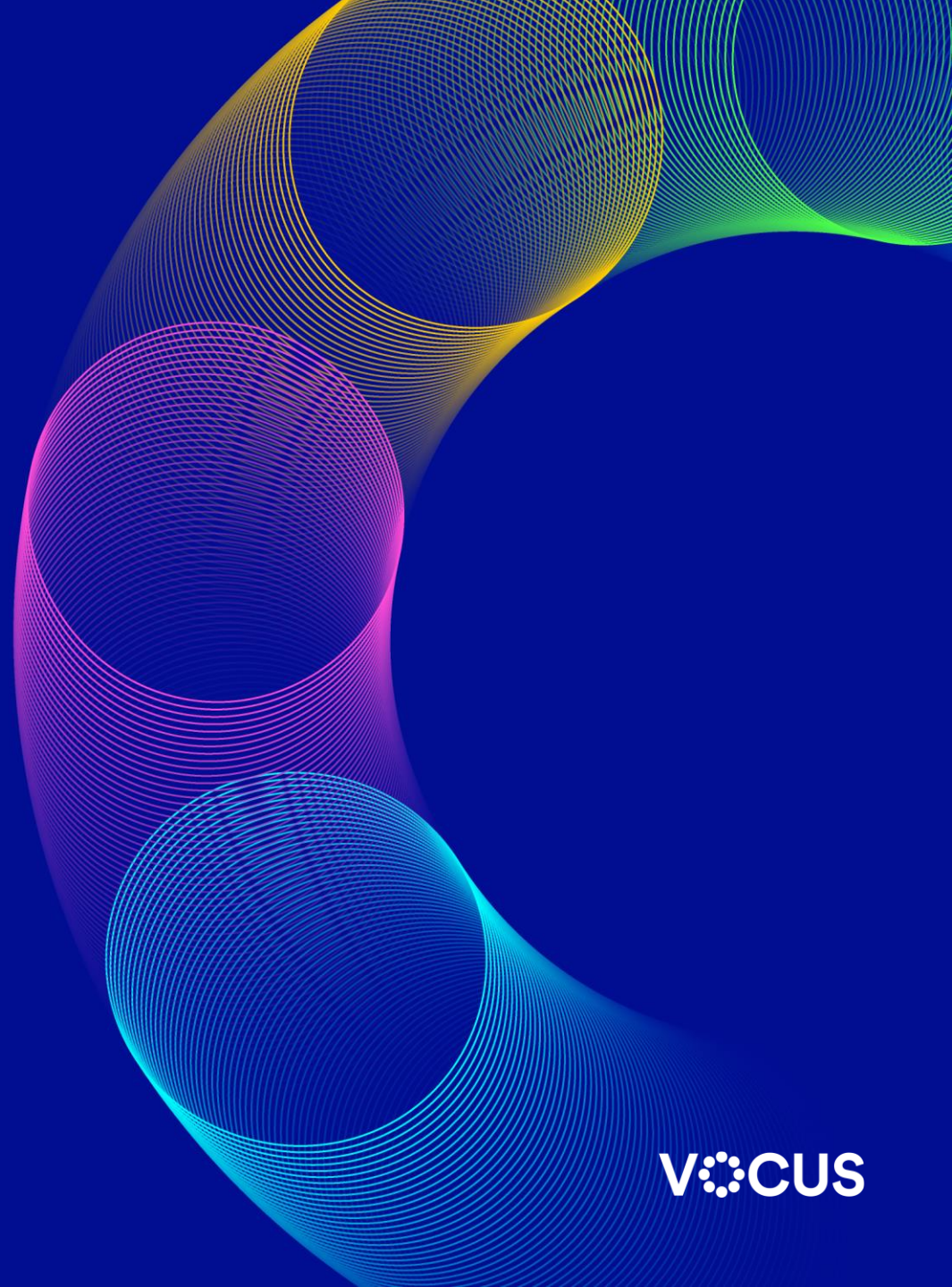
Building an OOB Management network

(Yet another MPLS network)

