



**KubeCon**



**CloudNativeCon**

North America 2019

# Specialized Network Protocols for IoT+Edge with Kubernetes

*Steven Wong, VMware*

*Dejan Bosanac, Red Hat*



# Abstract

This session will survey communication protocols and technologies used in the edge and IoT space.

These use cases can call for specialized protocols and transports:

publish subscribe, multicast

protocols tolerant of intermittent connectivity

Protocols popular in industry verticals (vehicle bus, industrial automation, building automation)

In some cases, support exists now for use with Kubernetes. If not, device gateways and protocol converters might be an option.

Agenda (Intro):

- survey of protocols and transport standards for IoT and edge
- Intro to how a device gateway or protocol converter works
- Intro to extending Kubernetes with CRDs to manage new device types

Agenda (Deep Dive):

- Futures: Could the service mesh concept be extended beyond TCP, HTTP(s)?
- Demonstration: Kubernetes management of an edge application using a specialized protocol
- Demonstration: Use a device gateway with Kubernetes



KubeCon



CloudNativeCon

North America 2019

# Agenda

## Part 1: Intro

- survey of protocols and transport standards for IoT and edge
- device gateways & protocol converter
- Intro to extending Kubernetes with CRDs to manage new device types

Intermission (5 minutes): Meet others, “birds of a feather”

## Part 2: Deep Dive

- Futures: Could the service mesh concept be extended beyond TCP, HTTP(s)?
- Demonstration: Kubernetes management of an edge application using a specialized protocol
- Demonstration: Use a device gateway with Kubernetes

How to get involved with the IoT Edge Working Group



KubeCon



CloudNativeCon

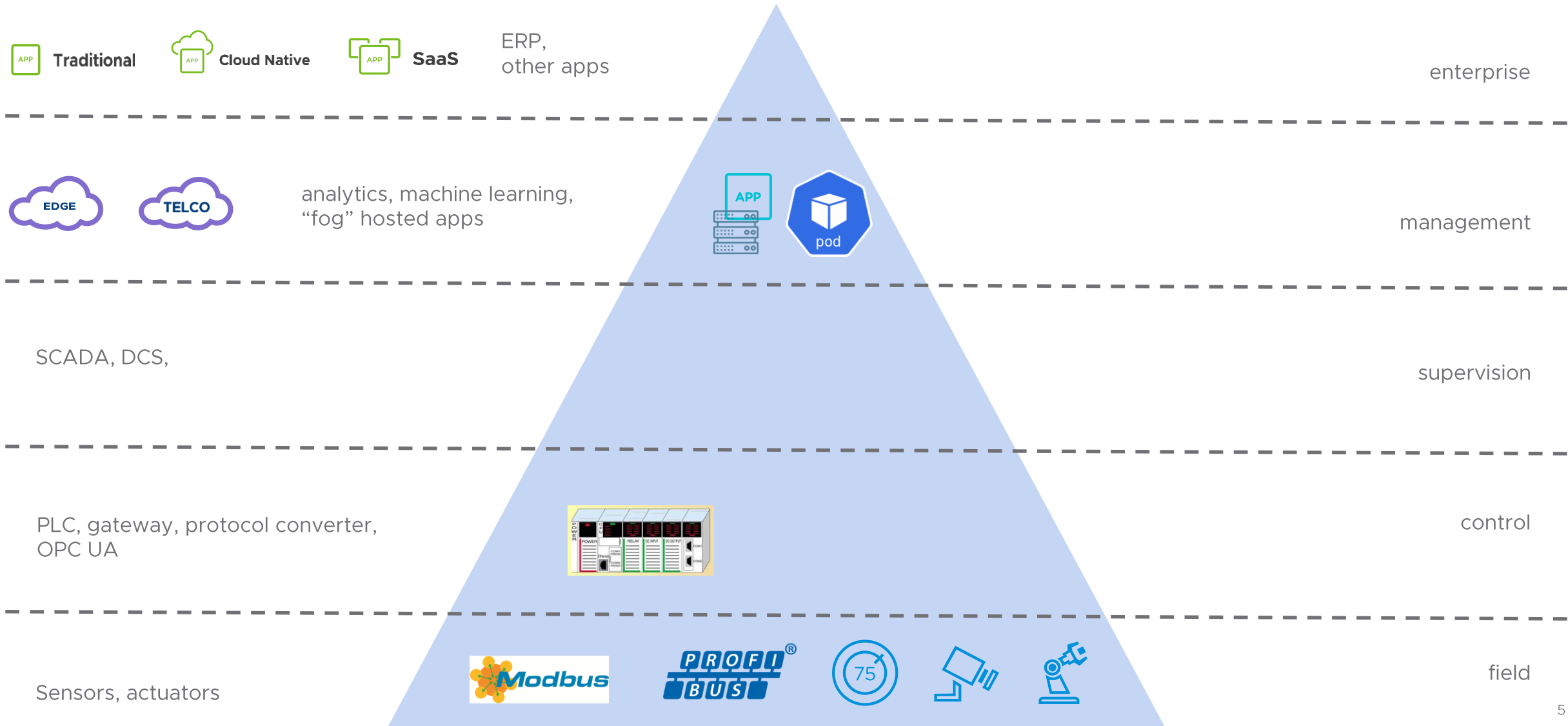
North America 2019

# Intro

Survey of protocols and transport standards for IoT and edge

# Data Communication is sometimes multi-level

## Tiers of software running at tiers of locations using tiers of protocols



# Data communication operates at multiple levels

Not unusual to have all these going on simultaneously



KubeCon



CloudNativeCon

North America 2019

May be multiple layers of protocols  
(OSI model)

**Hardware / physical media:** examples:  
ethernet, EIA-485 multidrop, EIA-232, etc.

**Data Link, Network, Transport**– example  
MAC, IP, TCP, UDP

**Application**– example http, domain  
specific APIs on http

data and control may be separated,  
data may be republished in a transformed context

Data Plane – low level “raw” data flows

Control Plane

- Onboard devices or services
- Monitor
- Manage
- Secure

Content Plane – data transformed to a different  
context (ETL)

# Protocols

## Evaluation considerations



KubeCon



CloudNativeCon

North America 2019

**Type:** built in support for specialized applications

Sync req-response, pub-sub, both, or higher level data exchange agnostic that abstracts low level transport. Low level transport may be connection based or RPC style

**Implementation resource demands** – suitability for constrained environments? is a broken/router needed?

**Behavior with lossy/unreliable networks** – latency limits, QoS support, order & delivery guarantees

**Security**

**Topology:** point to point, bus, routable

**Support for discovery of nodes and data content**

**Health of community** – standards and certification org, scope and openness of software and hardware platforms, popularity within an application domain

