



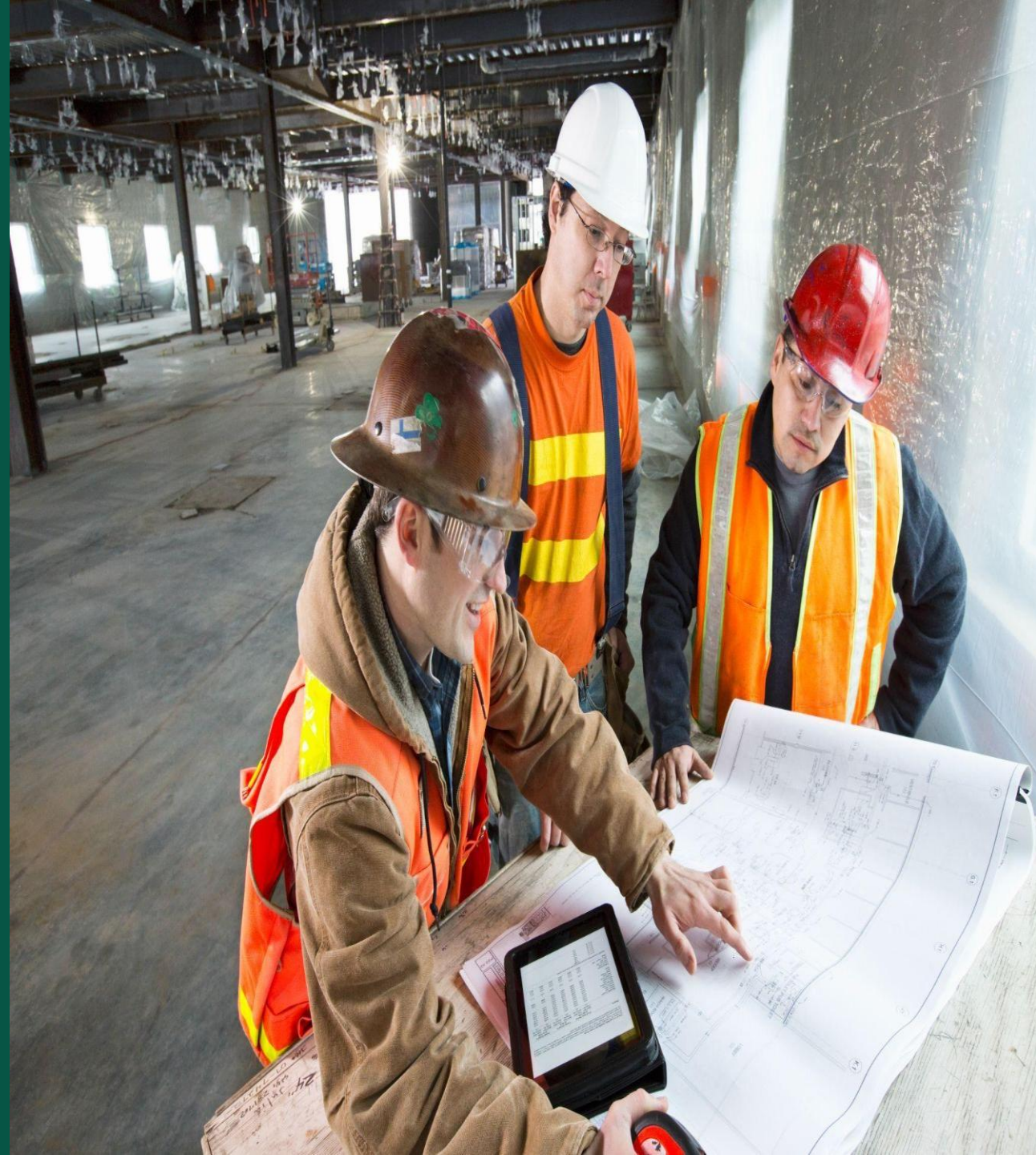
Cloud BMS Application Guide

Designing, deploying and commissioning cloud-hosted
Niagara 4 and other BMS supervisors with Neeve

For partner system integrator technical teams

Version 1.1 | October 2026

©2026 Neeve, Inc. All Rights Reserved. Confidential.



About this guide

Your field manual for Neeve Cloud BMS deployments

Everything a partner SI technical team needs to pick the right hosting model and architecture, prepare the site, configure each protocol and hand over a system that works first time.

Assumed knowledge

Niagara 4 Workbench and station configuration, BACnet/IP and MSTP, Modbus TCP, and basic IP networking (subnets, NAT, ports).

New in v1.1

Reference architectures are split into PaaS and IaaS, with new edge architectures 4 and 5 and a combined PaaS + IaaS design.



Who it's for

SI project engineers, network and IT leads, and commissioning technicians delivering Cloud BMS projects.



What's inside

Hosting models, architecture selection, prerequisites, reference designs, step-by-step configuration, commissioning tests and troubleshooting.



How to use it

Choose a hosting model and architecture in section 02, then work through sections 03 to 06 in order. Keep the IP and retnet worksheet as your as-built record.



Document status

Draft for Neeve engineering review. Procedures are generic; always confirm against current Neeve and Tridium documentation for your software versions.

Contents

01

p. 5

Solution overview

How Cloud BMS connects a cloud-hosted supervisor, in PaaS or IaaS, to on-prem building systems.

02

p. 9

Choosing your architecture

Pick a hosting model, then compare the reference architectures and choose the one that fits the site.

03

p. 14

Plan and prerequisites

Checklists, ports and the addressing worksheet to complete before anyone goes to site.

04

p. 18

Reference architectures

PaaS (p. 19), IaaS (p. 32) and combined PaaS + IaaS (p. 40) network designs and protocol options.

05

p. 43

Deployment procedures

Common build steps, then protocol configuration for each architecture.

06

p. 52

Commissioning and handover

Prove it works, record what was built and hand over with confidence.

07

p. 55

Troubleshooting

Common symptoms, likely causes and fixes, plus what to send Neeve when you escalate.

Start here

New to Cloud BMS? Read sections 01 and 02 before you quote.
Delivery teams: 03 to 06 are your working checklist.

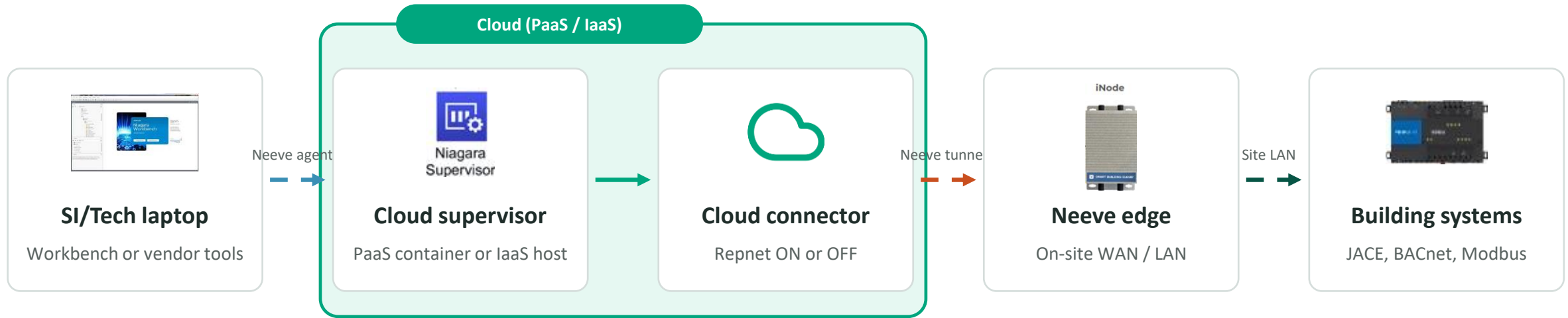
01

Solution overview

How Cloud BMS connects a cloud-hosted supervisor, in PaaS or IaaS, to on-prem building systems.

How Cloud BMS works

Four Neeve building blocks link your engineering laptop, the cloud supervisor and the building systems on site.



Cloud supervisor

PaaS: a Niagara 4 supervisor container hosted by Neeve. IaaS: a hosted Windows or Linux machine running any BMS platform. Example IP 10.0.10.11.

Cloud connector

Neeve component that terminates the Neeve tunnels from each site. Its repnet setting decides how the supervisor addresses on-prem devices.

Neeve edge

Secure edge installed on site with a WAN and LAN connection. Builds the Neeve tunnel to the cloud connector and connects to the site LAN.

Neeve agent

Connects the SI/Tech laptop to the cloud supervisor over a Neeve agent TCP connection, so engineers can work in Workbench remotely. IaaS platforms use the vendor's own tools.

Edge variants In PaaS Architectures 4 and 5 a containerized N4 also runs on the Neeve edge, so field protocols stay on site. See section 04.

Hosting models: PaaS, IaaS and PaaS + IaaS

Pick the hosting model first. It decides which reference architectures are open to you.

PaaS (Niagara)

Containerized Niagara supervisor in Neeve cloud.

- Architectures 1 to 3: cloud supervisor with repnet ON or OFF, or BACnet/SC
- Architectures 4 and 5: containerized N4 on the Neeve edge, with or without a cloud supervisor
- Engineers use Workbench through the Neeve agent

IaaS (any hosted BMS)

Hosted Windows or Linux in Neeve cloud, with any BMS platform (for example N4, WebCTRL, EBO).

- Architectures 1 to 3: same network designs as PaaS
- BDT, SC hub and Modbus settings live in the BMS application
- Engineers use the vendor-specific programming tools

PaaS + IaaS

Fully custom solutions combining PaaS and IaaS.

- Hosted platform or custom applications in IaaS, edge N4 containers from PaaS
- Decide the on-prem architecture and protocols from the PaaS and IaaS designs
- Validate the design with Neeve before ordering

Naming convention Architecture numbers repeat between hosting models. Always write PaaS Architecture 1 (P1) or IaaS Architecture 1 (I1) in quotes, drawings and the worksheet. Architectures 4 and 5 exist only in PaaS (P4, P5).

Key concepts to know before you design



Repnet ON

- On-prem devices are presented to the cloud on repnet IP addresses, e.g. 192.168.1.140 becomes 172.17.0.140.
- Each site gets its own repnet range (Site 1 172.17.0.x, Site 2 172.18.0.x), so sites can reuse the same LAN CIDR.
- Devices are added in the supervisor using their repnet IP.



Repnet OFF

- The supervisor reaches devices on their native IP addresses.
- Every site on the same connector needs a unique CIDR range.
- Overlapping ranges need add-on cloud connector infrastructure (contact sales@neve.ai).



BBMD and BDT

- A BBMD (BACnet Broadcast Management Device) forwards BACnet/IP broadcasts between IP subnets on UDP 47808.
- Each BBMD holds a BDT (Broadcast Distribution Table) listing its peer BBMDs as IP:port with mask 255.255.255.255.
- Alternative: register the cloud supervisor as a foreign device to the on-prem BBMD.



BACnet/SC (Secure Connect)

- Nodes connect to a hub over TLS-secured WebSockets using certificate-based authentication.
- The hub relays traffic between nodes, including broadcasts, so no BBMD is needed.
- Requires hub and node configuration plus certificate management.

02

Choosing your architecture

Pick a hosting model, compare the reference architectures and choose the one that fits the site.

PaaS architectures at a glance

P1 to P5. Architectures 1 to 3 use a cloud supervisor; 4 and 5 add a containerized N4 on the edge.

