SCTE ISBE CABLE-TEC EXPO '16

SEPTEMBER 26-29 PHILADELPHIA

Autonomic Networking Infrastructure

The Foundation For Next-Generation Operations, Maintenance And Automated, Software Defined Networks

Toerless Eckert

Principal Engineer

Cisco Systems Inc.

SCTE Society of Cable Telecommunications Engineers

ISBE International Society of Broadband Experts

Essential Knowledge for Cable Professionals™

#CableTecExpo

Abstract

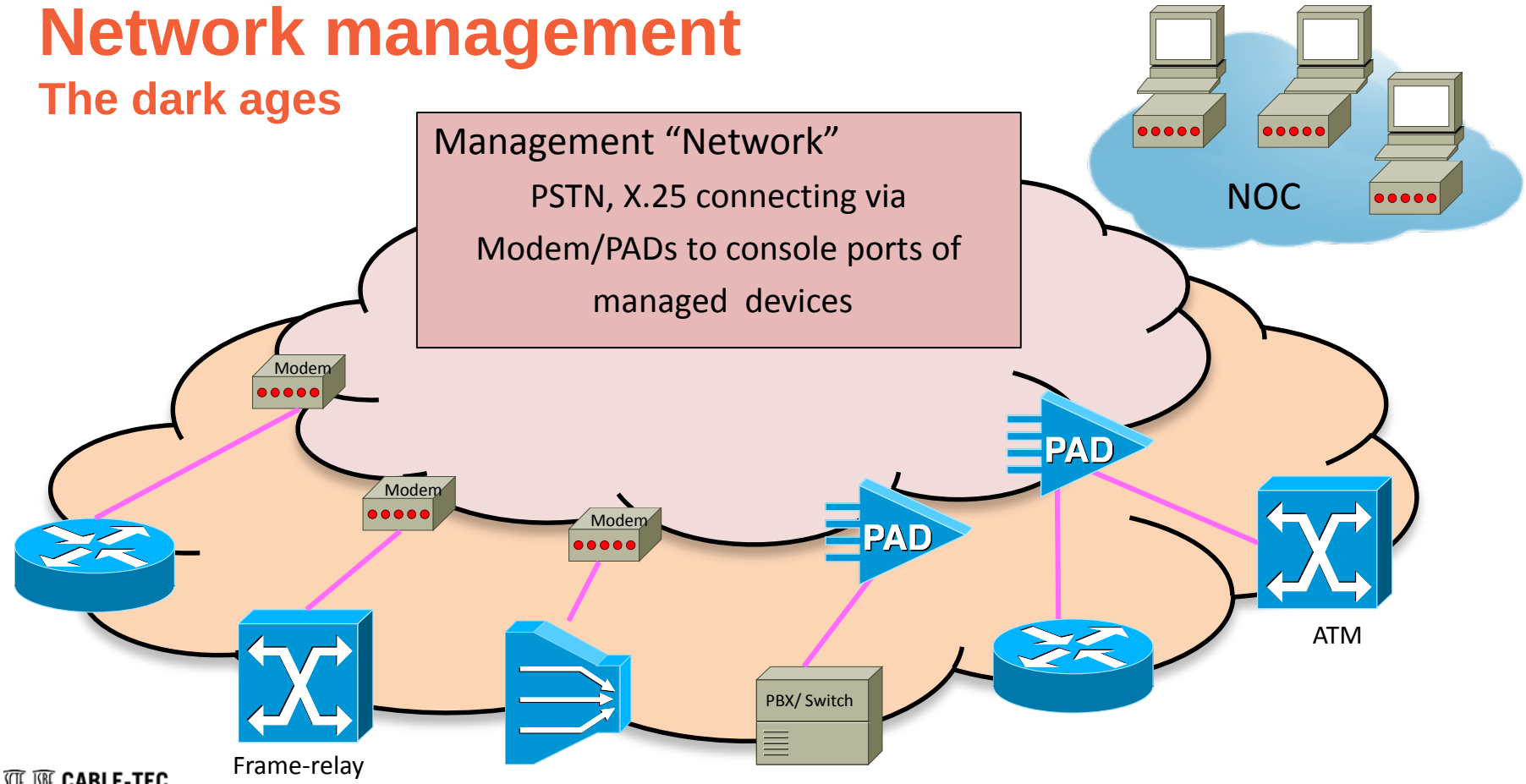
Operations, administration and management (OAM) of large network today relies most often on so called in-band connectivity: The same (IP) network managed is also used to provide the OAM connectivity between the managed devices and Network Operation Centers.

During booting of new topologies, the core part of network services and security needs to be configured hop-by-hop to allow OAM of the next device. During day-to-day operations, the need to provide in-band OAM connectivity makes change management of these services fragile and dangerous because of the circular dependency created. Applications written for SDN controllers need to model all these dependencies to perform reliable change management.

This paper shows how an autonomically built and maintained in-band OAM management plane, called the “Autonomic Control Plane” can help to provide for complex IP/MPLS networks a reliable, secure, indestructible and standardized OAM communications fabric to solve those issues.