**Stability and maturity**



# Protocols

## General Purpose



KubeCon



CloudNativeCon

North America 2019

protocol	standard	info	req-reply	pub-sub	QoS	
HTTP	<a href="#">IETF</a>	<a href="#">Wikipedia</a>	✓		no	
HTTP/2	<a href="#">IETF</a>	<a href="#">Wikipedia</a>	✓	✓	no	
MQTT	<a href="#">OASIS</a>	<a href="#">Wikipedia</a>		✓	yes	<a href="#">mqtt.org</a>
AMQP	<a href="#">OASIS</a>	<a href="#">Wikipedia</a>	✓	✓	yes	<a href="#">amqp.org</a>
COAP	<a href="#">IETF</a>	<a href="#">Wikipedia</a>	✓	✓	yes	
DDS	<a href="#">OMG</a>	<a href="#">Wikipedia</a>		✓	yes	
XMPP	<a href="#">IETF</a>	<a href="#">Wikipedia</a>	✓	✓	no	<a href="#">xmpp.org</a>



# Protocols

## Higher Level



KubeCon



CloudNativeCon

North America 2019

protocol	standard	info	transport
LWM2M	<a href="#">OMA</a>	<a href="#">WikipediA</a>	COAP, on UDP or SMS
OGC SensorThings API	<a href="#">OGC</a>	<a href="#">WikipediA</a>	CoAP, MQTT, HTTP, 6LowPAN
PPMP	<a href="#">eclipse</a>	<a href="#">WikipediA</a>	
One2M	<a href="#">one2m.org</a>	<a href="#">WikipediA</a>	

# Specialized Protocols

## Industrial, Building Automation



KubeCon



CloudNativeCon

North America 2019

protocol	standard	info
Modbus	<a href="#">Modbus Organization</a>	<a href="#">Wikipedia</a>
BACnet	<a href="#">bacnet.org</a>	<a href="#">Wikipedia</a>
OPC UA	<a href="#">OPC Foundation</a>	<a href="#">Wikipedia</a>

# Specialized Protocols

## Transportation (Automotive, Avionics, Rail)



KubeCon



CloudNativeCon

North America 2019

protocol	standard	info
A <sup>2</sup> B	proprietary	<a href="#">link</a>
AFDX	proprietary	<a href="#">WikipediA</a>
ARINC 429	<a href="#">ARINC</a>	<a href="#">WikipediA</a>
Byteflight	<a href="#">byteflight</a>	<a href="#">WikipediA</a>
CAN	<a href="#">ISO</a>	<a href="#">WikipediA</a>
D2B	IEC 61030	<a href="#">WikipediA</a>
IDB-1394	IEEE, <a href="#">1394 trade assoc</a>	<a href="#">WikipediA</a>
IEBus	proprietary	<a href="#">Wikipedia</a>
I <sup>2</sup> C	proprietary	<a href="#">Wikipedia</a>
ISO 9141-1/-2	<a href="#">ISO</a>	<a href="#">Wikipedia</a>

protocol	standard	info
J1708,J1587	SAE	<a href="#">WikipediA</a>
J1850	SAE	<a href="#">WikipediA</a>
J1939, ISO 11783	ISO	<a href="#">WikipediA</a>
Keyword protocol 2000	ISO	<a href="#">WikipediA</a>
LIN	ISO	<a href="#">WikipediA</a>
MOST	proprietary	<a href="#">WikipediA</a>
Multifunction Vehicle Bus	IEC	<a href="#">WikipediA</a>
SPI	defacto	<a href="#">WikipediA</a>
VAN	proprietary	<a href="#">WikipediA</a>



KubeCon



CloudNativeCon

North America 2019

# Device Gateways and Protocols Converters

# Why use a Gateway / Protocol convertor



KubeCon



CloudNativeCon

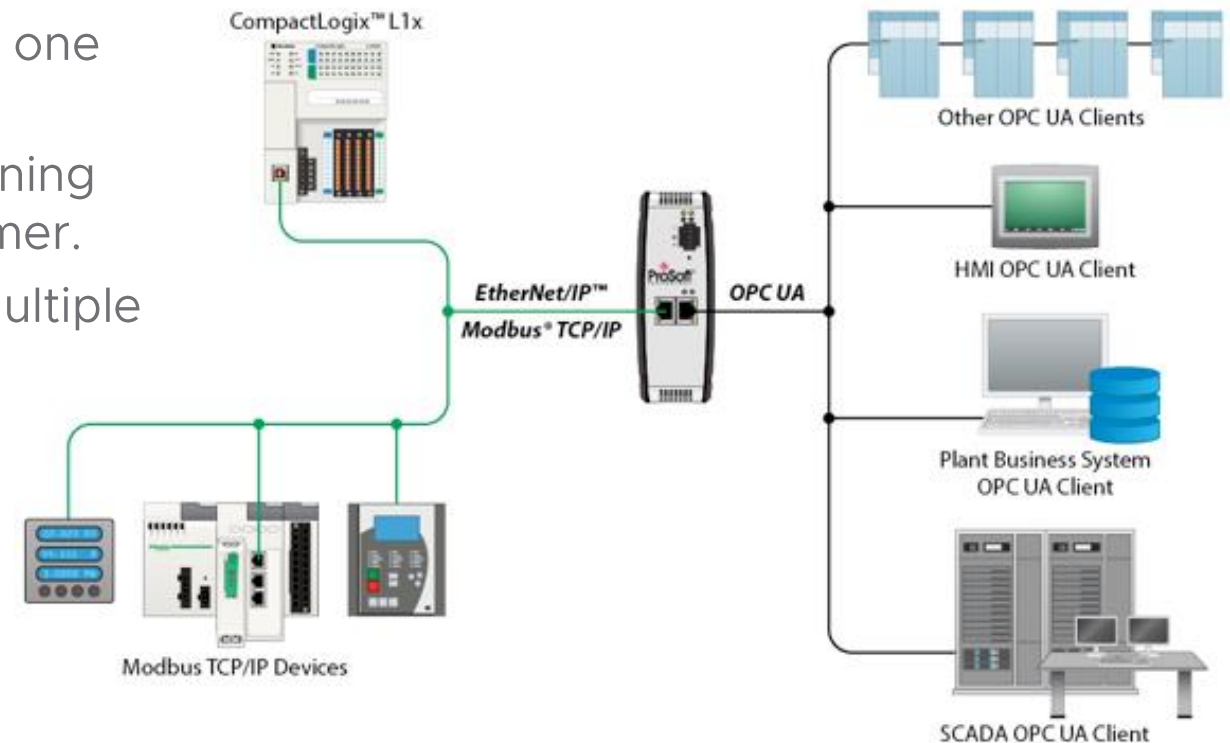
North America 2019

Convert point to point, and local bus protocols to a protocol that is routable

Allow efficient sharing of data sources across multiple consumers

- Low level devices often lack bandwidth and compute to respond to multiple consumers
- Higher tier consumers can be written to utilize just one protocol –
  - better than alternative of building and maintaining huge libraries of device drivers in *each* consumer.
  - Better than putting physical media NICs into multiple consumers

Picture source [opcfoundation.org](http://opcfoundation.org)