	P1: BACnet/IP repnet ON	P2: BACnet/SC repnet ON	P3: BACnet/IP repnet OFF	P4: Edge + cloud repnet ON	P5: Edge only repnet ON
Supervisor	Cloud N4 container	Cloud N4 container	Cloud N4 container	Cloud N4 plus an N4 per edge	N4 per edge; Neeve portal in cloud
Cloud connector	Repnet ON	Repnet ON	Repnet OFF	Repnet ON	Repnet ON
Device addressing	Repnet IP (e.g. 172.17.0.140)	BACnet: native IP via SC hub. Modbus, Fox: repnet IP	Native IP (e.g. 192.168.1.140)	Field: native LAN IP at edge. Cloud: edge N4 repnet IP	Native LAN IP at the edge N4
BACnet discovery	Unicast only. Broadcast scan will not work (NAT)	Works natively	Works	Local, at the edge N4	Local, at the edge N4
BACnet MSTP devices	Cannot be added manually	Discovered as in on-prem experience	Can be installed	Handled at the edge N4	Handled at the edge N4
BBMD configuration	Required: cloud N4 and on-prem BBMD	Not required. Hub and node config plus certificates	Required: cloud N4 and on-prem BBMD	On-prem only, for multi-subnet sites	On-prem only, for multi-subnet sites
Same CIDR across sites	Supported	Supported	Not supported on the same connector	Supported (unique repnet per site)	Supported (unique repnet per site)
Add-on infra cost	None	None	Add-on connector if devices share CIDR	Confirm with Neeve	Confirm with Neeve
Traffic security	Via Neeve tunnel	Encrypted, certificate-based authentication	Via Neeve tunnel	Neeve tunnel; Cloudflare to 3rd-party cloud	Neeve tunnel; Cloudflare to 3rd-party cloud
Watch out for	Managing repnet IPs on large systems	Hub and node setup is challenging the first time	CIDR planning across sites	One N4 per site to license and back up	Supervision runs per site: plan remote access

IaaS architectures at a glance

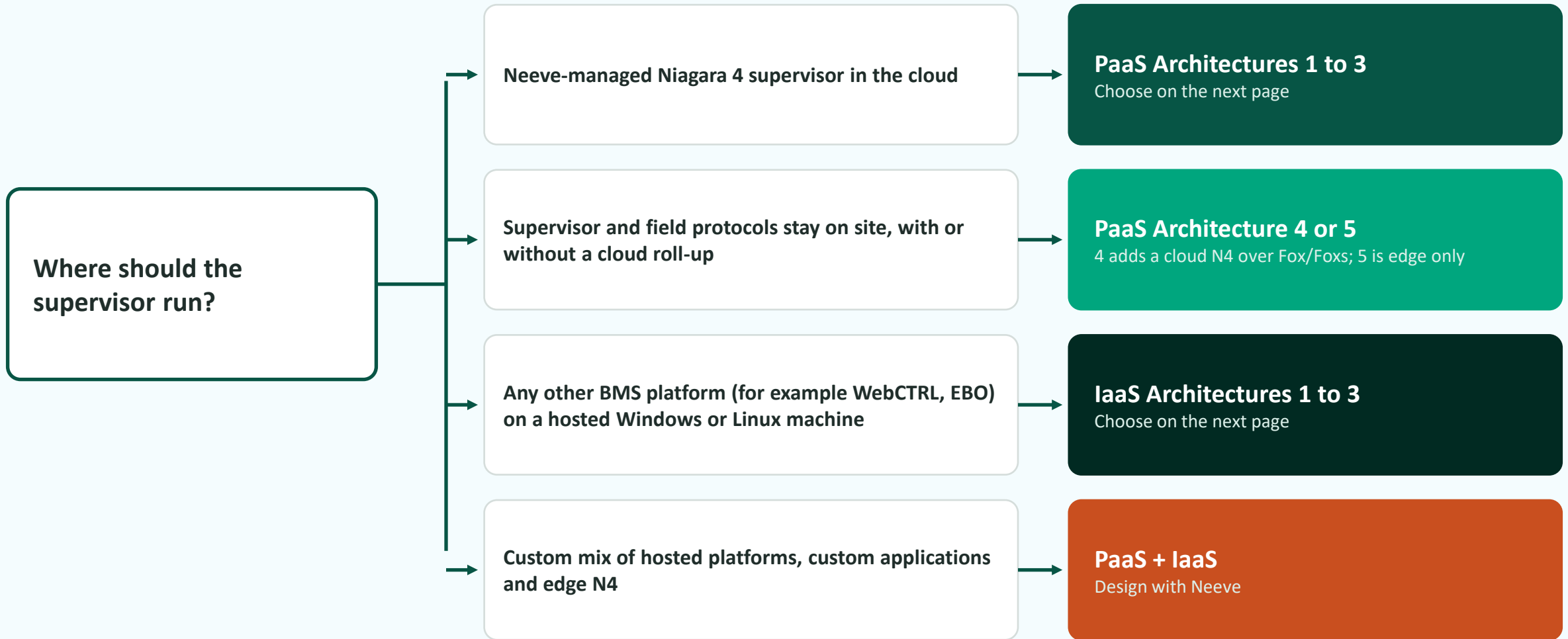
I1 to I3. Hosted Windows or Linux in Neeve cloud, running any BMS platform.

	I1: BACnet/IP repnet ON	I2: BACnet/SC repnet ON	I3: BACnet/IP repnet OFF
Hosted platform	Windows or Linux host, any BMS platform	Windows or Linux host, any BMS platform	Windows or Linux host, any BMS platform
Cloud connector	Repnet ON	Repnet ON	Repnet OFF
Device addressing	Repnet IP (e.g. 172.17.0.140)	BACnet: via SC hub. Modbus: repnet IP	Native IP (e.g. 192.168.1.140)
BACnet discovery	Unicast only. Broadcast scan will not work (NAT)	Depends on the BACnet/SC and routed BACnet topology	Broadcast scan works
BACnet MSTP devices	Cannot be added manually	Via the on-prem JACE/router; verify routing per topology	Can be installed
BBMD configuration	Required: BMS application and on-prem BBMD	Not required. Hub and node config plus certificates	Required: BMS application and on-prem BBMD
Same CIDR across sites	Supported	Supported	Not supported on the same connector
Add-on infra cost	None	None	Add-on connector if devices share CIDR
Engineering tools	Vendor-specific programming tools	Vendor-specific programming tools	Vendor-specific programming tools
Watch out for	Managing repnet IPs on large systems	Hub and node setup is challenging the first time	CIDR planning across sites

PaaS + IaaS Custom designs that combine a hosted platform with PaaS edge N4 containers are covered on page 40.

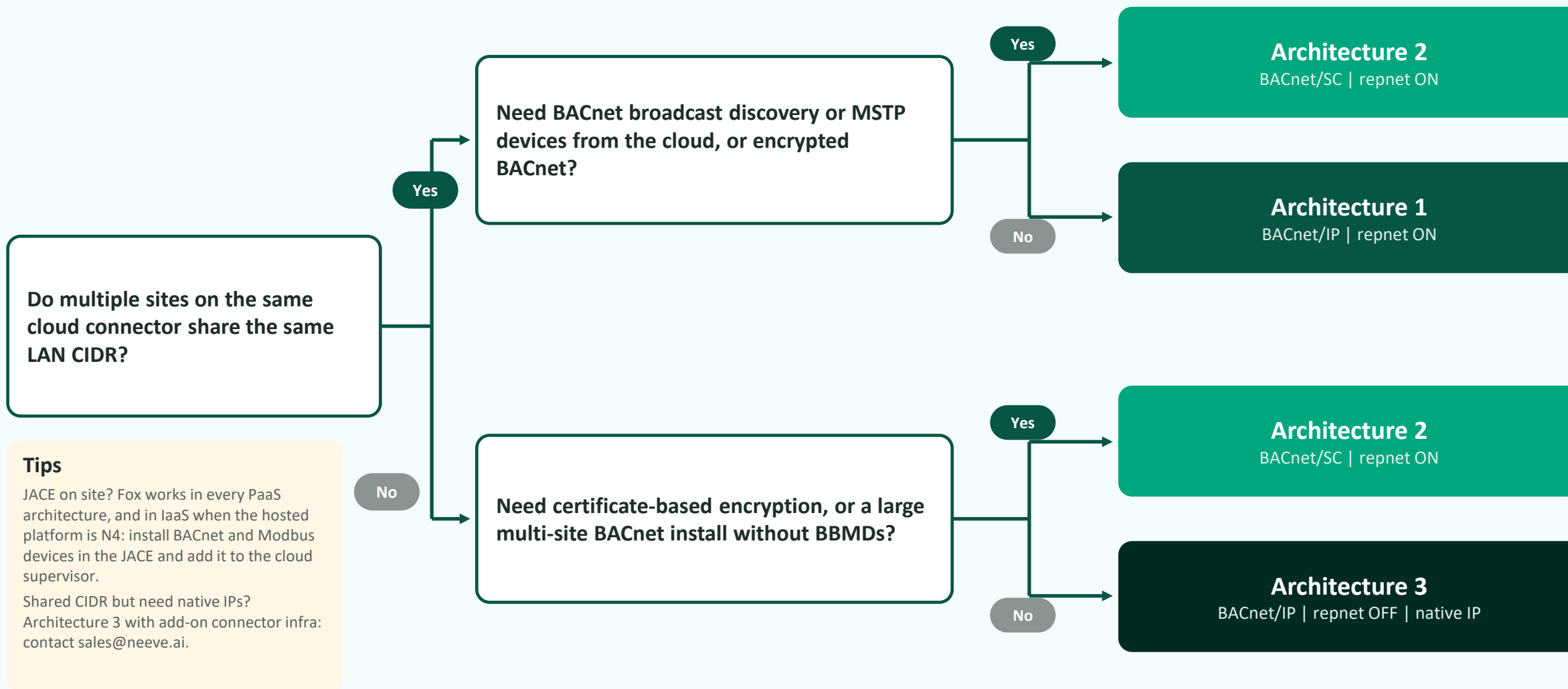
Which hosting model should I use?

Start with where the supervisor and the field protocols should live. Validate the choice with the Neeve team before ordering.



Which architecture should I use?

PaaS and IaaS Architectures 1 to 3. Answer two questions, then validate the choice with Neeve before ordering.



03

Plan and prerequisites

Checklists, ports and the addressing worksheet to complete before anyone goes to site.

Pre-deployment checklist

Tick every item before mobilising. Gaps found on site cost the most time.



Site and OT network

- ☐ Site LAN CIDR, gateway and free LAN IPs for the Neeve edge (and the edge N4 container in P4 and P5) confirmed
- ☐ Internet (WAN) connection available for the Neeve edge
- ☐ Device inventory: BACnet/IP, MSTP, Modbus TCP and JACEs with IPs, device instances and network numbers
- ☐ BBMD-capable device identified on site (JACE or BACnet router) for Architectures 1 and 3
- ☐ BACnet device instances and network numbers unique across all sites
- ☐ Modbus register maps and unit IDs available



Cloud and platform

- ☐ PaaS: N4 supervisor container provisioned. IaaS: Windows or Linux host and BMS platform provisioned. IP recorded
- ☐ Licence covers required drivers (BACnet, Modbus, Niagara network or platform equivalents) and device/point counts
- ☐ Supervisor, edge N4 and JACE Niagara versions compatible
- ☐ Cloud connector deployed with repnet set to match the chosen architecture
- ☐ Architecture 2: BACnet/SC support confirmed on all nodes; hub location and certificate plan agreed
- ☐ P4 and P5: 3rd-party cloud apps and Cloudflare tunnel agreed with Neeve



Access and governance

- ☐ Named Neeve agent access for each engineer
- ☐ Workbench (PaaS) or the vendor's tools (IaaS) and the Neeve agent installed on each SI/Tech laptop
- ☐ Customer IT approval for the edge install and its WAN connection
- ☐ Site contacts, access and change window agreed
- ☐ IP and repnet worksheet completed and approved
- ☐ Station and platform credentials managed per customer policy

Ports and protocols reference

Default ports shown. P = PaaS, I = IaaS. Confirm site-specific values and the Neeve network requirements with the Neeve team.

