Network Working Group
Internet-Draft
Intended status: Informational
Expires: December 13, 2018

B. Carpenter
Univ. of Auckland
S. Jiang
Huawei Technologies Co., Ltd

June 11, 2018

# Limited Domains and Internet Protocols
## draft-carpenter-limited-domains-00

Abstract

There is a noticeable trend towards network requirements, behaviours and semantics that are specific to a limited region of the Internet and a particular set of requirements. Policies, default parameters, the options supported, the style of network management and security requirements may vary. This document reviews examples of such limited domains and emerging solutions. It shows the needs for a precise definition of a limited domain boundary and for a corresponding protocol to allow nodes to discover where such a boundary exists.

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 December 13, 2018.

Table of Contents



## 1. Introduction

As the Internet continues to grow and diversify, with a realistic prospect of tens of billions of nodes being connected directly and indirectly, there is a noticeable trend towards local requirements, behaviours and semantics. The word "local" should be understood in a special sense, however. In some cases it may refer to geographical and physical locality - all the nodes in a single building, on a single campus, or in a given vehicle. In other cases it may refer to a defined set of users or nodes distributed over a much wider area, but drawn together by a single virtual network over the Internet, or a single physical network running partially in parallel with the Internet. We expand on these possibilities below. To capture the topic, this document refers to such networks as "limited domains".

The phrase "Balkanization of the Internet" has often been used to criticise mechanisms that block the free flow of information across the network. That is not the topic of this document, which does not discuss filtering mechanisms and does not apply to protocols that are designed for use across the whole Internet.

The requirements of limited domains will be different in different scenarios. Policies, default parameters, and the options supported may vary. Also, the style of network management may vary, between a completely unmanaged network, one with fully autonomic management, one with traditional central management, and mixtures of the above.

Finally, the requirements and solutions for security and privacy may vary.

This documents analyses and discusses some of the consequences of this trend, and how it impacts the idea of universal interoperability in the Internet. In particular, we challenge the notion that all Internet standards must be universal in scope and applicability. To the contrary, we assert that some standards need to be specifically limited in their applicability. This requires that the concepts of a limited domain, and of its boundary, need to be formalised.

NOTE: This document is incomplete. Comments on the following two sections are invited before we complete the later sections.

## 2. Examples of Limited Domain Requirements

This section describes various examples where limited domain requirements can be identified. It is of course not a complete list.

NOTE: The authors welcome more suggestions and references for this list.

1. A home network. It will be unmanaged, constructed by a non-specialist, and will possibly include wiring errors such as physical loops. It must work with devices "out of the box" as shipped by their manufacturers and must create adequate security by default. Remote access may be required. The requirements and applicable principles are summarised in [RFC7368].

2. A small office network. This is very similar to a home network, since whoever is in charge will probably have little or no specialist knowledge, but may have differing security and privacy requirements. Remote access may be required.

3. A vehicle network. This will be designed by the vehicle manufacturer but may include devices added by the vehicle's owner or operator. Parts of the network will have demanding performance and reliability requirements with implications for human safety. Remote access may be required to certain functions, but absolutely forbidden for others. Communication with other vehicles, roadside infrastructure, and external data sources will be required. See [I-D.ietf-ipwave-vehicular-networking] for a survey of use cases.

4. A building services network. This will be designed specifically for a particular building, but using standard components. Additional devices may need to be added at any time. Parts of

the network may have demanding reliability requirements with implications for human safety. Remote access may be required to certain functions, but absolutely forbidden for others. [I-D.martocci-6lowapp-building-applications] (need current reference!)

5. Supervisory Control And Data Acquisition (SCADA) networks in general, which will exhibit widely differing requirements, including tough real-time performance targets, of which building networks are a simple example. See for example [I-D.ietf-detnet-use-cases]

6. The three preceding cases will all include sensors, but some networks may be specifically limited to sensors and the collection and processing of sensor data. They may be in remote or technically challenging locations and installed by non-specialists.

7. "Traditional" enterprise and campus networks, which may be spread over many kilometres and over multiple separate sites.

8. Data centres and hosting centres, or distributed services acting as such centres. These will have high performance, security and privacy requirements and will typically include large numbers of independent "tenant" networks overlaid on shared infrastructure.

9. Content Delivery Networks, comprising distributed data centres and the paths between them, spanning thousands of kilometres.

10. Internet of Things (IoT) networks. While this term is very flexible and covers many innovative types of network, it seems reasonable to assert that many IoT edge networks will in fact have special requirements and protocols that are useful only within a specific domain, and that these protocols cannot, and for security reasons should not, run over the Internet as a whole.