# Why use a Gateway / Protocol convertor

## continued



KubeCon



CloudNativeCon

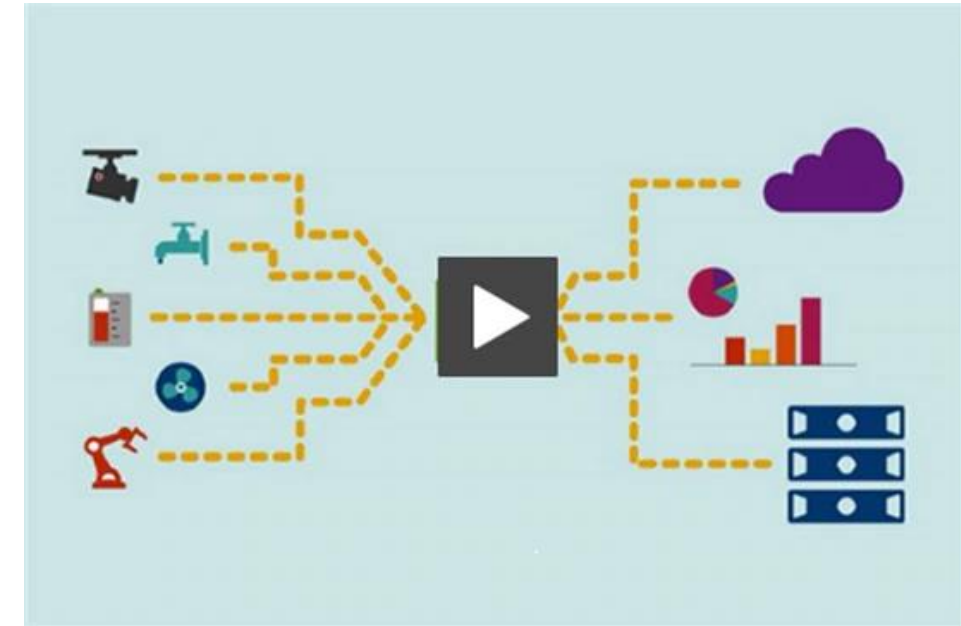
North America 2019

Enable load balancing and monitoring

Can be an injection point to add features to legacy or low level protocols

- Attach time stamps, location, other metadata
- Impose Security

Potentially enable base tier devices to interact with each other, while hiding details and operations from higher tiers.





KubeCon



CloudNativeCon

North America 2019

# CRDs to manage devices?



# Kubernetes API Server

A REST interface to the etcd database



KubeCon



CloudNativeCon

North America 2019

The API server manages CRUD operations on *resources* like Pods/Deployments/Services

Object properties:

- API version
- Kind
- Metadata
- Specs

The API server itself doesn't actually understand the build-in objects, they might as well be apples, oranges and bananas

Custom Resource Definitions (CRDs) allow you to add new objects

# Kubernetes

Based on control loops



KubeCon



CloudNativeCon

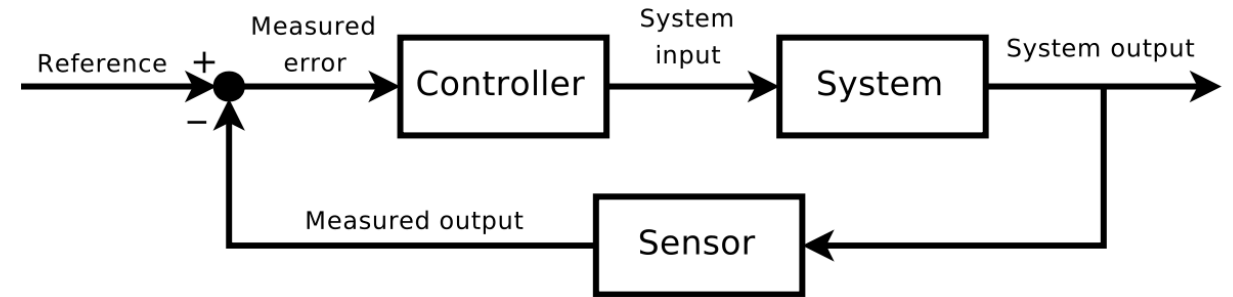
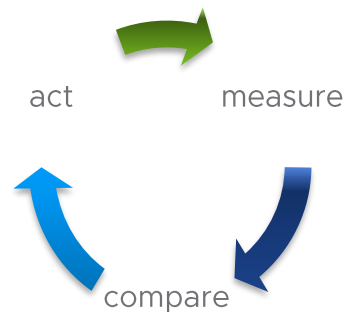
North America 2019

You tell Kubernetes the desired state

Kubernetes relentlessly:

- measures current state
- drives current state -> desired state

Recurring pattern of aspects in the system



# IoT Sensor

What if we managed via a CRD?



KubeCon



CloudNativeCon

North America 2019

Custom Resource

hamburg-sensor.yaml

apiVersion: containerdays.io/v1

kind: Sensor

metadata:

name: hamburg

namespace: germany

spec:

unit: Celcius

status:

