Core Network & Data Centre Interconnect | blueAPACHE

Canonical: https://www.blueapache.com/services/empower-core-netork-dc-interconnect

Details:

Summary

emPOWER Core Network and Data Centre Interconnect is the transport layer beneath our connectivity services — a fully meshed MPLS private core that we built in 2010 and operate ourselves, connecting offices, data centres and cloud platforms without routing traffic over the public internet.

The emPOWER Network brochure describes our owned and operated private core and its connections to other emPOWER services. Agree responsibility across core transport, access circuits, cloud and operations in the Service Description.

Key facts

Fact	Value
Built	2010, alongside emPOWER Cloud
Architecture	Fully meshed MPLS private core
Core routing	Cisco Aggregation Services Router (ASR), carrier-grade
Carrier position	Tier 1 carrier-agnostic — not tied to a single upstream
Peering	Traffic transits the Australian Internet Exchange
IP addressing	IPv6-ready
Security	Palo Alto Networks virtual firewalls integrated throughout
Points of presence	Pacific (Australia), United States, Europe (London), Asia (Singapore)
Data centre reach	165+ interconnected data centres worldwide
Redundancy	Multiple redundant transmission paths between PoPs, inherent to the design
Cloud interconnect	Azure ExpressRoute; AWS Direct Connect
Operations	24/7 network operations centre
Contract schedule	Schedule 5, emPOWER Network Services
Default term	General Terms v3.6 specify 36 months unless the Service Order or Service Description states otherwise; Professional Services are excluded

	from the default
ISO 27001	emPOWER Network Services is a named in-scope service on certificate 202507-118

Site-to-site connectivity without VPNs

Business-grade MPLS data services extend the corporate private network across locations without requiring a VPN between them . Each office becomes another IP address on the network rather than a tunnel endpoint that must be built, monitored, renewed and troubleshot.

The brochure describes this as an alternative to site-to-site VPN connectivity. Confirm encryption, segmentation and any VPN requirements at other boundaries in your design.

Data centre interconnection

The network interconnects with more than 165 data centres across Australia, New Zealand, the United States, the United Kingdom and Singapore. Discuss the available facilities, access paths and failure domains for your primary and recovery environments. The published footprint does not establish capacity, redundancy or commercial availability at every requested site.

Peering and IPv6 readiness

The network brochure states that traffic transits the Australian Internet Exchange . Peering creates opportunities for local traffic exchange, but does not establish the actual route or country of transit for every flow. Confirm routing and measured latency for the destinations that matter to your organisation.

The core is also IPv6-ready . That matters for organisations facing IPv4 exhaustion in their own addressing, running dual-stack applications, or subject to a government or sector requirement to demonstrate an IPv6 path.

Direct cloud connections

Azure ExpressRoute connectivity; Microsoft 365 connectivity requires separate authorisation and routing design

AWS Direct Connect

Direct connection into emPOWER Cloud ; the applicable services are listed in the scope of blueAPACHE's ISO/IEC 27001-certified information security management system

Secondary VPN-over-internet route for redundant pathways

Compare the bandwidth, latency, contention, redundancy and service commitments of each proposed path. A direct connection does not eliminate all performance dependencies. Microsoft recommends internet connectivity for most Microsoft 365 scenarios.

Quality of Service, end to end

We work with the customer to define business-critical applications and apply QoS across the network, prioritising voice and video. Confirm traffic classes, policy enforcement and hand-off boundaries across the complete path, including access carriers and cloud connections.

Four points of presence

Region	Point of presence
Pacific	Australia
Americas	United States
Europe	London
Asia	Singapore

The London point of presence went live in 2019 and Singapore in 2020. For an international deployment, confirm which paths remain on the private core and where carrier, internet or cloud-service boundaries apply.

