Autonomic Networking in Limited Domains

APAN Research Workshop 2018

Brian Carpenter

The University of Auckland

August 2018

Topics

- What is autonomic networking?
- What are limited domains?
- What next?

Acknowledgements

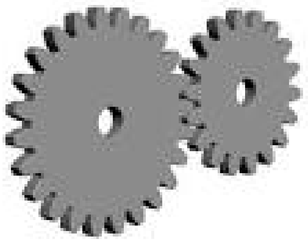
- This talk is based on work by
  - the IRTF Network Management Research Group (NMRG)
  - the IETF Autonomic Networking Integrated Model and Approach (ANIMA) Working Group
  - co-authors including Sheng Jiang, Bing Liu (Huawei), Carsten Bormann (U Bremen TZI), Laurent Ciavaglia (Nokia), Michael Behringer...

Topics

- What is autonomic networking?
- What are limited domains?
- What next?

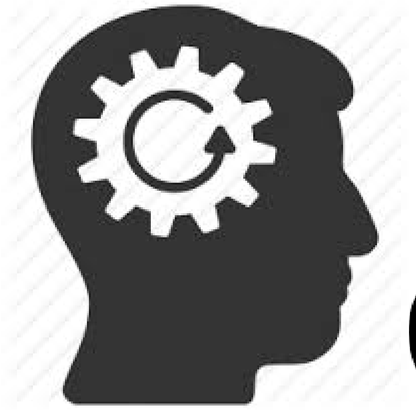
Autonomic Networking Terminology (1)

- Automatic
  - done <u>as if by machine</u>; self-acting or self-regulating mechanism



- Autonomous
  - <u>without outside control</u>; responding, reacting, or developing independently of the whole

- Autonomic
  - occurring involuntarily or <u>spontaneously</u>; occurring as a result of <u>internal stimuli</u>



Autonomic Networking Terminology (2)

- Autonomic Nervous System: a control system that acts largely unconsciously and regulates bodily functions such as heart rate.
- Autonomic Computing: self-managing distributed computing resources, adapting to unpredictable changes while hiding intrinsic complexity from operators and users (IBM, 2001).
- Autonomic Network: Self-managing (self-configuring, self-protecting, self-healing, self-optimizing) but allowing high-level guidance by a central entity ("Intent")
  - "Plug and play for the ISP" or "plug and play for the enterprise"

Autonomic Networking Terminology (3)

- Autonomic Function: A specific self-managing feature or function.
- Autonomic Service Agent (ASA): An agent that implements an autonomic function, in part (for a distributed function) or whole.
- Autonomic Node: A node that employs autonomic functions
- Autonomic Control Plane (ACP): Self-configuring fully secure virtual network used for all autonomic messaging.

For more details see RFC7575

Digression: Where do RFCs come from?

- Only some RFCs, especially Internet standards, come from the IETF.
- Research-oriented RFCs mainly come from the Internet Research Task Force, https://www.irtf.org
  - IRTF research groups are open to all
- RFC7575 and RFC7576 preceded the IETF standards work on autonomic networking.
  - They came from the Network Management Research Group, NMRG.

Autonomic Networking Integrated Model and Approach (ANIMA) WG in the IETF

- Initial work items (almost complete)
  - Bootstrapping & trust infrastructure
  - Secure Autonomic Control Plane (ACP)
  - Discovery for autonomic nodes
  - Negotiation & synchronisation for autonomic nodes

- Next steps
  - Defining the domain boundary
  - ASA life cycle, authorisation and coordination
  - NOC and YANG integration
  - Information distribution

- Left for later
  - Intent (high level policy)
  - Tie in to Machine Learning and other AI techniques

