

Autonomic Networking gets serious @IETF

3. KuVS Fachgespräch "Network Softwarization"
<https://kn.inf.uni-tuebingen.de/kuvs-fg-netsoft/2022>

Toerless Eckert, Futurewei USA (tte@cs.fau.de)

04/7-8/2022

Autonomic Networking in the IETF History

June 2012 draft-behringer-autonomic-network-framework-00.txt

Dec 2013 IRTF Network Management Research Group (NMRG) adopts autonomic networking work

Nov 2014 IETF ANIMA (Autonomic Networking Integrated Model and Approach) working group chartered

Jun 2015 NMRG releases 2 RFC

RFC7575 Autonomic Networking: Definitions and Design Goals

RFC7576 General Gap Analysis for Autonomic Networking

May 2021 Release of ANIMA “Autonomic Networking Infrastructure” (charter round 1: 350++ spec pages)

RFC8366: Validation use case 1: Stable Connectivity (23 pages)

RFC8368: BRSKI voucher (24 pages)

RFC8990: GRASP – Generic Autonomic Signaling Protocol (55 pages)

RFC8991: GRASP API (29 pages)

RFC8992: Validation use case 2: Prefix Management (19 pages)

RFC8993: Autonomic Networking Reference Model (26 pages)

RFC8994: ACP – Autonomic Control Plane (128 pages)

RFC8995: BRSKI – Bootstrap Remote Key Infrastructures (116 pages)

Internet Protocol Journal paper:

<https://ipj.dreamhosters.com/wp-content/uploads/2021/10/243-ipj.pdf>

Since then: Ongoing work in ANIMA (currently 11 working group drafts), NMRG (Internet) and several others (protocol details)

WHY/HOW ANIMA: Wide range of motivations / goals

Reliable/resilient and secure infrastructure management and services

Remote access. Hacking-safe, “critical infrastructure” support, ...

Intent-based networking

Operations/Automation from higher layer abstracted behavior → ongoing work

Self-X networks

Reliable/resilient and secure mechanisms to build decentralized/distributed network services

X = configuration, automation, optimization, securing, monitoring, ..

ANIMA vs. any other “autonomous, self-X” projects

Other projects top down: “Its all new magic in the SDN layers”. Don’t touch the infrastructure.

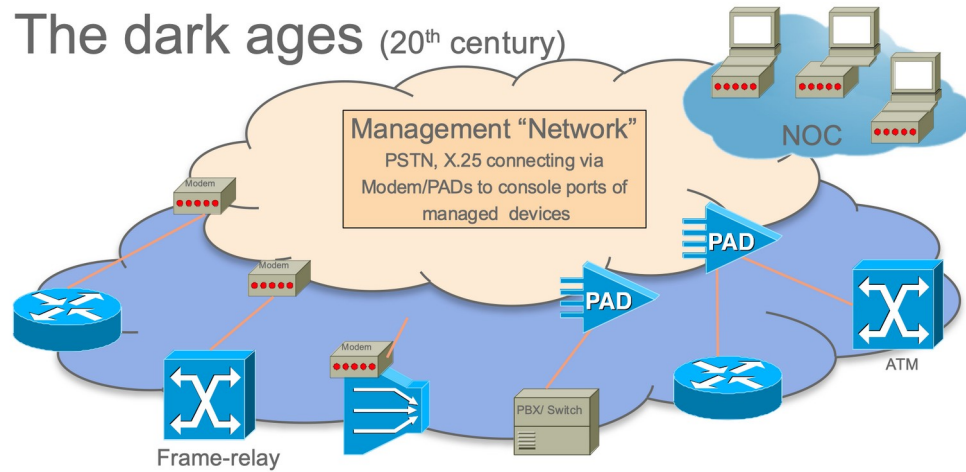
ANIMA is bottom up: **Not possible to achieve goals without fixing the infrastructure**

Example goal: Remote Network Management

Images © 2016 Cisco Systems (BRKSDN-2047)

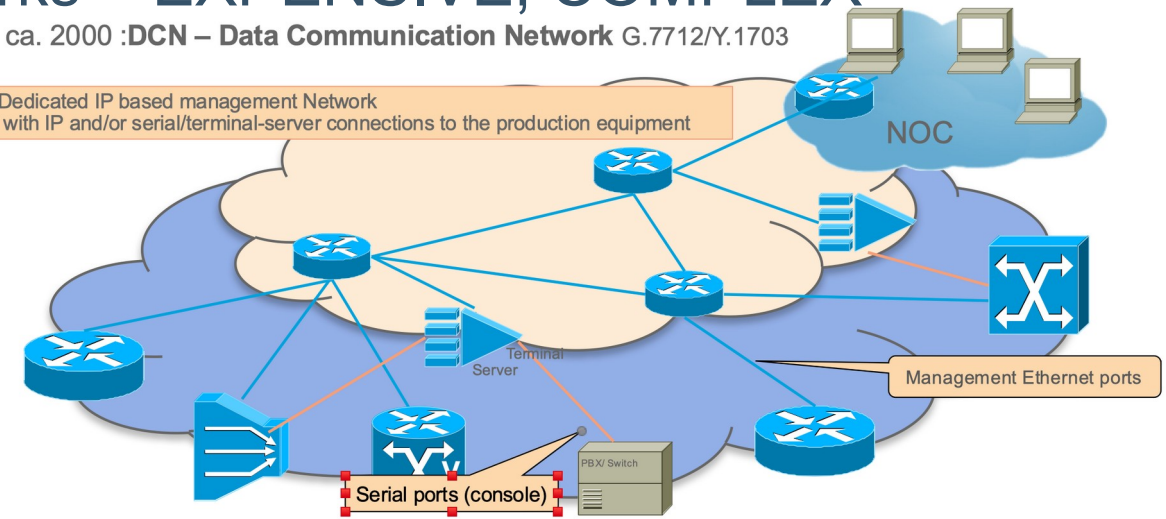
Out-of-band: Separate management networks – EXPENSIVE, COMPLEX

The dark ages (20th century)



ca. 2000 :DCN – Data Communication Network G.7712/Y.1703

Dedicated IP based management Network with IP and/or serial/terminal-server connections to the production equipment

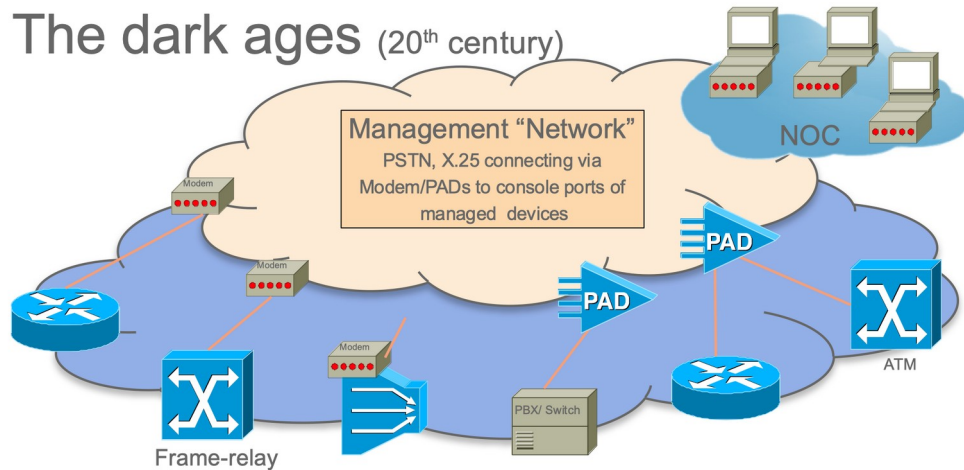


Example goal: Remote Network Management

Images © 2016 Cisco Systems (BRKSDN-2047)