Availability, and the condition attached

The emPOWER Connectivity brochure states minimum 99.99 per cent uptime for a specified redundant site design:

Multiple carriers

Multiple media types — fibre and fixed wireless

Multiple CPE devices and firewalls in high-availability configuration

Dual firewalls and dual carriage at each site

Multiple redundant transmission paths between points of presence are inherent to the core network design. Site-level redundancy is not — that is a per-site commercial decision. The brochure does not establish the uptime commitment for a single-carrier site. Confirm the applicable figure, measurement window, exclusions and credits in the service documentation.

Check the core and each site's redundancy separately, including the failure scenarios the design covers.

How this compares to the alternatives

Most organisations choosing a wide-area network are weighing three models. The trade-offs are structural rather than a matter of one being better.

A provider-owned MPLS core, as here. The brochure describes an owned private core and integrated services. Confirm end-to-end responsibilities, QoS boundaries, upstream dependencies, pricing and term. Addresses allocated by blueAPACHE are not portable on exit under the published terms.

SD-WAN using internet access. Compare the access services available at each site, installation lead times, path performance, security controls and who manages integration. Price and deployment speed require like-for-like quotes. The Connectivity brochure also describes MPLS, internet SD-WAN and hybrid architecture options.

Carrier-provided VPN or MPLS. Compare the carrier's contracted footprint, service levels and managed-service options. Where several suppliers are involved, document escalation and responsibility at each hand-off; the supplier category alone does not determine accountability.

We also offer emPOWER SASE for secure access requirements. Discuss how its access policies and network functions would integrate with the proposed core-network design.

Who this suits

It suits multi-site organisations with predictable inter-site traffic, latency-sensitive voice or virtual desktop workloads, a disaster recovery requirement that spans facilities, or a compliance position that benefits from traffic staying off the public internet. The Sealy and Archers engagements below are both of that shape.

For cloud-only or smaller estates, compare the proposed core-network design with internet and SD-WAN options against actual application paths, resilience needs, support responsibilities and total cost.

What we manage

Monitoring, 24x7 through the network operations centre

Operating system patch updates on CPE and firewalls

Configuration documentation retention

Nightly configuration backups

Change management

Support windows

Function	Availability
Service desk	7am to 7pm on Business Days
Priority network monitoring and NOC	24x7
Unified threat protection	24x7

These are the Connectivity brochure's stated windows. The Managed Services brochure separately describes unlimited 24/7 help desk support. Holding both services does not by itself establish the support window for every incident; confirm covered systems, escalation and response arrangements in your agreement.

Commercial points

IP addresses are not portable. Addresses allocated by us do not transfer on exit. Assess dependencies on those allocated addresses, such as firewall rules, allow-lists, DNS records and VPN peers, and plan any required renumbering or reconfiguration.

Upstream supplier changes. Clause 3.26 addresses suspension or cancellation where an upstream supplier withdraws or replaces a service, including notice, best-efforts mitigation and fee provisions. Confirm alternative carriers and failover behaviour for your design; carrier choice alone does not establish continuity.

Cost pass-through. Clause 12.5 permits proportional pass-through when a third-party supplier changes its charges to blueAPACHE, including exchange-rate-driven supplier changes. Clause 12.6 separately addresses fees based on an Agreed Rate specified in the Service Order. Check the mechanism applying to international circuits.

Default term. General Terms v3.6 specify a 36-month Minimum Service Period unless the Service Order or Service Description states otherwise; Professional Services are excluded from that default.

Our client outcomes

Sealy of Australia is the published multi-region deployment: an international voice and data network across 18 sites in Australia, New Zealand, the United Kingdom and Asia-Pacific, staged and migrated with no business disruption, live April 2022. See the Sealy case study .

Archers The Strata Professionals (2026) upgraded site links from 20/20Mbps to 400/400Mbps fibre on a private MPLS WAN as part of a wider managed services engagement. See the Archers case study .

Honan Insurance replaced an incumbent provider after repeated network outages, with a stated telecommunications cost reduction of around 65 per cent. See the Honan case study .