lastUpdated: 2010-03-26T15:13:42.05Z

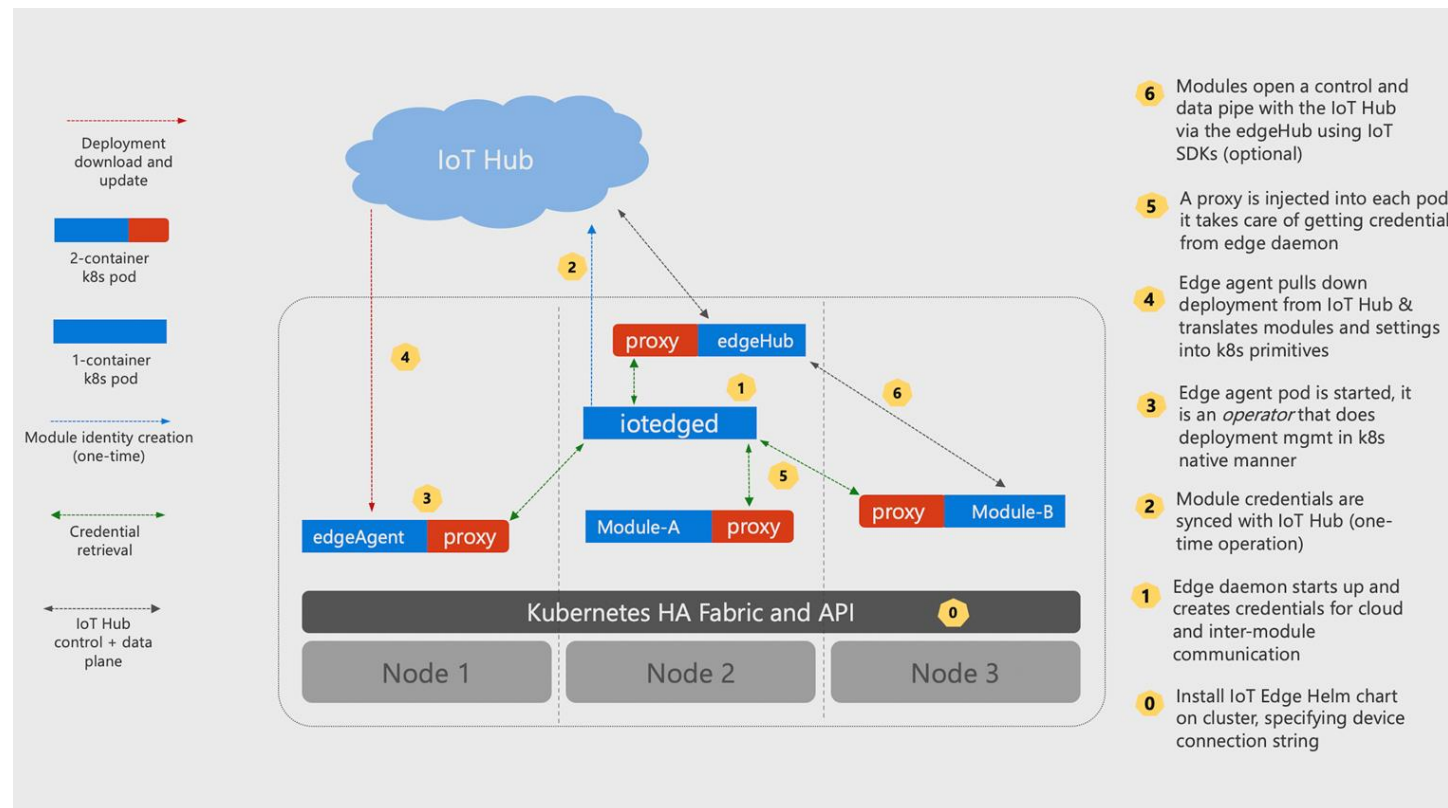
temperature: 28

Source: Stefan Schimanski presentation on Extending Kubernetes  
<https://www.slideshare.net/sttts/extending-kubernetes-with-customresourcedefinitions>

# Another example of a CRD for IoT

## Azure IoT Edge

Edge workloads deployed to on premise Kubernetes clusters. Uses [Custom Resource Definitions](#) (CRDs), with a [Controller](#) (IoT Edge Agent) that reconciles cloud managed desired state with the local device state



See details here:  
[github.com/Azure-Samples/iotedge-gateway-on-kubernetes](https://github.com/Azure-Samples/iotedge-gateway-on-kubernetes)



KubeCon



CloudNativeCon

North America 2019

# Intermission

5 minutes - birds of a feather



KubeCon



CloudNativeCon

North America 2019

# Deep Dive

Futures: Could the service mesh concept be extended beyond TCP, HTTP(s)?



Whether a location has devices, apps or both:  
configuration and software update  
management is needed

Photo: Rampion Offshore Wind Farm, United Kingdom  
Nicholas Doherty on [Unsplash](#)



Probably not the most efficient  
“over the air” update process

Photo: [Wikipedia / Tobias Klenze / CC-BY-SA 4.0.](#)



# Network Service Mesh

A CNCF Sandbox project



KubeCon



CloudNativeCon

North America 2019

[github.com/networkservicemesh/networkservicemesh](https://github.com/networkservicemesh/networkservicemesh)



## Network Service Mesh

- Service mesh for L2/L3 payloads
- On-demand, dynamic, negotiated connections
- gRPC API to publish and consume Network Services
- Without changes to Kubernetes
- Works with any CNI
- Workload-To-Workload granular level of connectivity
- Loosely coupled heterogeneous network configurations



KubeCon



CloudNativeCon

North America 2019

- Clients – consume Network Services
- Endpoints – implement Network Services
- Wires – responsible for the connections, payload agnostic

# Network Service Mesh

## Define a Network Service



KubeCon

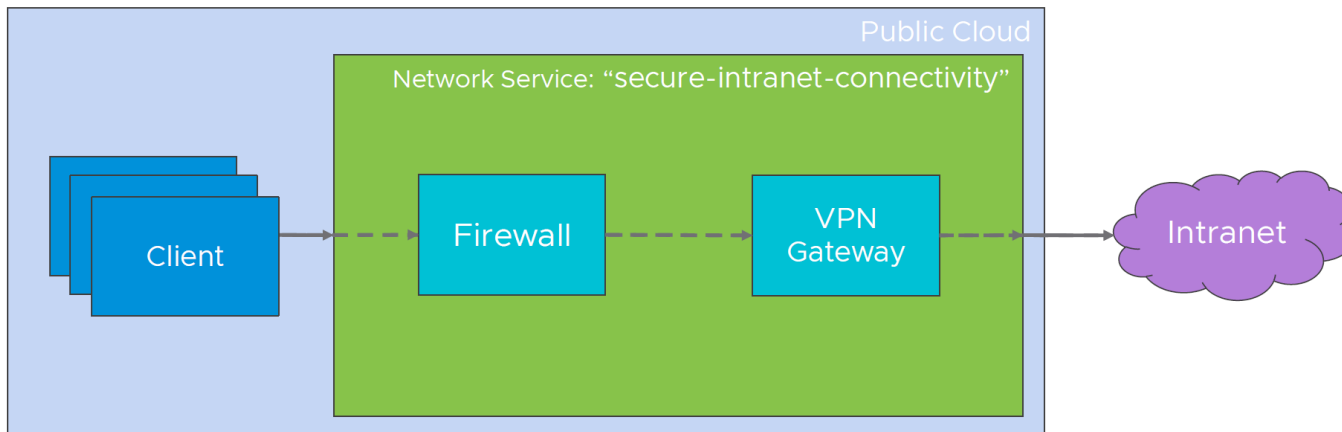


CloudNativeCon

North America 2019

- Specify type of payload
- Source and destination selection
- Service composition

```
apiVersion: networkservicemesh.io/v1
kind: NetworkService
metadata:
  name: secure-intranet-connectivity
spec:
  payload: IP
  matches:
    - match:
      sourceSelector:
        app: firewall
      route:
        - destination:
            destinationSelector:
              app: vpn-gateway
    - match:
      route:
        - destination:
            destinationSelector:
              app: firewall
```





KubeCon



CloudNativeCon

North America 2019

# Demonstrations

- Demonstration: Kubernetes management of an edge application using a specialized protocol
- Demonstration: Use a device gateway with Kubernetes





**KubeCon**



**CloudNativeCon**

North America 2019

# Edge computing



# Edge computing



KubeCon



CloudNativeCon

North America 2019

- Edge is everything outside of the core cloud
- Bring compute resources closer to the source
- Use cloud-native development
- ...



# THERE ARE MANY EDGES

## End-User Premise Edge



Device Edge



Infrastructure Edge

"last mile"

## Provider Edge



Provider Device Edge



Provider Access Edge



Provider Aggregation Edge

## Provider/Enterprise Core



Regional Data Center



Core Data Center

# Common requirements



KubeCon



CloudNativeCon

North America 2019

1. lowest latency between data and responses and decisions
2. pre-processing (reduction) before data moves to cloud,
3. remotely managed datasets for local access
4. remotely manage software deployment and updates
5. operate offline or with intermittent connectivity

	1	2	3	4	5
Remote office, retail			✓	✓	✓
Sensor data collection, analytics	✓	✓		✓	✓
Physical device control	✓			✓	✓
Gaming	✓	✓	✓	✓	
Telco edge cloud	✓	✓	✓	✓	



**KubeCon**



**CloudNativeCon**

North America 2019



**KubeCon**



**CloudNativeCon**

North America 2019

Better together?



# Rethinking IoT gateways

- Contenarization
- Adopt Cloud-native development practices
  - CI/CD
  - Gitops
  - ...

# Enabling new use cases



KubeCon



CloudNativeCon

North America 2019

- More resources on the Edge = new use cases
- Machine learning
- Store and forward
- Caching
- ...



