

IIoT
Internet-Draft
Intended status: Standards Track
Expires: September 6, 2018

M. Zhang
B. Liu
Huawei Technologies
M. McBride
Futurewei
C. Hu
Xilinx
L. Geng
China Mobile
March 5, 2018

Gap Analysis of Edge Computing for Industrial IoT
draft-zhang-iiot-edge-computing-gap-analysis-00

Abstract

This document investigates the requirements of Edge Computing in the Industrial Internet of Things (IIoT) domain and identifies 10 standardization gaps within 5 key requirements. The related works inside the IETF are also evaluated.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of [BCP 78](#) and [BCP 79](#).

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at <https://datatracker.ietf.org/drafts/current/>.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on September 6, 2018.

Copyright Notice

Copyright (c) 2018 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to [BCP 78](#) and the IETF Trust's Legal Provisions Relating to IETF Documents (<https://trustee.ietf.org/license-info>) in effect on the date of publication of this document. Please review these documents

carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

Table of Contents

1.	Introduction	2
2.	Inter-operability of the Industrial Internet	3
2.1.	Gateway between two Industrial Networks	3
2.2.	Overlay for the Industrial Internet	4
3.	Configuration and Management	5
3.1.	Central Configuration	5
3.2.	Firmware Update	5
3.3.	Naming and Addressing	5
4.	Mobility and Migration	6
5.	South bound Communication	6
6.	Orchestration between the Edge and the Cloud	7
7.	Summary	8
8.	IANA Considerations	9
9.	Security Considerations	9
10.	References	10
10.1.	Normative References	10
10.2.	Informative References	10
	Authors' Addresses	11

[1.](#) Introduction

Implementing intelligence only in the Cloud cannot fulfill all of the requirements of industrial IoT. The Cloud will not always provide the needed response within bounded latency requirements. Low latency requirements are often critical for applications such as automatic control, video surveillance/delivery, power distribution. and fault alarm. The massive number of assets connected to the Cloud require a large amount of bandwidth to transmit the raw data, and the Cloud needs large computation and storage resources to handle this high volume of data. The raw data often contains sensitive information and the leakage of this data from the Cloud may cause harm to the the business. Most industrial environments don't want to put all the data in one place, ie, the Cloud. Distributed Edge Computing is proposed to deal with these industrial requirements.

Edge computing is a distributed open platform at the network edge, close to the things or data sources, integrating the capabilities of networks, storage, and applications. By delivering edge intelligence services, edge computing meets the key requirements of industry digitalization for agile connectivity, real-time services, data

optimization, application intelligence, security and privacy protection.

Various organizations are working on the industrialization of Edge Computing. In 2017, ISO/IEC JTC 1/SC41 established the edge computing research group to promote the standardization of Edge Computing. In 2016, the Edge Computing Consortium (ECC) was set up to work on the commercial implementation in different industrial verticals. In 2017, the edge computing task group was established inside the Industrial Internet Consortium (IIC) to work on the reference architecture of edge computing.

Local, low latency computation, storage and communication are the three main aspects of Edge Computing. Communication is the key to enable data flow between assets, from assets to gateway, between gateways at the edge, from the gateway to the Cloud, etc., which all fall naturally into the scope of IETF.

This document identifies the requirements of Edge Computing in the industrial domain, and investigates the related standardization gaps for each requirement. Its the intention of this draft to identify the gaps which may need to be addressed within the IETF

[2.](#) Inter-operability of the Industrial Internet

According to a 2015 survey by IoT Nexus, 77% of professionals surveyed believe that interoperability is the largest challenge facing the Industrial Internet. Different industrial branches such as product lines, factories and logistics will need to interact closely with each other or even merge. And legacy machines will continue to exist until the factory is fully upgraded. The interoperability between legacy and upgraded equipment will need to become commonplace.

[2.1.](#) Gateway between two Industrial Networks

Currently, there are more than 40 fieldbus technologies being used in the industrial domain, such as Profibus, CANopen, Modbus, providing low cost digital industrial connection. However, their data rates are limited, and the hardware integration is complicated. Industrial Ethernet, like PROFINET, SECOSI, EtherCAT and POWERLINK, can provide a unified hardware interface, higher data rate and reusable Internet protocols. But the incompatibility between different technologies is still unresolved, which makes one local network unable to communicate with another if they speak different machine languages. When manufacturers want to extend their product line, they need to purchase equipment which speaks a specific language, which leads to vendor locked-in. Equipment which is using legacy fieldbus

technologies will need to be abandoned when the manufacturers want to upgrade their network.