Network management

The dark ages



Network management

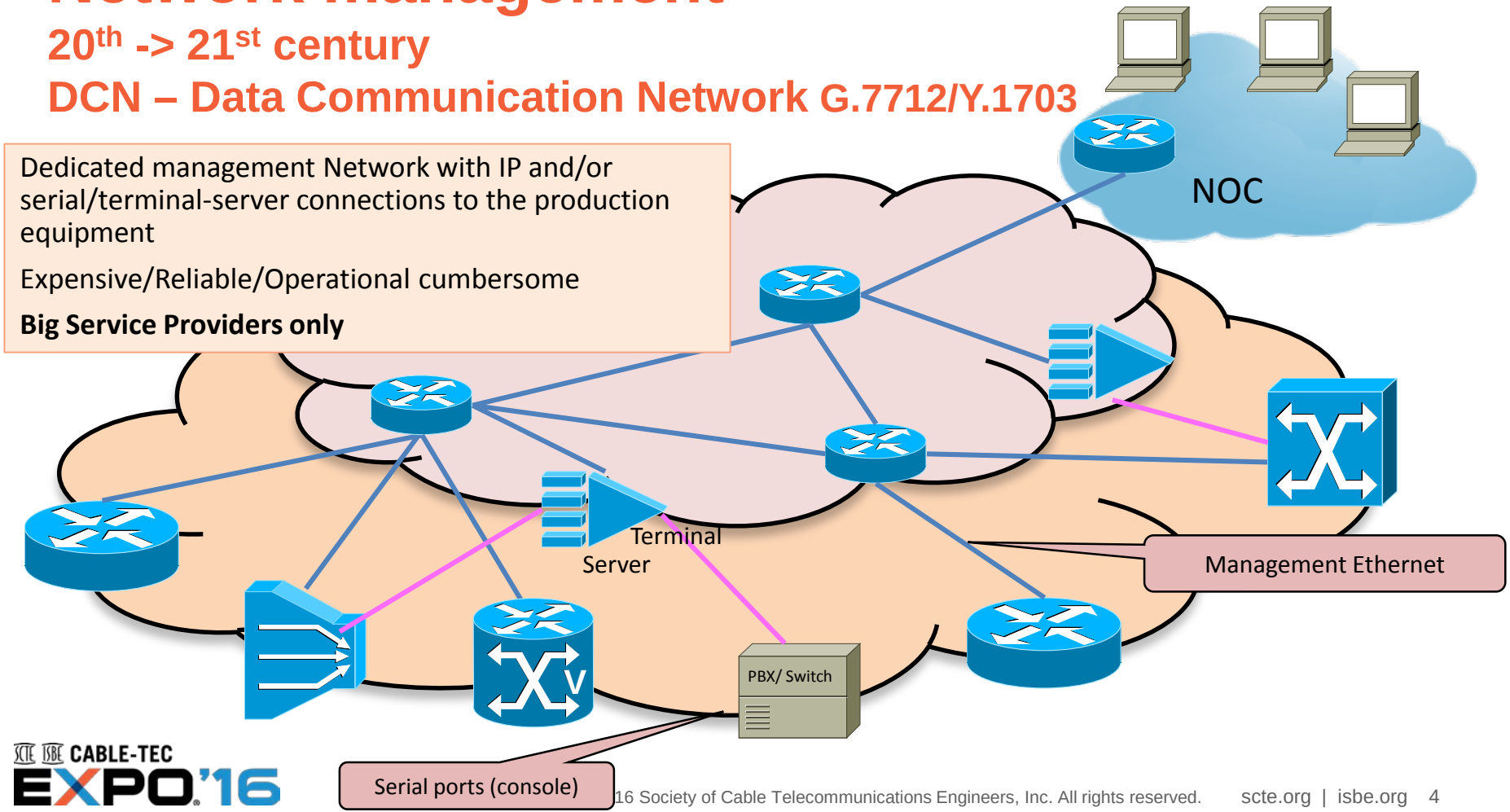
20th -> 21st century

DCN – Data Communication Network G.7712/Y.1703

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

Expensive/Reliable/Operational cumbersome

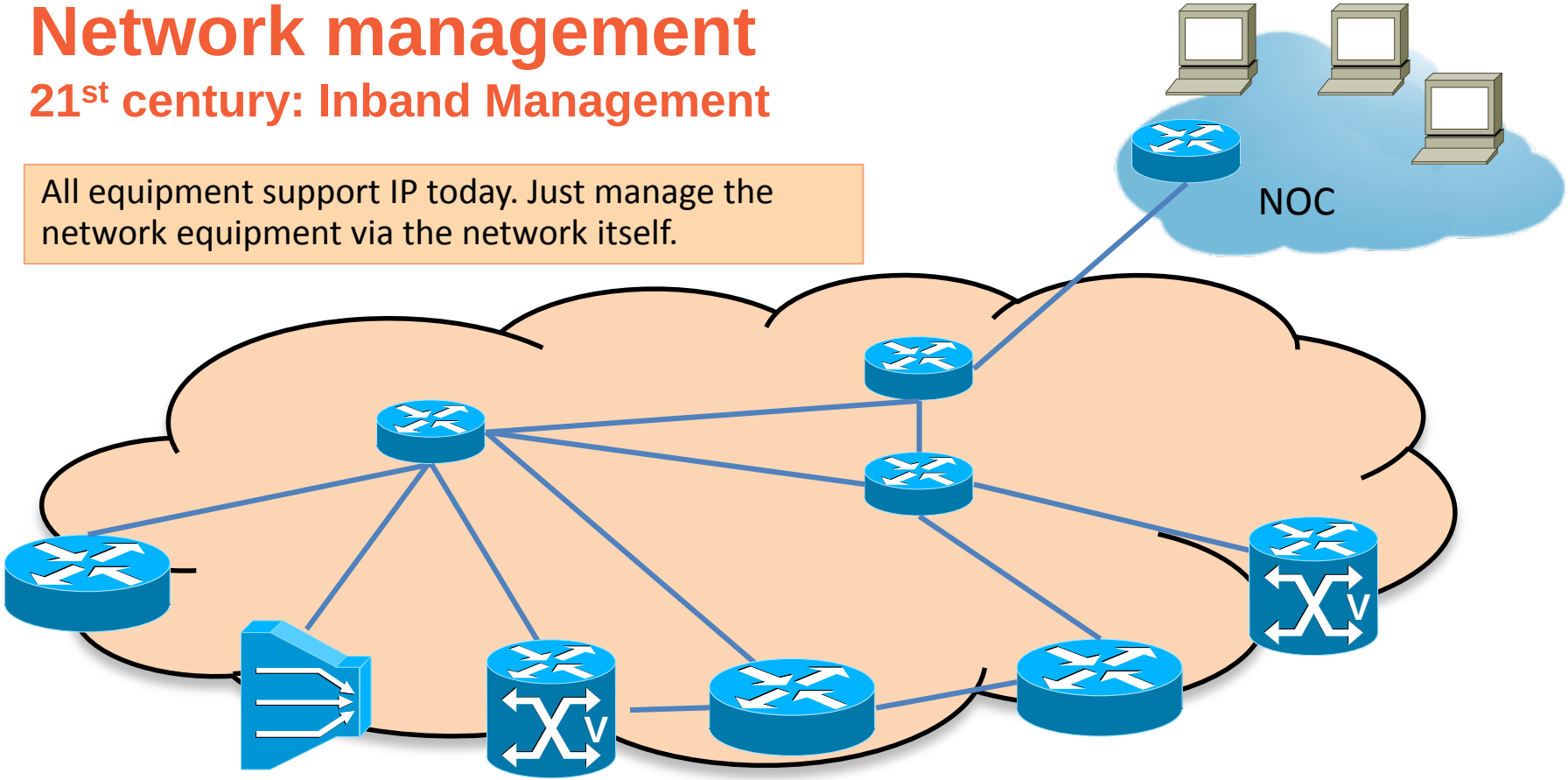
Big Service Providers only



Network management

21st century: Inband Management

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



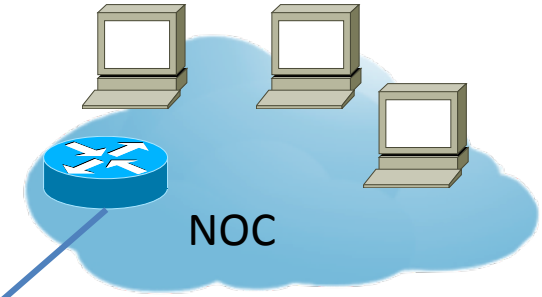
Inband management challenges

- Highly Fragmented
- L1/L2 technologies with in-band OAM HW support:
  - Optical Supervisory Channel (OSC) in DWDM (< 256kbps)
  - General Communication Channel (GCC) in OTN (< 256 kbps)
- Rest of networks use operator created ad-hoc methods