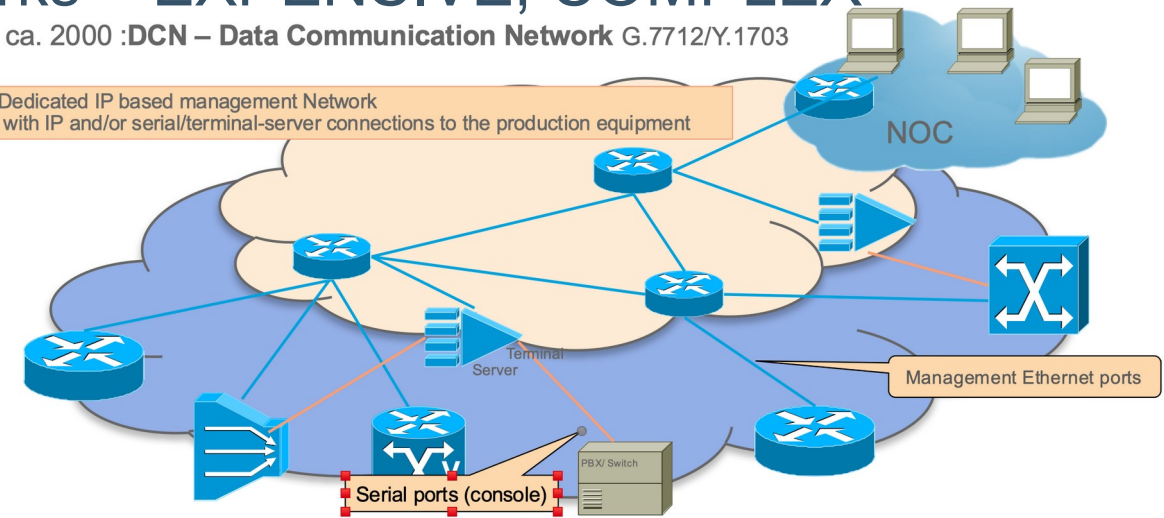
Out-of-band: Separate management networks – EXPENSIVE, COMPLEX

The dark ages (20th century)



ca. 2000 :DCN – Data Communication Network G.7712/Y.1703

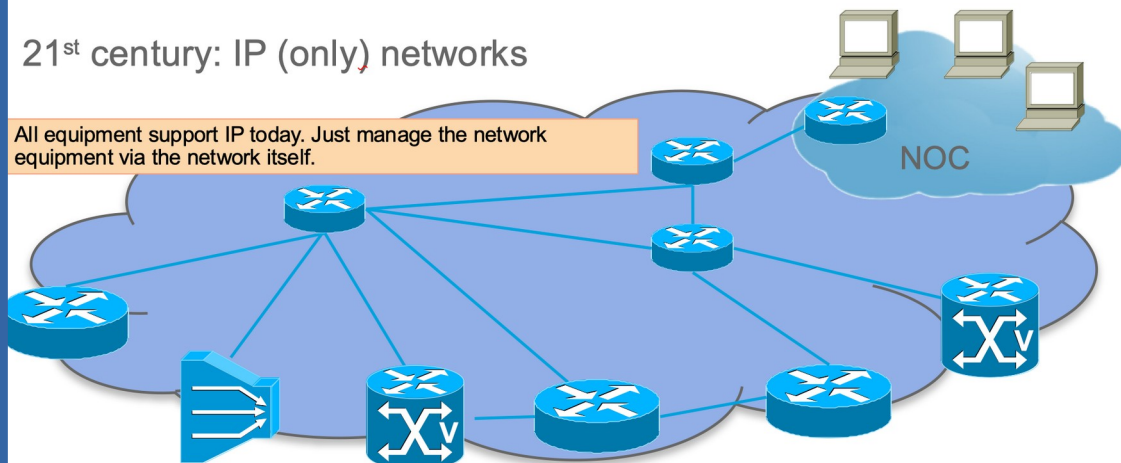
Dedicated IP based management Network with IP and/or serial/terminal-server connections to the production equipment



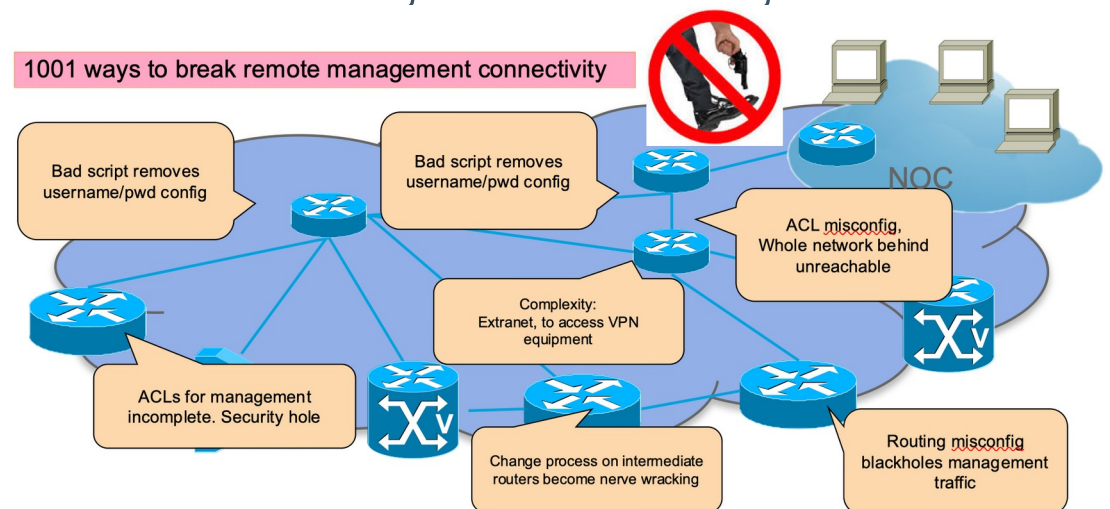
In-band: Use IP network to manage IP network: FRAGILE, ONE-OFFS, COMPLEX

21st century: IP (only) networks

All equipment support IP today. Just manage the network equipment via the network itself.



1001 ways to break remote management connectivity



In-band Remote Network Management: how bad is it ?

Day-0 issues: Expensive, obfuscated, insecure network bringup

Equipment shipping from/to pre-staging areas, Magically built “initial/bootstrap config”, ...

Day-N issues: Complex , fragile operations

Complex/unknown remote-management connectivity dependencies.

ACL (I2, L3, VPN), routing, policies, AAA, protocol securities, PKS chains, clock setting, competing automation systems

Typical recurring incidents: several hours outage in OTT, SP networks

Quantify cost/fragility: Great research topic ?

Except that it is mostly clouded in in-transparency

Sometimes blogs explain some tidbits “we had to send someone to location”, “competing automations killed routing”, ...

Unless there is regulation

USA: When network carries 911 (emergency) phone number service, interruptions are investigated by FCC

Results in public reports: Example from RFC8994 where ANIMA solution would have avoided lengthy outage:

*FCC, "June 15, 2020 T-Mobile Network Outage Report", A Report of the Public Safety and Homeland Security Bureau
Federal Communications Commission, PS Docket No. 20-183, October 2020,
<https://docs.fcc.gov/public/attachments/DOC-367699A1.docx>*

(Tenth of) millions of dollar fines !

No standards: hodgepodge of mechanisms to create “protected” in-band management plane

Mgmt address ranges, VRF, VLANs, VPNs, AAA authorizations (do not touch this config...), ...

From NMRG to ANIMA

NMRG Autonomic Networks:

Self-X networks. X = configuring, healing, managing, optimizing, protecting,

RFC7575/RFC7576

Network wide **Intent** based management

ASA - Autonomic Service Agents.

Distributed software modules embodying a decentralized or distributed function/service on network devices.