**KubeCon**



**CloudNativeCon**

North America 2019





**KubeCon**



**CloudNativeCon**

North America 2019

# Deep dive into field protocols



# Field protocols



KubeCon



CloudNativeCon

North America 2019

- Bluetooth
- Bluetooth BLE
- Zigbee
- NFC
- WIFI
- Zwave
- LoRaWAN
- Cellular
- Serial
- SigFox
- EnOcean



KubeCon



CloudNativeCon

North America 2019

- Industrial protocols
- Building automation
- Vehicle protocols

# Tools for field protocols



KubeCon



CloudNativeCon

North America 2019

- Hardware abstraction layer
- Bluetooth REST API (REST-BLUE)



**KubeCon**



**CloudNativeCon**

North America 2019



**KubeCon**



**CloudNativeCon**

North America 2019

# Deep dive into cloud protocols





KubeCon



CloudNativeCon

North America 2019

- HTTP
- MQTT (eclipse mosquito) kubernetes, hono, others
- CoAP docker container available, hono
- AMQP enmasse, kubernetes, hono
- DDS, (brokerless unlike MQTT and CoAP)
- XMPP



# Navigating through the jungle

- Connection oriented vs RPC style
- Duplex communication challenges (command and control)





**KubeCon**



**CloudNativeCon**

North America 2019

# Eclipse Hono



KubeCon

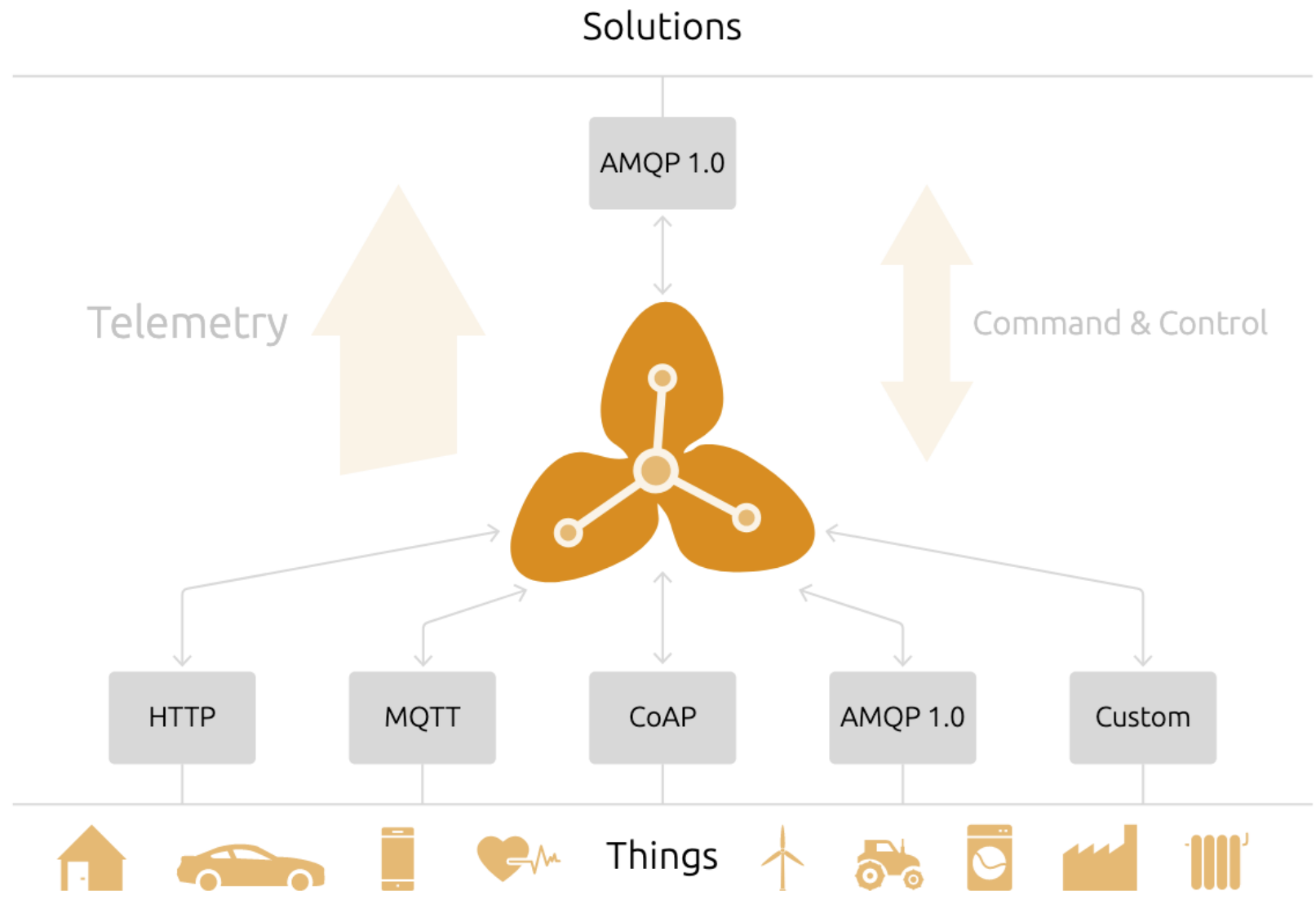


CloudNativeCon

North America 2019

- IoT Connectivity for the cloud
- Scalable, multi-protocol IoT connectivity
- K8s based