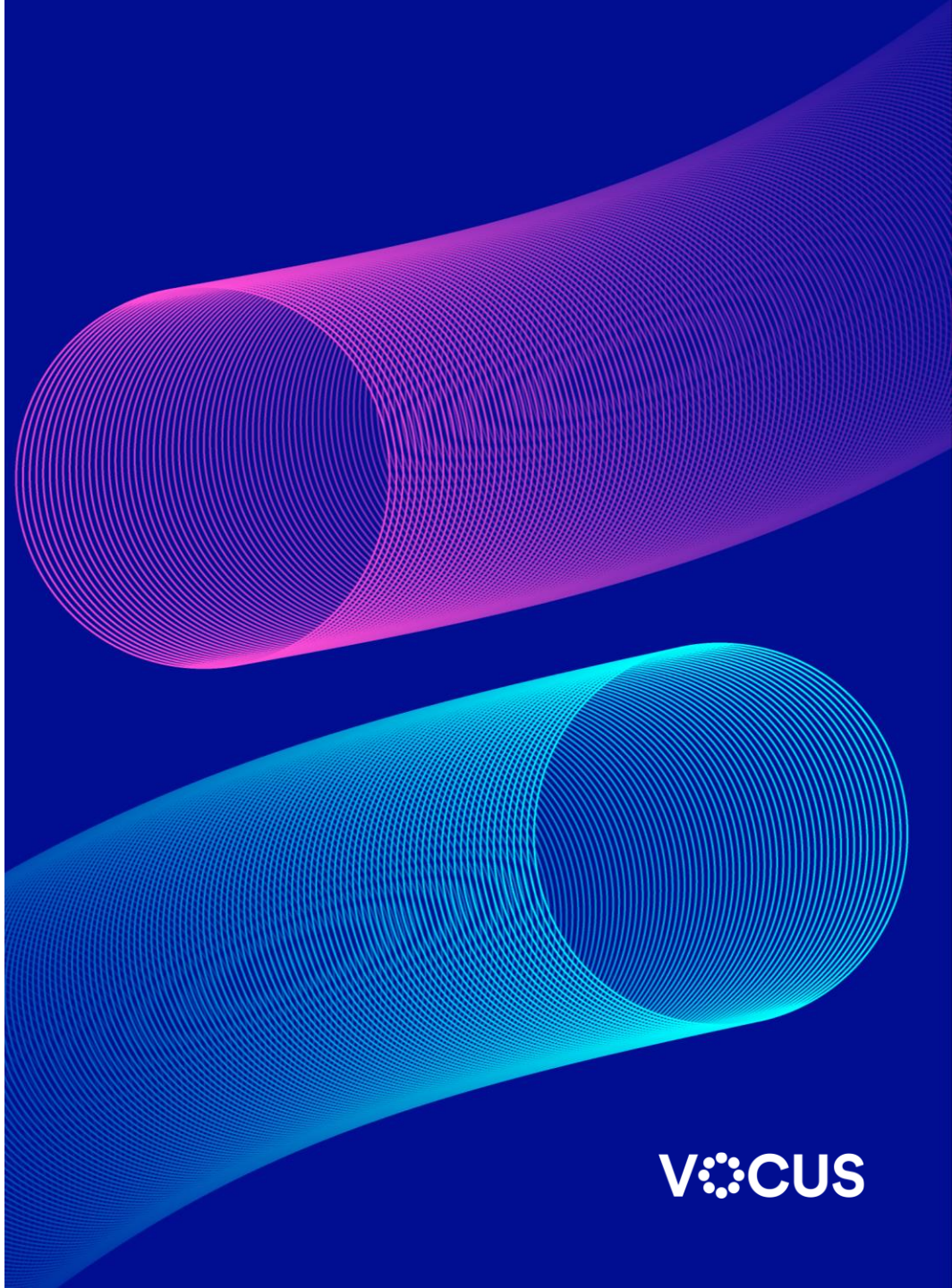
Phil Mawson

APRICOT 2026



Q) True or false?

OOB is only needed when your network breaks.



What lives in an management network?

Our management Network is our emergency network.

- Router management ports (FXP/Mgmt)
  - Juniper: mgmt_junos routing instance
  - Cisco: mgmt routing instance
- Console Servers/Routers
- Managed power rails
- Environmental Monitoring



So what happens if your network goes offline?



Real world impact

- National outage for Optus (AS7474) in Australia on Wednesday 8th November 2023
- Facebook (META) October 4th 2021 (approx. 6 hours)

How do I get back into my network?