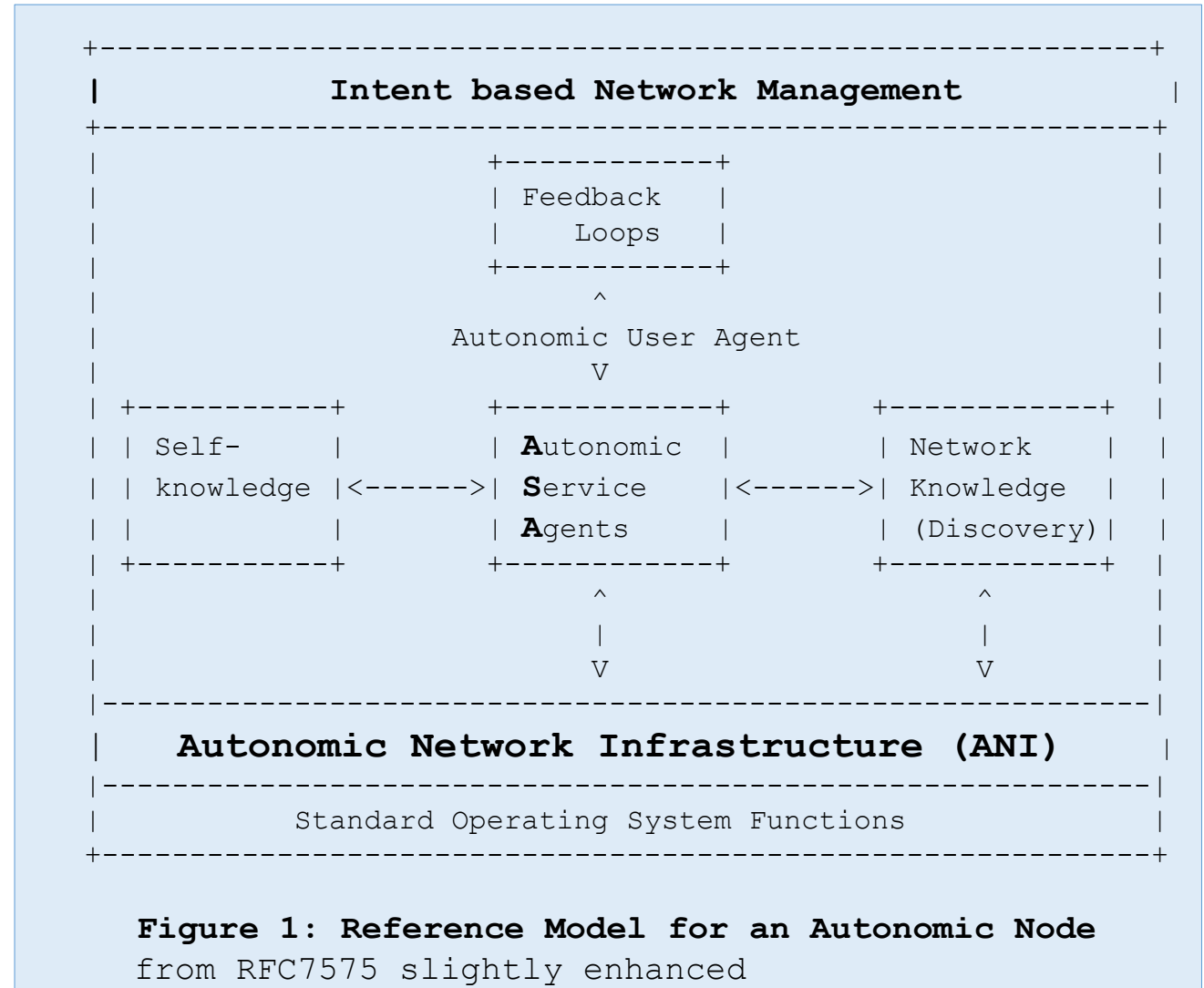
ANI - Autonomic Network Infrastructure

Common infra for ASA and secure automation of legacy networks

BRKI: Secure, zero-touch bootstrap/onboarding

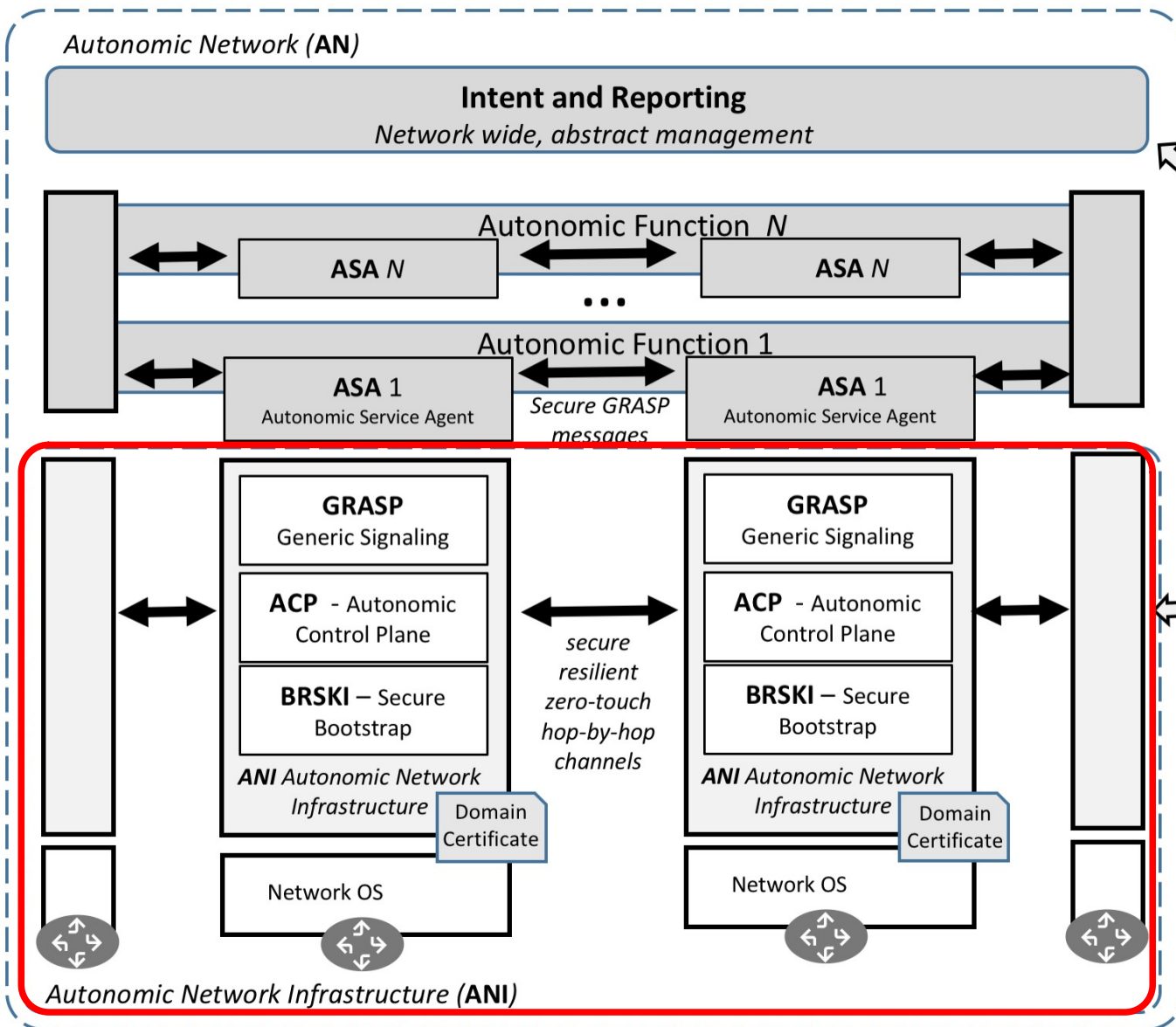
ACP: Secure zero-touch network wide connectivity

GRASP: Secure zero-touch extensible signaling

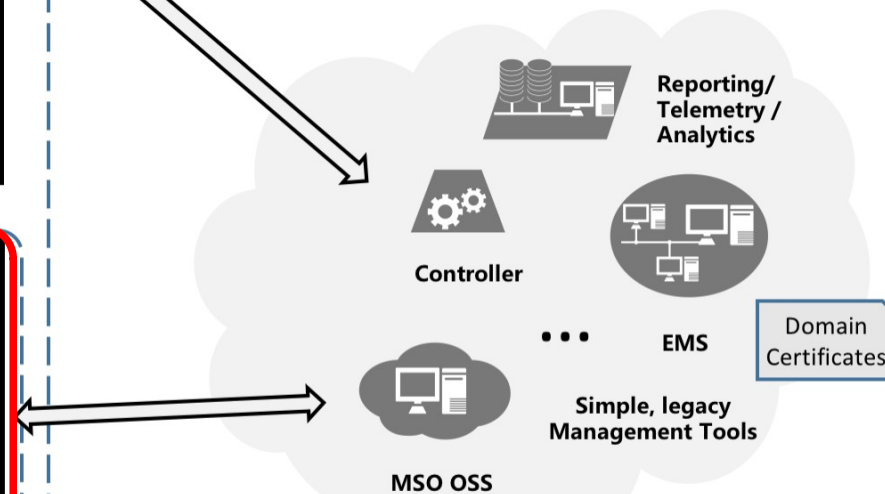




Autonomic Network according to ANIMA RFC8993 (Reference model RFC)



