the Autonomic Control Plane (ACP)

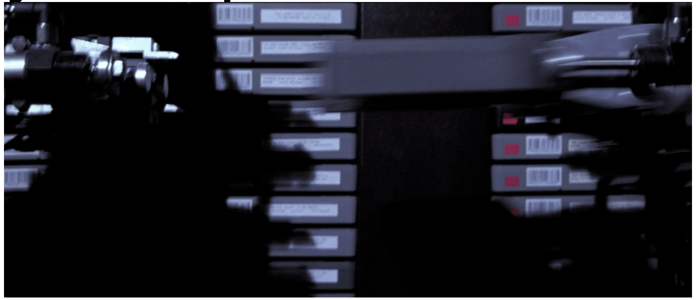
Michael Richardson
mcr+ietf@sandelman.ca

RFC8990 (GRASP), RFC8994 (ACP)
RFC8995 (BRSKI)
also 8991,8992 and 8993

slides at https://www.sandelman.ca/SSW/talk/2025-ipsec-workshop

Goal

- ISP and Enterprise operators
- Operator always has management access to all equipment.
  - telcos call it “craft console” access
  - the rest of us think of it as serial console
- It’s easy: just hook up a modem and pay for a phone line.
  - what could go wrong?



Virtual out-of-band access

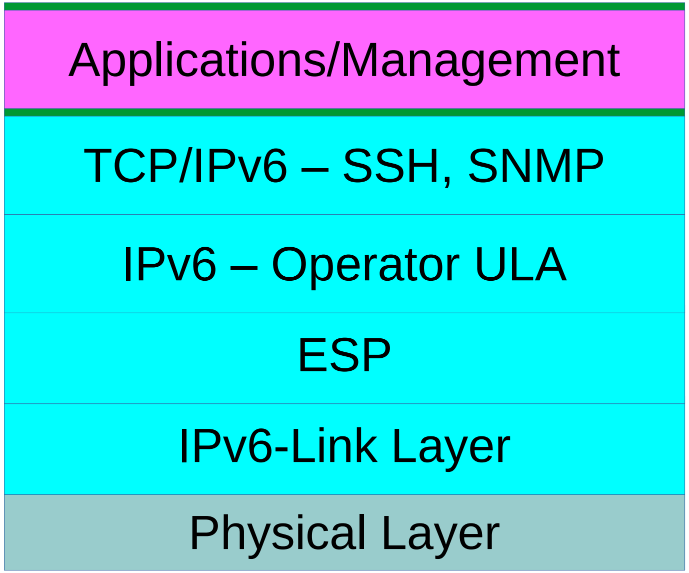
- But, phone lines are gone: Voice over IP
  - so if network is down, then no emergency access to fix network
  - cf: Rogers Canada’s “SDN” upgrade in July 7, 2023 toasts all of Canada for 24h
    - many banks learnt that their “redundant” links were not in fact resilient to Rogers’ breaking their L2
    - Rogers could not even do “phone tree” to reach their people, because... they used Rogers phones
- So, we need an always on overlay network
- RFC8994: Autonomic Control Network

ACP: Virtual out-of-band access

- ~~automatically~~ **autonomically** forming/bootstraped
- strongly authenticated
- self-healing
- includes all L2 equipment as well as L3
- independant of high-speed forwarding plane
  - can use high speed network as redundant link
  - MPTCP, QUIC, etc. could be used if you need “high throughput”
- Routing on Top

- ACP needs to be used for frequent management uses
- otherwise nobody knows when it broke
- SNMP connections
- SSH connections
- all manner of SDN