Build another network for your network

Vocus Journey

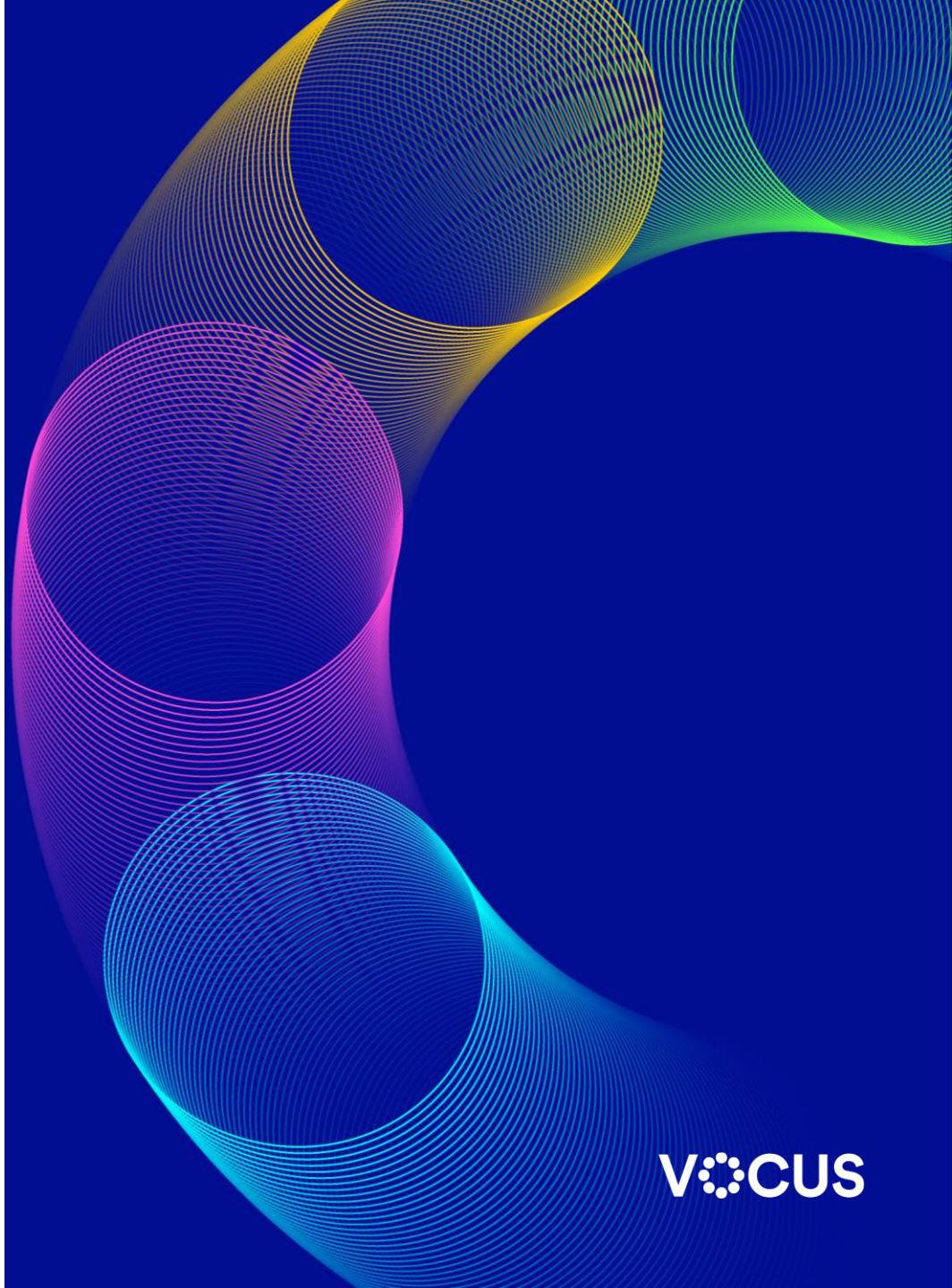
Vocus has grown by acquisition, we had acquired many networks each with their own bespoke OOB solution varying from using LTE on Console boxes only, to old end of life hardware using third party backhaul circuits across Australia.

We had a requirement to use zero touch provisioning for a new aggregation network that was being rolled out with no common way of doing this across all the sites.

Solution: Build a new network for the new network.

Bonus: Use this as an opportunity to consolidate, uplift and standardise existing OOB networks

Network Design & Equipment choices



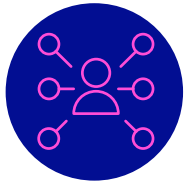
Network Design considerations



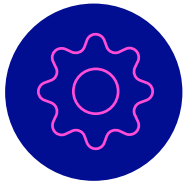
Use our own transmission services interstate, diverse paths



OOB needs to not rely on any founder IP network



Each state it’s own region, two routers in each site are used as route reflectors for that local region



OSPF was chosen as the underlining IGP



Dark fiber used within the metro between sites, where possible diverse paths used in rings



Not every site requires full level of redundancy.