In order to enable the direct communication between two subnets which speak different languages or to realize backward compatibility, protocol translation is indispensable. Edge computing nodes will serve as the gateway between two industrial networks and will be an ideal place to implement this translation function. Therefore, one identified gap is to define the mapping between any two machine languages that are considered to be popular. It is suggested that SDOs (such as the IETF) or commercial consortiums related to operational technologies, will provide a solution to this item.

[2.2.](#) Overlay for the Industrial Internet

Usually the processing plants, workshops or factory locations of a specific manufacturer have their own unique products within various industrial verticals, and the control logic is locally closed to achieve high reliability and robustness. The data is also kept in local networks and cannot be used by the others, creating information silos. Next generation manufacturing requires close interaction of different branches to achieve flexibility, optimality and efficiency. For example, two parallel assembly lines can synchronize their paces via interconnection; when one processing section sends out alarms, the other sections will be informed and react proactively. The robot in the logistics network, for example, can transport various materials to the production network within the necessary response time.

The industrial networks speak different physical languages. Therefore, an overlay is required to achieve the interconnection between multiple networks. Different machine languages are translated into a common protocol used as the overlay. The edge computing nodes can realize the protocol conversion at the ingress of the overlay and act as routers in the overlay network. For small or medium scale, e.g. inside a workshop or a factory, the overlay can be done by TSN tunnelling or thru a dedicated fiber-optic channel. For large scale, e.g. two factories in two cities, L2VPN/L3VPN on public network can be used. If time sensitive applications are carried, the bonded-latency requirement should be added.

Industrial IoT systems are both delay sensitive and loss sensitive, which rely on very robust and predictable network connections. The overlay must meet these requirements. The recent paradigm in transportation layer congestion control to avoid loss and provide short delay still has a long tail for the perform, which does not meet the requirement of Industrial IoT. The traditional industrial systems use redundancy to guarantee the high availability for

networks on critical infrastructure (HSR: High-availability Seamless Redundancy, PRP: Parallel Redundancy Protocol), which is a high cost solution and faces the interoperability problem among different systems. IEEE 802.1 defined the TSN (time-sensitive- network) technical standards, aiming to promote standardization and interoperability of real-time Ethernet networks, so that data flows demanding bounded latency and best effort data flows can be transmitted in one single network. Inside IETF, the DETNET working group is working on an L3 overall architecture for deterministic networking. It is promising to have foo-over-DETNET/TSN in the future. Therefore a gap may or may not exist to provide a solution to this protocol conversion overlay.

[3.](#) Configuration and Management

[3.1.](#) Central Configuration

The network SHOULD be configured before the industrial operation. And the configuration can also be changed during the operation to better meet the requirements. The configuration MAY include Node_ID, connectivity between nodes, the network topology, the end to end paths and their bandwidth and latency requirements. The connectivity

between nodes can be configured by Pub/Sub pattern, in which the senders publish the messages in different classes, and the receivers subscribe to the classes they are interested in. The publishers don't have knowledge about the subscriber, and vice versa.

The configuration can be done in a centralized way via Netconf and YANG model. The information model of different verticals to describe the data type in YANG should be unified, so that a data in one vertical can be recognized by another verticals.

[3.2.](#) Firmware Update

The firmware of devices needs to be updated on-demand to deal with security vulnerabilities, to update the installed applications or to install new ones. The update can be conducted via HTTP or FTP. However, how to update the firmware for constrained devices in a more secure and efficient way is still an open issue. The SUIT (BOF) is aiming to work on the related solutions.

[3.3.](#) Naming and Addressing

Given massive amount of heterogeneous devices deployed across different Industrial IoT platforms, naming and addressing play as a key role to coordinate the back-end data center, edge and end devices, e.g., the efficient upstream sensory data collection,

content-based data filtering and matching, and downstream efficient control by applications.

Currently used schemes like IP and URI are experiencing some big challenges, which are not efficient in the context of Industrial IoT. The changes in data centers/edge/end devices should be transparent to others and the changes including but not limited to the migration of the service (like storage, database) in data centers/edge, the update of the program in end devices and so on.

