SYMBEEO

PUBLIC

DESIGN STUDY

# Carrier-grade peering and edge routing for a regional service provider

Complete design on current platforms

| CAPABILITY | INDUSTRY | SETTING |
| --- | --- | --- |
| Networking | Global Service Providers | Regional service provider |
| **DOCUMENT** | **VERSION** | **DATE** |
| NET-005 | 1.3 | Oct 10, 2026 |

WRITTEN BY

**Mark Winston**, Principal Network Architect



© 2026 Symbeeo. All rights reserved.

## Document control

| | | | |
|---|---|---|---|
| Document | NET-005 | Version | 1.3 |
| Issued | Oct 10, 2026 | Status | Issued by Symbeeo |
| Classification | Public | Supersedes | 1.2, Sep 27, 2026 |
| Capability | Networking | Industry | Global Service Providers |
| Author | Mark Winston | Role | Principal Network Architect |
| Credentials | CCIE, CISSP, CCSP, CCISO, CISM, Adopting Zero Trust (Forrester) | | |
| Approval | Approved by Edwin Ozer, Founder, Oct 10, 2026. Issued by Symbeeo, Oct 10, 2026. Design study: every figure is vendor-published, a design target or a marked assumption. | | |
| Sign-off | "An engagement under this design is signed by the practice lead before any build proceeds." | | |

## Contents

1 · Scope 3
1c · Public implementations this design follows 4
2 · Requirements register 4
3 · Architecture overview 5
4 · Design by subsystem 6
5 · Failure behavior 7
6 · Limits 7
7 · Lessons learned 7
8 · The author 8

© 2026 Symbeeo. All rights reserved. · Public

CONVENTIONS

**Source tags.** [S] figure read from the vendor's own current page on Sep 18, 2026 · [S*] figure from the vendor's page summary where the page itself could not be opened · [A] design assumption, to be confirmed by the signing engineer · [T] design target: the record's outcome figure and anything derived from it. No figure comes from any engagement, file or asset. A row with more than one tag is counted once: as a published figure if any tag is [S] or [S*], otherwise as an assumption if any tag is [A], otherwise as a design target.

**Table 1.** Revision history

| Date | Version | Change |
|---|---|---|
| Sep 18, 2026 | 1.0 | First issue. |
| Sep 20, 2026 | 1.1 | Public implementations added; figures reconciled with published sources. |
| Sep 27, 2026 | 1.2 | Figures and platform details rechecked against published sources. |
| Oct 10, 2026 | 1.3 | Approval line now reads: approved by the Founder, issued by Symbeeo. Mark Winston remains the author. |

## 1 · Scope

**Who it is for.** The head of network engineering of a regional service provider whose peering edge is at 100G on a platform past its software support date, who needs 400G ports, RPKI on every external session, and encryption on the links between its two sites.

**Typical buyer [A].** A regional service provider with 200,000 subscribers, two points of presence 30 km apart, one internet exchange in the metro, two upstream transit providers, and roughly 40 direct peers. Peak outbound-to-subscriber traffic 600 Gbps, growing 25 % a year.

**What is in.** Two peering edge routers, the inter-site links with MACsec, RPKI validation, BGP policy structure, and the interfaces to the exchange and transits. **What is out.** The subscriber aggregation and BNG layer; the optical transport between sites (assumed leased wavelengths, [A]); DDoS scrubbing (the edge exports flow telemetry to it; the scrubber is someone else's design).

**Assumptions.** Juniper carries the peering edge [A]; Cisco carries the core-facing router at each site, so that the two-vendor arrangement the operator already runs is kept [A]. Four 400G wavelengths between sites, two for the peering edges and two for the core-facing routers, on diverse paths [A]. RPKI validator software is run in-house on two servers [A].