Equipment Choices

Routers

Juniper ACX7024X

SRX345 series





Switches

Juniper EX3400 + 4100



Console Routers

Opengear CM series

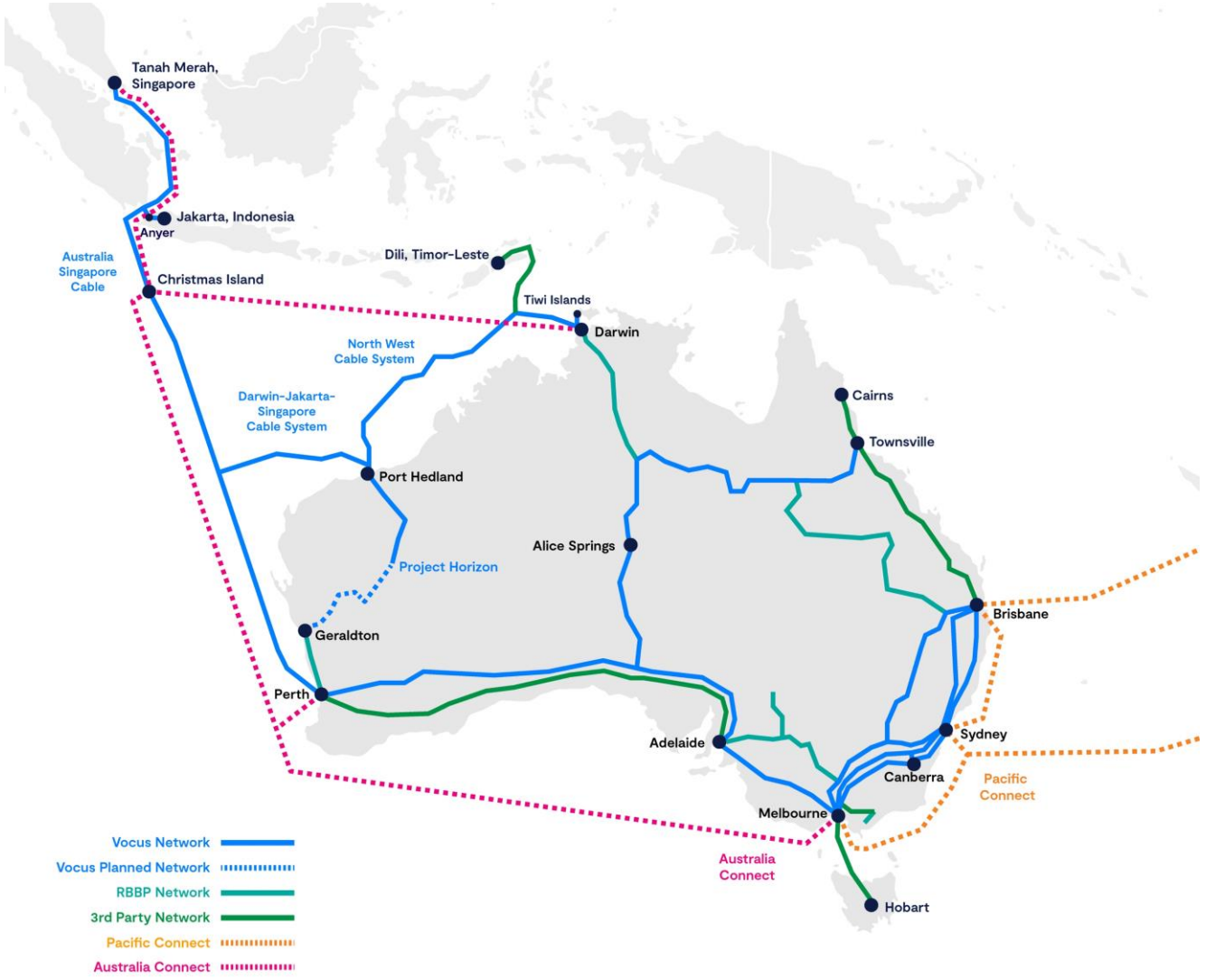


Combined Boxes

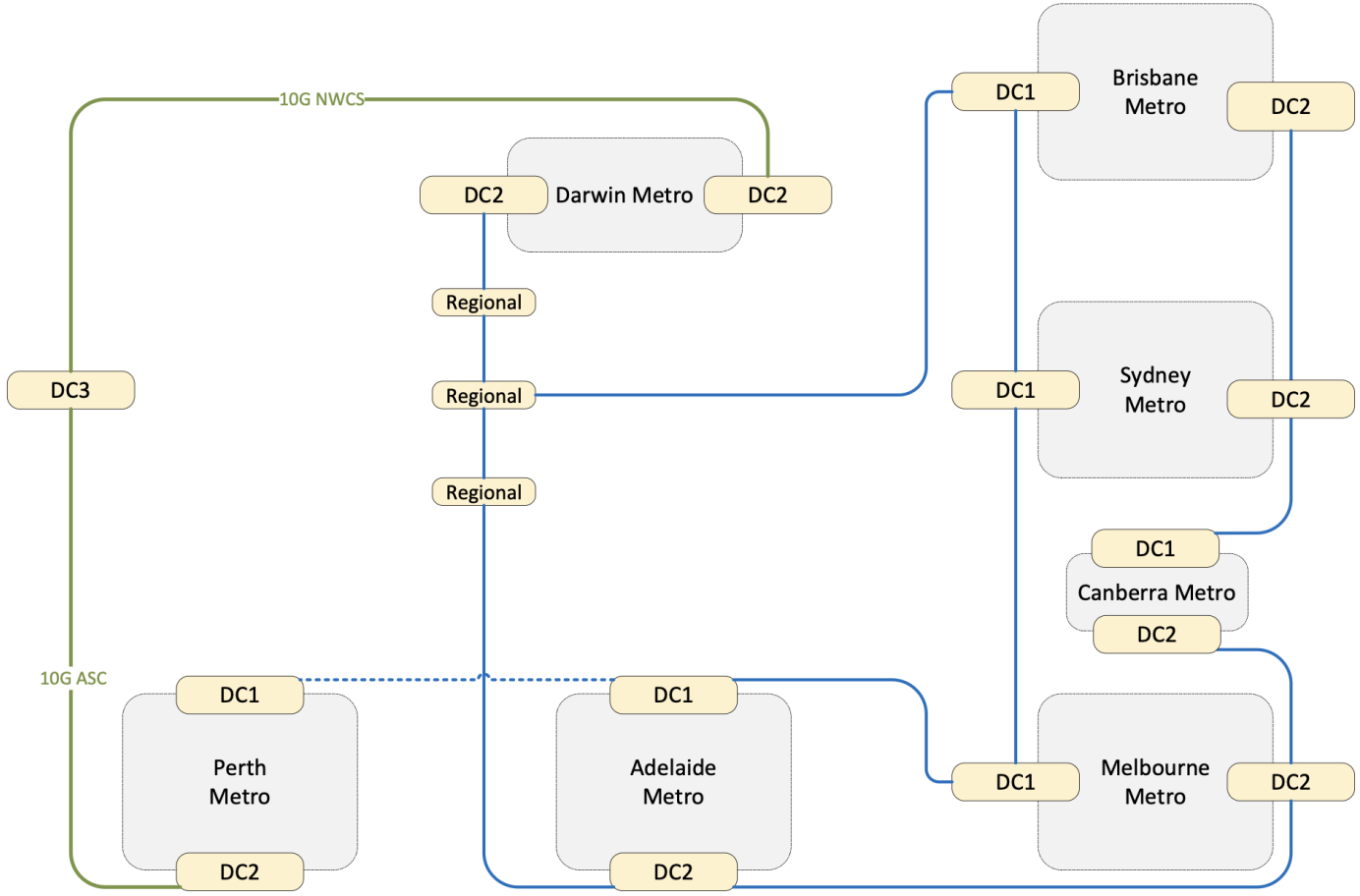
Cisco C1100TG



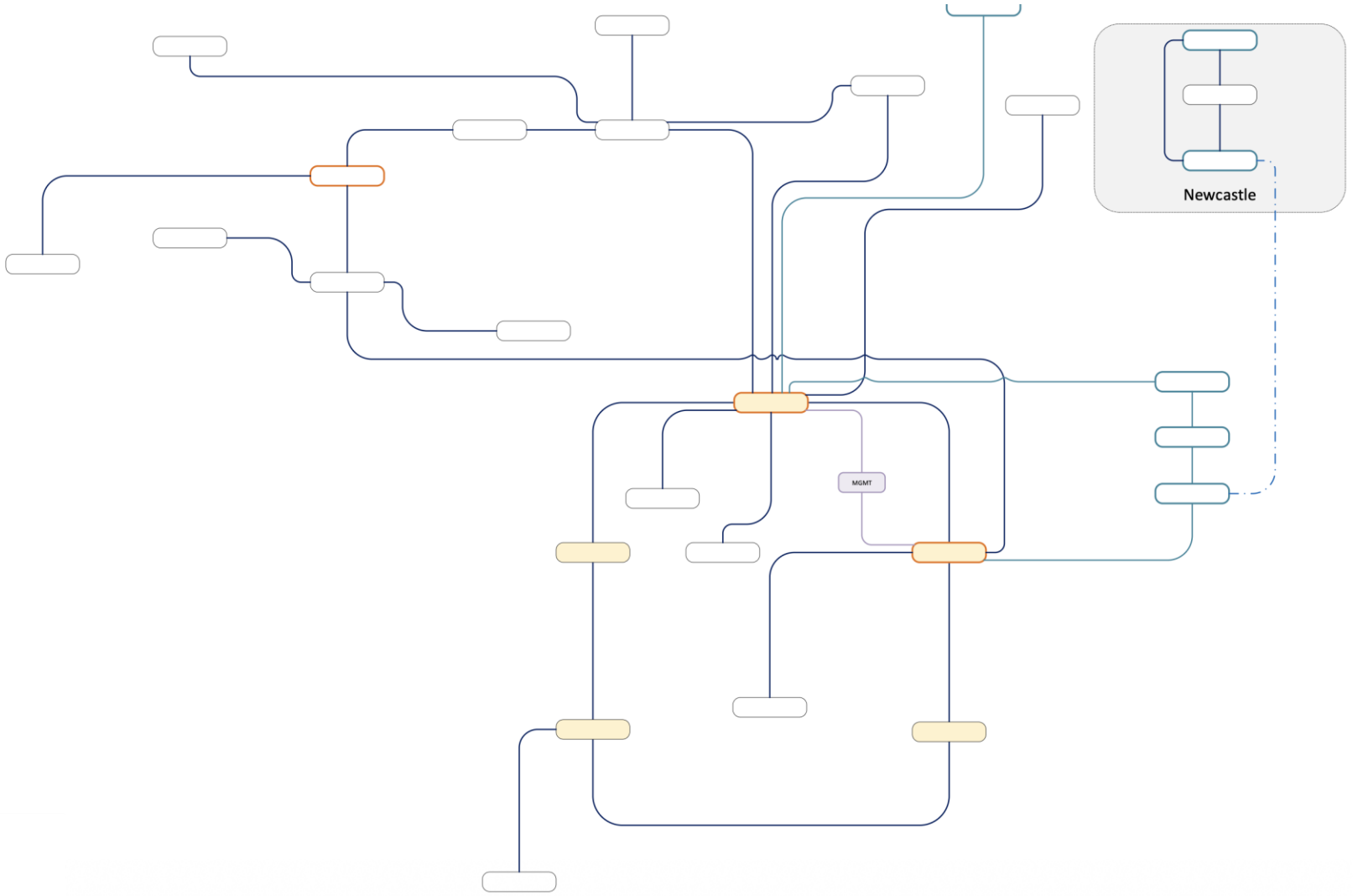
Vocus Network



National OOB Network



State Level Example (Sydney)



International Sites

International sites for Vocus had to follow a different model. We do not own transmission to the majority, and turning up 10GB waves for OOB would be expensive on third party services.

After looking at multiple options, including just using a third party internet service in each site, we chose to go with Megaport who provide Layer2 VLLs (VXCs) back to a headend link within Australia.

Noting our OOB network internationally is only used if our network equipment fails, there is less requirement for resiliency for our international sites for our OOB management.

Accessing OOB/Management network

Your OOB/Management should be kept separate from production

