabella 2 – Terminal server per gestione OOB (Cisco 2811)	16
Tabella 3 – Sonde per QXN (Cisco 2811).....	16
Tabella 6 – Classificazione del traffico in base al TOS/DSCP.....	25

	Qualified Exchange Network
Specifica di Realizzazione del servizio InterC	QXN-InterC-SpecRealizzazione

0. Generalità

0.1 Definizione ed Acronimi

Definizione / Acronimo	Descrizione
ACL	Access Control List
ADM	Add Drop Multiplexer
ASn	Autonomous System number
BGP	Border Gateway Protocol
BR	Border Router
BRqx	Border Router del Q-ISP
BRqxn	Border Router della QXN
CED	Centro Elaborazione Dati
CE	Customer Edge
CNIPA	Centro Nazionale per l'Informatica nella Pubblica Amministrazione
CPE	Customer Premise Equipment
CdS	Classe di Servizio
CPU	Cantral Processing Unit
DNS	Domain Name System
DMZ	DeMilitarized Zone
EBGP	External Border Gateway Protocol
HSRP	Hot Standby Routing Protocol
IGP	Interior Gateway Protocol
IP	Internet Protocol
ISP	Internet Service Provider
LAN	Local Area Network
MAC	Media Access Control
MAN	Metropolitan Area Network
MD5	Message Digest algorithm v.5
MIX	Milan Internet Exchange
MPLS	Multi Protocol Label Switching
NaMeX	Nautilus Mediterranean Exchange
NAP	Neutral Access Point
NAT	Network Address Translation
NIDS	Network Intrusion Detection System
NTP	Network Time Protocol
OOB	Out Of Band
OPA	Offerta Per la Amministrazioni
OPO	Offerta Per gli altri Operatori
OSPF	Open Shortest Path First
OWD	One Way Delay
PA	Pubblica Amministrazione
PAS	Punto di Accesso al Servizio
PE	Provider Edge

	Qualified Exchange Network
Specifica di Realizzazione del servizio InterC	QXN-InterC-SpecRealizzazione

Definizione / Acronimo	Descrizione
PIR	Punto di Interconnessione RUPA
PoP	Point of Presence
PPS	Pacchetti Per Secondo
Q-ISP	Qualified Internet Service Provider
QoS	Quality of Service
QXN	Qualified eXchange Network
RTD	Round Trip Delay
RUPA	Rete Unitaria della Pubblica Amministrazione
SC-QXN	Società Consortile QXN
SDH	Synchronous Digital Hierarchy
SLA	Service Level Agreement
SMQS	Sistema di Misura della Qualità del Servizio
SPC	Servizi di Pubblica Connettività
TCP	Transmission Control Protocol
TUR	Tempo Ufficiale di Rete
VLAN	Virtual Local Area Network
VPN	Virtual Private Network
VRF	Virtual Routing and Forwarding
WAN	Wide Area Network

	Qualified Exchange Network
Specifica di Realizzazione del servizio InterC	QXN-InterC-SpecRealizzazione

1. Caratteristiche del servizio

Nell'ambito del Progetto SPC (Sistema Pubblico di Connettività) promosso da CNIPA, è prevista la realizzazione di una rete – denominata QXN – di interconnessione tra le reti degli Internet Service Provider Qualificati (Q-ISP) dallo stesso CNIPA per erogare servizi di comunicazione tra le Pubbliche Amministrazioni aderenti a SPC (PA SPC).

Gli afferenti della rete QXN sono gli Internet Service Provider, qualificati (Q-ISP) dal CNIPA per la fornitura di servizi di telecomunicazione alle Pubbliche Amministrazioni 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 (PA SPC). 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 SPC, le quali sono connesse a Q-ISP 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 SPC connessa in parte ad un Q-ISP assegnatario (Wind, British Telecom, Telecom Italia) ed in parte alla rete del Q-ISP aggiudicatario (FastWeb) in accordo con l'Offerta Per gli altri Operatori (OPO).

Le specifiche del servizio di interconnessione erogato da QXN sono descritte in *QXN-InterC-SpecificaServizio*.

	Qualified Exchange Network
Specifica di Realizzazione del servizio InterC	QXN-InterC-SpecRealizzazione

1.1 Infrastruttura della rete del QXN

L'impiego di quattro apparati Cisco 7609 (BRqxn) di uguale equipaggiamento, interconnessi tra loro tramite collegamenti geografici ridondati, costituisce, in sintesi, la dorsale dell'impianto infrastrutturale della QXN. 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.

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 in ciascun nodo è di tipo GigabitEthernet in fibra ottica. Tra i due apparati dello stesso nodo geografico è previsto l'impiego di configurazione GigaEtherChannel per l'aggregazione in un unico circuito logico di quattro collegamenti GigabitEthernet in fibra ottica.

I due circuiti geografici previsti per il collegamento tra gli apparati dei due nodi di Roma e Milano sono realizzati per mezzo di tecnologia di trasporto SDH, con circuiti protetti sulla coda locale (nodo PoP di lunga distanza) e con percorsi differenziati

Il dimensionamento iniziale di ciascun circuito geografico è pari a 100 Mbps.

In funzione delle esigenze future di traffico, sarà comunque possibile ampliare la banda di ciascun circuito, portandola ad 1 Gbps, sempre utilizzando i medesimi e le medesime connessioni fisiche.

La decisione di procedere all'upgrade di banda dei due circuiti Roma-Milano verrà presa in base alla seguente policy.

Con riferimento a ciascuno dei due circuiti, viene definita una soglia B_s che rappresenta il livello di occupazione del link che fa scattare la procedura di upgrade di banda. In relazione al requisito QXN n. 78, la soglia B_s viene fissata pari al 50% della capacità trasmissiva massima configurata sul circuito (per quanto detto in precedenza, inizialmente $B_s = 50$ Mbps).

Vengono, quindi, rilevati su intervalli di osservazione T_i della durata di 5 minuti, i valori della banda misurata sul circuito (B_i) nelle due direzioni di traffico ($B_{i\text{ RM->MI}}$, $B_{i\text{ MI->RM}}$). Viene, quindi, definito come **valore giornaliero di picco** ($B_{\text{MAX}_{\text{day}_J}}$) dell'occupazione di banda sul circuito per ciascuna delle due direzioni di traffico nel giorno j -esimo, il massimo tra i valori dell'occupazione di banda misurati negli intervalli di osservazione T_i rilevati nell'arco delle 24 ore ($i=1..288$).

$$B_{\text{MAX}_{\text{day}_J\text{ RM->MI}}} = \max B_{i\text{ RM->MI}} \quad (i=1.....288)$$

$$B_{\text{MAX}_{\text{day}_J\text{ MI->RM}}} = \max B_{i\text{ MI->RM}} \quad (i=1.....288)$$

L'indicatore di riferimento è quindi il picco giornaliero della banda misurata su ciascun circuito, per ciascuna direzione di traffico: tuttavia per filtrare alcuni eventi, quali una convergenza che sposta il traffico in uno solo dei link della tratta o la diminuzione di traffico nel week end, se ne calcola una media su un periodo di un mese solare. Quindi, per ciascuno dei due circuiti Roma-Milano, si avranno i seguenti valori:

$$B_{\text{RM->MI}} = \text{avg} (B_{\text{MAX}_{\text{day}_J\text{ RM->MI}}}) \quad \text{per } j=1..30 \text{ (su un intervallo di 30 gg)}$$

$$B_{\text{MI->RM}} = \text{avg} (B_{\text{MAX}_{\text{day}_J\text{ MI->RM}}}) \quad \text{per } j=1..30 \text{ (su un intervallo di 30 gg)}$$

	Qualified Exchange Network
Specifica di Realizzazione del servizio InterC	QXN-InterC-SpecRealizzazione

Per l'occupazione di banda sui due circuiti, la metrica è quindi la media dei picchi giornalieri, per ciascuna direzione di traffico sul circuito, consolidata in intervallo di un mese solare.