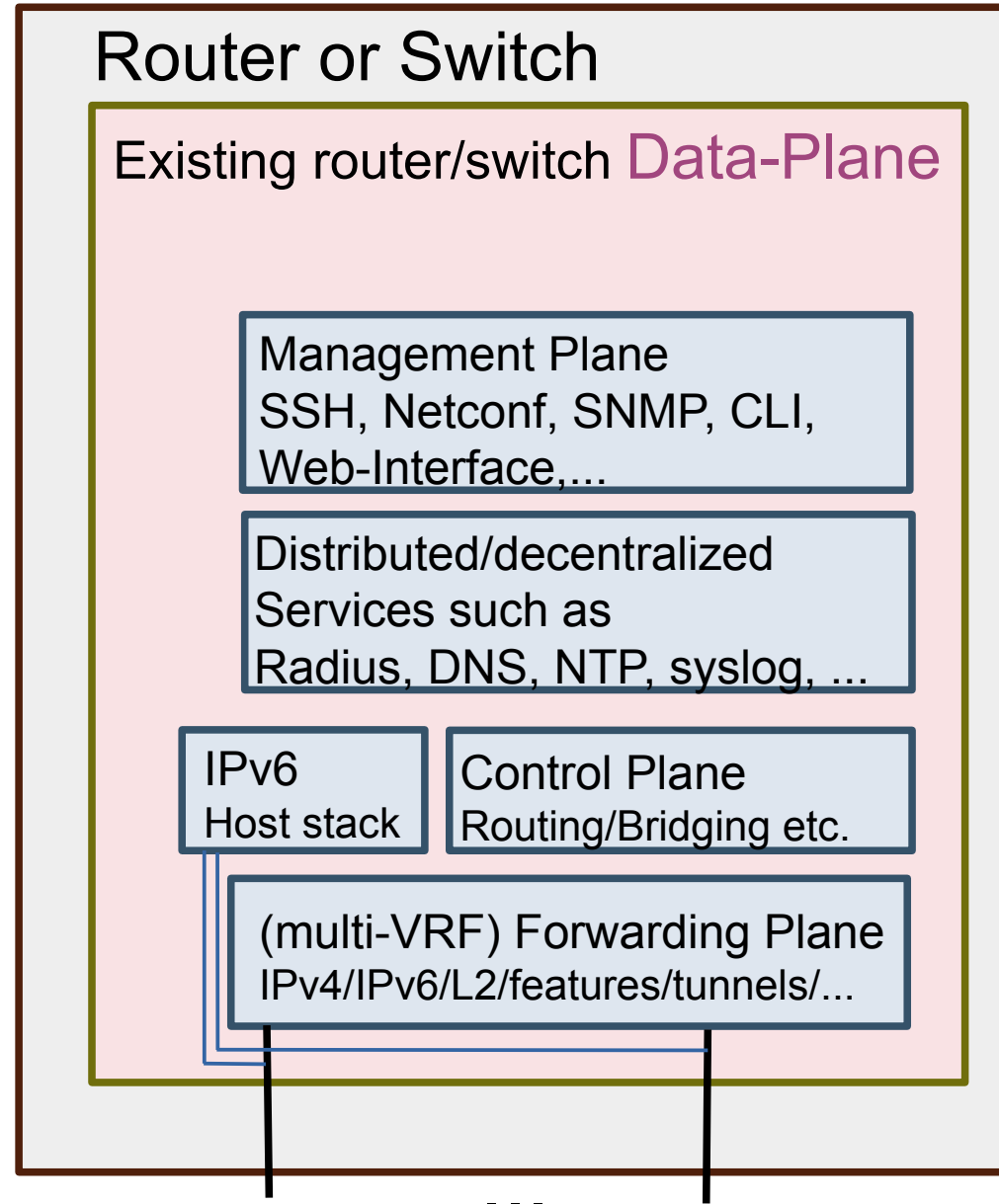
Autonomic Network (AN):
Intent based
network management



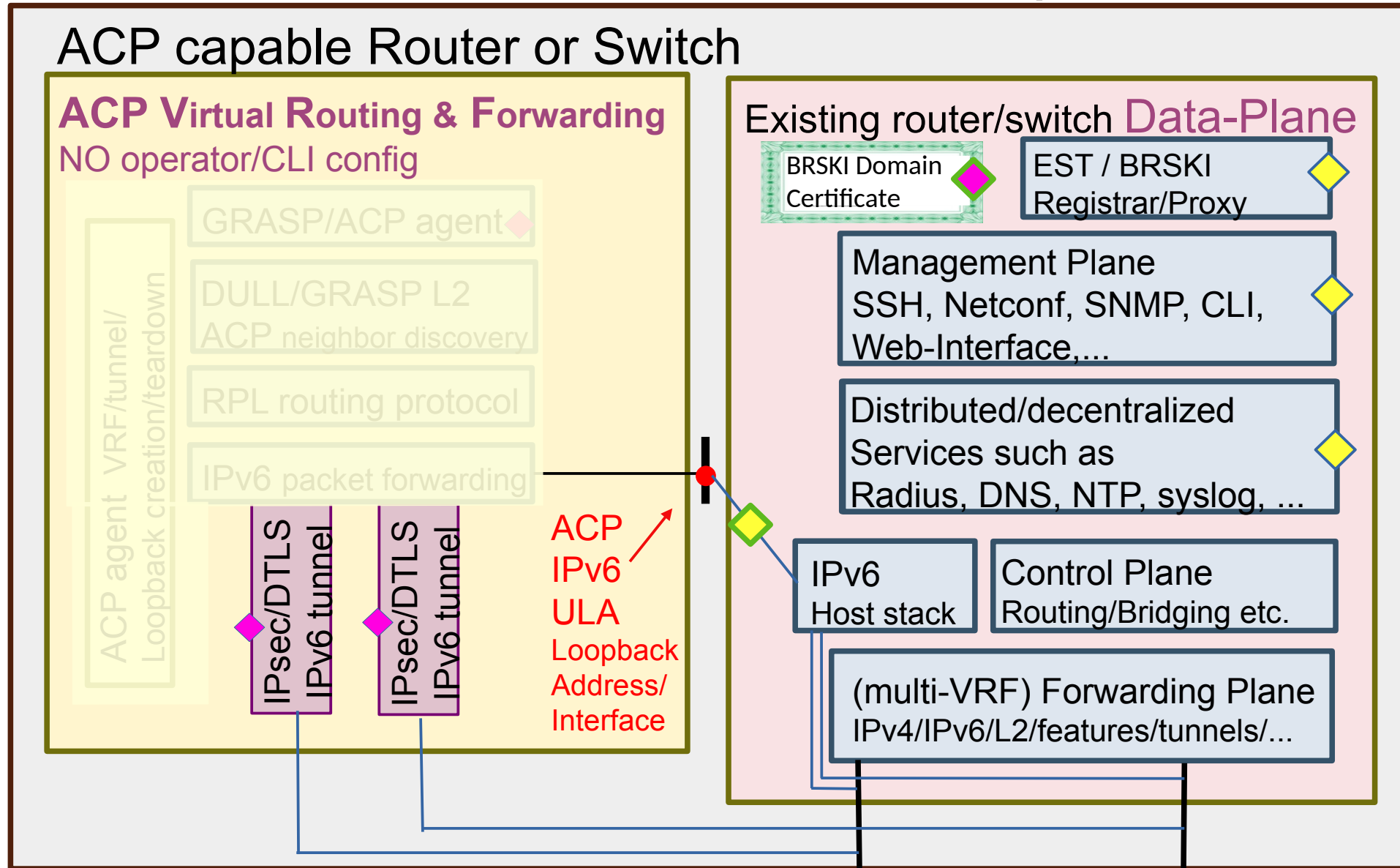
ANI:
Secure, reliable and automatic IPv6 NOC connectivity,
Secure bootstrap, Zero touch service auto configuration
Domain wide (NOC and infrastructure) zero-touch certificates





NOC – Network Operations Center
OAM – Operation, Administration, Maintenance

Autonomic Control Plane (ACP) (1)



Autonomic Control Plane (ACP) (2) – example/minimum design



  provide/use ACP connectivity
  provide/use certificate for security

...
physical router interfaces

Autonomic Control Plane (ACP)