Protocol	Transport and port	Path	Architectures	Notes
BACnet/IP	UDP 47808	Cloud supervisor to on-prem BBMD and devices, via Neeve tunnel	P1, P3, I1, I3	BDT entries use IP:47808 with mask 255.255.255.255
BACnet/SC	TLS over WebSocket (wss); port set on the hub	Cloud and on-prem nodes to SC-Hub	P2, I2	Certificate-based authentication; no BBMD
Modbus TCP	TCP 502	Supervisor (cloud, or edge N4 in P4 and P5) to Modbus device	All	Open port 502; add device IP and register addresses manually
Niagara Fox / Foxs	TCP 1911 / TCP 4911	Cloud N4 to on-prem JACE (P4: cloud N4 to edge N4)	P1 to P4; I (N4 only)	Prefer Foxs (TLS) where supported
Niagara platform	TCP 3011 / TCP 5011 (TLS)	Workbench to JACE or supervisor platform	All with N4	Commissioning, software install, backups
Engineer access	Neeve agent TCP connection	SI/Tech laptop to cloud supervisor (IaaS: vendor tools)	All	Access provisioned per engineer
Neeve tunnel	Outbound from Neeve edge WAN	Neeve edge to cloud connector	All	Confirm firewall requirements with Neeve before install
Cloudflare tunnel	Outbound; confirm with Neeve	Neeve cloud (P4) or edge N4 (P5) to 3rd-party cloud apps	P4, P5	Confirm requirements with Neeve

IP and repnet planning worksheet

One row per device the cloud supervisor talks to. Example rows use P1 values.

Site	Device	Role	Local IP	Repnet IP	Protocol	BDT entry (IP:port)
Cloud	N4 supervisor / BMS host	Supervisor / BBMD	10.0.10.11	n/a	BACnet/IP, Modbus, Fox	10.0.10.11:47808
Site 1	Neeve edge	Secure edge	LAN 192.168.1.211	n/a	WAN 14.151.161.171	n/a
Site 1	BACnet/IP Router	On-prem BBMD	192.168.1.140	172.17.0.140	BACnet/IP, MSTP	Cloud BDT: 172.17.0.140:47808
Site 1	Jace-01	JACE	192.168.1.141	172.17.0.141	Fox	n/a
Site 1	Modbus TCP/IP	Energy meter	192.168.1.142	172.17.0.142	Modbus TCP 502	n/a
Site 2	BACnet/IP Router	On-prem BBMD	192.168.1.140	172.18.0.140	BACnet/IP, MSTP	Cloud BDT: 172.18.0.140:47808

Rules of thumb Repnet ranges must be unique per site. With repnet OFF, LAN CIDRs must be unique per site. BACnet device instances and network numbers must be unique across every site. Keep this worksheet current: it becomes the as-built record at handover. For P4 and P5 add a row per edge N4 (e.g. 192.168.1.210, repnet 172.17.0.210).

04

Reference architectures

PaaS, IaaS and combined network designs, with protocol options for each.

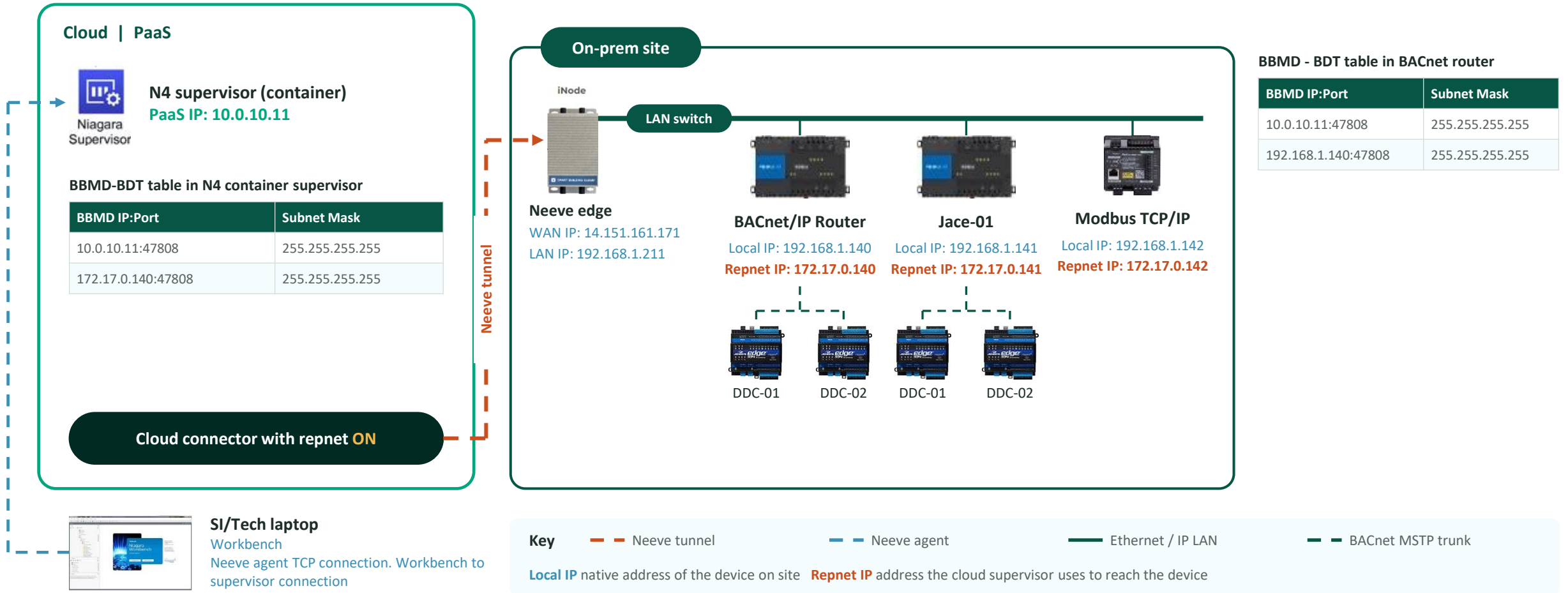
04A

PaaS (Niagara)

Containerized Niagara supervisor in Neeve cloud. Architectures 1 to 5.

PaaS Architecture 1 (P1): BACnet/IP, repnet ON

Cloud BMS – PaaS – Architecture 1. Cloud connector with repnet ON. Devices are reached on repnet IPs.



PaaS Architecture 1 (P1): protocol options and trade-offs

Supervisor reaches on-prem devices on repnet IPs. Best for existing and new customers with no add-on infra.

Containerized Niagara supervisor in Neeve cloud. Cloud to on-prem protocol options on this network config:



BACnet/IP comm

- Only unicast BACnet will work (scan/discovery will not work due to NAT).
- Enable BBMD in the N4 in cloud and a JACE or BBMD-capable device (e.g. BACnet router) on-prem, or configure the cloud supervisor as a BACnet foreign device with the on-prem BACnet router as BBMD. Example BBMD table config shown in the diagram.
- Add a BACnet/IP device manually in the N4 supervisor station using its repnet IP (e.g. 172.17.0.140).
- BACnet/IP device points can be discovered, as it is unicast BACnet communication.

! BACnet MSTP devices cannot be added manually.



Modbus/IP comm

- Open port 502.
- Add a Modbus device repnet IP (172.17.0.142) and its register addresses manually in the N4 supervisor station.



Fox protocol comm

- Install all BACnet and Modbus devices in the on-prem JACE.
- Add the JACE repnet IP (172.17.0.141) manually in the cloud N4 supervisor as a Niagara network.

Pros

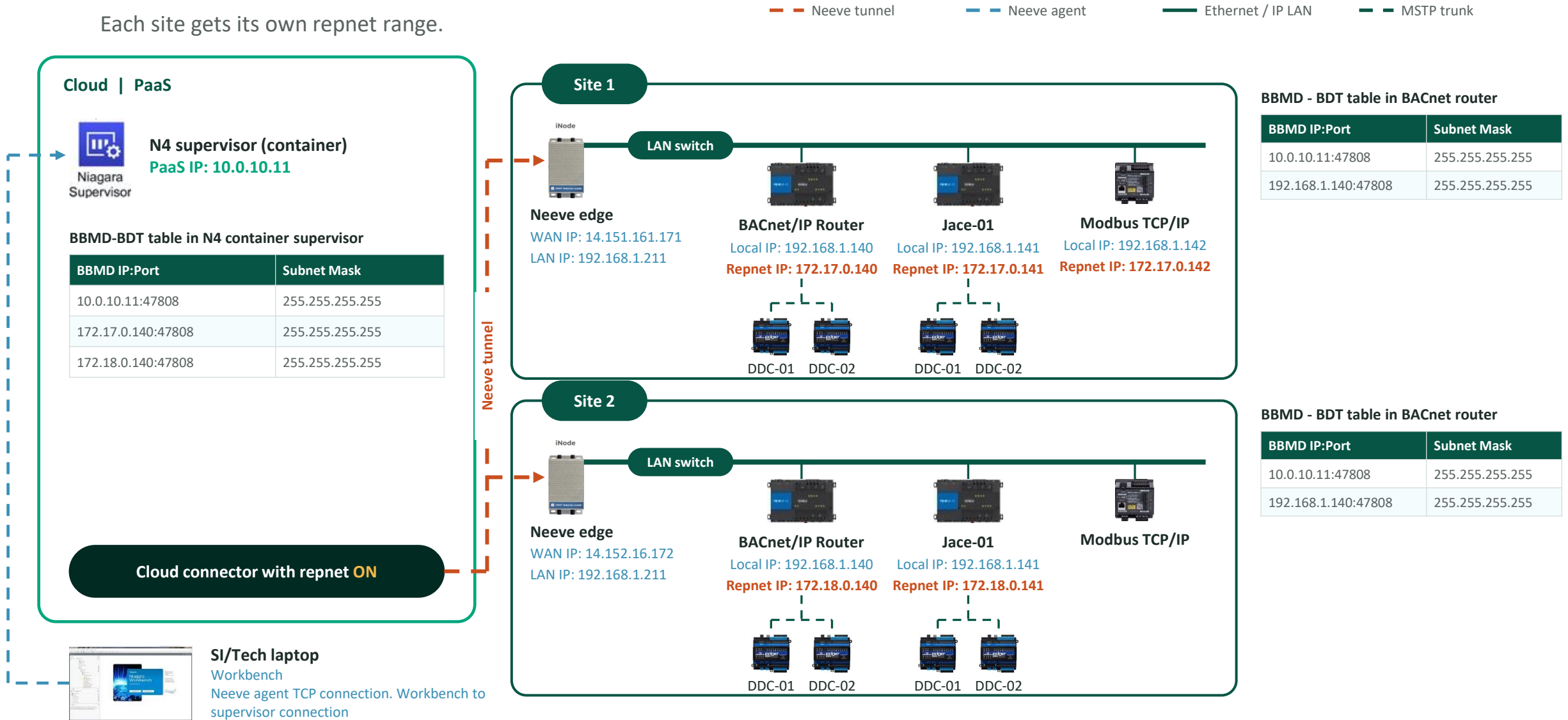
- + Existing customer and new customer support with no add-on infra cost
- + Same CIDR range network supported across sites (edges)

Cons

- Cannot use native device IP for device installation in the supervisor
- Managing repnet IP addresses on a large scaling system