  - VLAN, VRF, IP-address ranges, ACLs, OAM-QOS,....
  - **fragile** and/or insecure and/or complex
- Prediction: variety of multi-vendor / 3rd party SDN applications will make fragility risk even larger.

Network management

21st century: Inband Management

Difficult concept… when manual/NMS/multi-vendor-controller-apps give you 10,000 wrong config options. And complex dependencies exist between features.



Bad script removes username/pwd config

Bad script removes username/pwd config

ACL misconfig, Whole network behind unreachable

Complexity: Extranet, to access VPN equipment

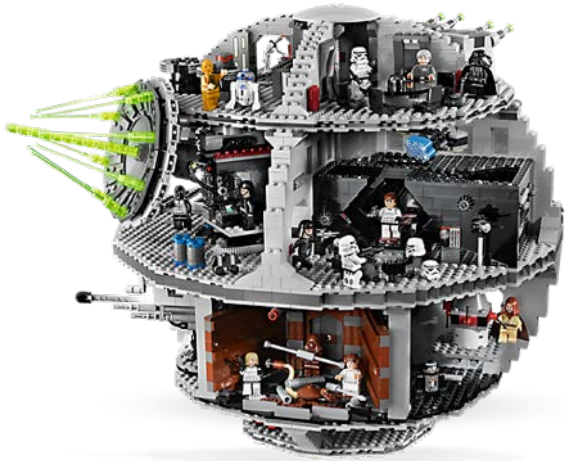
ACLs for management incomplete. Security hole

Change process on intermediate routers become nerve wracking

Routing misconfig blackholes management traffic

How can we make..