Geographical diversity is just as important as site diversity.

OOB Management network is firewalled off from our critical infrastructure management network, with multiple links between each environment in each main state.

Geographical diverse jump hosts (bastions) to gain access to management network – Sydney, Melbourne and Perth

What if your transit network goes offline?

Third Party to the rescue

Vocus chose a third party transit provider for a small link to connect to a VPN concentrator in a third party datacenter. This meant if AS4826 goes completely offline, there is access still for remote staff to connect back to the network to try and restore.

Break glass details

Sometimes you need to login when your authentication servers are offline or unreachable. Keep your break glass (local account) passwords in a safe location that can be accessed by a limited group of people if your network goes offline.

Do you print these off and store in a fireproof lockable safe?

Do not permit these logins to work if authentication is up and working

Alarm when local account is used

Notes on Authentication order

Juniper (JunOS inc Evo)

set system authentication-order tacplus

For Juniper, if you add local to the above line it will allow local authentication, even if TACACS+ is available. If the router can not connect to the remote authentication server, it will fall back to local.

Cisco will reject local login if it gets a reject from the first authentication server in the config

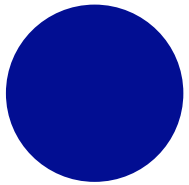
Cisco XR

aaa authentication login default group TACACS-INBAND group TACACS-OOB local

```
aaa group server tacacs+ TACACS-INBAND
 server-private 123.123.123.123 port 49
  key superSecretKeyHere
 !
 server-private 124.124.124.124 port 49
  key SuperSecretKeyHere
!
aaa group server tacacs+ TACACS-OOB
 ! Use the TACACS IP that is reachable via OOB
 vrf mgmt
 server-private 192.168.5.5 port 49
```

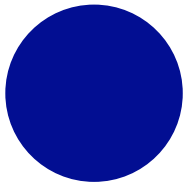

VOCUS

Secure it, document it.