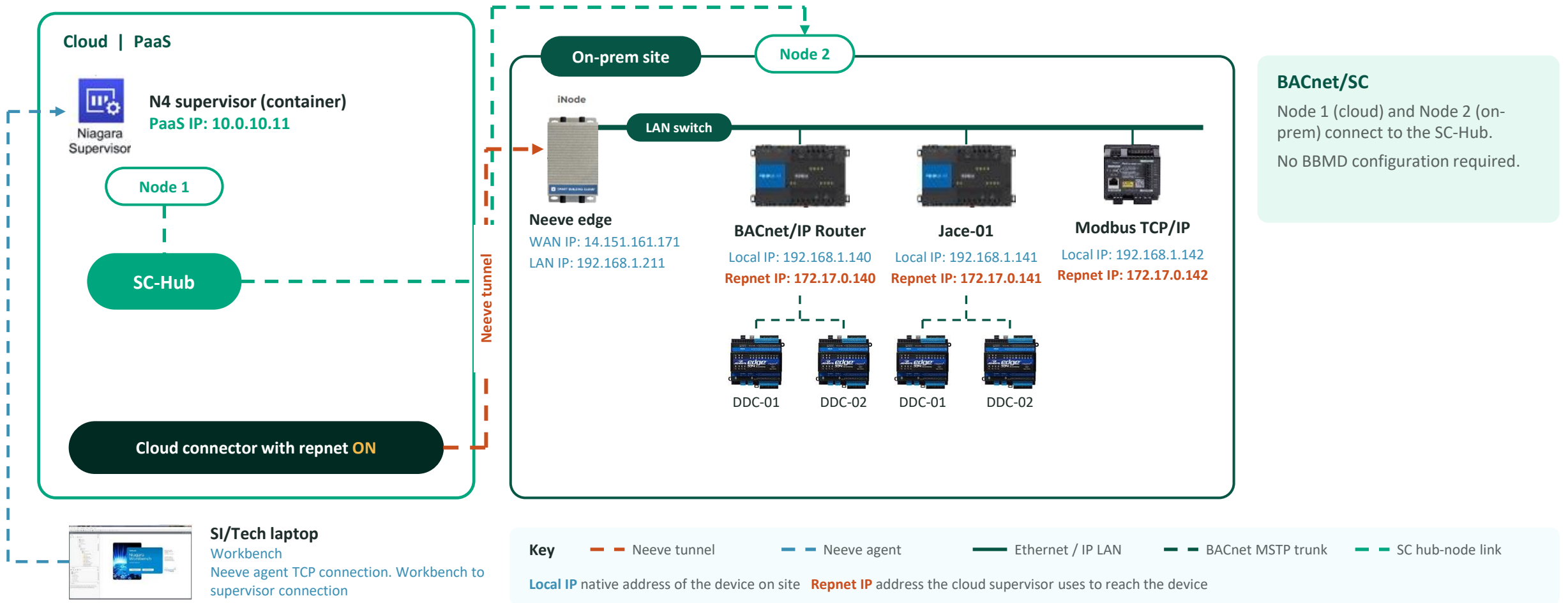
PaaS Architecture 1 (P1) scaled: multiple sites, repnet ON

Each site gets its own repnet range.



PaaS Architecture 2 (P2): BACnet/SC, repnet ON

Cloud BMS – PaaS – Architecture 2. Repnet ON with BACnet/SC hub and nodes.



PaaS Architecture 2 (P2): protocol options and trade-offs

BACnet/SC gives encrypted, certificate-authenticated BACnet across sites.

Containerized Niagara supervisor in Neeve cloud. Cloud to on-prem protocol options on this network config:



BACnet/SC (secure connect)

- BACnet broadcast scan/discovery will work natively.
- Hub and node configuration to be done. Certificate management to be done.
- No BBMD configuration required. Easily scalable to large installation.
- BACnet/IP and MSTP devices and points can be discovered as in on-prem experience with all native IP.



Modbus/IP comm

- Open port 502.
- Add a Modbus device repnet IP (172.17.0.142) and its register addresses manually in the N4 supervisor station.



Fox protocol comm

- Install all BACnet and Modbus devices in the on-prem JACE.
- Add the JACE repnet IP (172.17.0.141) manually in the cloud N4 supervisor as a Niagara network.

Pros

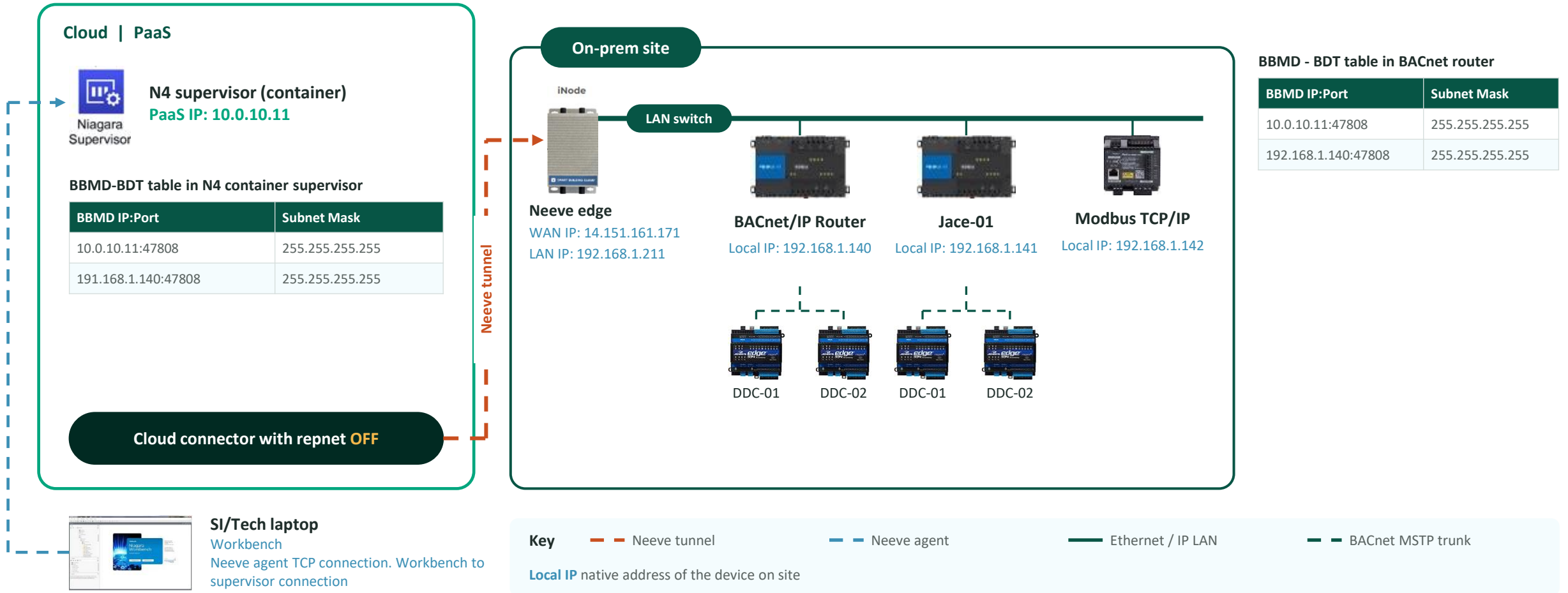
- + Existing customer and new customer support with no add-on infra cost
- + Same CIDR range network supported across sites (edges)
- + Scalable across multiple sites
- + Encrypted traffic, using certificate-based authentication

Cons

- Hub and node configuration can be challenging the first time

PaaS Architecture 3 (P3): BACnet/IP, repnet OFF

Cloud BMS – PaaS – Architecture 3. Repnet OFF: native IPs end to end.



PaaS Architecture 3 (P3): protocol options and trade-offs

Native IP addressing across the system. Each site on a connector needs its own CIDR range.

Containerized Niagara supervisor in Neeve cloud. Cloud to on-prem protocol options on this network config:



BACnet/IP comm

- BACnet broadcast scan/discovery will work.
- Enable BBMD in the N4 in cloud and a JACE or BBMD-capable device (e.g. BACnet router) on-prem, or configure the cloud supervisor as a BACnet foreign device with the on-prem BACnet router as BBMD. Example BBMD table config shown in the diagram.
- BACnet/IP device points can be discovered, as it is unicast BACnet communication.
- BACnet MSTP devices can be installed.



Modbus/IP comm

- Open port 502.
- Add a Modbus device using its native IP address and register addresses manually in the N4 supervisor station.



Fox protocol comm

- Install all BACnet and Modbus devices in the on-prem JACE.
- Add the JACE native IP manually in the cloud N4 supervisor as a Niagara network.

Pros

- + Native IP address across the system
- + BACnet broadcast scan will work

Cons

- Add-on infra cost for the cloud connector if devices share CIDR ranges (contact sales@neve.ai)
- Same CIDR range network not supported when the same connector is used across sites

PaaS Architecture 3 (P3) scaled: multiple sites, repnet OFF

Unique CIDR per site; every BBMD lists every peer.

Neeve tunnel

Neeve agent

Ethernet / IP LAN

MSTP trunk

Cloud | PaaS



N4 supervisor (container)
PaaS IP: 10.0.10.11

BBMD-BDT table in N4 container supervisor

BBMD IP:Port	Subnet Mask
10.0.10.11:47808	255.255.255.255
191.168.1.140:47808	255.255.255.255
192.168.2.140:47808	255.255.255.255

Cloud connector with repnet **OFF**



SI/Tech laptop

Workbench

Neeve agent TCP connection. Workbench to supervisor connection

Neeve tunnel

Site 1



Neeve edge

WAN IP: 14.151.161.171
LAN IP: 192.168.1.211

LAN switch

BACnet/IP Router

Local IP: 192.168.1.140

Jace-01

Local IP: 192.168.1.141

Modbus TCP/IP

Local IP: 192.168.1.142



DDC-01 DDC-02



DDC-01 DDC-02

Site 2



Neeve edge

WAN IP: 14.152.16.172
LAN IP: 192.168.2.211

LAN switch

BACnet/IP Router

Local IP: 192.168.2.140

Jace-01

Local IP: 192.168.2.141

Modbus TCP/IP



DDC-01 DDC-02



DDC-01 DDC-02

BBMD - BDT table in BACnet router

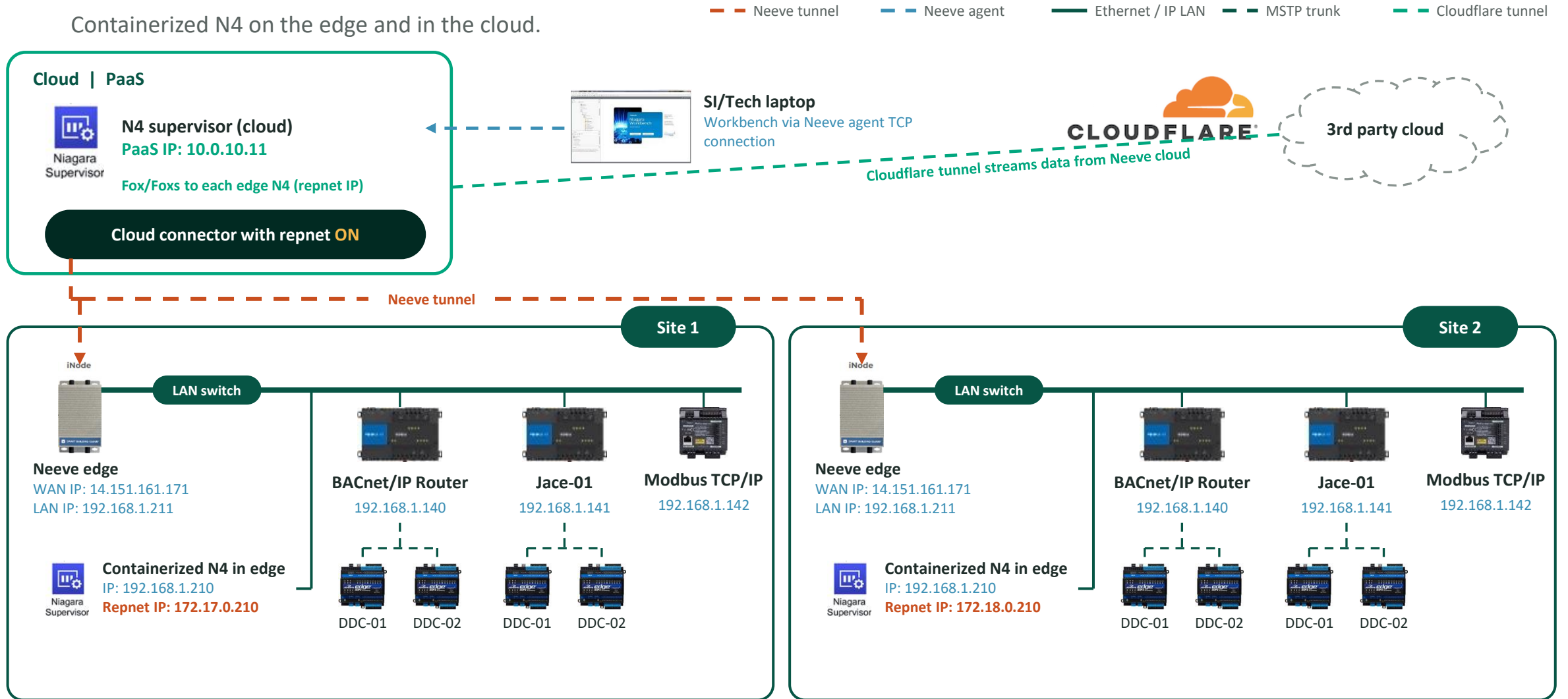
BBMD IP:Port	Subnet Mask
10.0.10.11:47808	255.255.255.255
192.168.1.140:47808	255.255.255.255
192.168.2.140:47808	255.255.255.255