Two other concepts, while not tied to specific network types, also strongly depend on the concept of limited domains:

1. Intent Based Networking. In this concept, a network domain is configured and managed in accordance with an abstract policy known as "Intent", to ensure that the network performs as required [I-D.moulchan-nmrg-network-intent-concepts]. Whatever technologies are used to support this, they will be applied within the domain boundary.

2. Network Slicing. A network slice is a virtual network that consists of a managed set of resources carved off from a larger network [I-D.geng-netslices-architecture]. Whatever technologies are used to support slicing, they will require a clear definition of the boundary of a given slice.

While it is clearly desirable to use common solutions, and therefore common standards, wherever possible, it is increasingly difficult to do so while satisfying the widely varying requirements outlined above. However, there is a tendency when new protocols and protocol extensions are proposed to always ask the question "How will this work across the open Internet?" This document suggests that this is not always the right question. There are protocols and extensions that are not intended to work across the open Internet. On the contrary, their requirements and semantics are specifically limited (in the sense defined above).

A common argument is that if a protocol is intended for limited use, the chances are very high that it will in fact be used (or misused) in other scenarios including the so-called open Internet. This is undoubtedly true and means that limited use is not an excuse for bad design or poor security. In fact, a limited use requirement potentially adds complexity to both the protocol and its security design, as discussed later.

Nevertheless, because of the diversity of limited environments with specific requirements that is now emerging, specific standards will necessarily emerge. There will be attempts to capture each market sector, but the market will demand standardised limited solutions. However, the "open Internet" must remain as the universal method of interconnection. Reconciling these two aspects is a major challenge.

## 3. Examples of Limited Domain Solutions

This section lists various examples of specific limited domain solutions that have been proposed or defined. It intentionally does not include Layer 2 technology solutions, which are by definition defined for limited domains.

NOTE: Please suggest additional items for this list.

1. Differentiated Services. This mechanism [RFC2474] allows a network to assign locally significant values to the 6-bit Differentiated Services Code Point field in any IP packet. Although there are some recommended codepoint values for specific per-hop queue management behaviours, these are specifically intended to be domain-specific codepoints with traffic being classified, conditioned and re-marked at domain boundaries

(unless there is an inter-domain agreement that makes re-marking unnecessary).

2. Network function virtualisation. As described in [I-D.irtf-nfvrg-gaps-network-virtualization], this general concept is an open research topic, in which virtual network functions are orchestrated as part of a distributed system. Inevitably such orchestration applies to an administrative domain of some kind, even though cross-domain orchestration is also a research area.

3. Service Function Chaining (SFC). This technique [RFC7665] assumes that services within a network are constructed as sequences of individual functions within a specific SFC-enabled domain. As that RFC states: "Specific features may need to be enforced at the boundaries of an SFC-enabled domain, for example to avoid leaking SFC information". A Network Service Header (NSH) [RFC8300] is used to encapsulate packets flowing through the service function chain: "The intended scope of the NSH is for use within a single provider's operational domain."

4. Data Centre Network Virtualization Overlays. A common requirement in data centres that host many tenants (clients) is to provide each one with a secure private network, all running over the same physical infrastructure. [RFC8151] describes various use cases for this, and specifications are under development. These include use cases in which the tenant network is physically split over several data centres, but which must appear to the user as a single secure domain.

5. Segment Routing. This is a technique which "steers a packet through an ordered list of instructions, called segments" [I-D.ietf-spring-segment-routing]. The semantics of these instructions are explicitly local to a segment routing domain or even to a single node. Technically, these segments or instructions are represented as an MPLS label or an IPv6 address, which clearly adds a semantic interpretation to them within the domain.

6. Autonomic Networking. As explained in [I-D.ietf-anima-reference-model], an autonomic network is also a security domain within which an autonomic control plane [I-D.ietf-anima-autonomic-control-plane] is used by service agents. These service agents manage technical objectives, which may be locally defined, subject to domain-wide policy. Thus the domain boundary is important for both security and protocol purposes.

7. Homenet. As shown in [RFC7368], a home networking domain has specific protocol needs that differ from those in an enterprise network or the Internet as a whole. These include the Home Network Control Protocol (HNCP) [RFC7788] and a naming and discovery solution [I-D.ietf-homenet-simple-naming].

8. Creative uses of IPv6 features. As IPv6 enters more general use, engineers notice that it has much more flexibility than IPv4. Innovative suggestions have been made for:

   * The flow label, e.g. [RFC6294], [I-D.fioccola-v6ops-ipv6-alt-mark].

   * Extension headers, e.g. for segment routing [I-D.ietf-6man-segment-routing-header].

   * Meaningful address bits, e.g. [I-D.jiang-semantic-prefix]. Also, segment routing uses IPv6 addresses as segment identifiers with specific local meanings [I-D.ietf-spring-segment-routing].