Così definiti $B_{RM->MI}$ e $B_{MI->RM}$ per ciascuno dei due circuiti, al superamento della soglia B_s da parte di almeno uno di questi valori, si procede all’ampliamento della capacità trasmissiva su entrambi i circuiti, con step minimi di 50 Mbps.

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

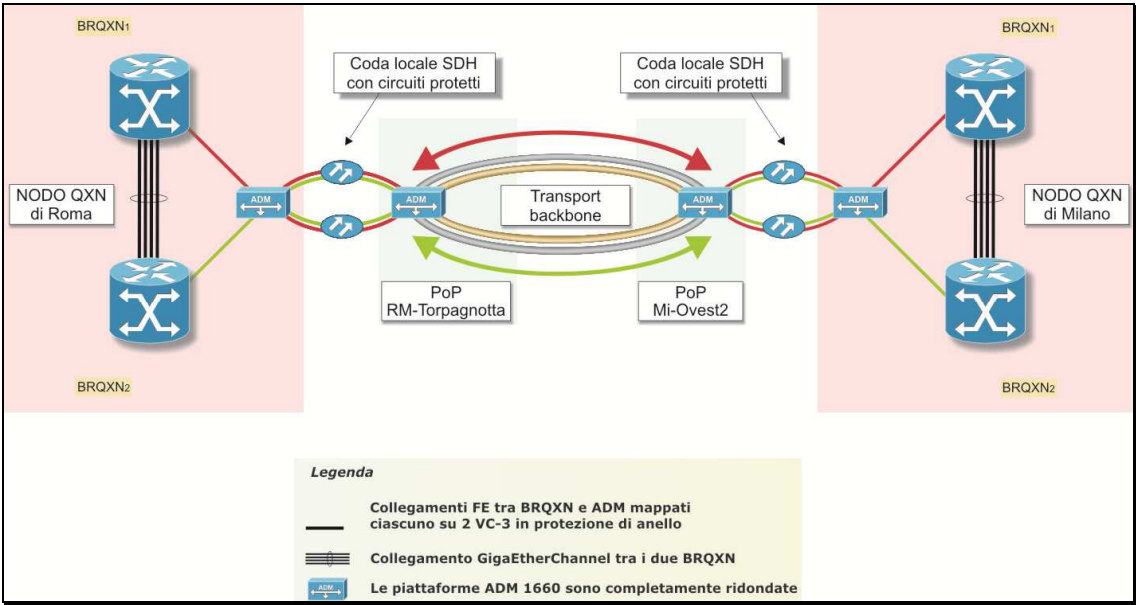


Figura 1 – Architettura di interconnessione tra i due nodi QXN

	Qualified Exchange Network
Specifica di Realizzazione del servizio InterC	QXN-InterC-SpecRealizzazione

1.2 Interconnessione per trasporto di traffico Infranet nativo OPA tramite rete QXN (offerta OPA)

Allo scenario descritto nel precedente paragrafo si devono aggiungere 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 l’utilizzo di tecnologia GigabitEthernet in fibra ottica (connessione multimodale short length) o in rame (categoria 6).

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.

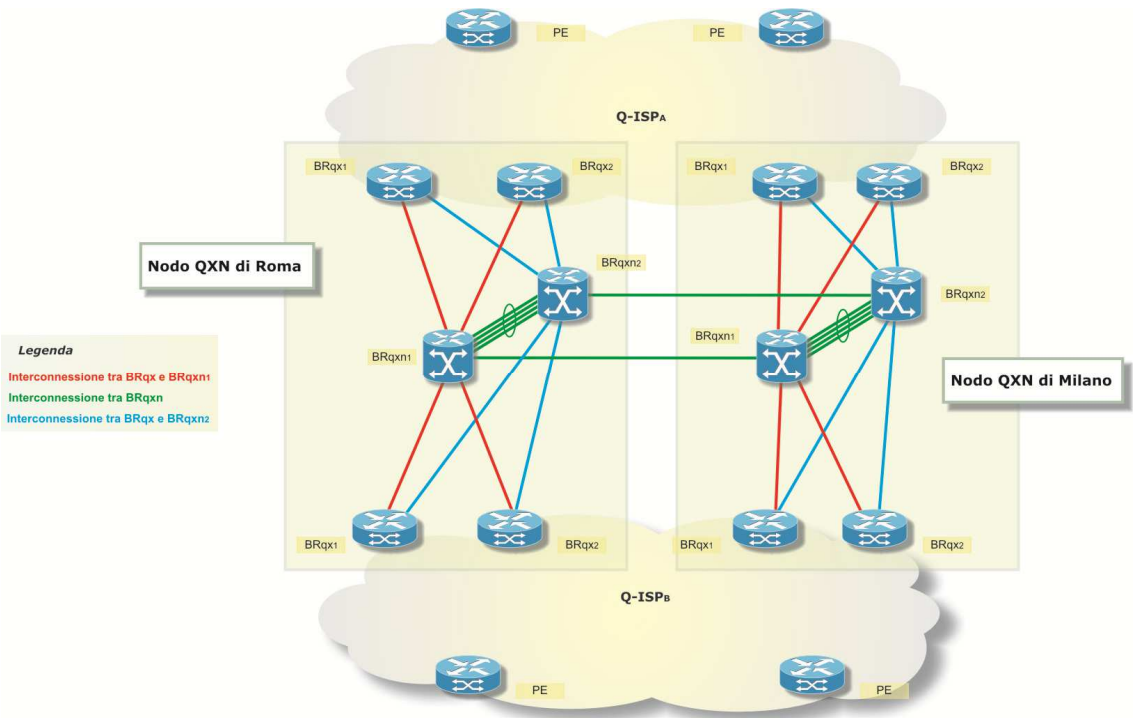


Figura 2 – Infrastruttura del backbone QXN

	Qualified Exchange Network
Specifica di Realizzazione del servizio InterC	QXN-InterC-SpecRealizzazione

1.3 Interconnessione per trasporto di traffico nativo OPA in modalità OPO tramite rete QXN (offerta 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 (FastWeb), 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 Q-ISP 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 PE o un CPE "VRF aware".

Il livello di affidabilità e ridondanza, in termini di numero di BRopo che ciascun Q-ISP può dislocare presso un nodo QXN è demandato al Q-ISP stesso, fermo restando il limite massimo di due apparati Bropo per ciascun nodo QXN.

Il BRopo di interconnessione per ciascuna VPN cliente sarà univoco su ciascun nodo QXN, perciò ciascun Q-ISP potrà essere autonomo nello 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 fornitore assegnatario SPC (BRqx con funzionalità di BRopo oppure apparato dedicato, singolo o doppio su ciascun nodo), la modalità base di interconnessione prevede che il Q-ISP interfacci la propria rete al QXN su entrambi i nodi di Roma e Milano, considerando come nodo QXN principale quello di Roma e come nodo QXN di backup quello di Milano.

Pertanto, tutto il traffico OPO scambiato tra FastWeb e ciascun fornitore assegnatario SPC sarà scambiato prioritariamente su Roma, salvo passare su Milano in caso di guasto che determini l'indisponibilità del collegamento principale.

Alternativamente, a seguito di una specifica richiesta di un fornitore assegnatario e/o aggiudicatario SPC (che dovrà essere comunque concordata con QXN e con l'altro fornitore SPC interconnesso), il traffico potrà essere scambiato prioritariamente su Milano e passare su Roma in caso di guasto del nodo definito come primario. E' comunque demandato ai fornitori aggiudicatario e assegnatario concordare le politiche di routing più opportune da impiegare all'interno del proprio Backbone IP, al fine di garantire la simmetria del traffico OPO tramite il collegamento QXN.