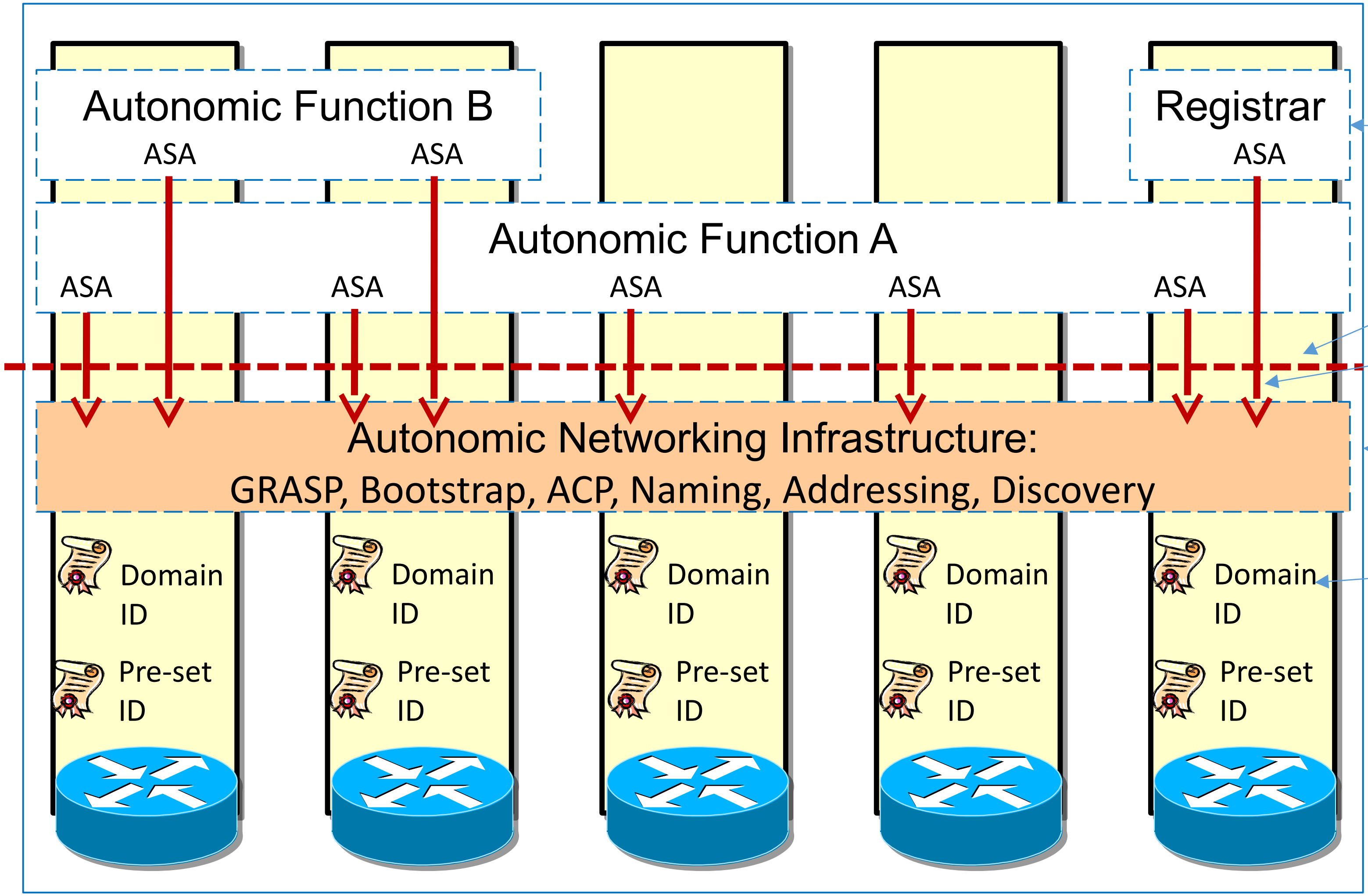
Bootstrap and Autonomic Control Plane

- Secure bootstrap – all nodes must start (out of the box or after a factory reset) by using a registrar to authenticate themselves and obtain a domain certificate. This is coordinated with related work for IoT devices. No human intervention except to create the registrar.
- ACP – the ACP will bootstrap itself using only link-local IPv6 addresses and IPv6 Unique Local Address prefix. All links secured (IPsec). No human intervention except to define the domain boundary.