BBMD - BDT table in BACnet router

BBMD IP:Port	Subnet Mask
10.0.10.11:47808	255.255.255.255
192.168.1.140:47808	255.255.255.255
192.168.2.140:47808	255.255.255.255

PaaS Architecture 4 (P4): edge + cloud, repnet ON

Containerized N4 on the edge and in the cloud.



PaaS Architecture 4 (P4): protocol options and trade-offs

Field protocols stay on site; the cloud N4 rolls the sites up over Fox/Foxs.

Cloud to on-prem protocol options on this network config:



Fox protocol comm (cloud to edge)

- Fox/Foxs protocol between the N4 in the edge and the N4 in the cloud.
- Add the N4 container repnet IPs (172.17.0.210, 172.18.0.210) manually in the cloud N4 supervisor as a Niagara network.
- All graphics can be streamed from the on-prem N4 supervisor in the edge.



Field protocols (on prem)

- BACnet/IP, Modbus/IP, KNX and other protocols all stay on prem.
- Handled by the N4 container running at the edge.
- Device discovery and BBMD configuration for multi-subnet networks stay on prem.
- Typical on-prem commissioning and programming at the edge N4.



3rd-party cloud apps

- Containerized N4 runs in the Neeve edge and in the cloud.
- Stream data to 3rd-party cloud apps from Neeve cloud using a Cloudflare tunnel.

Pros

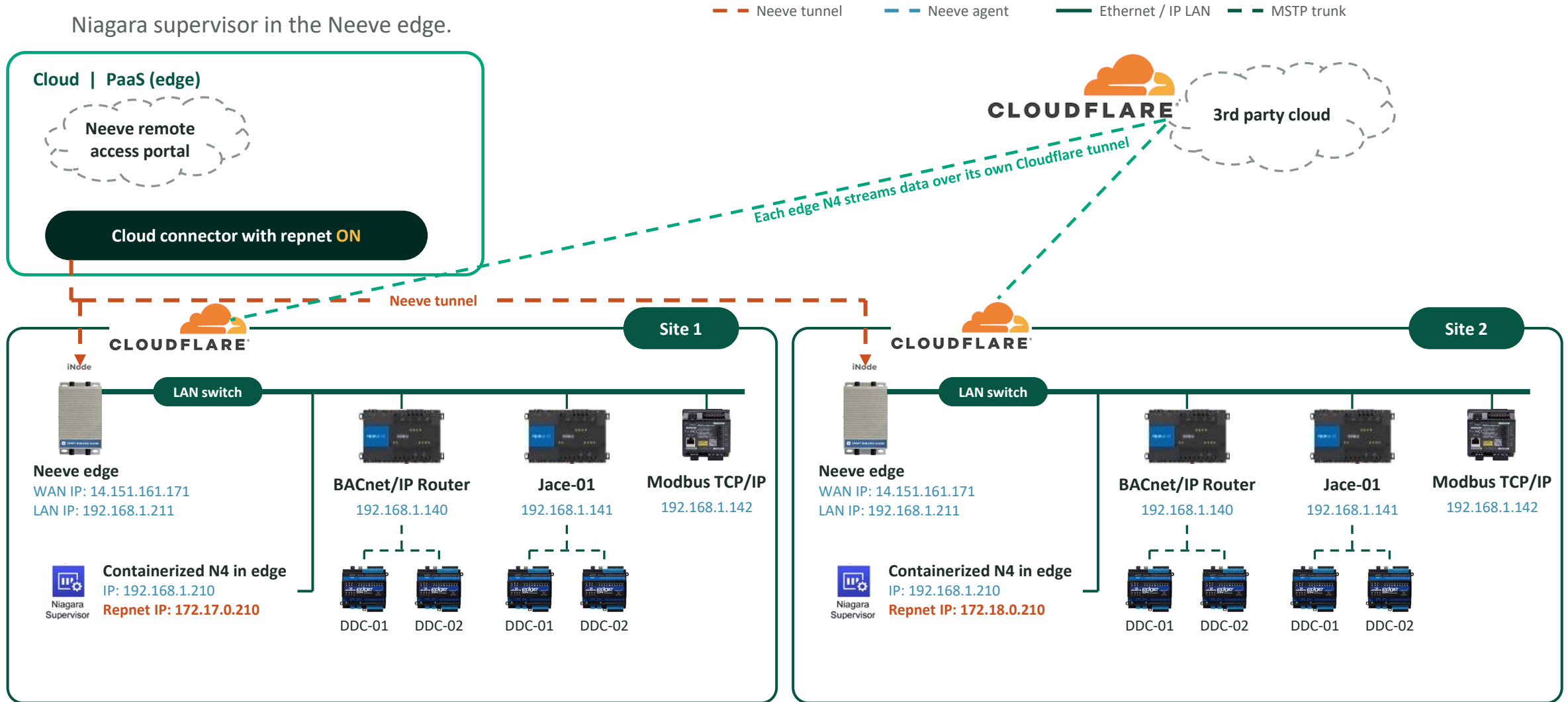
- + Field-level protocols, discovery and BBMD stay on site
- + Same LAN CIDR across sites, with a unique repnet IP per edge N4
- + Graphics and commissioning at the edge N4

Cons

- One N4 container per site to commission, license and back up
- Cloud supervisor depends on the Fox/Foxs link to every edge N4

PaaS Architecture 5 (P5): edge only, repnet ON

Niagara supervisor in the Neeve edge.



PaaS Architecture 5 (P5): protocol options and trade-offs

Everything runs on site. The cloud side is remote access and data streaming.

Cloud to on-prem protocol options on this network config:



Edge supervisor

- Niagara supervisor runs in the Neeve edge, one per site (e.g. IP 192.168.1.210).
- All protocols, BACnet/IP, Modbus/IP, KNX and so on, stay on prem.
- Typical on-prem commissioning and programming at the edge N4.



Remote access

- Neeve remote access portal in the cloud.
- Cloud connector with repnet ON; each edge N4 has its own repnet IP (172.17.0.210, 172.18.0.210).
- Workbench reaches the edge N4 over the Neeve agent TCP connection.



3rd-party cloud apps

- Stream data to 3rd-party cloud apps using a Cloudflare tunnel from each edge.

Pros

- + Supervision and field protocols stay on site
- + Same LAN CIDR across sites, with a unique repnet IP per edge N4

Cons

- One N4 per site to license, back up and maintain
- No single cloud supervisor view of all sites

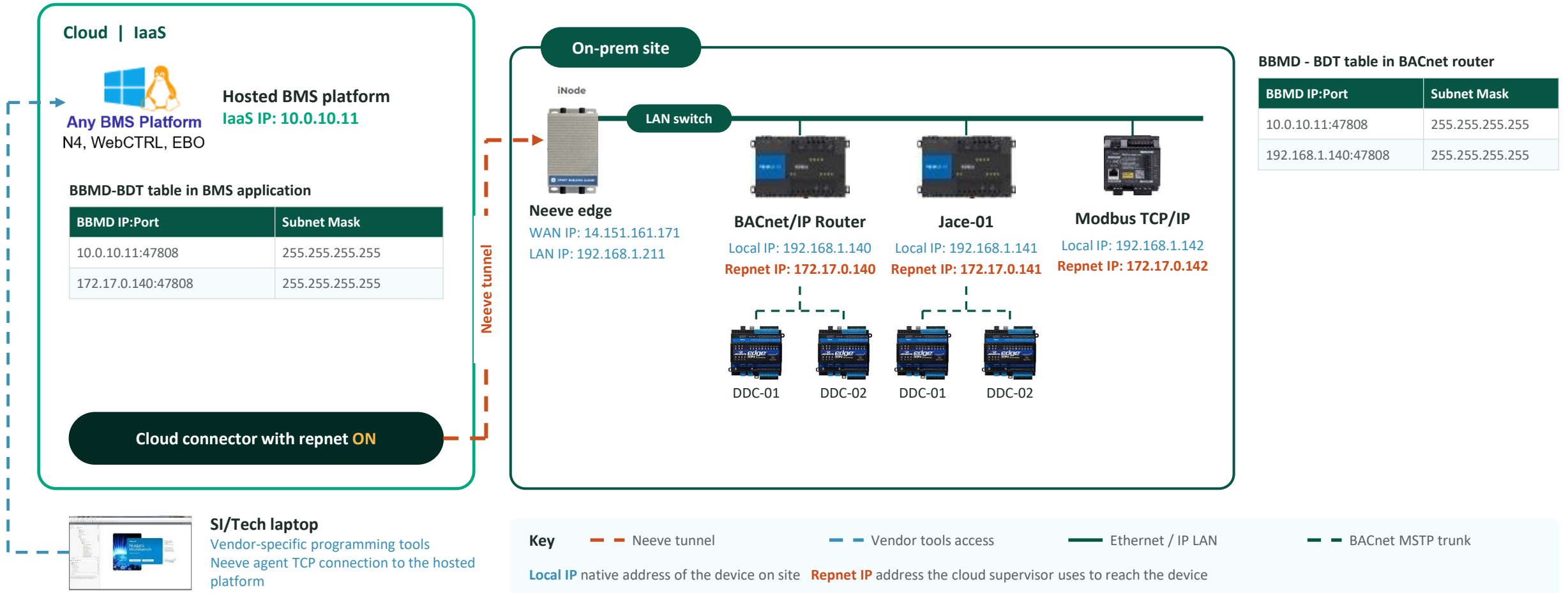
04B

IaaS (any hosted BMS)

Hosted Windows or Linux in Neeve cloud, running any BMS platform. Architectures 1 to 3.

IaaS Architecture 1 (I1): BACnet/IP, repnet ON

Cloud BMS – IaaS – Architecture 1. Cloud connector with repnet ON. Devices are reached on repnet IPs.



IaaS Architecture 1 (I1): protocol options and trade-offs

Supervisor reaches on-prem devices on repnet IPs. Best for existing and new customers with no add-on infra.

Hosted Windows or Linux in Neeve cloud, with any BMS platform. Cloud to on-prem protocol options on this network config:



BACnet/IP comm

- Only unicast BACnet will work (scan/discovery will not work due to NAT).
- Enable BBMD in the BMS application in cloud and a JACE or BBMD-capable device (e.g. BACnet router) on-prem, or configure the cloud supervisor as a BACnet foreign device with the on-prem BACnet router as BBMD. Example BBMD table config shown in the diagram.
- Add a BACnet/IP device manually in the BMS application using its repnet IP (e.g. 172.17.0.140).
- BACnet/IP device points can be discovered, as it is unicast BACnet communication.