**Related documents, read Sep 18, 2026.**

- Juniper PTX10002-36QDD fixed configuration router datasheet — https://www.juniper.net/us/en/products/routers/ptx-series/ptx10002-fixed-configuration-packet-transport-routers-datasheet.html
- Juniper Junos OS, BGP Origin Validation — https://www.juniper.net/documentation/us/en/software/junos/bgp/topics/topic-map/bgp_origin_validation.html
- Cisco 8200 Series Routers data sheet — https://www.cisco.com/c/en/us/products/collateral/routers/8000-series-routers/8200-series-routers-ds.html
- NIST SP 1800-14, Protecting the Integrity of Internet Routing: BGP Route Origin Validation (Jun 28, 2019), read Sep 20, 2026 — https://csrc.nist.gov/pubs/sp/1800/14/final

© 2026 Symbeeo. All rights reserved. · Public

- NIST SP 1800-14B, Volume B: Approach, Architecture, and Security Characteristics (June 2019), read Sep 20, 2026 — https://www.nccoe.nist.gov/publication/1800-14/VolB/index.html
- Juniper Validated Design, Metro Ethernet Business Services with Updated Platform Recommendations (JVD-METRO-EBS-03-03, v1.0, May 9, 2025), read Sep 20, 2026 — https://www.juniper.net/documentation/us/en/software/jvd/metro-ethernet-business-services-with-updated-platform-recommendations.pdf

## 1c · Public implementations this design follows

Deployment rows are real public deployments, each dated. Where no public deployment matches, the row is Vendor documentation: the vendor's document that this design, Symbeeo's own, is built on.

**Table 2.** Public implementations this design follows

| Implementation | Who published it · date | What it settles for this design | URL |
|---|---|---|---|
| **Vendor documentation.** NIST SP 1800-14, BGP Route Origin Validation practice guide (Volume B) | NIST NCCoE · Jun 28, 2019 (Vol. B June 2019) | A built reference with Juniper MX and Cisco routers doing origin validation from two independent validators (RIPE NCC Validator and the rpki.net toolkit) over RPKI-to-router (RFC 6810, RFC 8210); the action on valid, invalid and not-found routes is local policy — the R7/R8 pattern of two validator sessions and an explicit reject-invalid policy | https://www.nccoe.nist.gov/publication/1800-14/VolB/index.html |
| **Vendor documentation.** Metro Ethernet Business Services with Updated Platform Recommendations, JVD-METRO-EBS-03-03 | Juniper · v1.0, May 9, 2025 | Scale figures in Table 2 (Scale Numbers for the Devices Under Test) — about 1.2M RIB and about 966k FIB routes — belong to the MX10004 device under test (MSE2); the fixed PTX10001-36MR appears only as a helper node, with no published scale figure in this JVD | https://www.juniper.net/documentation/us/en/software/jvd/metro-ethernet-business-services-with-updated-platform-recommendations.pdf |

NIST's build predates 400G platforms and the JVD's scale figures are for an MX10004, not a PTX, so R12 route scale on the PTX10002-36QDD remains unconfirmed before order (§6).

## 2 · Requirements register

**Table 3.** Requirements register

| # | Requirement | Value | Source |
|---|---|---|---|
| R1 | Subscribers and sites | 200,000 · 2 PoPs 30 km apart | [A] |
| R2 | Peering edges | 2, one per site, 400G ports | [T] |
| R3 | Aggregate peering capacity | 1.2 Tbps | [T] |
| R4 | Peering edge platform | 28.8 Tbps, 36 × 800GbE or 72 × 400GbE, inline MACsec, 2U | [S] PTX10002-36QDD |
| R5 | Peering edge silicon | Juniper Express 5 | [S] PTX10002-36QDD |