PRE

X.500 certificate for the ACP <DOMAIN>

Includes IPv6 ACP loopback address field

Any PKI Mechanism: manual ... BRSKI

ACP

0. Simple, scalable routing protocol (RPL) runs in ACP

All routes are /128 ACP loopback address routes

1. ACP neighbor auto-discovered on subnets DULL-GRASP

2. Single-hop secure-channel built to ACP neighbor

Requiring peers with X.500 DOMAIN certificate

Negotiated; IPsec, DTLS or other

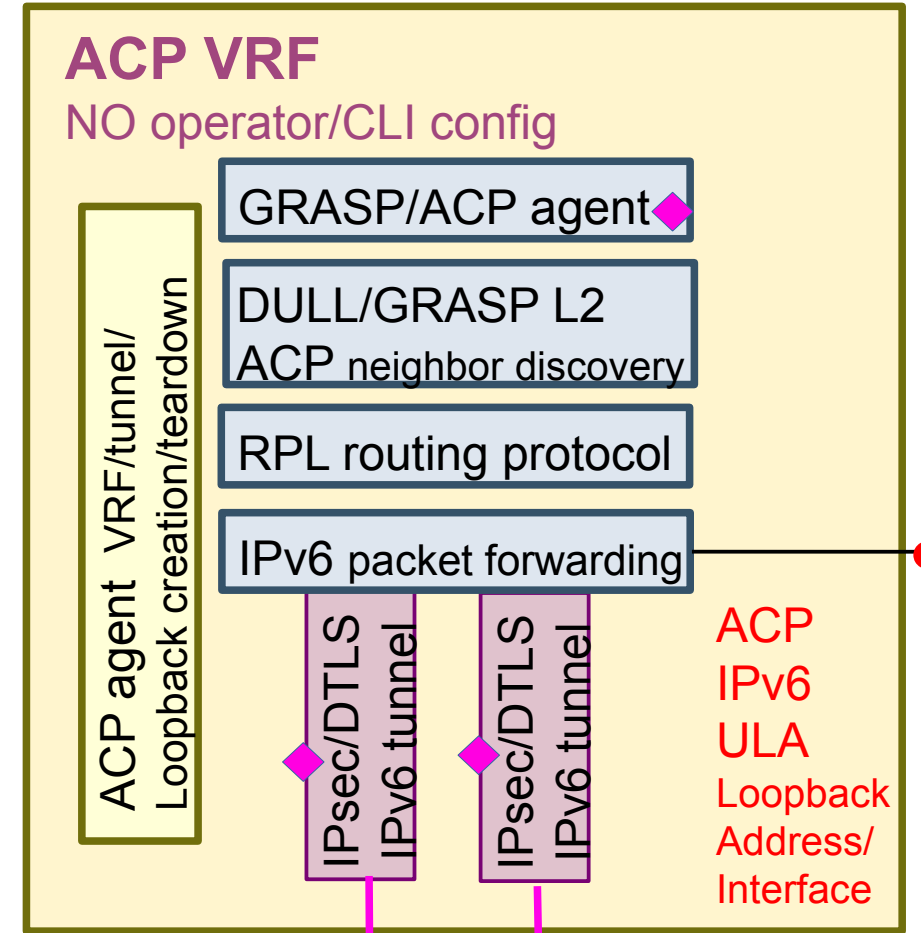
Uses only link-local IPv6 addresses

3. Secure channels become P2P interfaces in the ACP VRF

Uses only link-local IPv6 addresses

4. GRASP/ACP provides network-wide signaling

Reliable hop-by-hop multicast for service discovery



For Host stack apps accessing ACP

Classic **Broken** remote automated PKI enrollment



PKI Registrar

Drives/coordinates process

E.g: EST RFC7030 enrollment protocol

Admission Control

How to give connectivity to Pledge ?

Pledge connected in remote location

Pledges are router/switches

Today all IP/routing manually configured

Enrollment of hosts easier

When they can assume a working/secure network infra

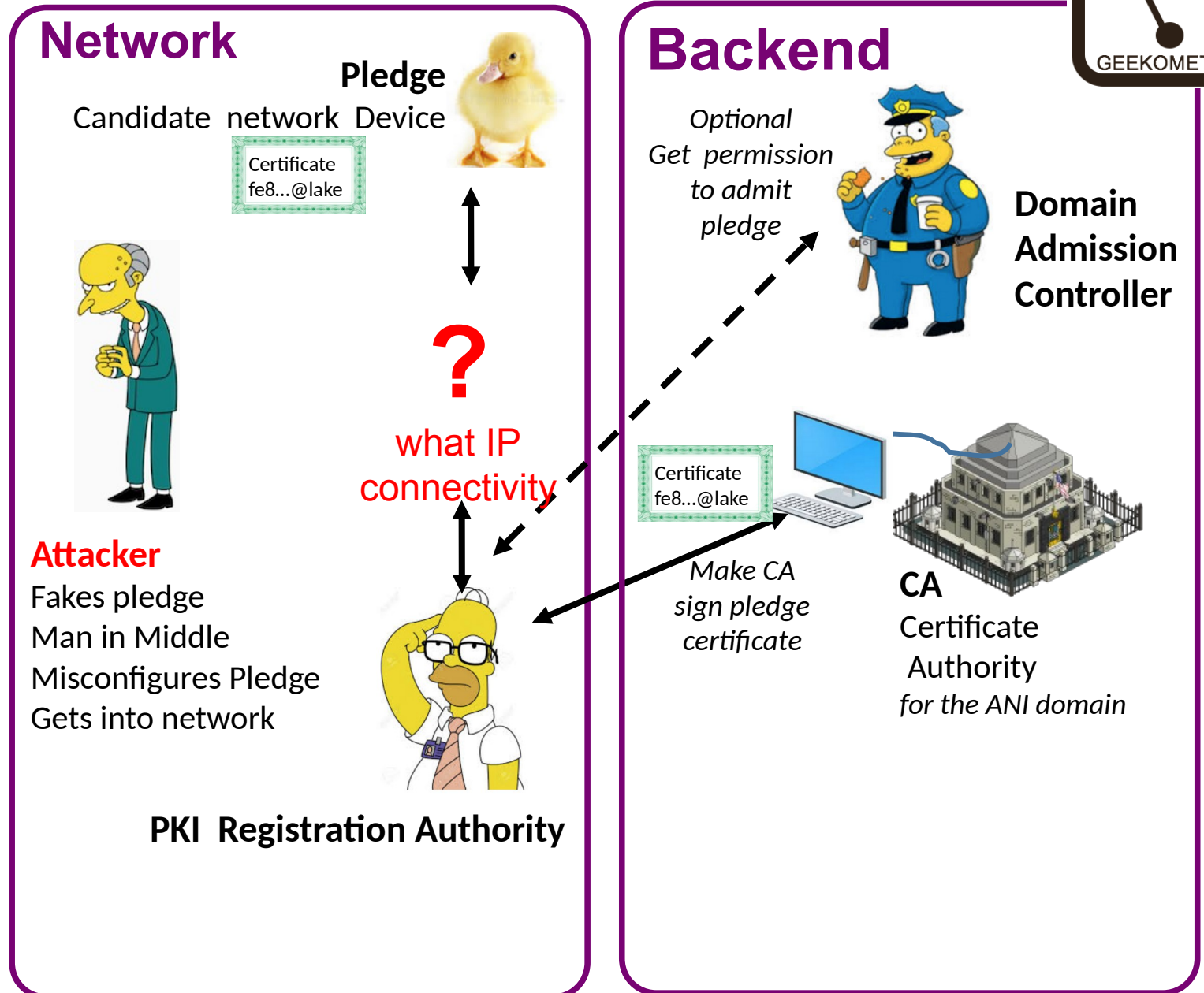
How to protect against attacks ?

How does Pledge trust Registrar instead of attacker ???

Today: They don't!

Remote cert enrollment easily attackable

Today: Secure/local pre-staging location



Bootstrap to ANI (ACP+BRSKI) DOMAIN membership

PKI enrollment with ACP/Voucher/MASA



Voucher – new crypto artefact

New digital artefact to indicate to Pledge that Registrar is authorized to control Pledge

Manufacturer (MASA) – new cast member

Run on behalf of manufacturer of Pledge

Pledge can trust MASA because Pledge software can have its manufacturers Trust anchors