! BACnet MSTP devices cannot be added manually.



Modbus/IP comm

- Open port 502.
- Add a Modbus device repnet IP (172.17.0.142) and its register addresses manually in the BMS application.



Fox comm (Windows/Linux N4)

- Install all BACnet and Modbus devices in the on-prem JACE.
- Add the JACE repnet IP (172.17.0.141) manually in the cloud N4 supervisor as a Niagara network.

Pros

- + Existing customer and new customer support with no add-on infra cost
- + Same CIDR range network supported across sites (edges)

Cons

- Cannot use native device IP for device installation in the supervisor
- Managing repnet IP addresses on a large scaling system

IaaS Architecture 1 (I1) scaled: multiple sites, repnet ON

Each site gets its own repnet range.

— Neeve tunnel — Vendor tools — Ethernet / IP LAN — MSTP trunk

Cloud | IaaS



Any BMS Platform
N4, WebCTRL, EBO

Hosted BMS platform
IaaS IP: 10.0.10.11

BBMD-BDT table in BMS application

BBMD IP:Port	Subnet Mask
10.0.10.11:47808	255.255.255.255
172.17.0.140:47808	255.255.255.255
172.18.0.140:47808	255.255.255.255

Cloud connector with repnet ON



SI/Tech laptop

Vendor-specific programming tools
Neeve agent TCP connection to the hosted platform

Neeve tunnel

Site 1



Neeve edge

WAN IP: 14.151.161.171
LAN IP: 192.168.1.211

LAN switch

BACnet/IP Router

Local IP: 192.168.1.140
Repnet IP: 172.17.0.140

Jace-01

Local IP: 192.168.1.141
Repnet IP: 172.17.0.141

Modbus TCP/IP

Local IP: 192.168.1.142
Repnet IP: 172.17.0.142



DDC-01 DDC-02



DDC-01 DDC-02

Site 2



Neeve edge

WAN IP: 14.152.16.172
LAN IP: 192.168.1.211

LAN switch

BACnet/IP Router

Local IP: 192.168.1.140
Repnet IP: 172.18.0.140

Jace-01

Local IP: 192.168.1.141
Repnet IP: 172.18.0.141

Modbus TCP/IP



DDC-01 DDC-02



DDC-01 DDC-02

BBMD - BDT table in BACnet router

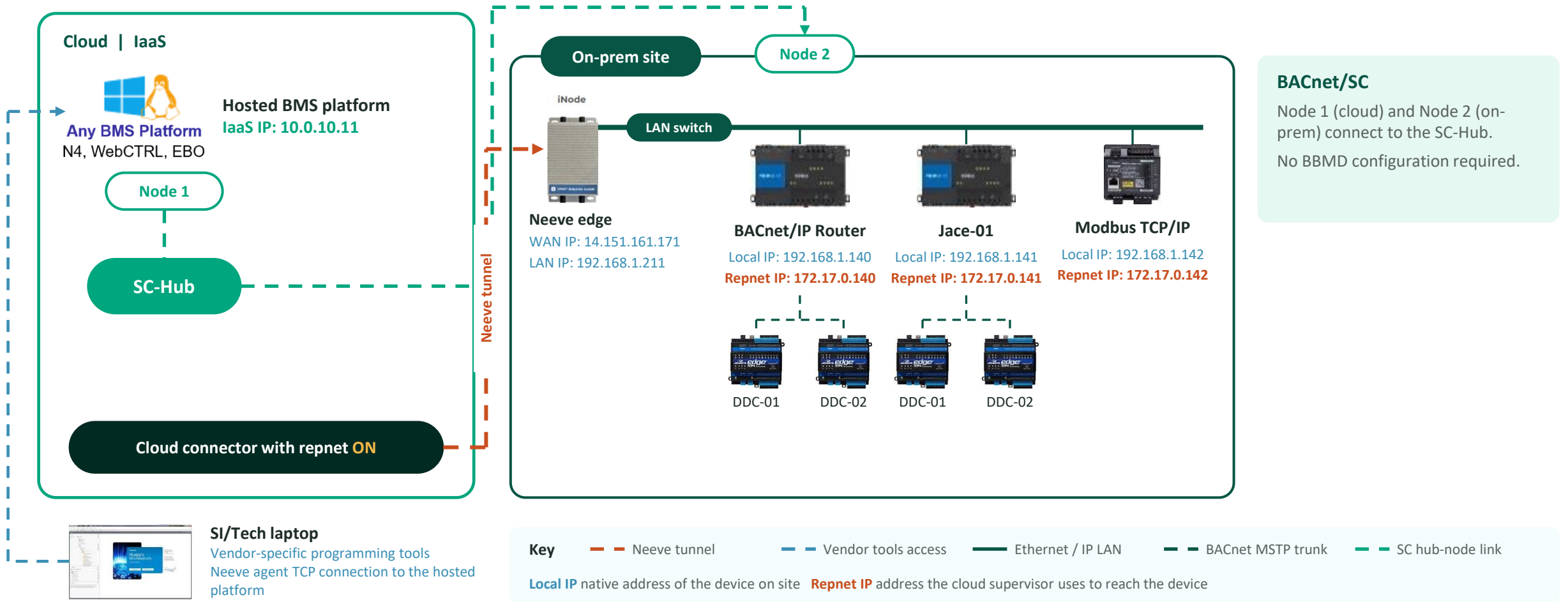
BBMD IP:Port	Subnet Mask
10.0.10.11:47808	255.255.255.255
192.168.1.140:47808	255.255.255.255

BBMD - BDT table in BACnet router

BBMD IP:Port	Subnet Mask
10.0.10.11:47808	255.255.255.255
192.168.1.140:47808	255.255.255.255

IaaS Architecture 2 (I2): BACnet/SC, repnet ON

Cloud BMS – IaaS – Architecture 2. Repnet ON with BACnet/SC hub and nodes.



IaaS Architecture 2 (I2): protocol options and trade-offs

BACnet/SC gives encrypted, certificate-authenticated BACnet across sites.

Hosted Windows or Linux in Neeve cloud, with any BMS platform. Cloud to on-prem protocol options on this network config:



BACnet/SC (secure connect)

- BACnet/SC uses secure hub-and-node connections; discovery depends on the configured BACnet/SC and routed BACnet topology.
- Hub and node configuration to be done. Certificate management to be done.
- No BBMD configuration required. Easily scalable to large installation.
- The on-prem JACE/router can route between BACnet/SC and supported local BACnet/IP or MS/TP networks; verify routing and discovery for the deployed topology.



Modbus/IP comm

- Open port 502.
- Add a Modbus device repnet IP (172.17.0.142) and its register addresses manually in the BMS application.

Pros

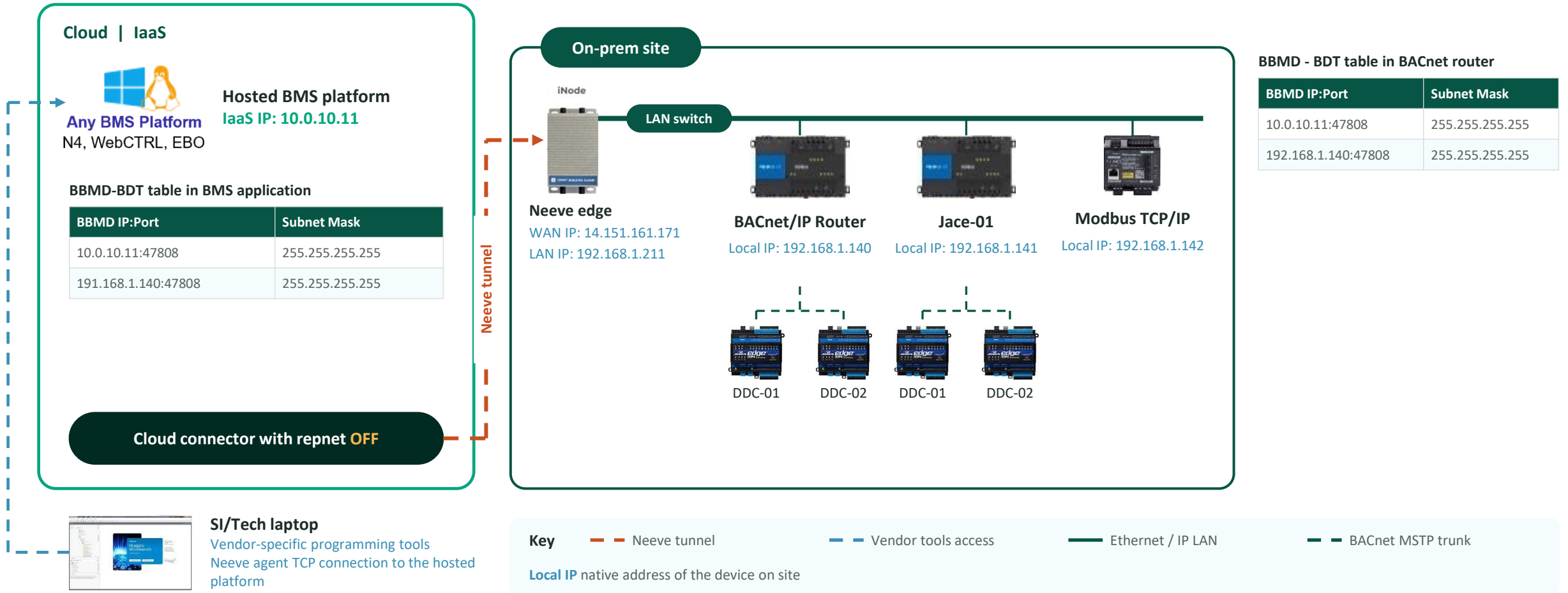
- + Existing customer and new customer support with no add-on infra cost
- + Same CIDR range network supported across sites (edges)
- + Scalable across multiple sites
- + Encrypted traffic, using certificate-based authentication

Cons

- Hub and node configuration can be challenging the first time

IaaS Architecture 3 (I3): BACnet/IP, repnet OFF

Cloud BMS – IaaS – Architecture 3. Repnet OFF: native IPs end to end.



IaaS Architecture 3 (I3): protocol options and trade-offs

Native IP addressing across the system. Each site on a connector needs its own CIDR range.

Hosted Windows or Linux in Neeve cloud, with any BMS platform. Cloud to on-prem protocol options on this network config:



BACnet/IP comm

- BACnet broadcast scan/discovery will work.
- Enable BBMD in the BMS application in cloud and a JACE or BBMD-capable device (e.g. BACnet router) on-prem, or configure the cloud supervisor as a BACnet foreign device with the on-prem BACnet router as BBMD. Example BBMD table config shown in the diagram.
- BACnet/IP device points can be discovered, as it is unicast BACnet communication.
- BACnet MSTP devices can be installed.



Modbus/IP comm

- Open port 502.
- Add a Modbus device using its native IP address and register addresses manually in the BMS application.



Fox comm (Windows/Linux N4)

- Install all BACnet and Modbus devices in the on-prem JACE.
- Add the JACE native IP manually in the cloud N4 supervisor as a Niagara network.

Pros

- + Native IP address across the system
- + BACnet broadcast scan will work

Cons

- Add-on infra cost for the cloud connector if devices share CIDR ranges (contact sales@neve.ai)
- Same CIDR range network not supported when the same connector is used across sites

IaaS Architecture 3 (I3) scaled: multiple sites, repnet OFF

Unique CIDR per site; every BBMD lists every peer.