© 2026 Symbeeo. All rights reserved. · Public

| # | Requirement | Value | Source |
|---|---|---|---|
| R6 | Core-facing router | 32 × 400G, 12.8 Tbps, MACsec, 2 RU | [S] Cisco 8202-32FH-M |
| R7 | RPKI | origin validation on every external BGP session; invalid routes rejected | [T]; [S] Junos origin validation, valid/invalid/unknown states |
| R8 | RPKI cache servers | 2 validator sessions per router, grouped | [A]; [S] Junos supports multiple cache server sessions in a group |
| R9 | Inter-site link encryption | MACsec on all 4 × 400G inter-site links (2 edge-to-edge, 2 core-to-core) | [T]; [S] PTX10002-36QDD inline MACsec; 8202-32FH-M MACsec |
| R10 | Peak traffic day one | 600 Gbps, +25 %/year | [A] |
| R11 | Capacity headroom | ≥ 50 % at any site with the other site down | [A] |
| R12 | Route scale | full internet table plus peers, IPv4 and IPv6 | [A] |
| R13 | Convergence on peer or link loss | < 1 s with BFD | [A] |
| R14 | Flow telemetry | sampled flow export to the DDoS scrubber | [A] |

Fourteen rows; six carry a vendor figure, six are design assumptions, two are design targets.

## 3 · Architecture overview

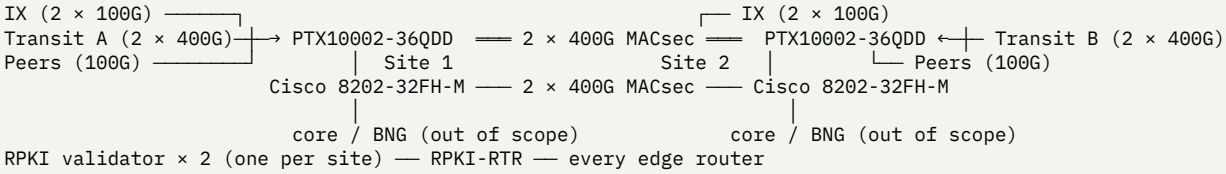



**Figure 1.** Peering edge, two sites

One peering edge per site, one core-facing router per site, encrypted 400G pairs between the sites, edge to edge and core to core, 2 × 400G from each edge to its site's core-facing router, and a validator at each site feeding both edges.

**Table 4.** Architecture overview

| Role | Product (exact model) | Qty | Capacity used | Why this unit |
|---|---|---|---|---|
| Peering edge | Juniper PTX10002-36QDD | 2 | 600 Gbps per unit, 2 % of 28.8 Tbps [T] [S]; 8 of 72 × 400GbE per unit [A] | 400G/800G ports, inline MACsec, 2U [S] |
| Core-facing router | Cisco 8202-32FH-M | 2 | 4 of 32 × 400G [A] | MACsec, 12.8 Tbps, 2 RU [S] |
| RPKI validator | validator software on a server (vendor not named here) | 2 | — | [A] |

© 2026 Symbeeo. All rights reserved. · Public

| Role | Product (exact model) | Qty | Capacity used | Why this unit |
|---|---|---|---|---|
| Inter-site optics | 400G coherent pluggables on leased wavelengths (family) | 8 | 2 × 400G edge-to-edge + 2 × 400G core-to-core [A] | [A] |

## 4 · Design by subsystem

### 4.1 Peering edge.

PTX10002-36QDD: 28.8 Tbps, 36 × 800GbE or 72 × 400GbE with inline MACsec, 2U, Express 5 silicon [S]. Per site day one: 2 × 400G transit, 2 × 100G to the exchange (broken out), 4 × 100G direct peers, 2 × 400G inter-site, 2 × 400G to the core-facing router [A]. The 1.2 Tbps aggregate (R3) is 600 Gbps per site; each unit could carry the whole load alone: with the other site down, its external ports (2 × 400G transit, 2 × 100G exchange, 4 × 100G peers = 1.4 Tbps) run the 600 Gbps at 43 %, leaving 57 % headroom (R11) [A]. One 400G transit link per site would leave 1.0 Tbps at 60 % used, 40 % headroom, below R11. Rejected: a modular chassis — the fixed 2U unit covers ten years of 25 % growth before a port is short [A].

### 4.2 RPKI.

Junos origin validation: one or more RPKI cache servers, prefixes marked valid, invalid or unknown, sessions grouped with per-session parameters [S]. Policy: reject invalid, accept valid and unknown, prefer valid over unknown by local preference [A]. Two in-house validators, one per site, each edge with a session to both [A] (R8). Validator software is named by function only; its vendor is not named here. Rejected: a single hosted validator — one session, one dependency (R8).