DEPLOYMENT and



© Lego

PROVISIONING AND MANAGEMENT more

© Lego

RELIABLE

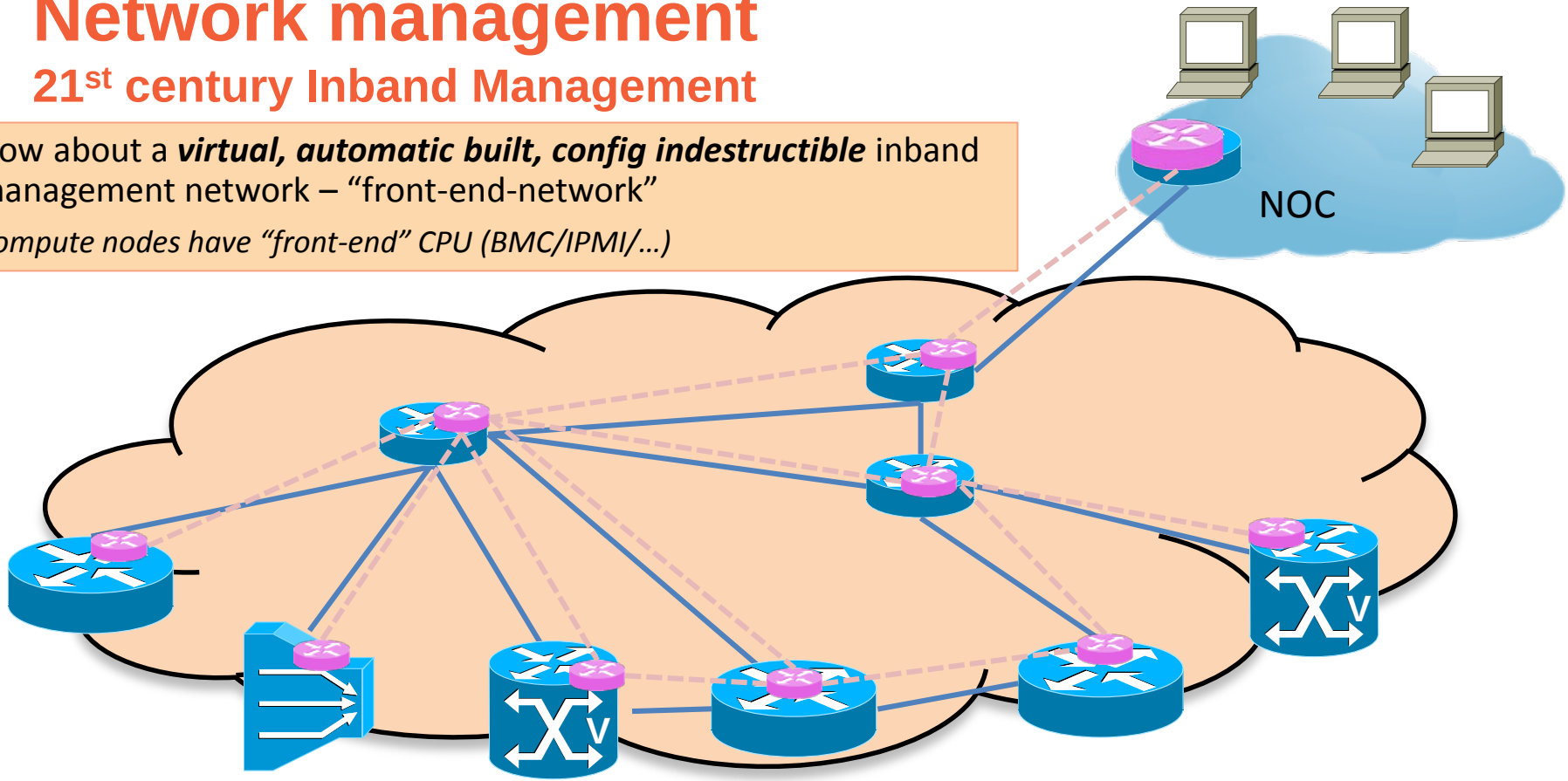
© Philips

Network management

21st century Inband Management

How about a ***virtual, automatic built, config indestructible*** inband management network – “front-end-network”