MASA generates voucher for Registrar

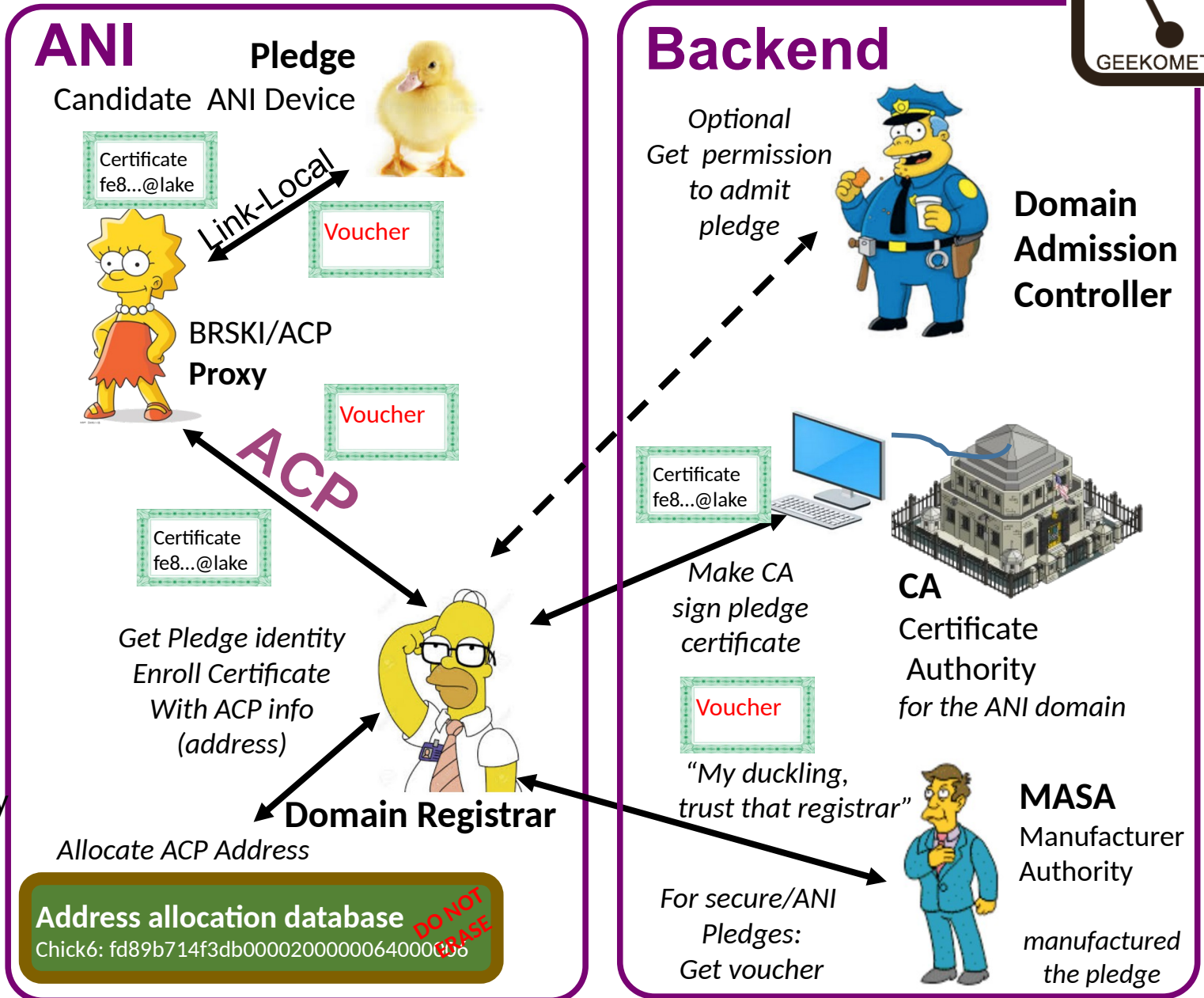
After it has validated DOMAIN owns Pledge

Proxy – new cast member

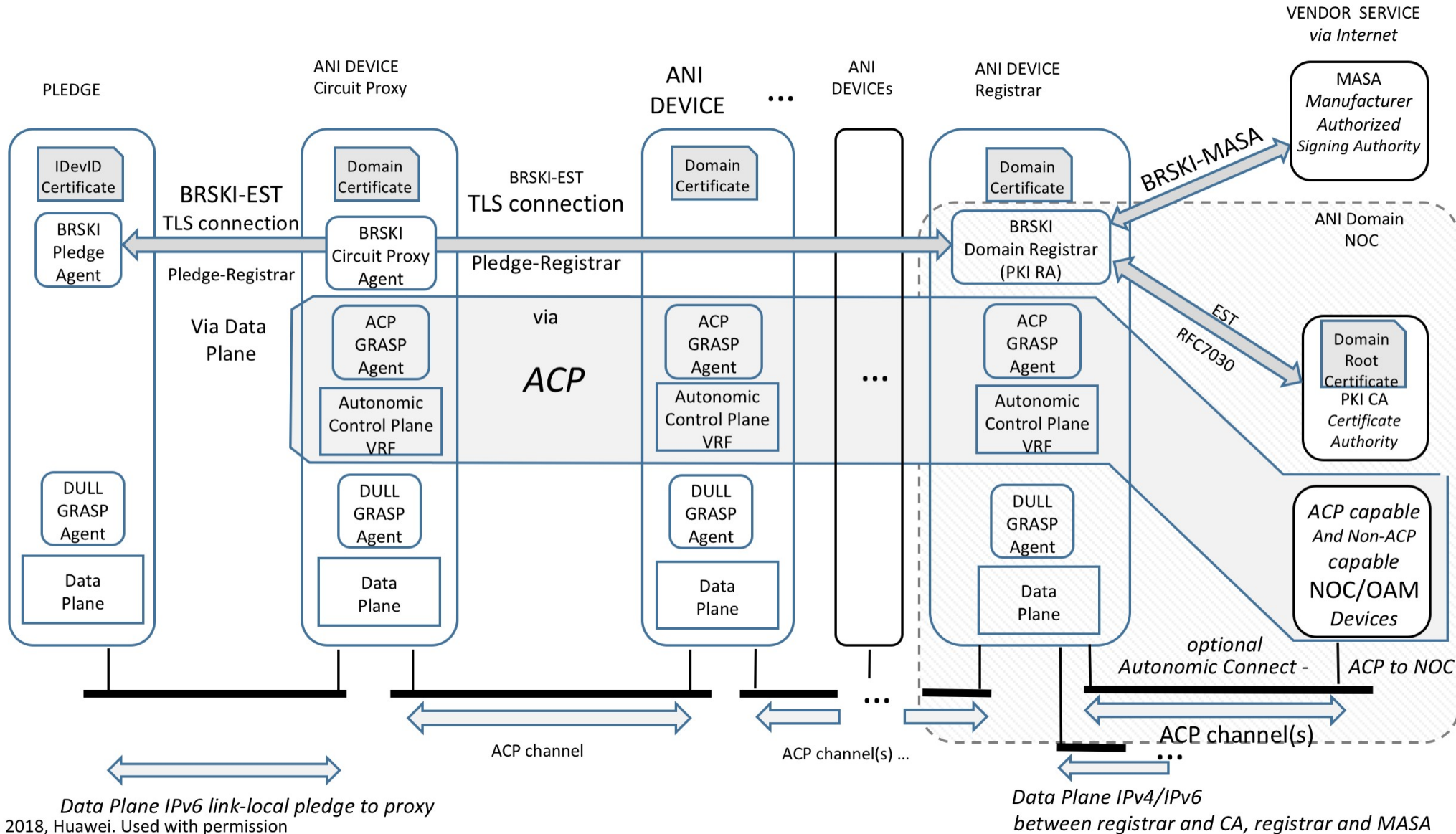
Distributed Agent to give registrar connectivity to adjacent pledge