### 4.3 BGP policy.

Per-peer prefix limits, bogon and own-prefix filters, communities for traffic engineering, and no-export on the inter-site iBGP [A]. BFD on every external session at 300 ms × 3 [A] (R13). Rejected: relying on RPKI alone — origin validation does not catch a leaked but validly originated route.

### 4.4 Core-facing routers.

Cisco 8202-32FH-M: 32 × 400G, 12.8 Tbps, MACsec, 2 RU, Silicon One [S]. Two 400G links to the site's edge, two to the other site's core-facing router (MACsec), the rest to the core [A]. Rejected: 8201-32FH — same ports, no MACsec [S] (R9).

### 4.5 Inter-site links.

Four 400G links: edge-to-edge and core-to-core, each pair on diverse leased wavelengths [A], MACsec on every link [S] for both platforms (R9). Coherent 400G pluggable optics are named by family; the wavelength provider is out of scope.

### 4.6 Telemetry.

Sampled flow export from both edges to the DDoS scrubber, streaming telemetry to the operator's NMS, and RPKI validation counters graphed per session [A] (R14).

© 2026 Symbeeo. All rights reserved. · Public

## 5 · Failure behavior

**Table 5.** Failure behavior

| Failure | Behavior | Source |
|---|---|---|
| One transit link down | BFD detects in under 1 s; traffic moves to the site's second transit link, or to the other site's transit over the inter-site link | [A] |
| One peering edge down | the other site's edge carries 600 Gbps, 2 % of its 28.8 Tbps; peers on the failed site are lost until repair | [S] capacity; [A] |
| One inter-site wavelength down | second link on diverse path carries the load; MACsec session re-forms on recovery | [A] |
| Both RPKI validators unreachable | routes fall to unknown state; policy accepts unknown, so no traffic loss; alarm raised | [S] unknown state; [A] policy |
| An invalid route announced by a peer | rejected at import; never enters the routing table | [S] invalid state; [A] policy |
| Core-facing router down at one site | site's edge routes via the inter-site link to the other core-facing router | [A] |

## 6 · Limits

- Each edge is used at 2 % of its switching capacity; the choice is driven by 400G ports, MACsec and route scale, not throughput.
- Route scale (R12) is assumed adequate on both platforms; the FIB figures were not on the pages read and must be confirmed before order. The nearest public figure is Juniper's JVD-METRO-EBS-03-03 (May 9, 2025), Table 2: about 1.2M RIB / 966k FIB on the MX10004 device under test [S]; the PTX10001-36MR in that JVD is a helper node with no scale figure, so no PTX figure is on the public record here.
- Cisco 8212-48FH-M also lists MACsec at 48 × 400G; it was not chosen because 32 ports suffice at 25 % annual growth for over five years.
- RPKI validator software and coherent optics are named by family only; their vendors are not named here.
- Subscriber aggregation, BNG and DDoS scrubbing are not designed here.

## 7 · Lessons learned

None yet — this is a design study; populated after the first build against it.

© 2026 Symbeeo. All rights reserved. · Public

## 8 · The author

WRITTEN BY

**Mark Winston**

Principal Network Architect

CCIE, CISSP, CCSP, CCISO, CISM, Adopting Zero Trust (Forrester)

Signed off by Edwin Ozer, Founder.

© 2026 Symbeeo. All rights reserved. · Public

SYMBEEO

Each vendor's tool shows you their option. We show you all of them against one requirement.

## Compared. Then Delivered.

hello@symbeeo.com · symbeeo.com

© 2026 Symbeeo. All rights reserved.

Product and company names and logos are their owners' trademarks, shown only to identify the lines Symbeeo sources. Naming a vendor or showing its logo does not mean the vendor sponsors or approves Symbeeo's comparisons or any recommendation Symbeeo makes.

Figures are as published by their sources on the dates given in this document; figures marked [A] are assumptions.

NET-005 · Version 1.3 · Oct 10, 2026