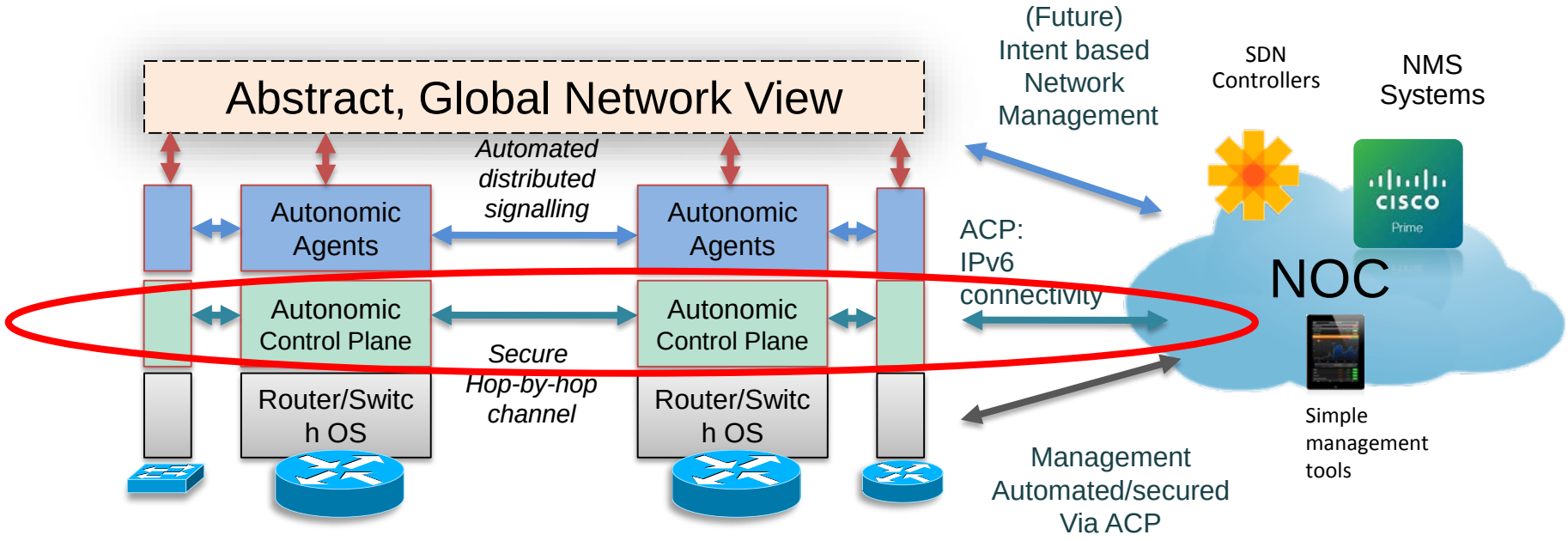
Compute nodes have “front-end” CPU (BMC/IPMI/…)



Network wide, abstract management

Secure by default

Simpler NOC



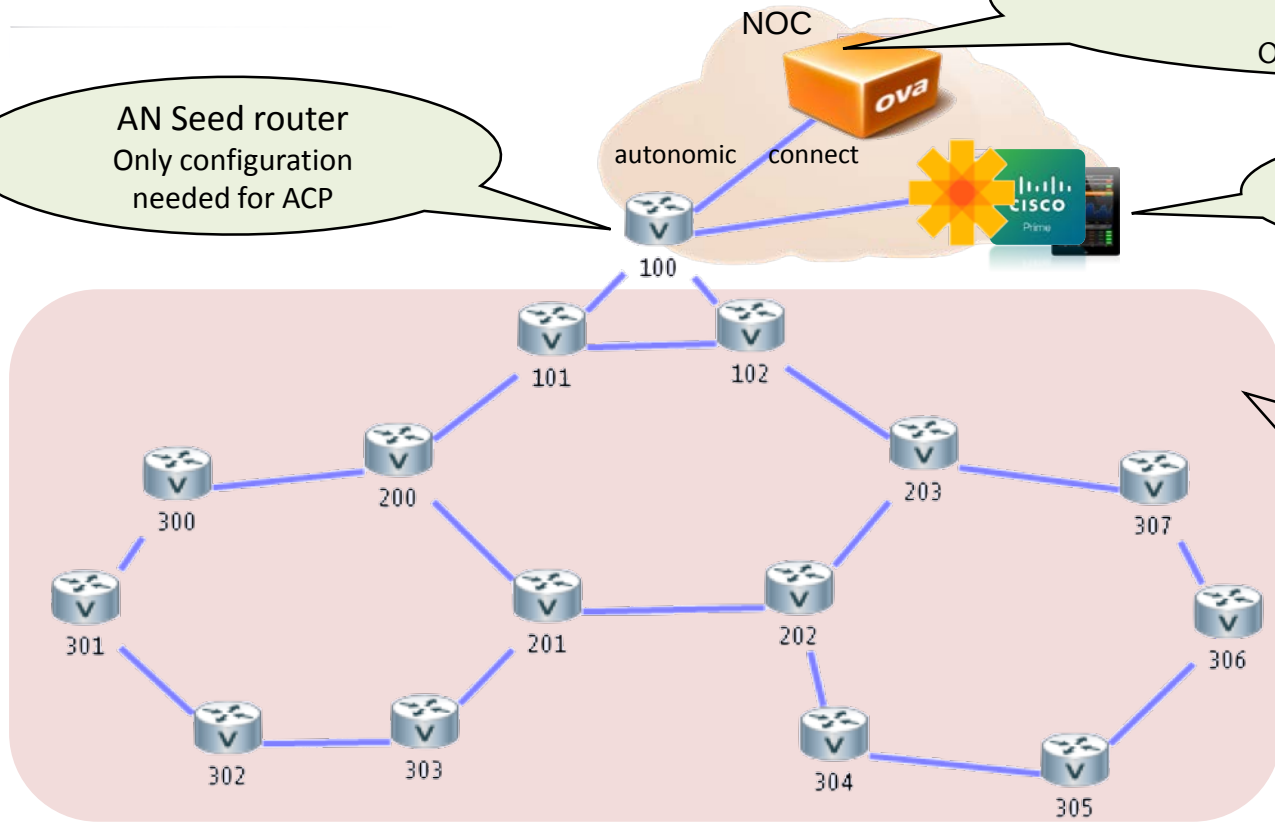
Reliable, indestructible connectivity

Virtual Lab network

Radius Server
authenticate acces into network devices via SSH
Opional: tftp, syslog