Relies on ACP to talk to Registrar

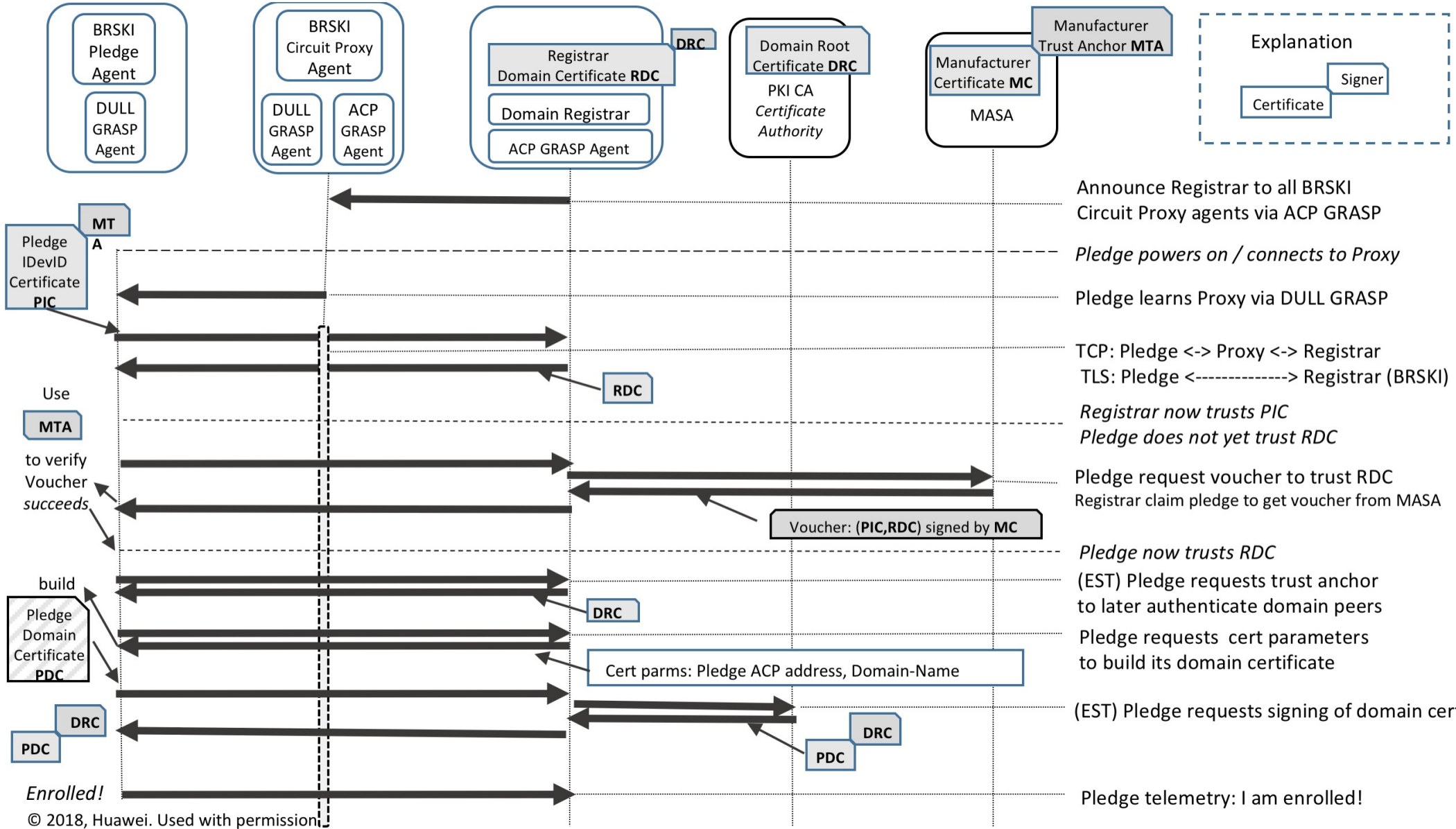
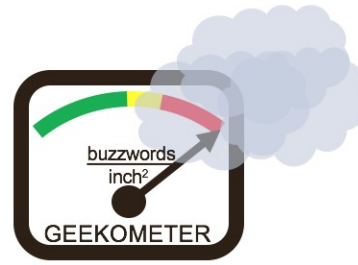
ACP Address allocation – new feature



For self-study: How does it really work – ANI (1)



For self-study: How does it really work - BRSKI (2)

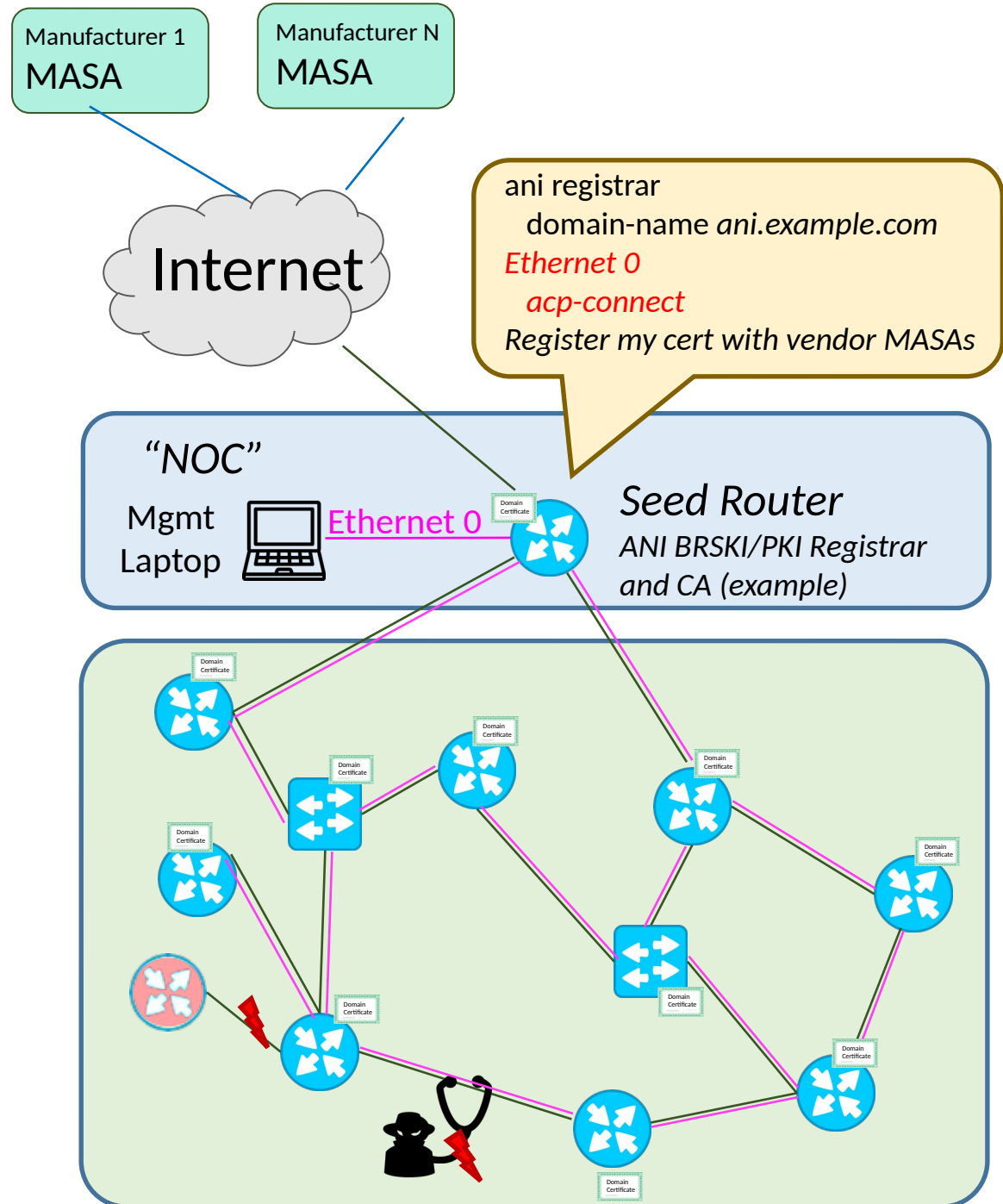


Example Minimum ANI Setup/Config



Münchhausen

O. Herfurth pinx



Where are we now on the Autonomic Network vision ?

Since Q2' 2020 on 2nd Charter

Added ASA work to charter

Added ANI enhancement

Pushed out Intent back to NMRG

NMRG nicely working on the research steps

ANI: Bootstrap sees quite wide proliferation/adoption across IETF and industry (next slide)

Hackathons, Also iot-onboarding / MUD adjacencies

Relatively little new code (on top of existing PKI, tool chains), but quite security critical, open source available

Many different protocol preferences in different markets = many variations needed/worked on in IETF.

ANI: ACP seeing little movement yet

Logical ? Bootstrap must first work

Pre-standard industry implementations exist. Legacy router implementation complex.