IPv6 is expected to be the base of IoT in the future and its lack of mobility and security inherently has been extending for a while. It is a very essential requirement for the computing purpose that the naming and addressing could be far more flexible, agile and secure than what we could provide today. Besides IP related solutions, some

other naming schemes have been developed (e.g., Object Name Service (ONS), IoT@Work naming scheme, NDN, MobilityFirst, etc.), each which could have a place in some certain domains but not a cure to a general IIoT naming and addressing problem.

4. Mobility and Migration

Some scenarios require mobility, e.g. when a mobile robot moves from one workshop to another, it may also roam between two edge computing nodes. The applications, running in the previous edge computing node SHOULD migrate to the current node, so that the robot's task is uninterrupted. The applications can migrate between edge computing nodes with different capabilities and different hardware, e.g. gateways, server clusters and all types of nodes in between.

The applications can be encapsulated in containers or virtual machines to facilitate the migration between edge computing nodes. The states in the previous ECN SHOULD be synchronized to the new ECN, so that the latter can run the application continuously. Common APIs SHOULD be defined for different types of ECNs to shield the heterogeneity. A layer-2 network SHOULD be created to facilitate the VM mobility [[RFC8302](#)] [[I-D.ietf-nvo3-vm](#)]. New API migration solutions may be needed.

5. South bound Communication

In the south bound, the edge computing node MAY connect to various devices using different kinds of protocols, such as Ethernet, WiFi, Bluetooth, Power Line Communication, RF, RS485, etc. Thus the ECNs will be versatile protocol speakers.

The applications, which belong to different users, SHOULD be able to operate simultaneously on the ECNs. Tenant segregation MUST be

implemented to ensure a user's data, configuration and functionalities are not impacted by another user. TRILL may help realize the segregation by logical isolation of network traffic. Default TRILL configuration supports 4094 VLANs, which is enough since the tenants at the edge would not be as many as those in a data center. If edge cloud orchestration applies, however, tenant segregation on the cloud may exceed 4094. For such case, a longer label than 12-bit VLAN label should be used [[RFC7172](#)] [[RFC7348](#)].

Inside the IETF, ROLL (routing protocols in LLN), 6lo (IP adaptation of Bluetooth, PLC, RS485, etc.) and LPWAN (RF communication protocols including LoRa, Sigfox, Wi-SUN and NB-IoT) may provide southbound solutions. The 6TiSCH WG's work is promising to handle the requirement of adding deterministic features in RF networks.

6. Orchestration between the Edge and the Cloud

In Edge Computing, the distribution of intelligence is hierarchical. For example, in manufacturing, Edge Computing Nodes can be deployed on the machine tools for process configuration and status monitoring; at the pipeline level, Edge Computing Nodes can be used for product flow orchestration; higher at the factory level, Edge Computing Nodes takes care of the coordination of different pipelines.

The data sent out by the terminals should be processed with various requirements, which hopefully can be fulfilled at different levels. For example, the data in automatic control should be processed at low level to guarantee the bounded latency. And some key data should be stored for a long time at higher level, e.g. on the Cloud. The sample data for complex deep learning algorithms should be sent to higher level possessed enough processing power.

The terminals can generate data with various processing requirements. How to deliver the data to the right level of Edge Intelligence remains a gap to be covered. A potential solution is to introduce these requirements inside the packet, so an Edge Computing Node can know whether to process it locally or upload it to the higher level. A primary idea for this to add requirement options into the IPv6 header and define objective functions (OF) deployed at the Edge Computing Node to make the decision.

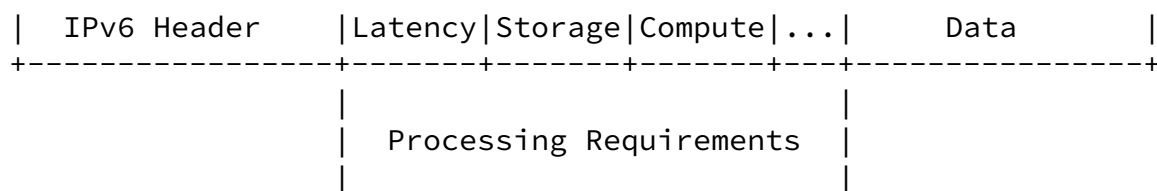


Figure 1: Processing requirements in the IPv6 header

Similar idea can be found in [\[I-D.purkayastha-sfc-service-indirection\]](#), where dynamic service insertion model is used to steer traffic to the requisite service resources.