   All of these suggestions are only viable within a specified domain. The case of the extension header is particularly interesting, since its existence has been a major "selling point" for IPv6, but it is notorious that new extension headers are virtually impossible to deploy across the whole Internet [RFC7045], [RFC7872]. It is worth noting that extension header filtering is considered as an important security issue [I-D.ietf-opsec-ipv6-eh-filtering]. There is considerable appetite among vendors or operators to have flexibility in defining extension headers for use in limited or specialised domains, e.g. [I-D.voyer-6man-extension-header-insertion] and [BIGIP].

9. Deterministic Networking (DetNet). The Deterministic Networking Architecture [I-D.ietf-detnet-architecture] and encapsulation [I-D.ietf-detnet-dp-sol] aim to support flows with extremely low data loss rates and bounded latency, but only within a part of the network that is "DetNet aware". Thus, as for differentiated services above, the concept of a domain is fundamental.

## 4. Common Aspects of Limited Domains

This section derives common aspects of limited domains from the examples above.

TBD

## 5. The Need to Define a Limited Domain Boundary

This section justifies the need for a precise definition of a limited domain boundary and for a corresponding protocol to allow nodes to discover where such a boundary exists.

TBD

## 6. Defining Protocol Scope

This section suggests that protocols or protocol extensions should, when appropriate, be standardised to interoperate only within a Limited Domain Boundary. Such protocols are not required to operate across the Internet as a whole.

TBD

## 7. Security Considerations

Clearly, the boundary of a limited domain will almost always also act as a security boundary. In particular, it will serve as a trust boundary, and as a boundary of authority for defining capabilities. Within the boundary, limited-domain protocols or protocol features will be useful, but they will be meaningless if they enter or leave the domain.

The security model for a limited-scope protocol must allow for the boundary, and in particular for a trust model that changes at the boundary. Typically, credentials will need to be signed by a domain-specific authority.

## 8. IANA Considerations

This document makes no request of the IANA.

## 9. Acknowledgements

Useful comments were received from ...

## 10. Informative References

[BIGIP] Li, R., "HUAWEI - Big IP Initiative.", 2018, <https://www.iaria.org/announcements/HuaweiBigIP.pdf>.

[I-D.fioccola-v6ops-ipv6-alt-mark]
Fioccola, G., Velde, G., Cociglio, M., and P. Muley, "IPv6 Performance Measurement with Alternate Marking Method", draft-fioccola-v6ops-ipv6-alt-mark-01 (work in progress), June 2018.

[I-D.geng-netslices-architecture]
67, 4., Dong, J., Bryant, S., kiran.makhijani@huawei.com, k., Galis, A., Foy, X., and S. Kuklinski, "Network Slicing Architecture", draft-geng-netslices-architecture-02 (work in progress), July 2017.

[I-D.ietf-6man-segment-routing-header]
Previdi, S., Filsfils, C., Leddy, J., Matsushima, S., and d. daniel.voyer@bell.ca, "IPv6 Segment Routing Header (SRH)", draft-ietf-6man-segment-routing-header-13 (work in progress), May 2018.

[I-D.ietf-anima-autonomic-control-plane]
Eckert, T., Behringer, M., and S. Bjarnason, "An Autonomic Control Plane (ACP)", draft-ietf-anima-autonomic-control-plane-16 (work in progress), June 2018.

[I-D.ietf-anima-reference-model]
Behringer, M., Carpenter, B., Eckert, T., Ciavaglia, L., and J. Nobre, "A Reference Model for Autonomic Networking", draft-ietf-anima-reference-model-06 (work in progress), February 2018.

[I-D.ietf-detnet-architecture]
Finn, N., Thubert, P., Varga, B., and J. Farkas, "Deterministic Networking Architecture", draft-ietf-detnet-architecture-05 (work in progress), May 2018.

[I-D.ietf-detnet-dp-sol]
Korhonen, J., Andersson, L., Jiang, Y., Finn, N., Varga, B., Farkas, J., Bernardos, C., Mizrahi, T., and L. Berger, "DetNet Data Plane Encapsulation", draft-ietf-detnet-dp-sol-04 (work in progress), March 2018.

[I-D.ietf-detnet-use-cases]
Grossman, E., "Deterministic Networking Use Cases", draft-ietf-detnet-use-cases-16 (work in progress), May 2018.

[I-D.ietf-homenet-simple-naming]
Lemon, T., Migault, D., and S. Cheshire, "Simple Homenet Naming and Service Discovery Architecture", draft-ietf-homenet-simple-naming-01 (work in progress), March 2018.

[I-D.ietf-ipwave-vehicular-networking]
Jeong, J., "IP-based Vehicular Networking: Use Cases, Survey and Problem Statement", draft-ietf-ipwave-vehicular-networking-02 (work in progress), March 2018.