# Eclipse Hono



# Eclipse Hono

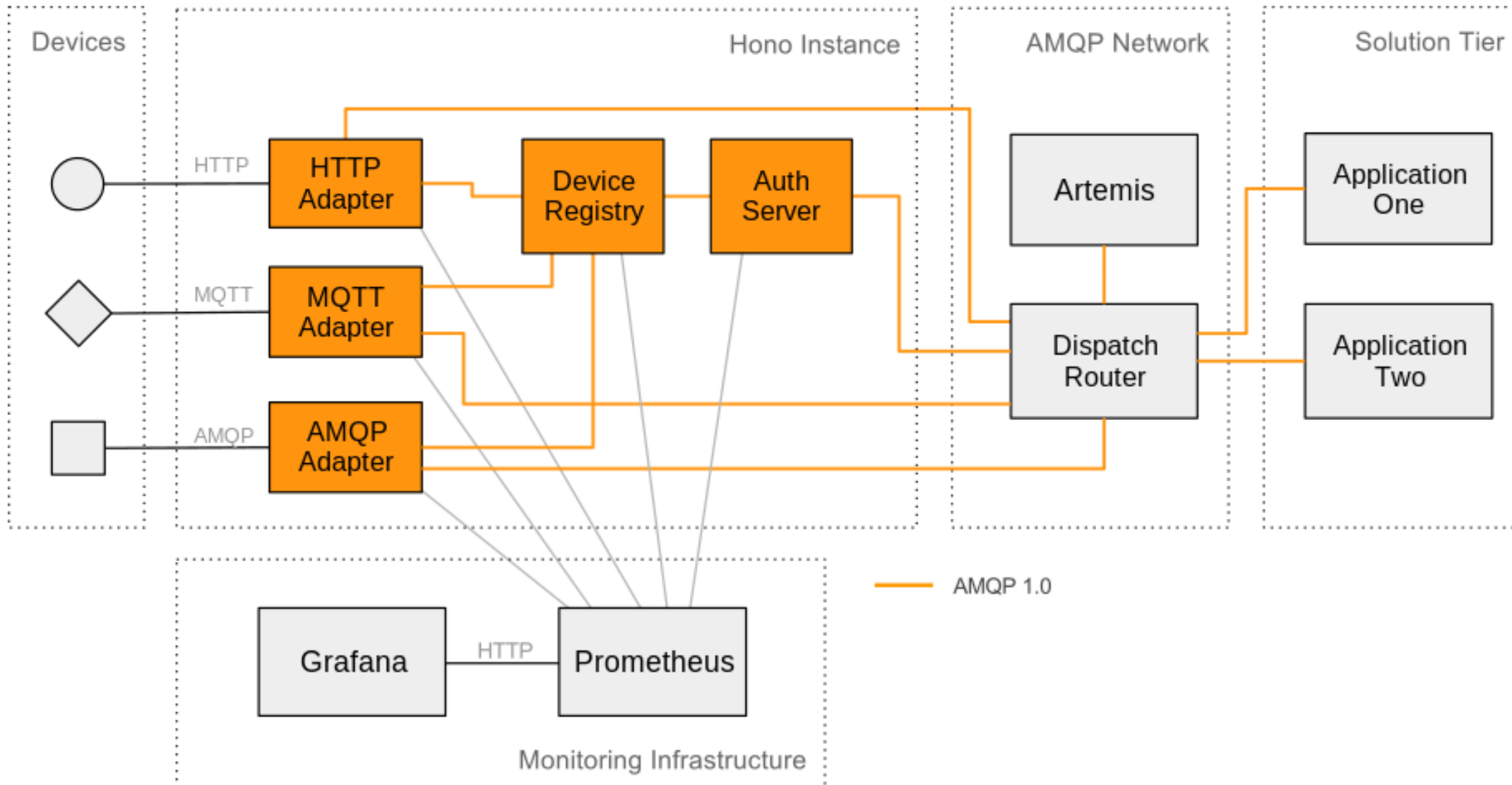


KubeCon



CloudNativeCon

North America 2019





**KubeCon**

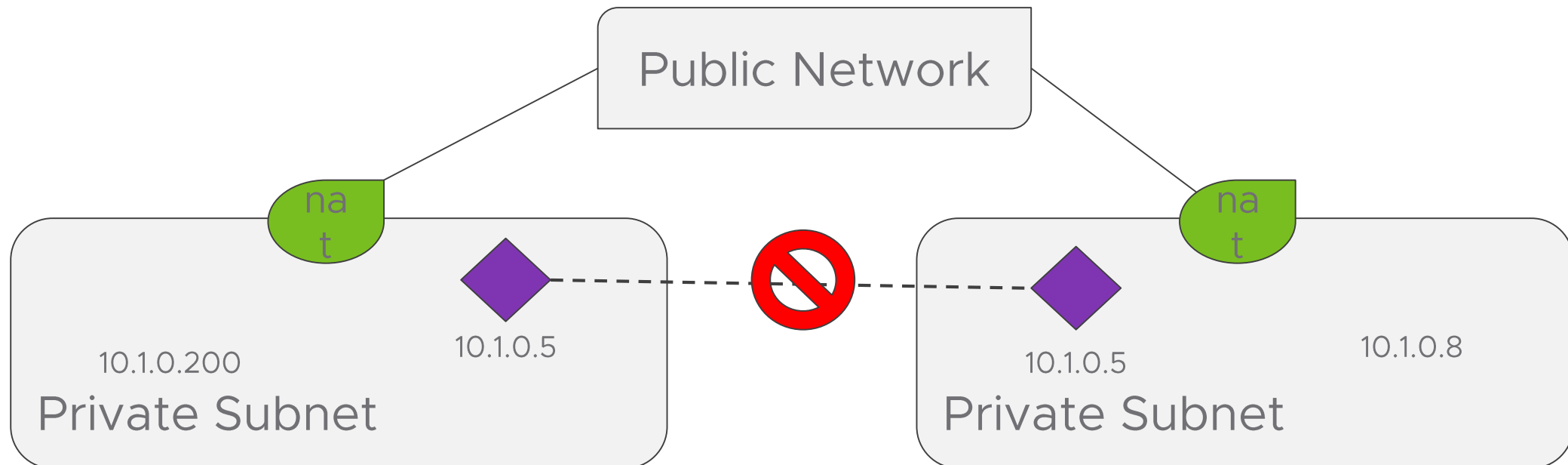


**CloudNativeCon**

North America 2019

# Edge networking

- Hybrid cloud, microservice architecture, agile integration, etc.
  - Not client/server
  - Services/processes want to be deployable and addressable everywhere (north/south/east/west)
- Edge computing - Lots of private subnetworks