7. Summary

Requirements	Gaps
Req 1: Inter-operability of Industrial Internet	Gap 1: Mapping definition between any two machine languages Gap 2: Overlay for the Industrial Internet
Req 2: Configuration and Management	Gap 3: Unified information model for all kinds of verticals Gap 4: Secure firmware update Gap 5: Flexible, agile and secure naming and addressing
Req 3: Mobility and Migration	Gap 6: A large layer-2 network to facilitate the VM mobility Gap 7: Containers and VMs to facilitate App mobility
Req 4: South bound communication	Gap 8: LPWAN technologies Gap 9: Add deterministic features into RF network
Req 5: Orchestration between the Edge and the Cloud	Gap 10: Differentiated service at the Edge Computing Node

Figure 2: Requirements and Gaps of Edge Computing in IIoT

8. IANA Considerations

N/A

9. Security Considerations

Security considerations will be a critical component of IIoT edge computing particularly as intelligence is moved to the extreme distributed edge.

[10.](#) References

[10.1.](#) Normative References

- [RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", [BCP 14](#), [RFC 2119](#), DOI 10.17487/RFC2119, March 1997, <<https://www.rfc-editor.org/info/rfc2119>>.

[10.2.](#) Informative References

- [I-D.geng-iiot-edge-computing-problem-statement] 67, 4., Zhang, M., McBride, M., and B. Liu, "Problem Statement of Edge Computing beyond Access Network for Industrial IoT", [draft-geng-iiot-edge-computing-problem-statement-00](#) (work in progress), October 2017.
- [I-D.ietf-nvo3-vmm] Sarikaya, B., Dunbar, L., Khasnabish, B., Herbert, T., and S. Dikshit, "Virtual Machine Mobility Protocol for L2 and L3 Overlay Networks", [draft-ietf-nvo3-vmm-01](#) (work in progress), October 2017.
- [I-D.purkayastha-sfc-service-indirection] Purkayastha, D., Rahman, A., Trossen, D., Despotovic, Z., and R. Khalili, "Alternative Handling of Dynamic Chaining and Service Indirection", [draft-purkayastha-sfc-service-indirection-02](#) (work in progress), March 2018.
- [RFC7172] Eastlake 3rd, D., Zhang, M., Agarwal, P., Perlman, R., and D. Dutt, "Transparent Interconnection of Lots of Links (TRILL): Fine-Grained Labeling", [RFC 7172](#), DOI 10.17487/RFC7172, May 2014, <<https://www.rfc-editor.org/info/rfc7172>>.
- [RFC7348] Mahalingam, M., Dutt, D., Duda, K., Agarwal, P., Kreeger, L., Sridhar, T., Bursell, M., and C. Wright, "Virtual eXtensible Local Area Network (VXLAN): A Framework for Overlaying Virtualized Layer 2 Networks over Layer 3

Networks", [RFC 7348](https://www.rfc-editor.org/info/rfc7348), DOI 10.17487/RFC7348, August 2014, <<https://www.rfc-editor.org/info/rfc7348>>.

[RFC8302] Li, Y., Eastlake 3rd, D., Dunbar, L., Perlman, R., and M. Umair, "Transparent Interconnection of Lots of Links (TRILL): ARP and Neighbor Discovery (ND) Optimization", [RFC 8302](https://www.rfc-editor.org/info/rfc8302), DOI 10.17487/RFC8302, January 2018, <<https://www.rfc-editor.org/info/rfc8302>>.

Zhang, et al.

Expires September 6, 2018

[Page 10]

Internet-Draft

Edge Computing Gap Analysis

March 2018

Authors' Addresses

Mingui Zhang
Huawei Technologies
No. 156 Beiqing Rd. Haidian District
Beijing 100095
China

Email: zhangmingui@huawei.com

Bing Liu
Huawei Technologies
No. 156 Beiqing Rd. Haidian District
Beijing 100095
China

Email: remy.liubing@huawei.com

Mike McBride
Futurewei
2330 Central Expressway
Santa Clara 95055
Unites States

Email: michael.mcbride@huawei.com

Chengchen Hu
Xilinx
5 Changi Business Park Vista Singapore

Singapore 486040
Singapore

Email: CHENGCHE@xilinx.com

Liang Geng
China Mobile
32 Xuanwumen West Street
Beijing, Xicheng District 100053
China

Email: gengliang@chinamobile.com