AN Seed router
Only configuration needed for ACP

BYOS
Bring Your Own Servers (controller, NMS,…)



Your Network
ALL DEVICES WITHOUT CONFIG
Unbox
Wire-up
ANI does the rest

Autonomic “seed” router

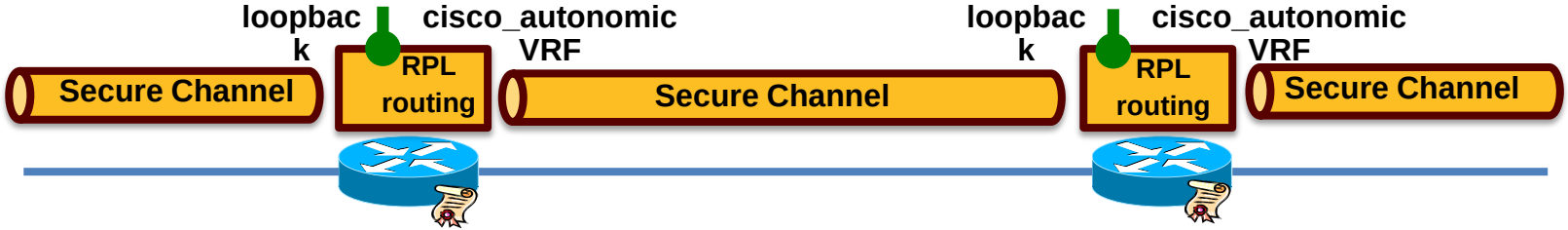
Complete config needed for ACP

```
autonomic registrar
  CA local                                ! Also run Certificate Authority
  whitelist flash:whitelist.txt           ! List devices permitted into ACP
  domain-id example.com                   ! Name of your autonomic domain
                                          ! Used to create IPv6 addresses for ACP
  no shut

autonomic                                 ! Make seed router itself autonomic

interface ethernet 0/0
  description connect to NOC services
  ipv6 address 2001::01/64
  autonomic connect
```

Autonomic Control Plane (ACP)

- Autonomic Control plane is “virtual DCN”
  - No operator/SDN changeable configuration, all created/maintained autonomic
  - Traffic securely passed hop-by-hop via secure virtual channel for OAM traffic
    - Virtual channels do not conflict with any user-configured network paths.
  - Follows hop-by-hop physical network topology
  - Automatic address assignment, no address management required

Autonomic Control Plane



- Example (Cisco IOS) implementation choices:
  - Virtual router is protected (non-configurable) VRF
- Proposed standards method
  - RPL routing – Proven in large scale, unmanaged IoT networks
  - IPv6 to enable automated addressing
  - Automatic best choosen encryption: IPsec, MacSec,…

Hop-by-hop security model – why ?

- Important insecure legacy protocols. Mostly OAM related
  - DNS, SNMP, TFTP, NTP, …

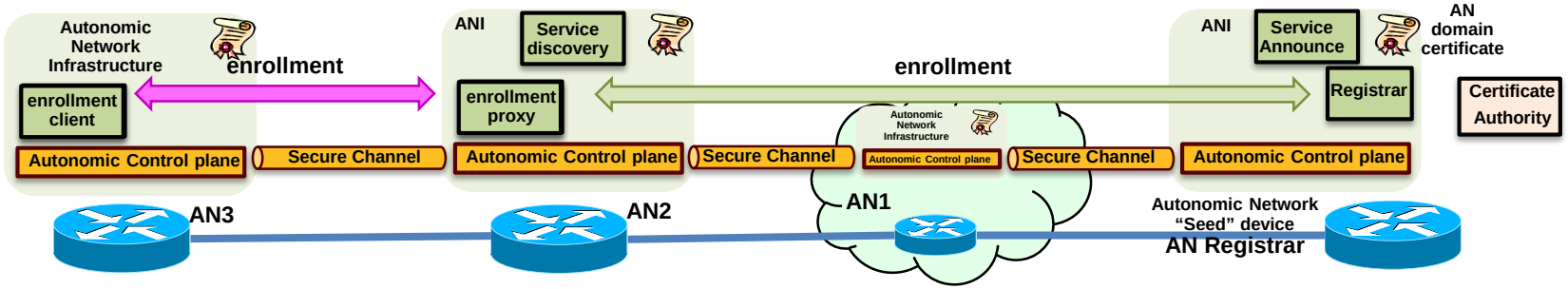
- END-TO-END SECURITY DOES NOT PROTECT INFRASTRUCTURE
  - Per-Pass, DoS / floow/traffic attacks against infra

  - ~~"gold~~" lead standard: "clamshell security"
    - security filters only on network boundary
    - Assume all "internal" links are physically secure
  - But network links often are not secured.
  - Clamshell security is also fragile – misconfiguration/security-holes

Zero-touch, secure device bootstrap

- ACP setup is automatic
  - But depends on trust anchor (domain cert)
- How do devices get that ? *Glad you asked*
- Traditional Device bootstrap to remote locations expensive
  - Pre-staging
  - predict all deployment site details
  - Rollback upon error
- With AN/ACP these steps are eliminated.
  - Every AN device help to enroll certificate in next connected device via ACP – automatic.