Su ciascun nodo QXN, l'interconnessione OPO sarà inizialmente realizzata da ciascun Q-ISP mediante un solo BRopo con due porte 1 GBE attestate alla coppia di BRqxn (sulle quali sarà bilanciato il traffico).

Qualora la banda richiesta per interconnessione tra FastWeb e il fornitore assegnatario SPC superi complessivamente la soglia di 1 Gbps, potranno essere considerate due alternative, da valutare in funzione di un'analisi di fattibilità tecnico-economica condotta congiuntamente da FastWeb, QXN ed il fornitore assegnatario SPC richiedente.

- ❑ Realizzare la banda aggiuntiva mediante incrementi di porte a 1 GBE verso ciascun BRqxn di entrambi i nodi QXN. Le porte incrementalì possono essere attestate, lato Q-ISP, sulla stessa macchina BRopo oppure su due macchine BRopo distinte, distribuendo opportunamente il traffico delle VLAN richieste, al fine di minimizzare

	Qualified Exchange Network
Specifica di Realizzazione del servizio InterC	QXN-InterC-SpecRealizzazione

la quantità di porte impiegate (con riduzione di complessità implementativa, di costi impiantistici e di esercizio). Questa soluzione non è percorribile qualora la singola VLAN associata alla VPN di una PA SPC abbia banda superiore ad 1 Gbps.

- ❑ Realizzare la banda aggiuntiva mediante porte a 10 GBE attestate su ciascun BRqxn di entrambi i nodi QXN. Tale soluzione è mandatoria qualora la singola VLAN associata alla VPN di una PA SPC abbia banda superiore a 1 Gbps.

Il paragrafo seguente descrive la soluzione che sarà adottata, per realizzare l'interconnessione tra le reti dei quattro Q-ISP membri della SC-QXN.

1.3.1 Interconnessione PE-to-PE

La soluzione rappresentata in Figura 3 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 SPC che richiedono connettività Intranet in accordo con l'offerta OPO. All'interno del backbone dei due Q-ISP le varie PA SPC saranno trattate come singole VPN (VRF o tecnologia comparabile).

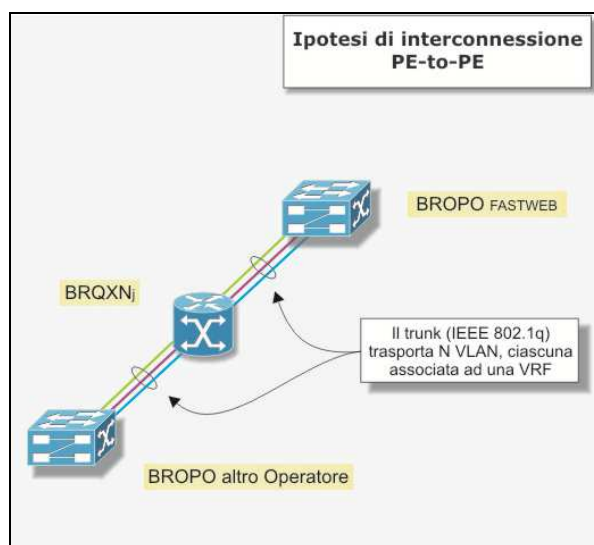


Figura 3 – Modello di interconnessione OPO PE-to-PE

L'interconnessione fisica tra i BRopo di ciascun Provider assegnatario (Wind, British Telecom, Telecom Italia) e il BRopo del Q-ISP aggiudicatario (FastWeb) 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 SPC che richiedono connettività Intranet in accordo con l'offerta OPO. L'identificativo di ciascuna VLAN (VLAN ID) viene assegnato da SC-QXN. Tale modalità di interconnessione, offre la possibilità di monitoraggio e visibilità del traffico OPO da parte CNIPA 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).

	Qualified Exchange Network
Specifica di Realizzazione del servizio InterC	QXN-InterC-SpecRealizzazione

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

La figura seguente mostra il dettaglio dell'architettura dell'interconnessione OPO dal punto di vista logico.

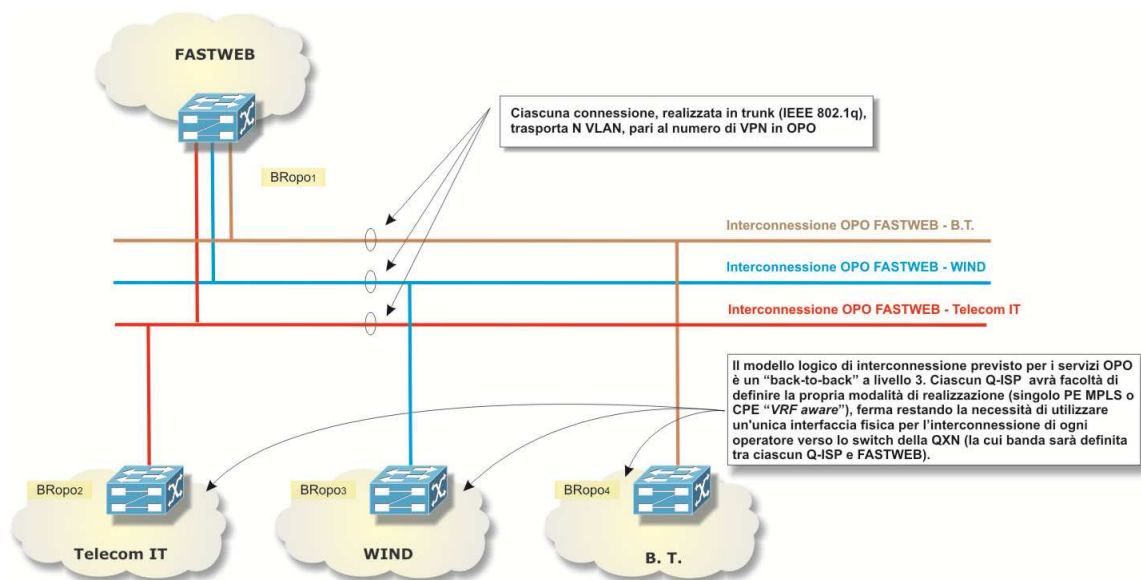


Figura 4 – Architettura logica dell'interconnessione OPO

	Qualified Exchange Network
Specifica di Realizzazione del servizio InterC	QXN-InterC-SpecRealizzazione

2. Equipaggiamento apparati del QXN

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

NOTA

Tutti gli apparati che intervengono a formare ciascun nodo, così come quelli dei vari Q-ISP, saranno dislocati in uno dei due NAP (MIX o NaMeX) e dovranno necessariamente essere alimentati in **corrente alternata** (AC 220V).

Ciascun nodo QXN è così composto:

- ❑ n° 4 x sonde per la misurazione degli SLA – Cisco 2811,
- ❑ n° 2 x BRqxn – Cisco 7609,
- ❑ n° 1 x terminal server per la gestione OOB dei dispositivi di rete - Cisco 2811,
- ❑ n° 2 x Network Intrusion Detection System & Firewall – Fortinet FG1000A,
- ❑ n° 1 x router Internet – Cisco 1801
- ❑ n. 4 server DNS Dell PE860

	Qualified Exchange Network
Specifica di Realizzazione del servizio InterC	QXN-InterC-SpecRealizzazione