# Application Layer Addressing

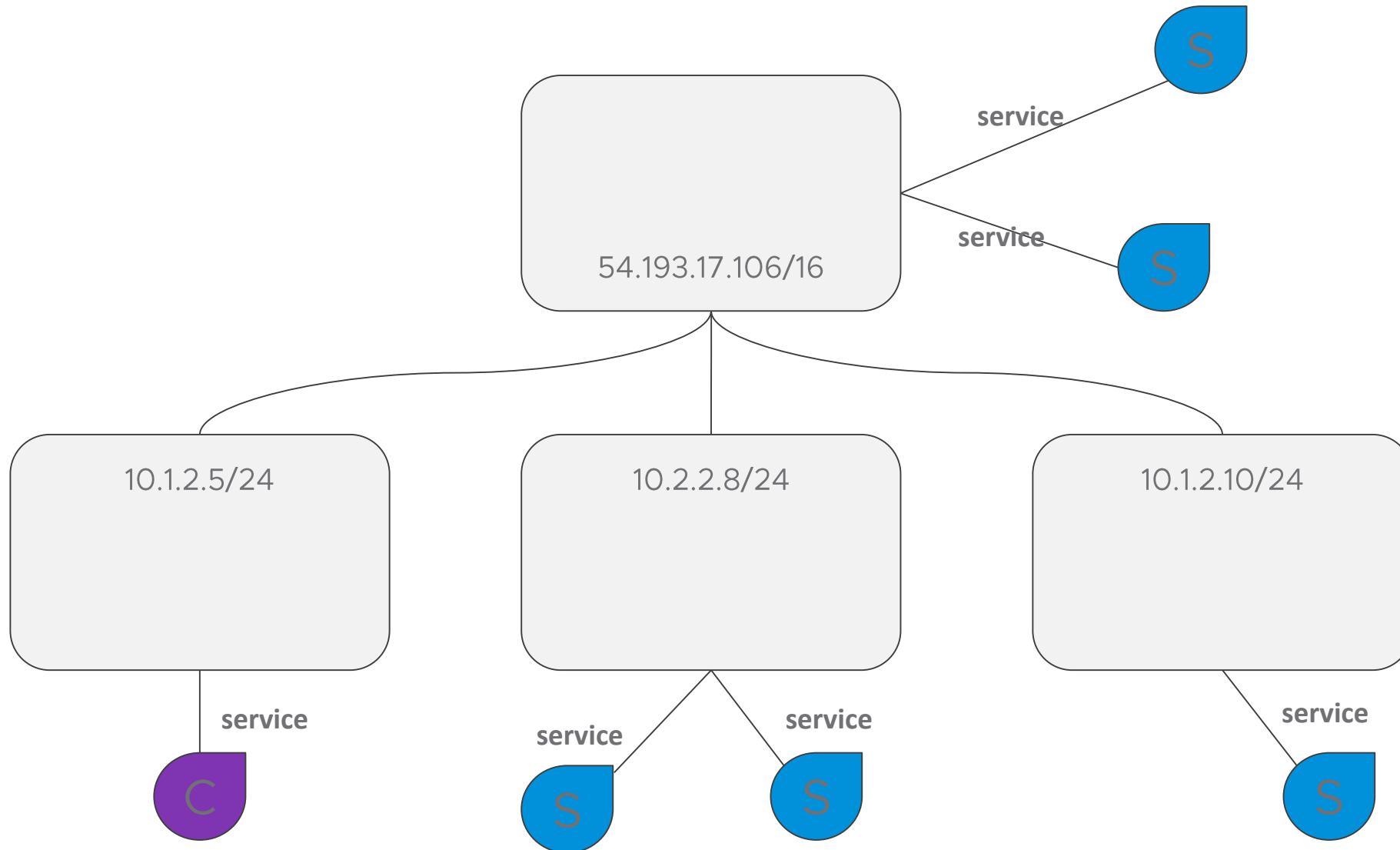


KubeCon

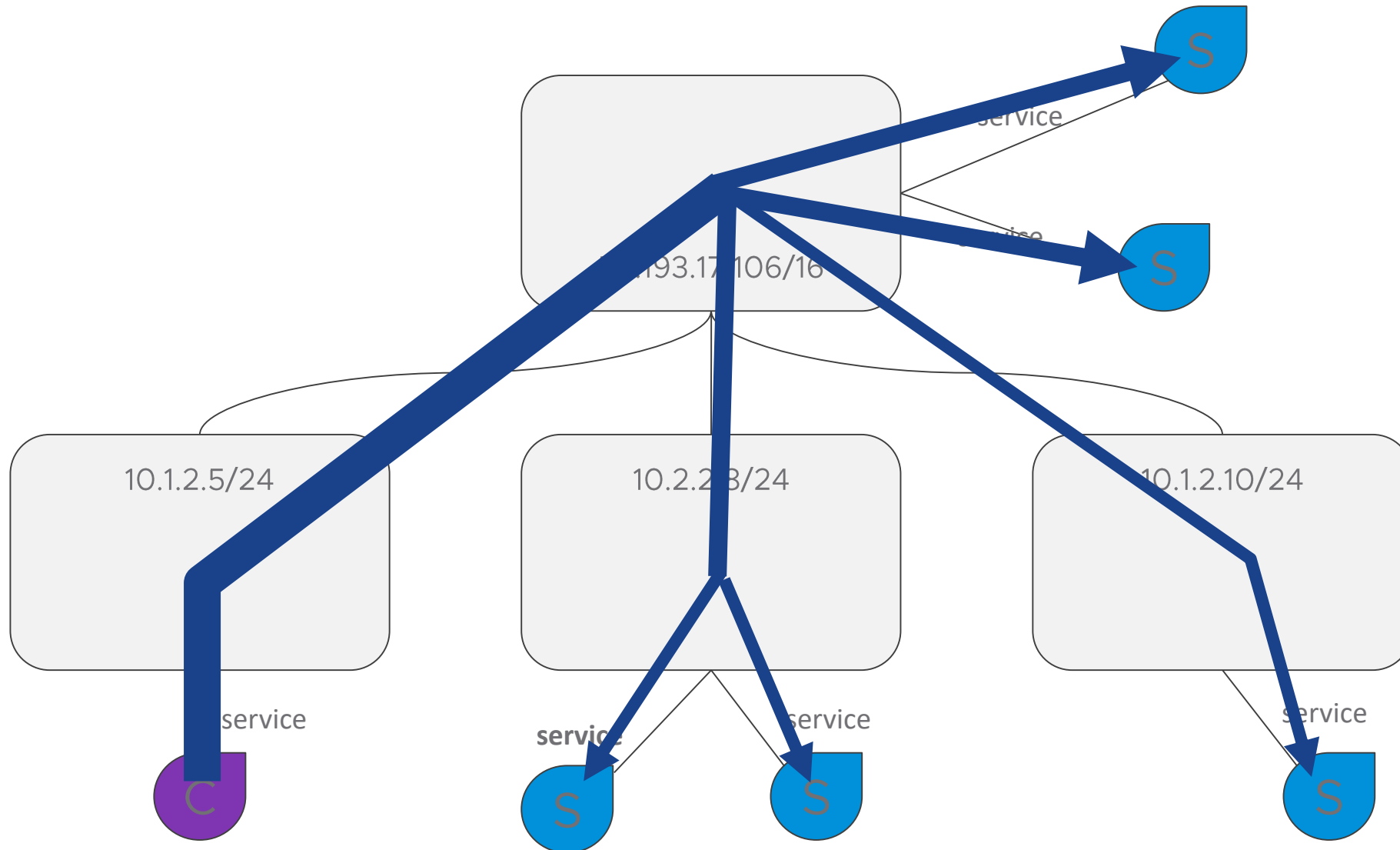


CloudNativeCon

North America 2019



# Application Layer Addressing





# Implications of Application Addressing



North America 2019

- Security
  - Access control for addresses - at the service/process/business resolution
  - Locked-down network membership - Mutual TLS for inter-site connections
  - Cross-cluster applications not exposed via Kube networking
    - Public exposure limited to ingress
  - Trusted and untrusted edges
- Management
  - Metrics collected at business resolution



- Operational Ease
  - Easy to deploy in a multi-cluster network
  - No advanced networking (SDN, VPNs, Tunnels, Firewall rules, etc.)
  - No need for elevated or admin privileges
  - No problem with overlapping CIDR subnets or mixes of IPv4 and IPv6
  - No single point of failure - use redundant topology
- Not just for messaging
  - Proxy maps HTTP, TCP, UDP, etc. to AMQP
- <http://skupper.io>
  - Examples, demo-videos, etc.
  - New, emerging project



**KubeCon**



**CloudNativeCon**

North America 2019

# Upcoming developments





KubeCon



CloudNativeCon

North America 2019

# Is cloud obsolete?

# Way forward



KubeCon



CloudNativeCon

North America 2019

- Cloud is not obsolete
- Cloud IoT platforms still needed
  - Business applications
  - Long term data storage
- Work on distributed Edge deployments for IoT services