Questions worth asking before signing

What are the service credits if the 99.99 per cent figure is missed, and what is the measurement window?

What is the provisioning lead time for a new site in each country where we operate?

Which upstream carriers sit behind each of our sites, and what happens to that site if one is withdrawn?

What is the renumbering scope if we exit, and will blueAPACHE document every allocated address during the term rather than at exit?

What are the measured latencies between the points of presence we will actually use?

Does the 36-month Minimum Service Period run per site or for the whole service, and what happens when a site is added late in the term?

What does the site readiness standard require of our premises before a circuit can be installed?

Is IPv6 enabled by default on our services, and what is the dual-stack migration path?

Documenting each network dependency

List endpoints, access circuits and responsibility for equipment at both ends. Distinguish core-network service from local access and any public-cloud connection beyond it. For redundancy, document what failure each second circuit or device is intended to cover and how this will be tested. Agree carrier escalation and configuration authority. A published network capability does not establish a guarantee for every link between a user and an application.

Which document defines the commitment

The published General Terms v3.6 give the Service Order precedence over the General Terms, followed by the Schedules and then the Acceptable Use Policy (clause 2.3). Record the agreed scope, exclusions and negotiated departures in that document set. Keep the versions supplied at signing with the executed order and signed variations. Two offers with the same service name can cover different systems, operating hours or responsibilities.

Responsibility across the delivery chain

The published terms allow us to subcontract all or part of the Service Agreement without customer consent or a notification requirement. Clause 27.5 nevertheless makes us liable for our subcontractors' acts and omissions to the same extent as for our employees. This differs from a third-party supplier contracted directly by the customer. Identify which arrangement applies to each dependency in the design. Where supplier identity, delivery location or change notification matters, request a documented supplier list and put any agreed notification or approval requirement in the Service Order; the general clause does not supply that visibility automatically.

Continuity when an external event interrupts service

Clause 23 addresses force majeure separately from normal incident management. Performance is suspended to the extent a qualifying event causes delay or failure. The definition includes specified events outside reasonable control; it is not a blanket classification of every outage. If the delay exceeds 20 Business Days, the other party may terminate by written notice. The clause also requires payment for services to termination and the applicable Early Termination Payment. A continuity plan should cover operational recovery and the commercial consequences of prolonged interruption. Confirm the Schedule's exit calculation rather than assuming an externally caused outage creates a cost-free exit.

Customer content and take-down requests

Clause 14 distinguishes operating the service from responsibility for the customer's content. It requires the customer to notify us promptly of relevant take-down notices or directions and comply with them. The terms also reserve rights for us to restrict or remove Customer Data in specified circumstances, including suspected agreement breaches or exposure to harm or liability. These rights are separate from routine availability commitments. Agree who receives regulatory notices and who can authorise operational action, and retain the notice and decision record. The full clause, including its discretion and good-faith wording, is explained in the terms guide.

Escalating a contractual dispute

A support escalation and a formal contractual dispute are different processes. Clause 26 begins with a Dispute Notice giving adequate particulars. Representatives meet within three Business Days; unresolved matters then move through the clause's senior-representative referral and meeting stages before court proceedings. Urgent equitable relief and disputes over whether the agreement was validly terminated are exceptions. Keep incident records, service measurements, approvals and correspondence together so the disputed obligation and requested outcome can be identified. Raising a ticket does not necessarily satisfy a formal notice requirement; use the agreement's notice process for contractual disputes.

Do you own this network or resell it?

We built and operate the emPOWER Network, established in 2010, on Cisco ASR carrier-grade routing. It is Tier 1 carrier-agnostic rather than tied to one upstream carrier.

Do we still need site-to-site VPNs?

No. MPLS extends the corporate private network across sites without them — each office becomes another IP address on the network.

How many data centres can we reach?

More than 165, across Australia, New Zealand, the United States, the United Kingdom and Singapore.

Does the network support IPv6?

Yes, the core is IPv6-ready.