2.1 ApparatI di dorsale – BRqxn

Tabella 1 – ApparatI di dorsale di ciascun nodo QXN

ID	Codice Prodotto	Descrizione	Q.tà
1	CISCO7609	7609 Chassis Bundles	1
2	7609-2SUP720XL-2PS	Cisco 7609 9-slot, Redundant System, 2 SUP720-3BXL and 2 PS	1
3	SUP720-3BXL	Supervisor Engine 720-3BXL	1
4	CF-ADAPTER-SP	SP adapter with compact flash for SUP720	1
5	MEM-C6K-CPTFL512M	Catalyst 6500 Sup720/Sup32 Compact Flash Mem 512MB	1
6	SUP720-3BXL	Supervisor Engine 720-3BXL	1
7	CF-ADAPTER-SP	SP adapter with compact flash for SUP720	1
8	MEM-C6K-CPTFL512M	Catalyst 6500 Sup720/Sup32 Compact Flash Mem 512MB	1
9	6000W-AC-INT	6000W AC PowerSupply, International (cable attached)	2
10	GLC-SX-MM	GE SFP, LC connector SX transceiver	0
11	S763AIK9-12218SXF	Cisco 7600-SUP720 IOS ADVANCED IP SERVICES SSH	1
12	WS-X6724-SFP	Catalyst 6500 24-port GigE Mod: fabric-enabled (Req. SFPs)	1
13	WS-F6700-DFC3BXL	Catalyst 6500 Dist Fwd Card- 3BXL, for WS-X67xx	1
14	GLC-SX-MM	GE SFP, LC connector SX transceiver	24
15	WS-X6724-SFP	Catalyst 6500 24-port GigE Mod: fabric-enabled (Req. SFPs)	1
16	WS-F6700-DFC3BXL	Catalyst 6500 Dist Fwd Card- 3BXL, for WS-X67xx	1
17	GLC-SX-MM	GE SFP, LC connector SX transceiver	24
18	WS-X6748-GE-TX	Cat6500 48-port 10/100/1000 GE Mod: fabric enabled, RJ-45	1

Release software: IOS (tm) s72033_rp Software (s72033_rp-ADVIPSERVICESK9_WAN-M), Version 12.2(18)SXF7, RELEASE SOFTWARE (fc1)

Nella configurazione sopra riportata sono incluse porte Ethernet per connettività in rame o in fibra.(ID: 12; 15; 18). È inoltre previsto l'impiego di schede DFC per il Forwarding del traffico distribuito sulle line card (ID: 13; 16).

L'utilizzo delle schede DFC è conseguenza dal fatto che le performance di un router Cisco basato su Sup720 dipendono, oltre che dalla capacità del processore Supervisor, dal tipo di moduli utilizzato nel sistema. In particolare, la PFC3 installata sul processore Sup720 ha una capacità di forwarding di 50Mpps. Tuttavia, se utilizzata con schede di tipo CEF720, come nel caso delle schede WS-X6724 (ID: 12; 15) e WS-X6748 (ID: 18), previste nella configurazione di tabella 1, le performance sono limitate a 30Mpps per l'intero sistema. Le caratteristiche appena descritte sono una conseguenza del fatto che la decisione di forwarding presa dalla PFC3 sulla Supervisor e il bus di comunicazione tra schede e supervisor non consente di effettuare più di 30 milioni di lookup per secondo (per traffico IPv4).

Le performance ottenute con il forwarding centralizzato sono sufficienti per garantire il throughput wire-speed di circa 20 porte GigabitEthernet. Oltre questo numero di porte è consigliato quindi installare le DFC sulle line card: con le DFC le capacità di forwarding possono arrivare a 48Mpps per line card e fino a poco meno di 400Mpps per un intero 7609 completamente equipaggiato.

	Qualified Exchange Network
Specifica di Realizzazione del servizio InterC	QXN-InterC-SpecRealizzazione

2.1.1 Motivazioni della scelta tecnologica per i Cisco 7609 come BRqxn

Il brand Cisco è leader tecnologico a livello mondiale per le soluzioni dati IP/BGP, IP/MPLS e L2 Switching. Nell'ambito dell'offerta Cisco la piattaforma Cisco 76xx si posiziona al vertice delle soluzioni tecnologiche commercializzate ed è quindi oggetto di continui sviluppi di nuove funzionalità che ne garantiscono la continuità tecnologica necessaria per l'applicazione della rete QXN.

L'apparato Cisco 7609 supporta in un'unica piattaforma le funzioni di IP/BGP (necessarie per la gestione del traffico OPA) e di L2 Switching (necessarie per la gestione del traffico OPO), prevedendo porte di tipo ottico (a 1 e a 10 Gbps) ed elettrico (FE 10/100/1000 Mbps) per l'interconnessione con apparati degli altri Q-ISP e per l'attestazione di altri sistemi (management, sicurezza, DNS, NTP, etc).

La macchina, nel suo equipaggiamento massimo, è in grado di garantire una capacità di forwarding pari a 400 Mpps.

L'impiego di una piattaforma con funzionalità di IP/BGP e Multilayer Switching integrate, consente di ottimizzare i costi della soluzione (di fornitura ed esercizio), garantendo le prestazioni richieste.

Il dimensionamento proposto per gli apparati Cisco 7609 è funzione dell'attuale visibilità delle esigenze di traffico OPA e OPO comunicata dagli attuali Q-ISP.

Ciascun BR-QXN è attualmente equipaggiato con:

- ❑ 48 porte Gigabit Ethernet ottiche (di cui 23 già utilizzate) su 2 schede WS-X6724-SFP
- ❑ 48 porte 10/100/1000 Ethernet rame (di cui 11 già utilizzate) su una scheda WS-X6748-GE-TX

Sono inoltre disponibili ulteriori 4 slot di espansione che possono ospitare le seguenti tipologia di Line Card:

- ❑ WS-X6748-GE-TX 48 porte 10/100/1000 Ethernet rame
- ❑ WS-X6724-SFP 24 porte Gigabit Ethernet ottiche
- ❑ 7600-SIP-600 (con 2 porte ottiche a 2,5Gb o in alternativa 1 porta ottica a 10Gb)

Tale dimensionamento garantisce la copertura delle esigenze di traffico stimate dai Q-ISP SPC per almeno i prossimi 2-3 anni di esercizio, essendo comunque garantita la loro scalabilità in funzione della crescita del traffico che sarà rilevata sul campo.

Esiste un'ampia base installata di apparati della famiglia Cisco 76xx (di cui fa parte il 7609) sulla rete dei principali operatori TLC a livello nazionale ed internazionale, il che fornisce ampie garanzie di affidabilità, gestibilità ed esercibilità degli stessi. Sulla rete FastWeb, ad esempio, sono attualmente installate circa 50 macchine di questo tipo, utilizzate come nodi della rete di backbone IP.

	Qualified Exchange Network
Specifica di Realizzazione del servizio InterC	QXN-InterC-SpecRealizzazione

2.2 Terminal server per la gestione OOB

Tabella 2 – Terminal server per gestione OOB (Cisco 2811)

ID	Codice Prodotto	Descrizione	Q.tà
1	CISCO2811-V/K9	2811 Voice Bundle,PVDM2-16,SP Serv,64F/256D	1
2	Included: S28NSPSK9-12403	Cisco 2800 SP SERVICES	1
3	NM-16A	16 port Asynchronous Module	1
4	CAB-OCTAL-ASYNC	8 Lead Octal Cable (68 pin to 8 Male RJ-45s)	1
5	Included: PVDM2-16	16-Channel Packet Voice/Fax DSP Module	1
6	Included: MEM2800-256D-INC	256MB DDR DRAM Memory factory default for the Cisco 2800	1
7	Included: MEM2800-64CF-INC	64MB CF default for Cisco 2800 Series	1
8	CAB-ACE	Power Cord Europe	1

Release software: c2800nm-spservicesk9-mz.12.4-9.T

2.3 Firewall

Gli apparati previsti a protezione del QXN, con funzionalità di firewalling e Network IDS integrate, sono una coppia di Fortinet Fortigate 1000A, equipaggiati come segue:

- ❑ 10 interfacce 10/100/1000 (UTP).