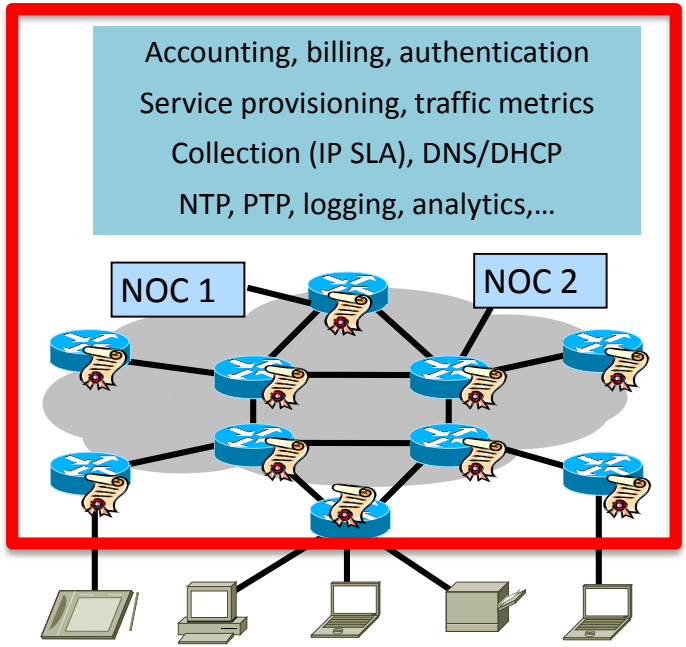
Secure Device Enrollment



- Headend has seed-router (Registrar) and CA (Certificate authority)
  - Traditionally configured
- Every AN enrolled device provides L2-proxy to to new AN devices
  - Greenfield devices try to become autonomic (always)
  - Brownfield devices may need simple config "try to become autonomic"
- Proxy device uses ACP to communicate with Registrar
  - Learns IPv6 ACP address of registrars via AN Service discovery (mDNS) inside ACP
- No configuration needed at all – no DNS/DHCP/..
  - As often required by other zero-touch systems

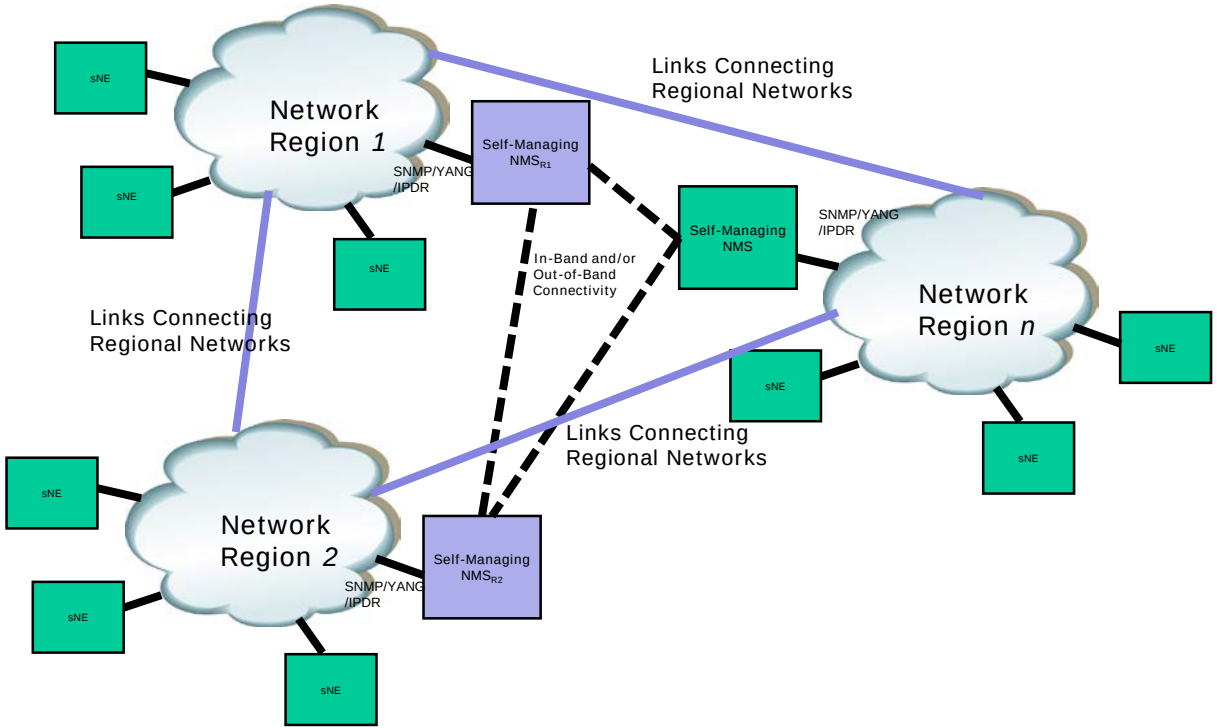
Autonomic security for network service

- Network services security is a maze
  - Every feature/service has its own security (concepts), secrets (certs/shared)
  - Key management also per-feature, often cumbersome/badly managed.
    - Shared secrets known to ex-operators long gone to the competition
  - Even otherwise simple to deploy features become complex when security is added
    - Because security was often an afterthought in services/SW development
- Historic / manual design approaches
- With AN domain security given services security can easily be automated
  - IGP, BGP, MACsec, Multicast, NOC<->Network services