ACP: Architecture



Applications/Management

TCP/IPv6 – SSH, SNMP

IPv6 – Operator ULA

ESP

IPv6-Link Layer

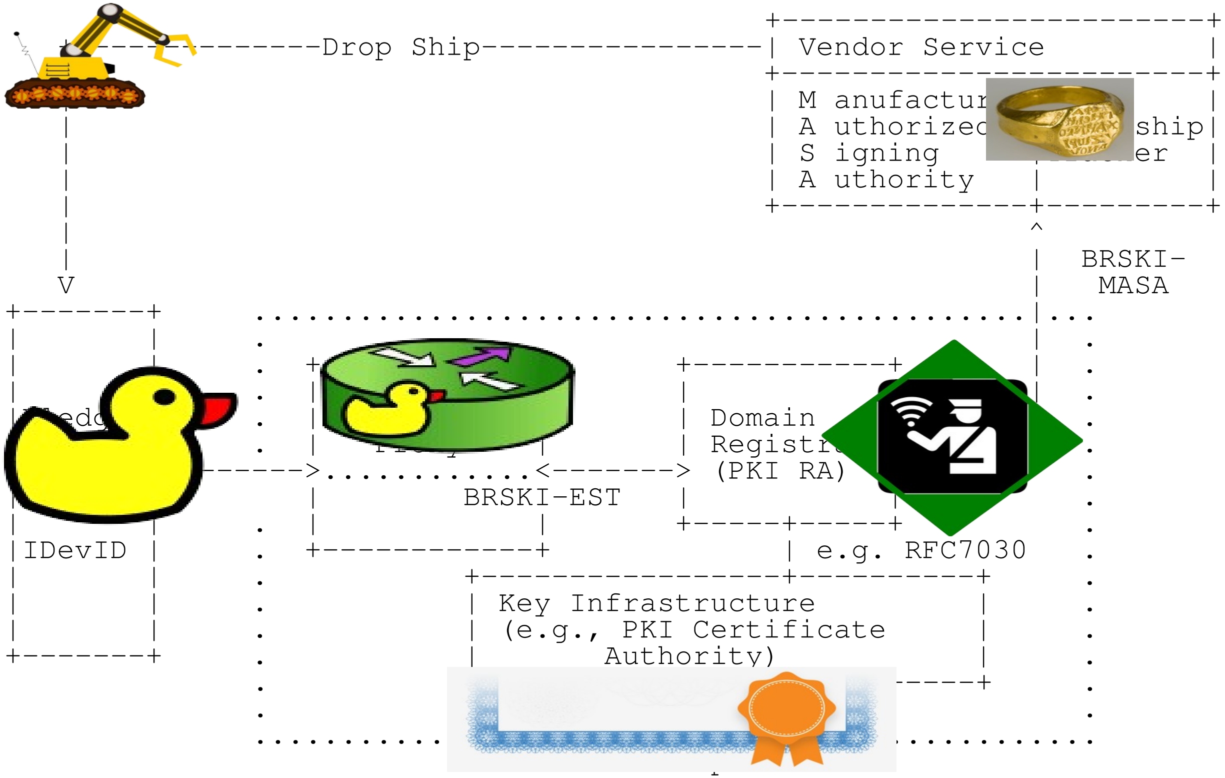
Physical Layer

- Laser would ideally stay on even when port is administratively “down”
- Each port of switch would have its own interface logical interface, even if switch is really L2 only
- ESP is hop-by-hop, ideally **L2** hop-by-hop.
- Overlay creates “full” mesh across network
- Authentication is all PKIX certificates, from a common (private) CA
  - authorization is private CA == good
- “IP over Transport Mode”, but really it’s IP ::/0<--> IP ::/0 over ESP tunnel mode.
- IP addresses are not strongly filtered

Onboarding: BRSKI

- RFC8995
  - transfer of ownership from manufacturer to operator
  - based upon RFC8366 voucher artifact
  - mediated by manufacturer (‘s authorized signing authority)
- many variations coming to an RFC near you, maybe this year
- become popular among IoT (no ACP)
- interest among building and security automation
- Zero-Touch: ship device from warehouse to target location/data-center.
  - supports things like 4Hr SLA, where vendor has to keep spares in each city, but does not have a spare per customer

BRSKI: Architecture Overview



Drop Ship

Vendor Service

M anufactur

A uthorized

S igning

A uthority

ship

er

BRSKI-MASA

V

edg

IDevID

BRSKI-EST

Domain

Registr

(PKI RA)

e.g. RFC7030

Key Infrastructure

(e.g., PKI Certificate

Authority)

Figure 1: Architecture Overview

RFC8995

https://www.sandelman.ca/SSW/talks/brski/

NIST IoT Onboarding

- 2022 to 2025 effort
- DPP(x2), BRSKI (x2), application onboarding
- Device Identity Forum

  https://iotsecurityfoundation.org/deviceid-wg/

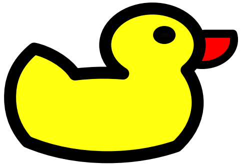
IoT Open House
Tech Deep Dive
Build 3 – BRSKI
Michael Richardson
Sandelman Software Works Inc

Anxiety, keep on tryin' me
I feel it quietly
Tryin' to silence me, yeah
My anxiety, can't shake it off of me
Somebody's watchin' me
And my anxiety, yeah
Oh
Oh, oh, oh, oh, oh

https://www.sandelman.ca/SSW/talk/2025-ssw-nccoe-iot-build3/

Some BRSKI terminology and icons!

- Pledge



Stajano, F. and Ross Anderson,
"The resurrecting duckling: security issues for ad-hoc wireless networks", 1999,
https://www.cl.cam.ac.uk/~fms27/papers/1999-StajanoAnd-duckling.pdf
Wikipedia, "Wikipedia article: Imprinting", July 2015,
https://en.wikipedia.org/wiki/Imprinting_(psychology)
https://en.wikipedia.org/wiki/Animal_House

20yr Old Ross Anderson paper

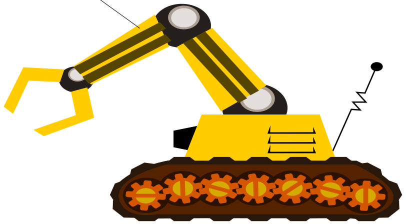
- Manufacturer

  Authorized

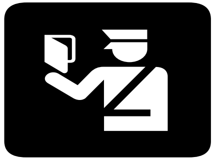
  Signing

  Authority

  -> MASA.



- Join Registrar/Coordinator
  - JRC
  - “Registrar”



- VOUCHER
  - RFC8366

Concentric Onboarding

- brski.org has many videos, talks and screencasts
-

- https://www.sandelman.ca/SSW/talks/brski/brski-animation.pdf

IPsec and ACP