2.4 Sonde per la misurazione degli SLA

Tabella 3 – Sonde per QXN (Cisco 2811)

ID	Codice Prodotto	Descrizione	Q.tà
1	CISCO2811-V/K9	2811 Voice Bundle,PVDM2-16,SP Serv,64F/256D	1
2	S28NSPSK9-12403	Cisco 2800 SP SERVICES	1
3	PVDM2-16	16-Channel Packet Voice/Fax DSP Module	1
4	MEM2800-256D-INC	256MB DDR DRAM Memory factory default for the Cisco 2800	1
5	MEM2800-64CF-INC	64MB CF default for Cisco 2800 Series	1
6	CAB-ACE	Power Cord Europe	1

Release software: c2800nm-spservicesk9-mz.12.4-9T

2.5 Firewall/Network Intrusion Detection System

In ciascun nodo QXN sono presenti due macchine con funzioni di firewalling e di NIDS sulle connessioni verso reti ritenute “non trusted” (link vs. NOC e SOC, link Internet). Ciascuna macchina ha il seguente equipaggiamento/caratteristiche:

Firewall/NIDS: Fortinet FG 1000A

ID	Codice Prodotto	Descrizione	
1	FORTINET FG 1000A	10/100/1000 Base-T (Copper): 10 FortiAccess SFP ports: 2 Modem ports: 1 USB ports: 1 Console: 1	

	Qualified Exchange Network
Specifica di Realizzazione del servizio InterC	QXN-InterC-SpecRealizzazione

ID	Codice Prodotto	Descrizione	
		Concurrent sessions: 600K News sessions/second: 15K Firewall throughput (Gbps): 2 168 bit 3-DES throughput (Mbps): 250 Users: Unrestricted Policies:30K Schedules: 256 Virtual domains (NAT/Transparent Mode): 2/10 Dedicated tunnels: 5000 Protection Profiles: 200	

2.6 Router di accesso Internet

In ciascun nodo QXN è presente un accesso Internet 2 Mbps terminato su un router con le seguenti caratteristiche:

Router Internet: Cisco 1801/K9

ID	Codice Prodotto	Descrizione	Q.ta
1	Cisco 1801/K9	ADSL/POTS Router with Firewall/IDS and IPSec 3 DES	1
2	S180AESK9-12402XA	Cisco 180x Series IOS ADV. ENTERPRISE SERVICES	1
3	CAB-ACE	Power Cord	1

2.7 Server DNS

In ciascun nodo QXN è presente un cluster costituito da quattro server DNS, tra loro identici, ciascuno con le seguenti caratteristiche:

ID	Codice Prodotto	Descrizione
	Server DELL PowerEdge 860	Processore Intel Xeon Dual Core 3060, 2,4 GHz S.O. RedHat Linux Enterprise 4 (upd. 5) - 64 bit 2GB RAM 2x80GB HD RAID 1 4 porte Ethernet 10/100/1000 n. 1 interf. Management remoto

2.8 Indirizzamento IP nella rete QXN

La rete del QXN è dotata di un proprio range di IP pubblici di tipo “Provider Independent” (**195.3.160.0 - 195.3.163.255**) e di un proprio ASn (**AS-41407**), entrambi assegnati da RIPE. Gli indirizzi IP pubblici assegnati dal RIPE alla QXN verranno utilizzati per numerare le interfacce di gestione (es. Loopback) e di collegamento (es. point-to-point) degli apparati che compongono la rete QXN.

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.

	Qualified Exchange Network
Specifica di Realizzazione del servizio InterC	QXN-InterC-SpecRealizzazione

2.9 Instradamento del traffico Infranet nativo OPA

Alla PA SPC che richiede un servizio di connettività Infranet OPA, il Q-ISP fornisce una subnet di indirizzi IP pubblici (di seguito indicata come SUBNET INFRANET OPA): tale Subnet è prelevata da un pool di indirizzi (di seguito POOL INFRANET OPA) appartenenti allo spazio di indirizzamento assegnato dal RIPE al Q-ISP e che quest'ultimo riserva per i servizi Infranet richiesti dalle PA SPC clienti.

Il traffico Infranet nativo OPA scambiato tra due PA SPC sarà, quindi, solo e soltanto quello scambiato tra un indirizzo IP sorgente ed un indirizzo IP destinazione appartenenti alle Subnet Infranet OPA delle due PA.

Se le due PA SPC afferiscono al medesimo Q-ISP, il traffico Infranet nativo OPA rimarrà confinato nella rete del Q-ISP stesso.

Se, invece, le due PA SPC afferiscono a Q-ISP differenti, il traffico Infranet nativo OPA attraverserà la QXN transitando, in via preferenziale, per uno dei due nodi di Roma o Milano. A tale scopo, ciascun Q-ISP deve annunciare ai BRqxn il proprio ASn ed esclusivamente le Subnet Infranet OPA delle PA SPC connesse alla propria rete. All'interno dell'infrastruttura QXN il suddetto traffico sarà bilanciato sui BRqxn che attraversa: due o quattro, a seconda che i BRqx di destinazione siano raggiungibili sul nodo locale o remoto rispetto al BRqx di uscita.

2.10 Soluzioni di routing per l'instradamento del traffico nella rete QXN

Il presente paragrafo e i successivi sottoparagrafi forniscono le linee guida che dovranno essere seguite per la realizzazione del QXN, per quanto concerne la scelta delle politiche di instradamento delle varie tipologie di traffico che attraversano il QXN medesimo.

Per il traffico di tipo Infranet (OPA) i BRqxn agiscono a livello 3 della pila ISO/OSI.

Gli annunci del Q-ISP verso la QXN non devono avere netmask superiore a 24 bit, garantendo comunque il massimo grado di aggregazione.

L'OSPF è il protocollo di routing IGP adottato dai quattro apparati del QXN (BRqxn). Non è previsto l'uso di aree OSPF diverse dall'area di Backbone.

I quattro apparati della dorsale QXN (BRqxn) sono configurati in modalità fully-meshed con sessioni I-BGPv.4 (vedi figura seguente).

Gli apparati del QXN (BRqxn) avranno una sessione E-BGP v.4 con i BRqx dei vari Q-ISP. Ciascun Q-ISP si presenta verso il QXN con il proprio ASn. L'ASn della rete QXN risulta quindi l'Autonomous System di transito per il traffico tra PA SPC connesse a due Q-ISP differenti.

Per garantire la sicurezza ed autenticità degli annunci scambiati tra i 4 BRqxn e tra questi e i BRqx dei Q-ISP, è previsto l'impiego della funzione di hash MD-5 per l'autenticazione dei pacchetti, attivata sui protocolli di routing BGPv4 e OSPF.

	Qualified Exchange Network
Specifica di Realizzazione del servizio InterC	QXN-InterC-SpecRealizzazione