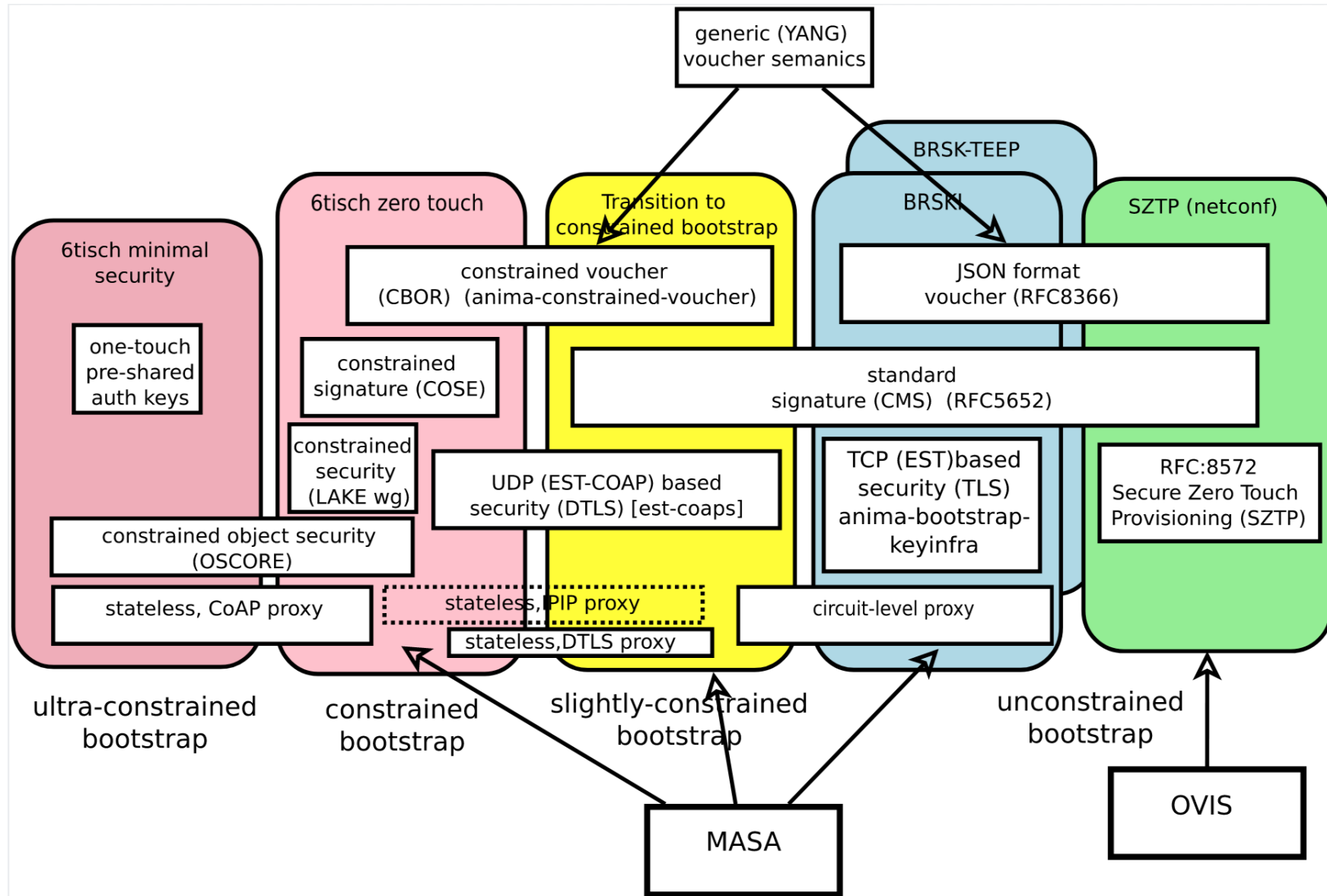
Open Source (linux, openwrt, rare?, ...) implementations missing

Open Source components exist (BRSKI, GRASP, IPsec(*Swan)).

Linux Name spaces should make it easy to build the ACP setup/teardown

For self-study: Bootstrap landscape / roadmap

<https://github.com/anima-wg/enrollment-roadmap> (somewhat stale)



Distributed Automation: ASA

Ongoing work in NMRG, then maybe ANIMA ?

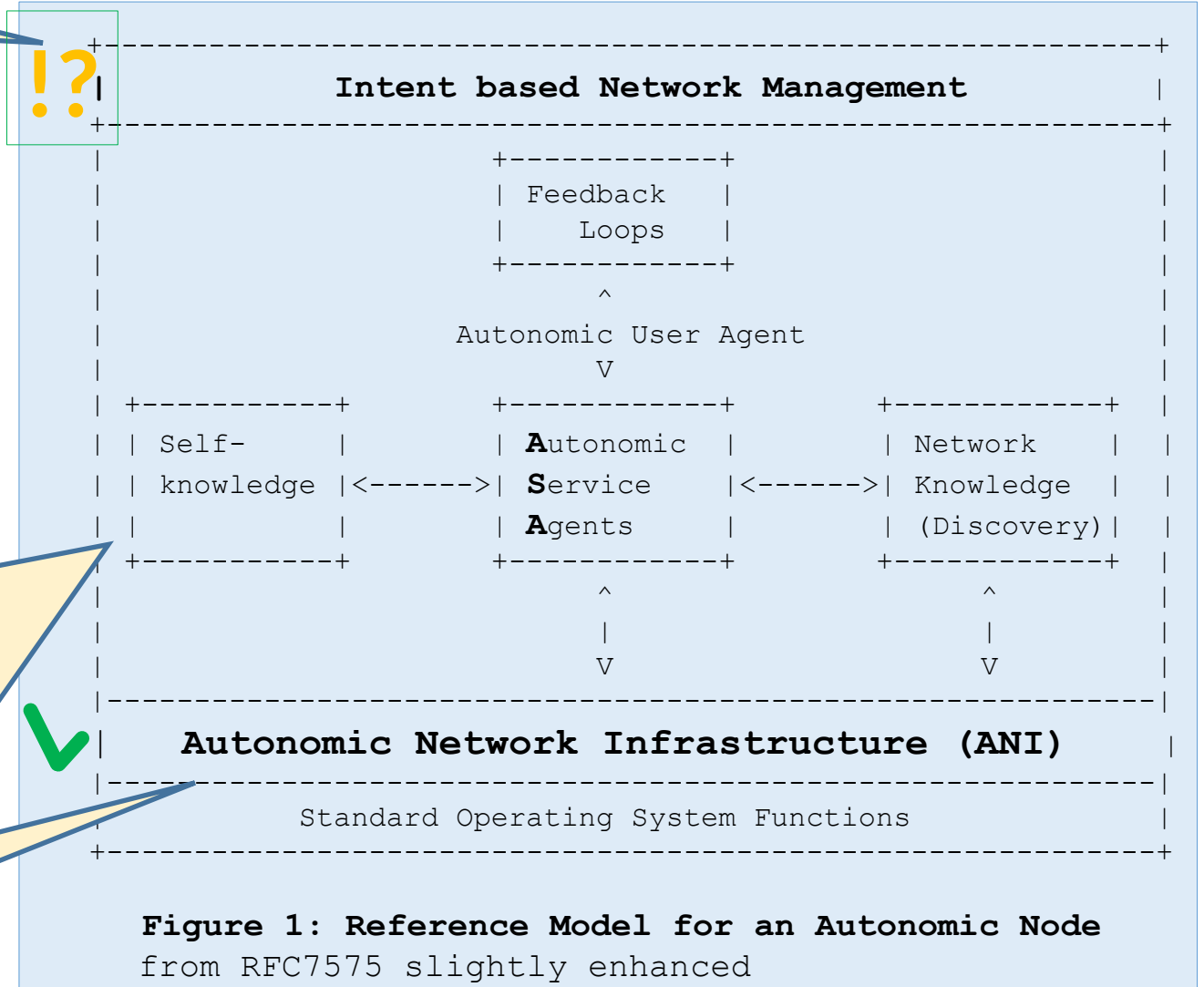
ACP provides network-wide any-to-any automatic reliable, secure connectivity,

GRASP/ACP provides any-to-any ASA discovery and communication primitives

Several comprehensive, ambitious architecture proposals in ANIMA over the years. Some simple WG drafts now.

Many options easy to implement, easy experimentation

ANI and extensions: ongoing in ANIMA and especially bootstrap also in other groups



Security: Many simple/incremental ANI use-cases

ANI Certificates for protocols/solutions with End-to-end security (e.g.: TLS, QUIC)

ANI: Strong, automatically renewed and flexible PKI certificates

Alternative to username/password and Web PKI

ANI resolves manual certificate management issues

ANI + simple script based ASA to secure many infrastructure services using Data-Plane

Many protocols with their own “security” mechanism (but no key management)

“auto-secure”: NTP, SMTP, MacSec, routing protocols (BGP, IGP, PIM), IPFIX and others

Also “auto-secure” TLS/QUIC solutions that can not use client-certificates (but only Web-PKI)

ACP makes legacy protocols (without security) more secure when they run across
ACP !

Hop-by-hop authentication/encryption

Self-driving: what if networks where cars



SDN-Controller
SDN-Orchestrator
SDN-Developer
Data Analyst
Network operator
Security Expert

In-network intelligence
→
ANIMA



↑
"self driving network" ?

The End

Please engage with us (proposal, questions, suggestion)
if you think this is useful for you !

anima@ietf.org