GeneRic Autonomic Signaling Protocol (GRASP)

- GRASP will be used for signaling between ASAs
  - That includes the special-purpose ASAs that support both secure bootstrap & ACP creation
  - After that, GRASP runs over the ACP to guarantee security
- GRASP provides discovery, flooding, synchronization and negotiation for the <u>technical objectives</u> supported by ASAs
  - Based on CBOR (Concise Binary Object Representation)
  - Objectives can be expressed in JSON or Python-like syntax & semantics

Reference Model – High Level View



ASAs deployed as needed

Base infra: Every node must support

draft-carpenter-anima-asa-guidelines *

draft-ietf-anima-bootstrapping-keyinfra

draft-liu-anima-grasp-api *

draft-ietf-anima-grasp

draft-ietf-anima-autonomic-control-plane

draft-ietf-anima-bootstrapping-keyinfra

* not current WG item

Network with autonomic functions

Slide from Michael Behringer

draft-ietf-anima-reference-model

More about a GRASP Objective

- A configurable parameter:
  - a logical, numerical or string value, or a more complex data structure.
  - used in Discovery, Negotiation, Flooding and Synchronization.
  - semantics depend on the autonomic function concerned, and are built into the code of each ASA.
- Example for IP prefix management:

["PrefixManager", flags, loop_count,
                              [IP_version, prefix_length, prefix]]