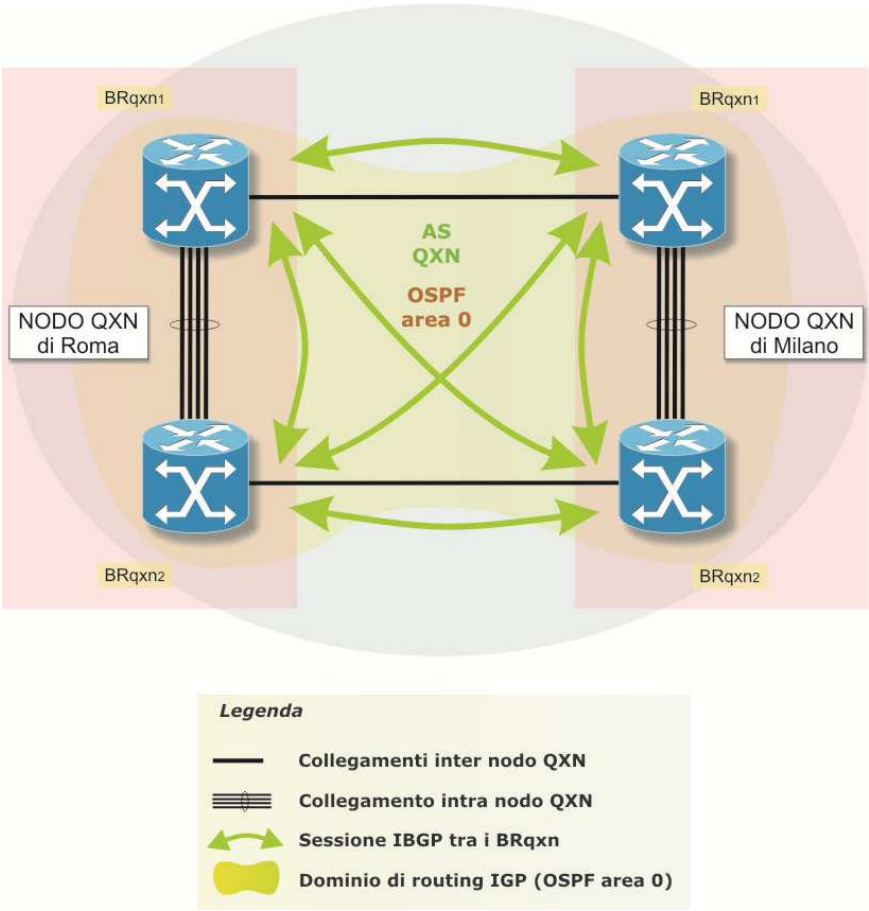


Figura 5 – Soluzioni di routing sul backbone QXN

2.10.1 Soluzioni di routing per il bilanciamento del traffico Infranet OPA

Al fine di garantire il rispetto degli SLA, il requisito di bilanciamento e rendendo la soluzione affidabile, a fronte di eventi che determinino l’indisponibilità di uno o più link di interconnessione tra la rete del Q-ISP (BRqx) e il QXN (BRqxn), fino a contemplare la completa indisponibilità di un nodo QXN, è prevista su ciascun dei quattro BRqxn la configurazione della funzionalità di E-BGP multipath. La stessa funzionalità deve essere inoltre implementata nelle sessioni E-BGP tra i BRqx e la coppia BRqxn.

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. Mentre per determinare univocamente verso quale BRqx debba essere instradato il traffico proveniente dalla rete QXN (originato dalle PA SPC afferenti agli altri Provider), i BRqx di ciascun Q-ISP devono annunciare i propri aggregati con communities diverse.

Il bilanciamento sul QXN avviene per sessione (identificata dalla coppia IP sorgente e IP destinazione), ciascuna delle quali segue uno dei due percorsi disponibili (BRqx_i del Q-ISP_A – BRqxn_j – BRqx_i del Q-ISP_B), in modo da distribuire il carico in maniera equivalente all’interno del nodo QXN e garantire il rispetto degli SLA anche in caso di guasto di un link tra BRqx e BRqxn o di un BRqxn stesso.

	Qualified Exchange Network
Specifica di Realizzazione del servizio InterC	QXN-InterC-SpecRealizzazione

Il bilanciamento del traffico delle singole PA SPC all'interno del backbone dei diversi Q-ISP assegnatari è demandato alle politiche di routing dello stesso operatore qualificato. Esistono due ipotesi:

- ❑ Il Q-ISP definisce il BRqx gateway per il traffico OPA diretto verso le PA SPC degli altri Provider (influenza solo il traffico interno al Provider).
- ❑ Realizzare il bilanciamento di tale traffico anche sulla coppia di BRqx del Provider.

Ciascun Q-ISP deve garantire l'implementazione almeno della prima soluzione (bilanciamento sul QXN), mentre la seconda soluzione (bilanciamento completo anche sul backbone del Provider) è opzionale e non vincolante per il Q-ISP.¹

2.10.2 Soluzioni di routing per il bilanciamento del traffico OPO

L'instradamento del traffico OPO verso il nodo principale è regolato mediante politiche di routing che prevedono l'uso di attributi BGP. All'interno del nodo QXN, il traffico di ciascuna VRF (VPN Intranet in OPO) è bilanciato su entrambi i BRqxn (a livello 2) mediante due sessioni EBGP instaurate tra il BRqx di FastWeb e quello dell'altro Q-ISP. Per garantire il bilanciamento, è necessario attivare la funzionalità EBGP multipath sui BRqx di entrambi i Q-ISP.

2.10.3 Soluzioni di routing per la simmetria del traffico Infranet nativo OPA

Al fine di rispettare il requisito di simmetria del traffico OPA, ciascun Q-ISP garantisce che il traffico generato da/diretto 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 illustrato nella figura che segue.

¹. Tale soluzione, peraltro, richiede l'attivazione di una serie di funzionalità di seguito esposte:

- ❑ è necessario che entrambi i BRqx propaghino le informazioni di raggiungibilità ricevute dai due BRqxn in maniera identica (medesimi attributi BGP) verso i PE remoti;
- ❑ ipotizzando che l'accesso al QXN per il traffico OPA sia realizzato da ciascun Q-ISP mediante una VPN MPLS (implica l'utilizzo del protocollo M-BGP all'interno del backbone di ciascun Provider), il bilanciamento completo presenta i seguenti requisiti:
 - ↳ attivazione delle funzionalità di IBGP multipath a livello di M-BGP su tutti i PE del Provider sui quali è configurata la VRF "QXN",
 - ↳ attivazione della funzionalità che consente l'import multiplo, all'interno della VRF "QXN" della medesima informazione IPv4 propagata da entrambi i BRqx ("maximum-paths import" o equivalente su tecnologia diversa da Cisco)

	Qualified Exchange Network
Specifica di Realizzazione del servizio InterC	QXN-InterC-SpecRealizzazione

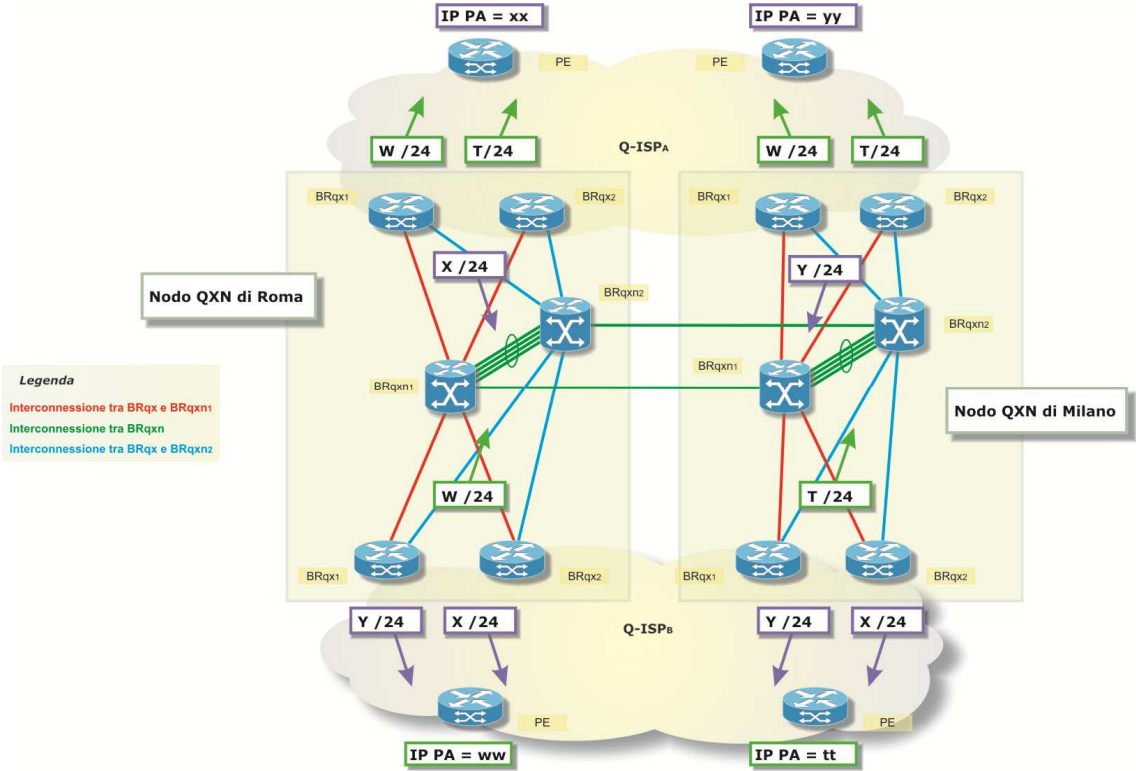


Figura 6 – Instradamento simmetrico del traffico sul QXN

Le reti W a T sono propagate dal Q-ISP_A in maniera preferita, rispettivamente sui nodi QXN di Roma e Milano. Analogamente, le reti X a Y sono propagate dal Q-ISP_B in maniera preferita, rispettivamente sui nodi QXN di Roma e Milano.