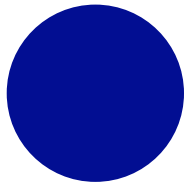
Console routers

Ensure password is required to connect to console server ports



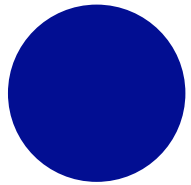
Network Segmentation

Think about lateral movement if a third party was able to access a device, what other local devices could then be accessed on the same management network subnet within the site?



In-band vs OOB

Make use of Juniper and Cisco devices being able to use TACACS+ servers over inband and OOB, including syslog



Document!

Where do you keep documentation of console port allocations? What if your network goes offline, how do you access that documentation?

VOCUS

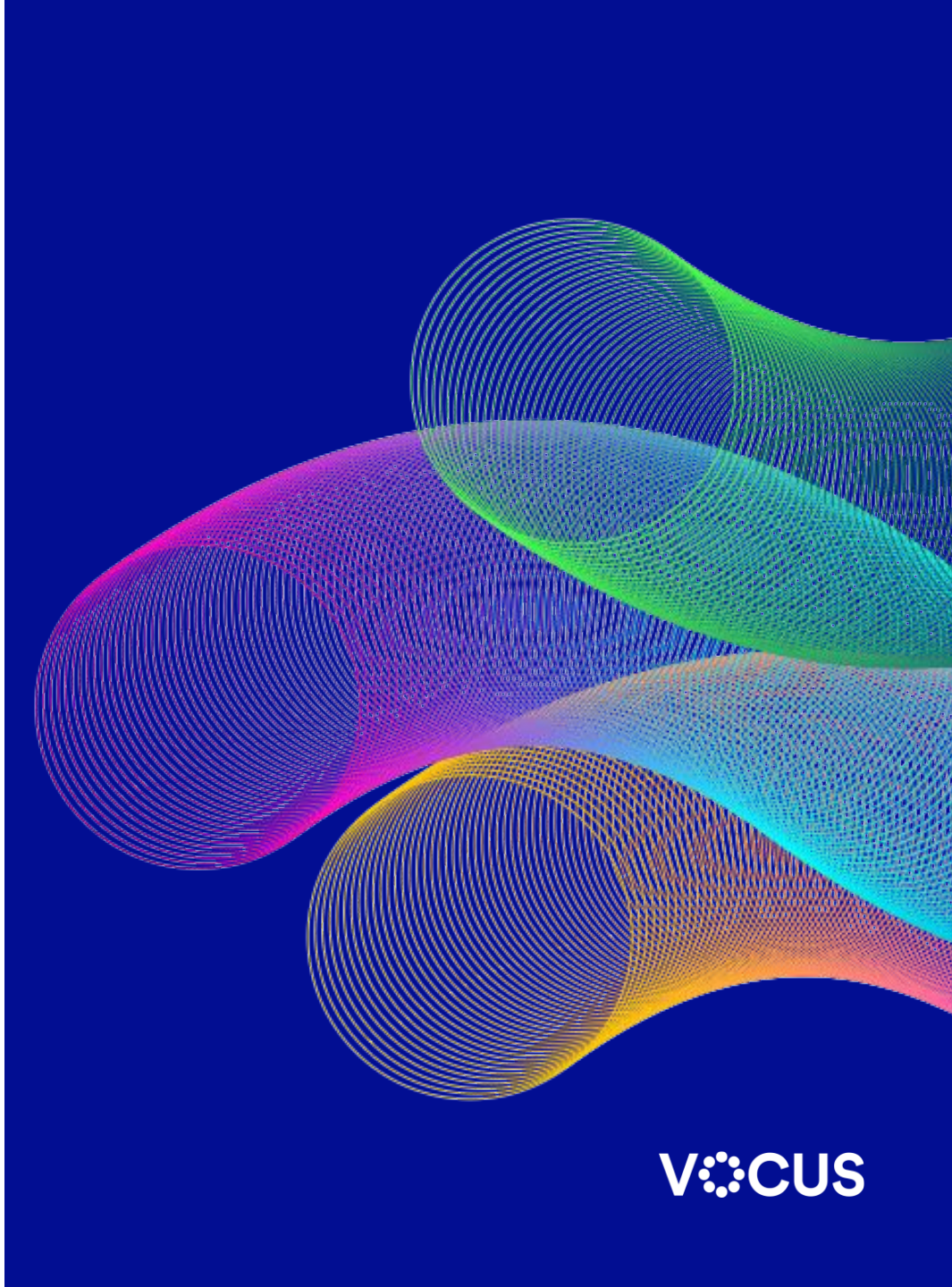
Learnings

Prepare for power works & failures. Single powered DC units require additional work (Juniper SRX345-DC and Cisco C110TG)