Autonomic / distributed fault management

- Fault isolation/processing mayor OPEX factor
- Leverage Autonomic Agents approach and ACP for communication to build better automated fault diagnostics and reporting
  - Minimize need for on-site technician (only when physical repairs needed)
  - Create common communications system across different layers of network services



Source: Mehmet Toy, Comcast - https://www.ietf.org/proceedings/92/slides/slides-92-anima-5.pdf

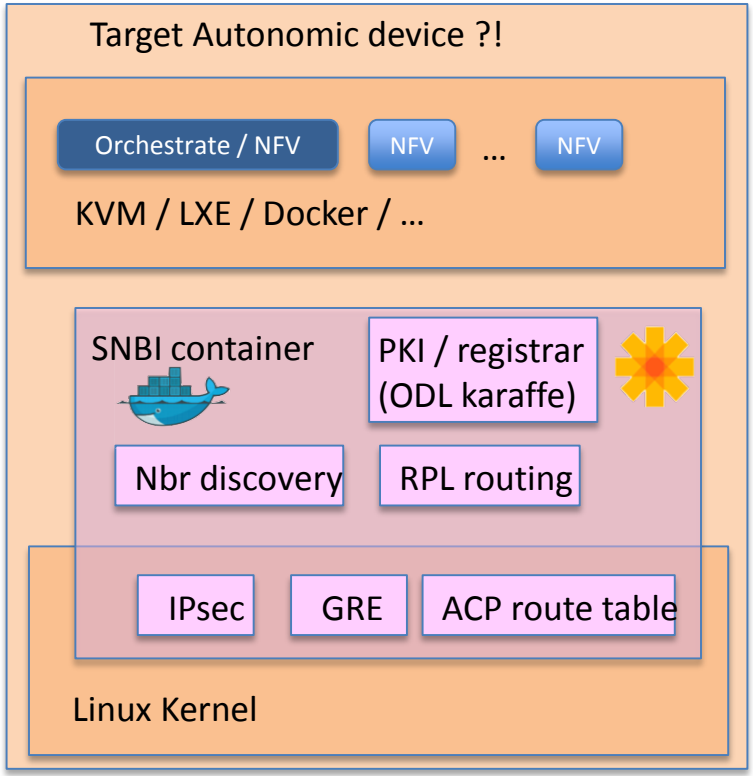
Standardization & Adjacencies

- **Autonomic Networking Integrated Model and Approach (anima)**
  - IETF working group … for “well managed networks” (aka: with operator/SDN OAM)
  - Reliable OAM connectivity:
    - **draft-ietf-anima-stable-connectivity**

    Using Autonomic Control Plane for Stable Connectivity of Network OAM
- **Homenet**
  - **Unmanaged network (“The best OAM is no OAM”)**
  - “Mrs. Jones does not do SDN” ?!
  - Much less complexity: no (separate) OAM plane needed? / desired?!.
- **Vendors**
  - **SMB vendor options: “Web based network management”**
  - Whole provisioning backend must ensure any config does not “shoot itself in the foot”
  - More limited topologies / feature sets.

Open Source Autonomic Network prototype

- Linux based
- Project under ODL
- SNBI –
  Secure Network Bootstrap Infrastructure
- Evolving / incomplete
- More detail slides:
- https://www.ietf.org/proceedings/95/slides/slides-95-anima-5.pdf



Candidate Design/Standards topics

- **Platform implementation architecture**
  - How to separate ACP from rest of system – with least cost (minimum addtl. HW)
  - Existing Cisco implementation inside monolithic IOS software.
    - Can not use ACP to manage router SW lifecycle and no separated failure domains.
- **Secure channel implementation architecture**
    - How to make it indestructible even if “shut” on router itself ?
    - Standard for OAM channel on “Ethernet”
    - Virtual PCI-E device abstraction ?
    - Accelerated encryption standard ?
      - MacSec ?
- **“Structured” ACP (OAM networks)**
  - Multiple operator access – Enterprise / SP providing services – “overlapping”
  - Virtualized routers – Virtualized ACP vs. underlay ACP ?

SCTE ISBE CABLE-TEC EXPO '16

SEPTEMBER 26-29 PHILADELPHIA

Toerless Eckert

Eckert@cisco.com

408-902-2043

CISCO

SCTE Society of Cable Telecommunications Engineers

ISBE International Society of Broadband Experts

#CableTecExpo

Essential Knowledge for Cable Professionals™