Il BRqx gateway per ciascuna PA SPC, all’interno della rete del generico Q-ISP_B, è il medesimo che ne propaga la raggiungibilità verso il QXN.

Per determinare univocamente verso quale BRqx debba essere instradato il traffico proveniente dalla rete QXN (originato dalle PA SPC afferenti agli altri Provider), i BRqx di ciascun Q-ISP devono annunciare i propri aggregati con communities diverse, determinandone univocamente il percorso preferenziale.

Le community sono quindi attributi associati ai diversi prefissi BGP e annunciati dai vari Q-ISP mediate le sessioni E-BGP con il QXN. L’uso delle communities BGP è obbligatorio e pertanto l’eventuale prefisso BGP sprovvisto di communities viene scartato dagli apparati della QXN. Tale metodologia dovrà essere univocamente utilizzata dai Q-ISP per propagare le informazioni di raggiungibilità delle proprie PA SPC verso il QXN, mentre, pur rappresentando una valida soluzione, non è vincolante sulla rete del singolo Operatore, lasciando a quest’ultimo la facoltà di optare per la soluzione a lui più congeniale, purché questa rispetti il vincolo di simmetria del traffico sul QXN.

Le communities utilizzate all’interno dei nodi QXN dovranno seguire il seguente formato: **ASn_QXN:nnn**

I Q-ISP avranno visibilità delle communities associate agli annunci provenienti dagli altri Q-ISP tramite QXN, poiché quest’ultimo girerà senza modificare le communities BGP ricevute. Gli stessi Q-ISP comunque non saranno tenuti a propagare

	Qualified Exchange Network
Specifica di Realizzazione del servizio InterC	QXN-InterC-SpecRealizzazione

obbligatoriamente le communities ricevuti dagli apparati del QXN all'interno del proprio Backbone IP.

Le communities definite per il QXN saranno di due tipi: Decisionali e Informative.

1) Community di tipo “decisionale”:

La community di tipo decisionale ha la funzione di determinare la priorità dei collegamenti dei vari Q-ISP al fine di dare indicazione del percorso preferenziale per il traffico di una specifica PA SPC attraverso il QXN.

La community decisionale è pertanto indispensabile per garantire la simmetria del traffico all'interno della rete QXN.

La community decisionale ha il seguente formato: **ASn_QXN:LP**

Dove:

- ❑ ASn_QXN corrisponde all'AS number del QXN (AS 41407).
- ❑ LP corrisponde al valore della Local Preference settata all'interno del QXN per l'annuncio specifico (LP = 130; LP = 120; LP = 110).

1. community **41407:130** = Setta la LP a 130 all'interno del QXN
2. community **41407:120** = Setta la LP a 120 all'interno del QXN
3. community **41407:110** = Setta la LP a 110 all'interno del QXN
4. community **41407:100** = Setta la LP a 100 all'interno del QXN
5. **no community** = no import: DROP del traffico

2) Community di tipo “informativo”:

La community di tipo informativo ha la funzione di determinare l'origine dell'annuncio E-BGP ricevuto dal QXN.

La community informativa ha la funzione di fornire informazioni e quindi agevolare il debugging all'interno della rete del Q-ISP e del QXN.

La community informativa ha il seguente formato: **ASn_QXN:yyx**

Non deve essere preclusa dai vari Q-ISP l'ipotesi che in futuro siano definite ulteriori communities del tipo: “ASn_QXN:nnnnn” per caratterizzare gli annunci BGP.

2.10.4 Soluzioni di routing per la simmetria del traffico OPO

L'interconnessione attraverso il QXN deve essere configurata in modo che il traffico OPO scambiato tra la rete del Q-ISP assegnatario e quella del fornitore aggiudicatario (Fastweb), 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

	Qualified Exchange Network
Specifica di Realizzazione del servizio InterC	QXN-InterC-SpecRealizzazione

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".

2.10.5 Resilienza dell'instradamento del traffico Infranet OPA a fronte di uno o più fault

Il presente sottoparagrafo analizza il comportamento del routing a fronte dei possibili scenari di fault, cui è soggetta l'infrastruttura di rete del QXN ed il cui impatto abbia ripercussioni sul traffico Infranet OPA.

- ❑ **In condizione di funzionamento normale**, ciascun nodo QXN funge da master per un pool di reti (aggregati /24 o meno specifici) e da backup o eventualmente Disaster Recovery per altre. La scelta per l'instradamento verso il nodo corretto sarà regolata mediante l'impostazione delle communities BGP predefinite, dai BRqx verso i BRqxn, in modo da consentire a questi ultimi di effettuare la decisione di instradamento mediante Local-Preference associata a tali communities.

Il traffico proveniente da ciascun Q-ISP è bilanciato dai BRqx verso entrambi i BRqxn, i quali, lo instradano verso il BRqx di destinazione.

- ❑ In caso di **indisponibilità dell'intero nodo QXN principale**, tutto il traffico Infranet, tra due o più PA SPC afferenti a Q-ISP differenti, passa sul nodo QXN secondario. Il reinstradamento del traffico è soggetto ai tempi di convergenza dei backbone di ciascun Provider.
- ❑ A fronte del **guasto di entrambi i BRqx del Q-ISP_A afferenti al nodo QXN principale**, il traffico in uscita dal Q-ISP_A, previa riconvergenza del routing BGP Intra-Provider, è reinstradato verso i BRqx attestati al nodo QXN di backup e, da questi, è bilanciato verso la coppia di BRqxn.

Il traffico in uscita dagli altri Q-ISP, destinato alle PA assegnate al Q-ISP_A, segue il percorso normale fino alla coppia di BRqxn del nodo principale, in funzione della soluzione di bilanciamento Intra-Provider scelta; da questi, è instradato verso la coppia di BRqxn sul nodo di backup, i quali lo inoltrano sul BRqx di destinazione.

- ❑ Qualora si **guasti un solo BRqxn**, il traffico viene instradato dai BRqx verso l'altro BRqxn, senza alcuna riconvergenza sul backbone dei Provider.
- ❑ A fronte di un **guasto di un BRqx del Q-ISP_A**, solo il traffico in uscita dal Q-ISP_A, per il quale il BRqx guasto è il gateway principale, è affetto dal disservizio. Tale traffico, previa riconvergenza del routing BGP Intra-Provider, è reinstradato sull'altro BRqx del Q-ISP_A e da questo è bilanciato sulla coppia di BRqxn, i quali, inoltrano sul BRqx di destinazione.
- ❑ In seguito al **guasto di un link tra il BRqx del Q-ISP_A e un BRqxn**, il traffico in uscita dal Q-ISP_A, che attraversa il BRqx affetto dal disservizio, è instradato solo verso il BRqxn raggiungibile, senza alcuna riconvergenza; il traffico in uscita dal Q-ISP_A, che attraversa l'altro BRqx, non è in alcun modo affetto da tale disservizio.
- ❑ A fronte di un **guasto contemporaneo del BRqx del Q-ISP_A e di un BRqxn sul medesimo nodo**, il traffico viene instradato dai PE remoti del Q-ISP_A verso l'unico BRqx ancora disponibile, senza alcuna riconvergenza, e da questo verso l'unico

	Qualified Exchange Network
Specifica di Realizzazione del servizio InterC	QXN-InterC-SpecRealizzazione

BRqxn disponibile, il quale, a sua volta, lo bilancia su entrambi i BRqx del Q-ISP di destinazione.