Just because you built a new MPLS network does not mean it should be used to carry non critical management traffic

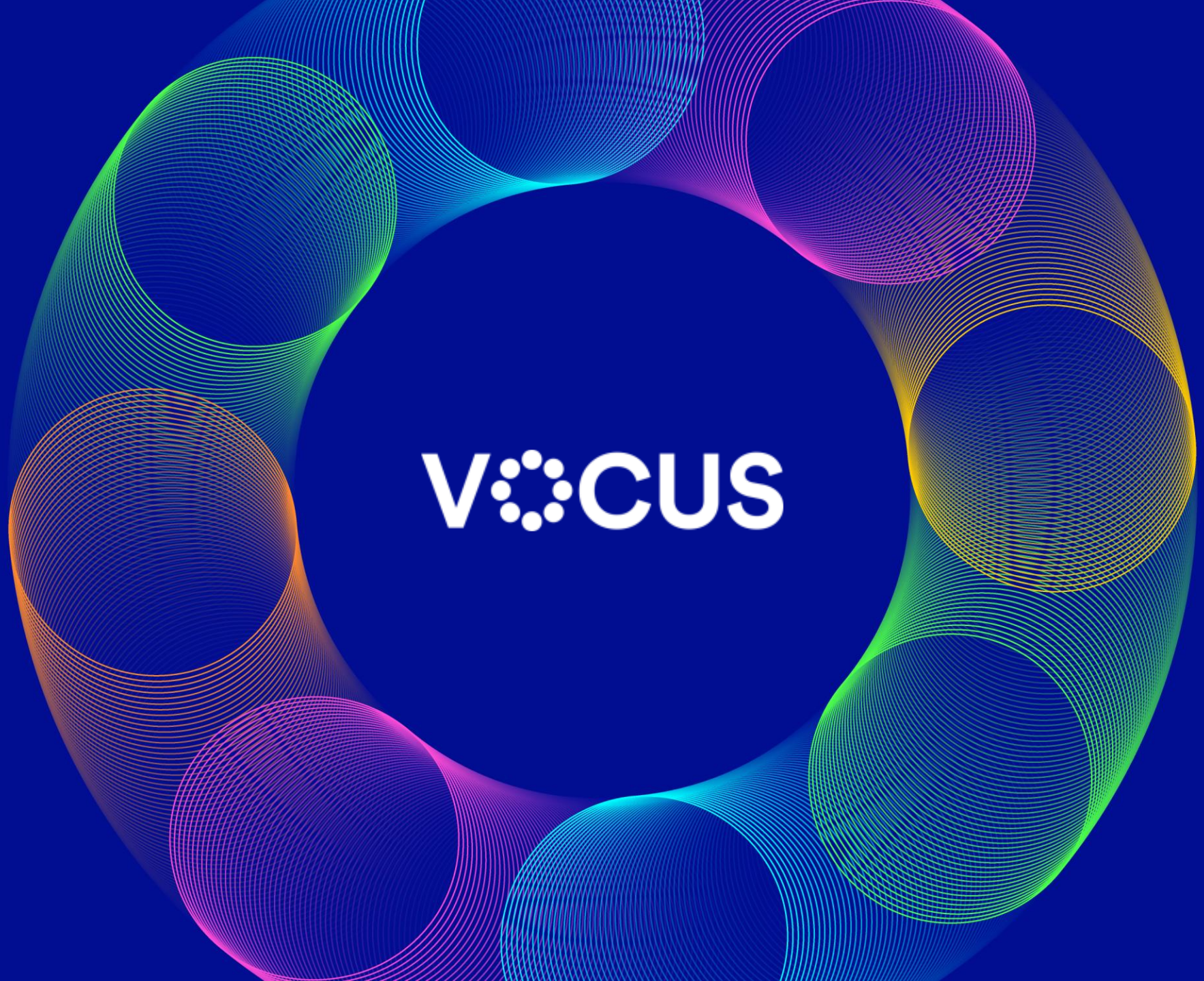
Management network should be the first “production” network to go live in a site.

Monitoring of OOB is just as important as production



DC ATS device deployed in a nbn site




VOCUS