Neeve tunnel

Vendor tools

Ethernet / IP LAN

MSTP trunk

Cloud | IaaS



Any BMS Platform
N4, WebCTRL, EBO

Hosted BMS platform
IaaS IP: 10.0.10.11

BBMD-BDT table in BMS application

BBMD IP:Port	Subnet Mask
10.0.10.11:47808	255.255.255.255
191.168.1.140:47808	255.255.255.255
192.168.2.140:47808	255.255.255.255

Cloud connector with repnet OFF



SI/Tech laptop

Vendor-specific programming tools
Neeve agent TCP connection to the hosted platform

Neeve tunnel

Site 1



Neeve edge

WAN IP: 14.151.161.171
LAN IP: 192.168.1.211

LAN switch

BACnet/IP Router

Local IP: 192.168.1.140

Jace-01

Local IP: 192.168.1.141

Modbus TCP/IP

Local IP: 192.168.1.142



DDC-01 DDC-02



DDC-01 DDC-02

Site 2



Neeve edge

WAN IP: 14.152.16.172
LAN IP: 192.168.2.211

LAN switch

BACnet/IP Router

Local IP: 192.168.2.140

Jace-01

Local IP: 192.168.2.141

Modbus TCP/IP



DDC-01 DDC-02



DDC-01 DDC-02

BBMD - BDT table in BACnet router

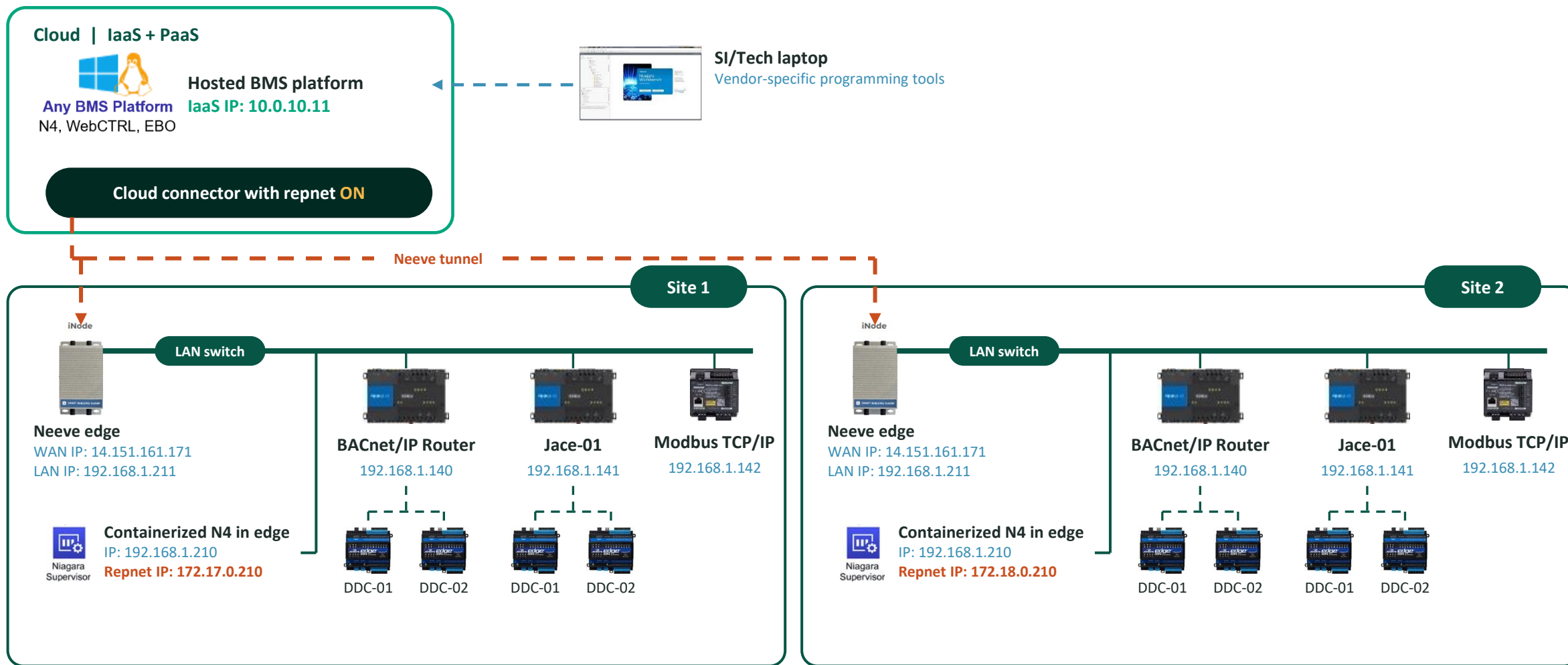
BBMD IP:Port	Subnet Mask
10.0.10.11:47808	255.255.255.255
192.168.1.140:47808	255.255.255.255
192.168.2.140:47808	255.255.255.255

BBMD - BDT table in BACnet router

BBMD IP:Port	Subnet Mask
10.0.10.11:47808	255.255.255.255
192.168.1.140:47808	255.255.255.255
192.168.2.140:47808	255.255.255.255

PaaS + IaaS: combined design

Hosted platform in the cloud, edge N4 on site.



PaaS + IaaS: design guidance

No fixed reference design. Build it from the PaaS and IaaS architectures and validate with Neeve.



What it is

- Hosted Windows or Linux in Neeve cloud, with any BMS platform or custom applications.
- Containerized N4 on the Neeve edge at each site, from PaaS.
- Cloud connector with repnet ON; unique repnet range per site.



How to design it

- Determine the on-prem architecture and communication protocols from the PaaS and IaaS solutions.
- Decide which protocols terminate at the edge N4 and which reach the hosted platform.
- Record every address in the IP and repnet worksheet.



Before you quote

- Share the site list, platforms and protocols with Neeve.
- Confirm connector, licensing and any add-on infra cost.
- Plan commissioning for each layer: edge N4, hosted platform and the links between them.

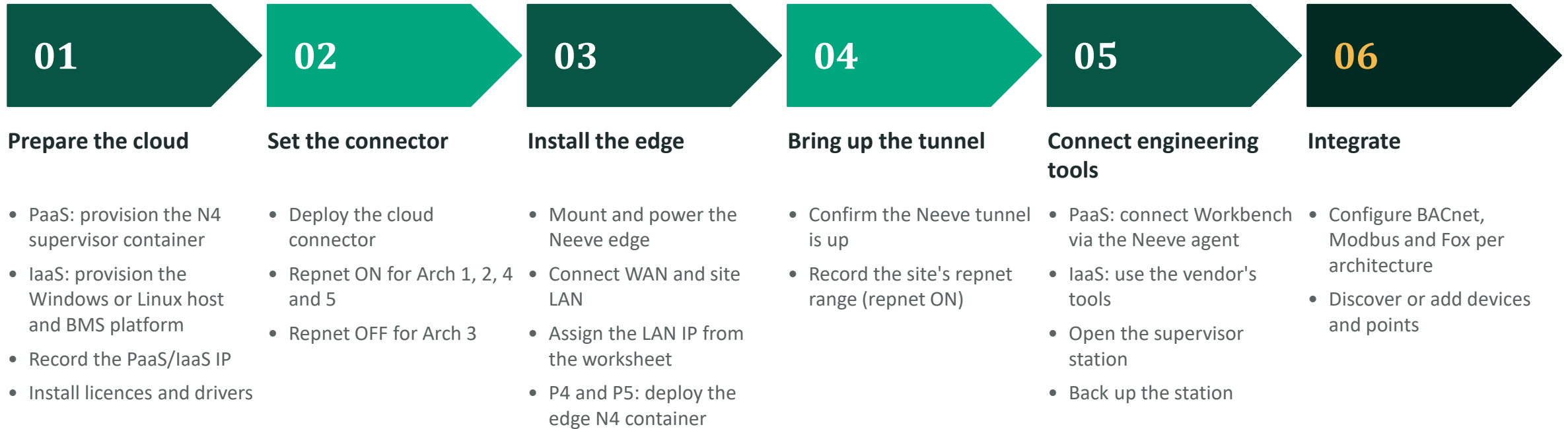
05

Deployment procedures

Common build steps, then protocol configuration for each architecture.

Deployment roadmap

Steps 1 to 5 are the same for every architecture. Step 6 follows the procedure for your architecture.



Before you integrate Take a station backup, confirm the tunnel is stable for each site, and have the IP and repnet worksheet open. Every IP you type into Workbench or the vendor's tool should come from it.

Procedure: Architecture 1 (BACnet/IP, repnet ON)

PaaS and IaaS. Complete roadmap steps 1 to 5 first. Use repnet IPs for every device you add in the cloud supervisor.

BACnet/IP

UDP 47808

- 1 In the cloud supervisor (N4 or BMS application), enable BBMD on the BACnet/IP port.
- 2 Add BDT entries: 10.0.10.11:47808 and the on-prem BBMD repnet IP 172.17.0.140:47808, mask 255.255.255.255.
- 3 On the on-prem BBMD (JACE or BACnet router), add 10.0.10.11:47808 and its own IP 192.168.1.140:47808.
- 4 Or: register the cloud supervisor as a foreign device to the on-prem BBMD instead of steps 1 to 3.
- 5 Add each BACnet/IP device manually using its repnet IP. Broadcast discovery will not work.
- 6 Discover points on each added device (unicast).

Modbus TCP

TCP 502

- 1 Confirm TCP 502 is open.
- 2 Add a Modbus TCP network in the cloud station if needed.
- 3 Add the device using repnet IP 172.17.0.142 and its unit ID.
- 4 Add register points manually from the register map.
- 5 Check device status and values.

Fox (via JACE)

TCP 1911 / 4911

- 1 Install and commission all BACnet and Modbus devices in the on-prem JACE.
- 2 In the cloud NiagaraNetwork, add the JACE manually using repnet IP 172.17.0.141.
- 3 Authenticate and accept the station certificate.
- 4 Import points, histories and alarms as required.

MSTP devices cannot be added manually in Architecture 1. Bring them in through the on-prem JACE over Fox, or choose Architecture 2 or 3.

Procedure: Architecture 2 (BACnet/SC, repnet ON)

PaaS and IaaS. Complete roadmap steps 1 to 5 first. Build and test the hub and node setup in a lab before site if it is your first.

BACnet/SC

TLS + certificates

- 1 Plan the topology: SC-Hub, Node 1 (cloud supervisor) and Node 2 (on-prem BACnet/SC device).
- 2 Create the certificates: a CA certificate plus operational certificates for the hub and each node. Record expiry dates.
- 3 Configure the hub function with its URI (wss://), port and certificates.
- 4 Configure each node with the hub URI, its operational certificate and the CA certificate.
- 5 Confirm every node shows as connected to the hub.
- 6 Run BACnet discovery from the cloud supervisor. PaaS: BACnet/IP and MSTP devices are discovered natively. IaaS: verify routing and discovery for the topology.

Modbus TCP

TCP 502

- 1 Confirm TCP 502 is open.
- 2 Add the device using repnet IP 172.17.0.142 and its unit ID.
- 3 Add register points manually from the register map.
- 4 Check device status and values.

Fox (via JACE)

TCP 1911 / 4911

- 1 Install all BACnet and Modbus devices in the on-prem JACE.
- 2 Add the JACE manually using repnet IP 172.17.0.141 as a Niagara network.
- 3 Authenticate and import points as required.
- 4 IaaS: only when the hosted platform is N4.

First time with BACnet/SC? Allow extra time for hub and node setup, confirm BACnet/SC support in your Niagara and device firmware versions, and keep a certificate register for renewals.

Procedure: Architecture 3 (BACnet/IP, repnet OFF)

PaaS and IaaS. Complete roadmap steps 1 to 5 first. Use native IPs for every device you add in the cloud supervisor.

BACnet/IP

UDP 47808

- 1 Confirm each site on this connector has a unique CIDR. Overlap needs add-on connector infra (sales@neve.ai).
- 2 In the cloud supervisor, enable BBMD and add BDT entries for 10.0.10.11:47808 and each on-prem BBMD native IP.
- 3 On each on-prem BBMD, add 10.0.10.11:47808 and every site BBMD IP (for example 192.168.1.140:47808).
- 4 Or: register the cloud supervisor as a foreign device to the on-prem BBMD.
- 5 Run a BACnet broadcast discovery from the cloud supervisor.
- 6 Discover and add MSTP devices behind the BACnet router, then their points.