[I-D.ietf-opsec-ipv6-eh-filtering]
Gont, F. and W. LIU, "Recommendations on the Filtering of IPv6 Packets Containing IPv6 Extension Headers", draft-ietf-opsec-ipv6-eh-filtering-05 (work in progress), March 2018.

[I-D.ietf-spring-segment-routing]
Filsfils, C., Previdi, S., Ginsberg, L., Decraene, B., Litkowski, S., and R. Shakir, "Segment Routing Architecture", draft-ietf-spring-segment-routing-15 (work in progress), January 2018.

[I-D.irtf-nfvrg-gaps-network-virtualization]
Bernardos, C., Rahman, A., Zuniga, J., Contreras, L., Aranda, P., and P. Lynch, "Network Virtualization Research Challenges", draft-irtf-nfvrg-gaps-network-virtualization-09 (work in progress), February 2018.

[I-D.jiang-semantic-prefix]
Jiang, S., Qiong, Q., Farrer, I., Bo, Y., and T. Yang, "Analysis of Semantic Embedded IPv6 Address Schemas", draft-jiang-semantic-prefix-06 (work in progress), July 2013.

[I-D.martocci-6lowapp-building-applications]
Martocci, J., Schoofs, A., and P. Stok, "Commercial Building Applications Requirements", draft-martocci-6lowapp-building-applications-01 (work in progress), July 2010.

[I-D.moulchan-nmrg-network-intent-concepts]
Sivakumar, K. and M. Chandramouli, "Concepts of Network Intent", draft-moulchan-nmrg-network-intent-concepts-00 (work in progress), October 2017.

[I-D.voyer-6man-extension-header-insertion]
daniel.voyer@bell.ca, d., Leddy, J., Filsfils, C., Dukes, D., Previdi, S., and S. Matsushima, "Insertion of IPv6 Segment Routing Headers in a Controlled Domain", draft-voyer-6man-extension-header-insertion-03 (work in progress), May 2018.

[RFC2474] Nichols, K., Blake, S., Baker, F., and D. Black, "Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers", RFC 2474, DOI 10.17487/RFC2474, December 1998, <https://www.rfc-editor.org/info/rfc2474>.

[RFC6294] Hu, Q. and B. Carpenter, "Survey of Proposed Use Cases for the IPv6 Flow Label", RFC 6294, DOI 10.17487/RFC6294, June 2011, <https://www.rfc-editor.org/info/rfc6294>.

[RFC7045] Carpenter, B. and S. Jiang, "Transmission and Processing of IPv6 Extension Headers", RFC 7045, DOI 10.17487/RFC7045, December 2013, <https://www.rfc-editor.org/info/rfc7045>.

[RFC7368] Chown, T., Ed., Arkko, J., Brandt, A., Troan, O., and J. Weil, "IPv6 Home Networking Architecture Principles", RFC 7368, DOI 10.17487/RFC7368, October 2014, <https://www.rfc-editor.org/info/rfc7368>.

[RFC7665] Halpern, J., Ed. and C. Pignataro, Ed., "Service Function Chaining (SFC) Architecture", RFC 7665, DOI 10.17487/RFC7665, October 2015, <https://www.rfc-editor.org/info/rfc7665>.

[RFC7788] Stenberg, M., Barth, S., and P. Pfister, "Home Networking Control Protocol", RFC 7788, DOI 10.17487/RFC7788, April 2016, <https://www.rfc-editor.org/info/rfc7788>.

[RFC7872] Gont, F., Linkova, J., Chown, T., and W. Liu, "Observations on the Dropping of Packets with IPv6 Extension Headers in the Real World", RFC 7872, DOI 10.17487/RFC7872, June 2016, <https://www.rfc-editor.org/info/rfc7872>.

[RFC8151] Yong, L., Dunbar, L., Toy, M., Isaac, A., and V. Manral, "Use Cases for Data Center Network Virtualization Overlay Networks", RFC 8151, DOI 10.17487/RFC8151, May 2017, <https://www.rfc-editor.org/info/rfc8151>.

[RFC8300] Quinn, P., Ed., Elzur, U., Ed., and C. Pignataro, Ed., "Network Service Header (NSH)", RFC 8300, DOI 10.17487/RFC8300, January 2018, <https://www.rfc-editor.org/info/rfc8300>.

## Appendix A. Change log [RFC Editor: Please remove]

draft-carpenter-limited-domains, 2018-06-11:

Initial version

## Authors' Addresses

Brian Carpenter
Department of Computer Science
University of Auckland
PB 92019
Auckland 1142
New Zealand

Email: brian.e.carpenter@gmail.com

Sheng Jiang
Huawei Technologies Co., Ltd
Q14, Huawei Campus, No.156 Beiqing Road
Hai-Dian District, Beijing, 100095
P.R. China

Email: jiangsheng@huawei.com