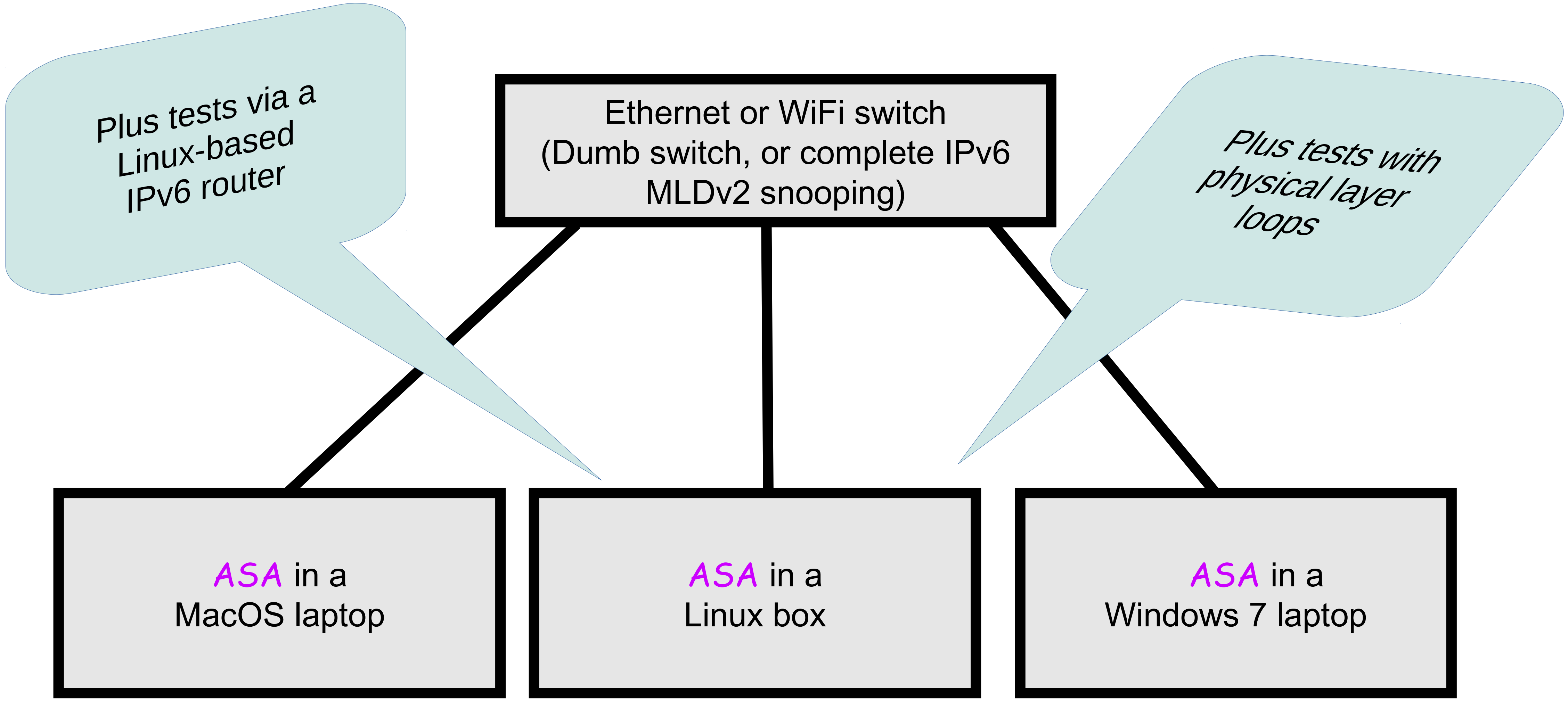
GRASP Messages

- Discovery (multicast)
  Discovery Response
- Request Synchronization
  Synchronization
- Flood Synchronization (multicast)
- Request Negotiation
  Negotiation
  Confirm Waiting
  Negotiation End

GRASP Prototype

- A Python 3 implementation of GRASP as a module `grasp.py`
- About 2300 lines of code
- A test suite to exercise as many code paths as possible
- Various demonstration ASAs to test operation across the network
- Some documentation
- Open source, available in GitHub

Tests



Plus tests via a Linux-based IPv6 router
Ethernet or WiFi switch (Dumb switch, or complete IPv6 MLDv2 snooping)
Plus tests with physical layer loops
ASA in a MacOS laptop
ASA in a Linux box
ASA in a Windows 7 laptop

Demonstration Autonomic Service Agents

Using the Python prototype:

- A toy example of a client negotiating a bank loan
- A multicast instant messaging tool
- A demo of the GRASP interactions involved in secure bootstrapping of an autonomic node
- Distributed IPv4 and IPv6 address prefix management
- DNS Service Discovery over GRASP
- Bulk data transfer (file transfer) over GRASP

Topics

- What is autonomic networking?
- What are limited domains?
- What next?