Where does the network peer?

The network brochure states that traffic transits the Australian Internet Exchange. Confirm actual routing and locality for your important traffic flows; peering participation alone does not guarantee an Australian-only path.

Can it connect directly to Azure and AWS?

Yes — Azure ExpressRoute and AWS Direct Connect, plus direct connection into emPOWER Cloud, with a secondary VPN-over-internet path for redundancy.

Is the 99.99 per cent uptime guaranteed for our sites?

The Connectivity brochure ties minimum 99.99 per cent uptime to a redundant design with multiple carriers, media, CPE and firewalls, and dual carriage. Confirm your site's design and the contractual measurement, exclusions and credits. The brochure does not establish the uptime commitment for other configurations.

How does this compare with SD-WAN over the internet?

Compare like-for-like designs and quotes for access availability, lead time, bandwidth, latency, resilience, security, management responsibilities and term. The Connectivity brochure describes MPLS, internet SD-WAN and hybrid options. Neither architecture label alone establishes lower cost, faster deployment or guaranteed performance.

What happens to our IP addresses if we leave?

They do not transfer. Allocated addresses are not portable on exit, so scope renumbering before signing if you have hard-coded dependencies.

Who monitors the network overnight?

The Connectivity brochure describes 24x7 network monitoring/NOC and a 7am–7pm business-day service desk. Managed Services has a separate published support model. Confirm which service and escalation window covers each incident in your agreement.

Is the network ISO 27001 certified?

emPOWER Network Services is listed in the scope of blueAPACHE's ISO/IEC 27001:2022 certificate 202507-118. The certificate covers the information security management system, rather than guaranteeing the security or availability of every network connection.

How long is the contract?

General Terms v3.6 specify a default 36-month Minimum Service Period unless the Service Order or Service Description states otherwise, with Professional Services excluded. Confirm the term and renewal rules for each ordered service.

Related

Connectivity

emPOWER SASE

Cloud
emPOWER Cloud
Public Cloud — Microsoft Azure
Disaster Recovery as a Service
Collaboration
Security
Managed services
Sealy of Australia case study
Archers case study
Glossary
Contact

What is emPOWER Core Network and Data Centre Interconnect?

emPOWER Core Network and Data Centre Interconnect is our service that connects offices, data centres and cloud environments over our own fully meshed Cisco ASR MPLS private core network, with points of presence in Australia, the United States, London and Singapore, and interconnection into more than 165 data centres.

What technology underpins the emPOWER Core Network?

The emPOWER Core Network is built on Cisco ASR carrier-grade technology, operating as a fully meshed MPLS private core network.

How many data centres can the network interconnect with?

The network provides interconnection into more than 165 data centres around the world.

Where are the network's points of presence located?

The network has points of presence in Australia, the United States, London, and Singapore.

How is the network monitored?

The network is proactively monitored 24/7, 365 days a year.

What carrier model do you use for this network?

We use a Tier 1 carrier-agnostic model, balancing globally recognised Tier 1 players with specialised regional carriers.

Who is this service intended for?

The service targets multi-site organisations connecting offices, data centres and public cloud environments.

Which countries does this service cover?

Published materials describe data-centre interconnection across Australia, New Zealand, the United States, the United Kingdom and Singapore, with core points of presence in Australia, the United States, London and Singapore. Confirm commercial availability, access circuits and delivery scope for each requested location.

What is the pricing and minimum term for this service?

Confirm pricing, link charges and the fee model in your Service Order. General Terms v3.6 specify a default 36-month Minimum Service Period unless the Service Order or Service Description states otherwise; Professional Services are excluded from that default.

What other services are related to Core Network and Data Centre Interconnect?

Related services include emPOWER SASE, emPOWER Cloud, Public Cloud - Microsoft Azure, and the Connectivity emPOWER pillar hub.

How can someone contact you about this service?

Interested parties can contact our sales team via phone at 1800 248 749 (AU) or through the contact page.