2.10.6 Resilienza dell'instradamento del traffico OPO a fronte di uno o più fault

Il presente sottoparagrafo analizza il comportamento del routing a fronte dei possibili scenari di fault, cui è soggetta l'infrastruttura di rete del QXN ed il cui impatto abbia ripercussioni sul traffico OPO.

- ❑ In **condizione di funzionamento normale**, ciascun BRopo presso un nodo di interconnessione (nodo primario Roma, nodo backup Milano) funge da backup e/o Disaster Recovery rispetto all'altro, in modo da distribuire il numero di PA (VRF o soluzione equivalente, ciascuna mappata su una apposita VLAN) sui 2 o 4 BRqx. L'instradamento del traffico OPO verso il nodo principale è regolato mediante politiche di routing che prevedono l'uso di attributi BGP.

All'interno del nodo QXN, il traffico di ciascuna VRF (VPN Intranet in OPO) è bilanciato su entrambi i BRqxn (a livello 2) mediante due sessioni EBGp instaurate tra il BRqx di FastWeb e quello dell'altro Q-ISP. Per garantire il bilanciamento, è necessario attivare la funzionalità EBGp multipath sui BRqx di entrambi i Q-ISP.

- ❑ In caso di **indisponibilità del BRqx di FastWeb con funzionalità di BRopo**, solo il traffico dei Q-ISP che utilizzano tale BRopo è affetto dal disservizio; tale traffico, previa riconvergenza del routing BGP Intra-Provider, è reinstradato da ciascun Q-ISP verso i rispettivi BRopo del nodo di backup.
- ❑ A fronte del **guasto di un BRopo del generico Q-ISP_A**, il traffico, previa riconvergenza del routing BGP Intra-Provider, è reinstradato da FastWeb e dal Q-ISP_A verso il corrispondente BRopo del nodo di backup.
- ❑ Qualora si **guasti un solo BRqxn sul nodo QXN principale**, il traffico, senza alcuna riconvergenza sul backbone del provider, è inoltrato solo al rimanente BRqxn del nodo stesso.
- ❑ In seguito al **guasto di un link tra il BRopo del Q-ISP_A e un BRqxn sul nodo QXN principale**, il traffico, previa riconvergenza del routing BGP Intra-QXN, è inoltrato solo al rimanente BRqxn del nodo. In futuro sarà possibile valutare l'introduzione della funzionalità di Bidirectional Forwarding Detection (BFD), tramite la quale il BRqx non affetto dalla rottura del link sarebbe in grado di rilevare il fault remoto entro 500 ms, inoltrando il traffico, senza alcuna riconvergenza, solo verso il rimanente BRqxn del nodo.
- ❑ In caso di **indisponibilità dell'intero nodo QXN principale (guasto di entrambi i BRqxn)**, tutto il traffico OPO che utilizza normalmente tale nodo, previa riconvergenza del routing BGP Intra-Provider, è reinstradato dai Q-ISP verso i rispettivi BRopo del nodo di backup.

2.11 Servizi di QoS

Sul backbone QXN saranno implementate le opportune tecniche di QoS, per garantire il rispetto degli SLA indicati nella Tabella 6, relativamente al traffico OPO (tutto) e OPA, quest'ultimo scambiato tra due PA connesse al QXN mediante le reti di due Q-ISP differenti.

	Qualified Exchange Network
Specifica di Realizzazione del servizio InterC	QXN-InterC-SpecRealizzazione

Al fine di semplificare ed ottimizzare la soluzione di QoS, è necessario che i Q-ISP “colorino” in maniera univoca il traffico, prima di inoltrarlo verso i BRqxn.

Ciò consentirà ai nodi di core del sistema (i BRqxn) di classificare ed accodare in maniera snella ed efficiente il traffico ricevuto dai BRqx, in base alla marcatura assegnata da questi ultimi (TOS/DSCP), senza peraltro modificarla (funzionalità di DSCP trust applicata in ingresso su tutte le interfacce).

La Tabella 4 indica i parametri di TOS/DSCP che dovranno essere univocamente adottati dai Q-ISP, per associare ciascuna tipologia di traffico OPO e OPA alla rispettiva Classe di Servizio (CdS), prima di consegnare il traffico ai BRqxn.

In caso di ricezione di valori diversi da quelli indicati in tabella, la QXN marcherà i pacchetti come relativi alla CdS Best Effort, ponendo il valore DSCP=0.

Tabella 4 – Classificazione del traffico in base al TOS/DSCP

Classificazione del traffico	Marcatura mediante TOS	Marcatura mediante DSCP
Real Time	TOS 4	AF 41
Mission Critical	TOS 3	AF 31
Streaming	TOS 2	AF 21
Best Effort	TOS 0	0

2.12 Servizio di erogazione del tempo ufficiale di rete (NTP)

L’architettura QXN deve prevedere la presenza di un proprio server NTP per la generazione del tempo ufficiale di rete. Tale funzionalità sarà assolta direttamente dai BRqxn, 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, ciascuna coppia di BRqxn renderà disponibile il Tempo Ufficiale di Rete (TUR), attraverso un indirizzo HSRP configurato su una LAN privata (ruotata verso i Q-ISP), fornendo, di fatto, un NTP server 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 deve essere configurato come NTP server primario e secondario sui propri apparati di rete che fungono da client del servizio.

La presenza di una coppia di Firewall, configurati in Alta Affidabilità e con funzioni di NIDS, sulla LAN verso il router Internet ha lo scopo di isolare l’ambiente QXN, ritenuto di per se affidabile, da una rete intrinsecamente “non trusted” qual’è appunto Internet.

2.13 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

	Qualified Exchange Network
Specifica di Realizzazione del servizio InterC	QXN-InterC-SpecRealizzazione

sistema DNS di assolvere a tale funzione è necessario garantirne l'accesso ad Internet protetto da un opportuno sistema di firewalling (il medesimo già previsto per la sincronizzazione del tempo ufficiale di rete).

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 4 server in bilanciamento tra loro, raggiungibili mediante un Virtual IP address (VIP). Sarà facoltà di ciascun Q-ISP scegliere il cluster primario e quello secondario (instradando verso il VIP preferito le richieste DNS).

2.14 Monitoring e gestione della rete QXN

Mediante VPN dedicate sarà garantito il collegamento per la gestione in banda di tutti gli apparati che compongono la rete del QXN dai due centri NOC e SOC preposti. Oltre alla sudetta gestione in-band, per i dispositivi di rete (BRqxn e sonde) è previsto un accesso out-of-band (OOB), mediante un terminal server, direttamente collegato alla porta console di ciascun apparato. La gestione OOB può rivelarsi fondamentale, sia in situazioni critiche di troubleshooting, a fronte di comportamenti non previsti di un apparato, sia per effettuare operazione di maintenance straordinaria, quali il software upgrade, che necessitano l'accesso alla console del dispositivo.

Oltre alla gestione degli apparati e alla verifica della normale operatività della rete QXN è previsto un sistema di sonde, posizionate nei PAS di 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 saà attestata una saonda 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 al documento specifico "QXN-InterC-Specifica Controllo x.y".