# Eclipse Hono in the cloud

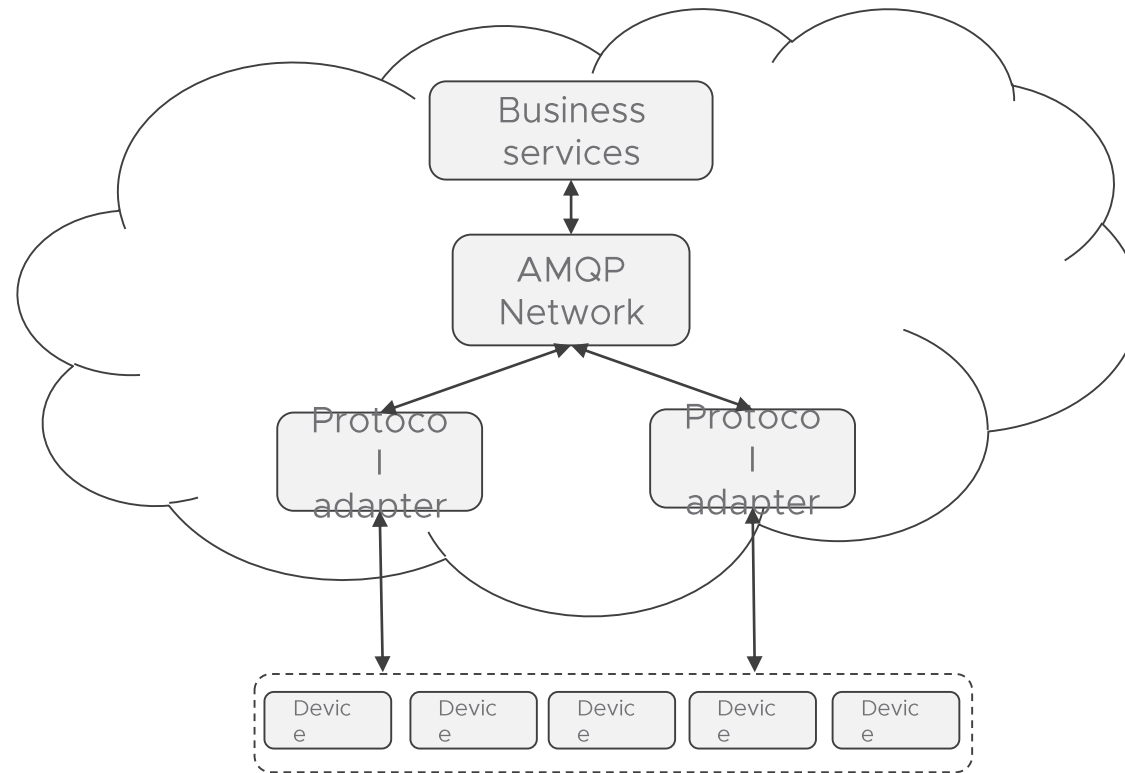


KubeCon



CloudNativeCon

North America 2019



# Eclipse Hono on the Edge

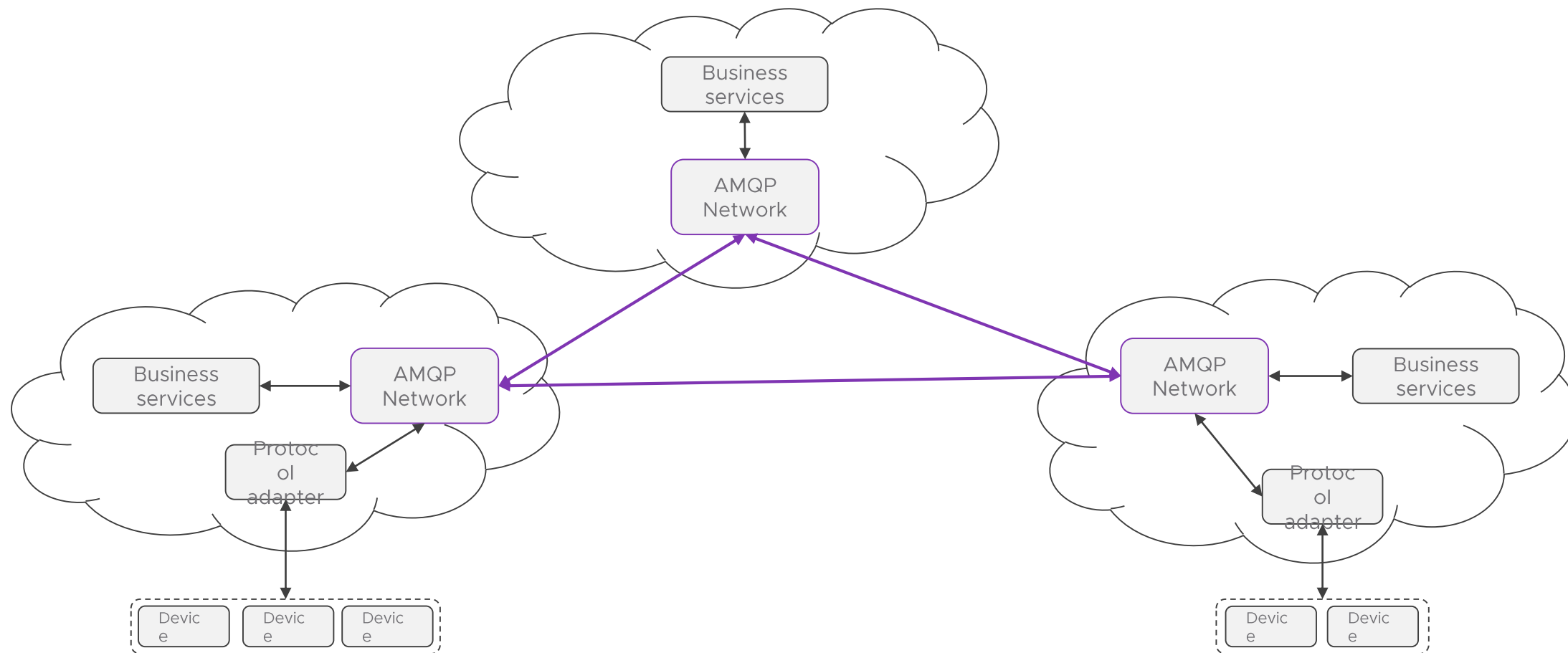


KubeCon



CloudNativeCon

North America 2019





# Full integration



KubeCon



CloudNativeCon

North America 2019

- Provide development continuum from field to cloud via edge
- Better integration
  - Platforms
    - KubeEdge
    - ioFog
  - Communication
    - Hono
    - Skupper



**KubeCon**



**CloudNativeCon**

North America 2019

# How to get involved with the IoT Edge Working Group

Learn more.....



KubeCon



CloudNativeCon

North America 2019

Regular Work Group Meeting:

USA WG Meeting Wednesday 9am PT, every 4 weeks, next on December 4

APAC WG meeting Wednesday 5 UTC every 4 weeks, next on November 20

- [Meeting notes and agenda](#)

Link to join the group

- [groups.google.com/forum/#!forum/kubernetes-wg-iot-edge](https://groups.google.com/forum/#!forum/kubernetes-wg-iot-edge)

Link to join Slack

- <https://kubernetes.slack.com/messages/wg-iot-edge>

White Paper

- <http://bit.ly/iot-edge-whitepaper>



KubeCon



CloudNativeCon

North America 2019

# Thank You

Please email any questions to [PowerPoint@vmware.com](mailto:PowerPoint@vmware.com)