Modbus TCP

TCP 502

- 1 Confirm TCP 502 is open.
- 2 Add the device using its native IP (e.g. 192.168.1.142) and unit ID.
- 3 Add register points manually from the register map.
- 4 Check device status and values.

Fox (via JACE)

TCP 1911 / 4911

- 1 Install all BACnet and Modbus devices in the on-prem JACE.
- 2 Add the JACE native IP (e.g. 192.168.1.141) manually as a Niagara network.
- 3 Authenticate and import points as required.

Keep BDTs identical. With BBMDs, every BDT should list the same peers. A missing or mistyped entry is the most common reason broadcast discovery fails.

Procedure: PaaS Architecture 4 (edge + cloud)

Complete roadmap steps 1 to 5 first. Commission each site at its edge N4, then roll the sites up in the cloud N4.

Edge N4 (each site)

Native LAN IPs

- 1 Deploy the containerized N4 on the Neeve edge and assign its LAN IP from the worksheet (e.g. 192.168.1.210).
- 2 Configure BACnet/IP, Modbus TCP, KNX and other field drivers using native LAN IPs.
- 3 For multi-subnet BACnet, configure BBMD at the edge and on the on-prem BBMD.
- 4 Discover devices and points, and commission as a typical on-prem station.
- 5 Build graphics at the edge N4.

Cloud supervisor

TCP 1911 / 4911

- 1 Record each edge N4 repnet IP (172.17.0.210, 172.18.0.210) in the worksheet.
- 2 In the cloud N4, add each edge N4 manually as a Niagara network using its repnet IP.
- 3 Authenticate and accept the station certificate (prefer Foxs).
- 4 Import points, histories and alarms as required. Graphics can be streamed from the edge N4.

3rd-party cloud

Cloudflare tunnel

- 1 Agree the destination apps and the data to stream with the customer.
- 2 Configure the Cloudflare tunnel from Neeve cloud with Neeve.
- 3 Verify data arrives and recovers after a brief WAN interruption.

Keep field devices at the edge. Discovery, BBMD tables and field-protocol commissioning stay on site. Do not add field devices to the cloud supervisor.

Procedure: PaaS Architecture 5 (edge only)

Complete roadmap steps 1 to 5 first. Each site is supervised by its own edge N4.

Edge N4 (each site)

Native LAN IPs

- 1 Deploy the containerized N4 on the Neeve edge and assign its LAN IP from the worksheet (e.g. 192.168.1.210).
- 2 Configure BACnet/IP, Modbus TCP, KNX and other field drivers using native LAN IPs.
- 3 Discover devices and points, and commission as a typical on-prem station.

Remote access

Neeve agent + portal

- 1 Confirm the cloud connector is deployed with repnet ON and the tunnel is up for each site.
- 2 Record each edge N4 repnet IP (172.17.0.210, 172.18.0.210).
- 3 Connect Workbench via the Neeve agent and open the edge N4 station.
- 4 Agree with Neeve how users reach each site through the Neeve remote access portal.

3rd-party cloud

Cloudflare tunnel

- 1 Agree the destination apps and the data to stream with the customer.
- 2 Configure a Cloudflare tunnel from each edge N4 with Neeve.
- 3 Verify data arrives and recovers after a brief WAN interruption.

Plan backups per site. There is no cloud supervisor in P5, so every edge N4 needs its own backup and licence record.

Procedure: IaaS differences

IaaS Architectures 1 to 3 follow the Architecture 1 to 3 procedures. These are the differences on a hosted BMS platform.

What stays the same

- Roadmap steps 1 to 5 and the connector settings: repnet ON for I1 and I2, OFF for I3.
- The IP and repnet worksheet and every IP rule in it.
- BDT, foreign device, SC hub and Modbus procedures, applied in the hosted platform.

What changes on a hosted platform

- Provision a Windows or Linux host in Neeve cloud and install the BMS platform (N4, WebCTRL, EBO or other).
- Enable BBMD, foreign-device registration or BACnet/SC in the platform's own BACnet settings. The BDT lives in the BMS application.
- Engineer with the vendor-specific programming tools rather than Workbench through the Neeve agent.
- Fox applies only when the hosted platform is Niagara 4.

Architecture 2 note

- The on-prem JACE or router can route between BACnet/SC and supported local BACnet/IP or MS/TP networks.
- Verify routing and discovery for the deployed topology before commissioning.
- Keep a certificate register with expiry dates.

Scaling to multiple sites

What changes when you add the second, tenth or hundredth site.

Architecture 1

Repnet ON

- Each site gets a unique repnet range (172.17.0.x, 172.18.0.x) even when LANs are identical (192.168.1.0/24).
- Add each site BBMD's repnet IP to the cloud BDT (172.17.0.140, 172.18.0.140).
- Repnet addressing grows with every site: keep the worksheet current.

Architecture 2

BACnet/SC

- Add each site's node to the same SC-Hub.
- No BBMD tables to maintain as sites grow.
- Track certificate issue and expiry per node.

Architecture 3

Repnet OFF

- Every site needs a unique CIDR (192.168.1.0/24, 192.168.2.0/24).
- Add every site BBMD's IP to the cloud BDT and to every on-prem BDT.
- Same CIDR at a new site means add-on connector infra: contact sales@neve.ai.

PaaS 4 and 5

Edge N4

- Each site runs its own edge N4 with a unique repnet IP (172.17.0.210, 172.18.0.210).
- P4: add each edge N4 to the cloud N4 as a Niagara network.
- Field BBMDs stay on site; nothing to add to a cloud BDT.



Applies to every architecture

BACnet device instances and network numbers must be unique across all sites connected to the same supervisor. Once sites share broadcasts or a hub, duplicates collide and devices drop in and out.

06

Commissioning and handover

Prove it works, record what was built and hand over with confidence.

Commissioning test plan

Run every applicable test per site and record the result. Arch numbers apply to PaaS and IaaS; 4 and 5 are PaaS only.

#	Test	How	Pass criteria	Arch	Result
1	Neeve tunnel	Check edge and connector status for the site	Tunnel established and stable	All	
2	Engineer access	Connect via Neeve agent (PaaS) or vendor tools (IaaS); open the supervisor station	Station opens and login succeeds	All	
3	BDT consistency	Read the BDT on the cloud supervisor and every on-prem BBMD	Entries match the worksheet on every BBMD	1, 3	
4	BACnet/SC links	Check hub connection status	All nodes connected with valid certificates	2	
5	BACnet devices	Add or discover devices	Every expected device found; status ok	All	
6	MSTP devices	Discover behind the BACnet router (edge N4 in 4 and 5)	All expected MSTP devices found	2, 3, 4, 5	
7	Point read / write	Compare live values; command a test point and release	Values match site; command applied and released	All	
8	Modbus polling	Check device and point status	Status ok, sensible values, no timeouts	All	
9	Fox to JACE	Check the Niagara network connection	Connected; points, histories and alarms flowing	All with N4	
10	Edge N4 to cloud	Check each edge N4 Niagara network in the cloud N4	Connected; points, histories and graphics available	4	
11	3rd-party data stream	Check data arriving in the 3rd-party cloud app	Expected data present and current	4, 5	
12	Recovery	Restart the Neeve edge or interrupt WAN briefly	Tunnel and device comms recover without intervention	All	

Handover pack and sign-off

Leave the customer, and the next engineer, everything needed to support the system.



Handover pack

- ☐ As-built architecture diagram for each site
- ☐ Hosting model, platform and licence details (PaaS or IaaS)
- ☐ Completed IP and retnet worksheet
- ☐ BDT exports or screenshots from every BBMD (Arch 1, 3)
- ☐ Certificate register with expiry dates (Arch 2)
- ☐ Edge N4 and cloud connector details (P4, P5)
- ☐ Signed commissioning test plan
- ☐ Engineer and user access list (Neeve agent, station users)
- ☐ Backups of the cloud supervisor, every edge N4 and every JACE station

Sign-off

Project: _____ Site: _____

Role	Name	Signature	Date
Partner SI lead			
Customer IT			
Customer facilities			
Neeve (optional)			

07

Troubleshooting

Common symptoms, likely causes and fixes, plus what to send Neeve for support escalation.

Troubleshooting: BACnet/IP and BBMD

Start with the worksheet: most BACnet faults are addressing faults.

Symptom	Likely cause	Fix
Discovery finds nothing from the cloud (Arch 1)	Expected: broadcast scan does not cross NAT with repnet ON	Add devices manually using their repnet IP, then discover points
Discovery finds nothing (Arch 3)	BBMD not enabled, BDT entry missing or mistyped, wrong mask or port	Compare every BDT with the worksheet. Use IP:47808 and mask 255.255.255.255
Device added but shows down	Wrong IP (repnet vs native), device instance mismatch, tunnel down	Check the IP against the worksheet, confirm the instance number and tunnel status
MSTP devices missing (Arch 1)	Not supported: MSTP devices cannot be added manually	Integrate through the on-prem JACE over Fox, or use Architecture 2 or 3
Devices flap after adding a site	Duplicate device instances or network numbers across sites	Renumber so every instance and network number is unique
Foreign device drops off	Registration time-to-live expired or not renewed	Check the registration TTL and that the on-prem BBMD accepts foreign devices

Troubleshooting: BACnet/SC, Modbus, Fox and access

If a whole site goes quiet at once, check the tunnel before anything else.

Symptom	Likely cause	Fix
BACnet/SC node will not connect	Expired or untrusted certificate, wrong hub URI or port, clock drift	Check certificate chain and expiry, hub URI and port, and time sync on each node
Modbus device times out	Port 502 blocked, wrong IP or unit ID, register offset	Open port 502, confirm IP (repnet vs native) and unit ID, check 0 or 1-based addressing
JACE will not connect over Fox	Wrong IP, Fox vs Foxs port mismatch, credentials or certificate	Use the right IP for the architecture, match the port, accept the certificate
Workbench cannot reach the supervisor	Neeve agent not connected or access not granted	Reconnect the agent and confirm the engineer's access
Every device at a site is down	Neeve tunnel down, edge offline or WAN outage	Check edge power and WAN, then tunnel status



Escalating to Neeve? Send this

Site name, hosting model and architecture, repnet state, Neeve edge WAN IP, time the issue started, screenshots of BDT or hub status, the worksheet, and the steps already taken.

Troubleshooting: edge N4 and hosted platforms

For PaaS Architectures 4 and 5, IaaS and combined designs.

Symptom	Likely cause	Fix
Edge N4 not visible from the cloud supervisor (P4)	Wrong repnet IP, tunnel down, Fox vs Foxs port mismatch, credentials or certificate	Check the edge N4 repnet IP on the worksheet (e.g. 172.17.0.210), tunnel status, port and certificate
Cannot discover field devices at the edge N4 (P4, P5)	Discovery or BBMD not configured at the edge, wrong LAN IP or subnet	Configure discovery and BBMD at the edge N4 against the on-prem LAN, not from the cloud
3rd-party cloud shows no data (P4, P5)	Cloudflare tunnel down or not configured, edge WAN outage	Check the WAN and Neeve tunnel, then the Cloudflare tunnel; escalate to Neeve with details
Cannot reach the hosted BMS platform (IaaS)	Vendor tool pointed at the wrong host IP, access not granted	Confirm the host IP from the worksheet, the tool settings and the engineer's access
BACnet/SC devices or MSTP devices missing (I2)	Routing between BACnet/SC and BACnet/IP or MS/TP not set up on the on-prem JACE or router	Verify routing and discovery for the deployed topology



Thank you

For more information please contact:
success@neeeve.ai