This is not about political or linguistic splintering of the Internet

This is not about DNS

Image: dreamstime.com

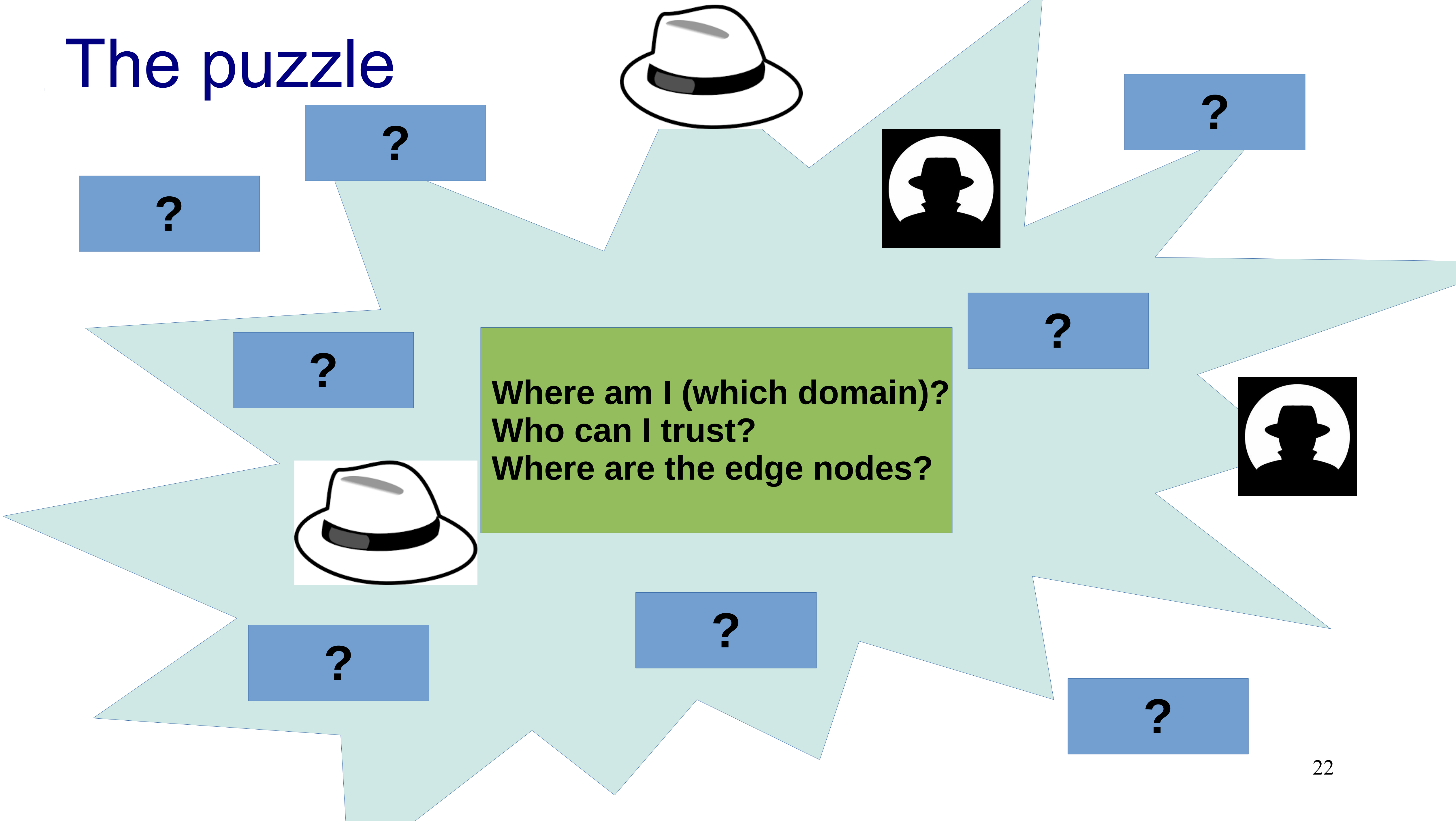
Many types of limited domain are appearing

- Home & small office networks
- In-vehicle networks
- Building services
- SCADA networks
- Sensor networks
- IoT edge networks
- Enterprise & campus networks
- Data & hosting centres (may be distributed)
- Network slices
- CDNs

Limited domain technologies are appearing

- Differentiated Services
- Network function virtualisation
- Service Function Chaining
- Data Centre Network Virtualization Overlays
- Segment Routing
- **Autonomic Networking (ACP)**
- Homenet (HNCP...)
- Creative use of IPv6 (flow label, extension headers, address bits)
- Deterministic Networking

The puzzle



?
?
?
?
?
?
?
?
Where am I (which domain)?
Who can I trust?
Where are the edge nodes?

Topics

- What is autonomic networking?
- What are limited domains?
- What next?

The challenge

- The doctrine: Internet standards should be universal in scope and applicability.
- But in the context of limited domains, some standards need to be limited in applicability (e.g., GRASP).
- A limited use requirement potentially *adds complexity* to the protocol and its security design.
- We know that, inevitably, a protocol intended for a particular scenario *will* be used elswhere.
- The challenge is to reconcile these aspects.

Open Questions

- What are the common aspects of Limited Domains?
- Should some protocols be standardised to interoperate only within a Limited Domain Boundary?
  - Such protocols are not required to operate across the Internet as a whole.
- How can we define a Limited Domain Boundary?
  - Can we specify protocol(s) to securely enrol as a domain member, discover other members, and discover boundary nodes?
  - Is the approach chosen for autonomic bootstrap the basis for a general solution?

Feedback?

- Reading list
  - RFC 7575
  - RFC 7576
  - https://datatracker.ietf.org/wg/anima/documents/
  - https://github.com/becarpenter/graspy
  - https://datatracker.ietf.org/doc/draft-carpenter-limited-domains/