Stable Connectivity

IETF 91 11/2014 Honolulu

draft-eckert-anima-stable-connectivity-00

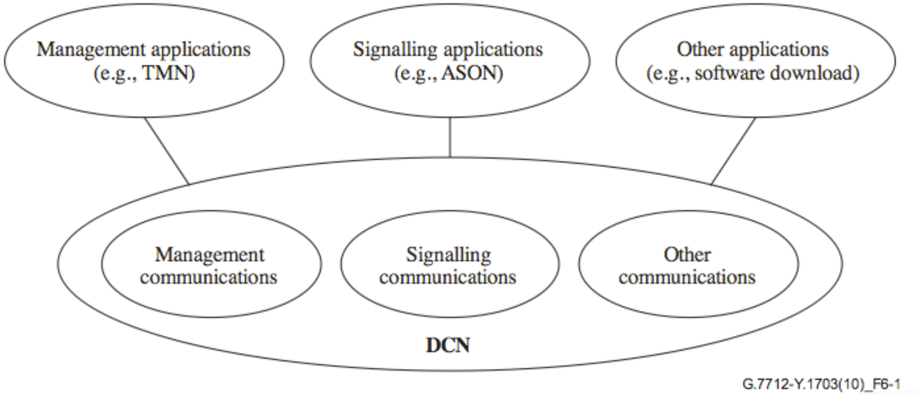
T.Eckert

M. Behringer

Overview

- AN components: ACP… enables…
  - Stable, secure connectivity for (un)configured device
  - Immediately after enrolling devices in into AN Domain
- Solutions: How do we use it ?

- Enrollment proxy (not in scope)
- Inband "DCN" for NOC/OAM
  - Connectivity NOC / network device
  - Assuming ACP has better connectivity properties than "data-plane

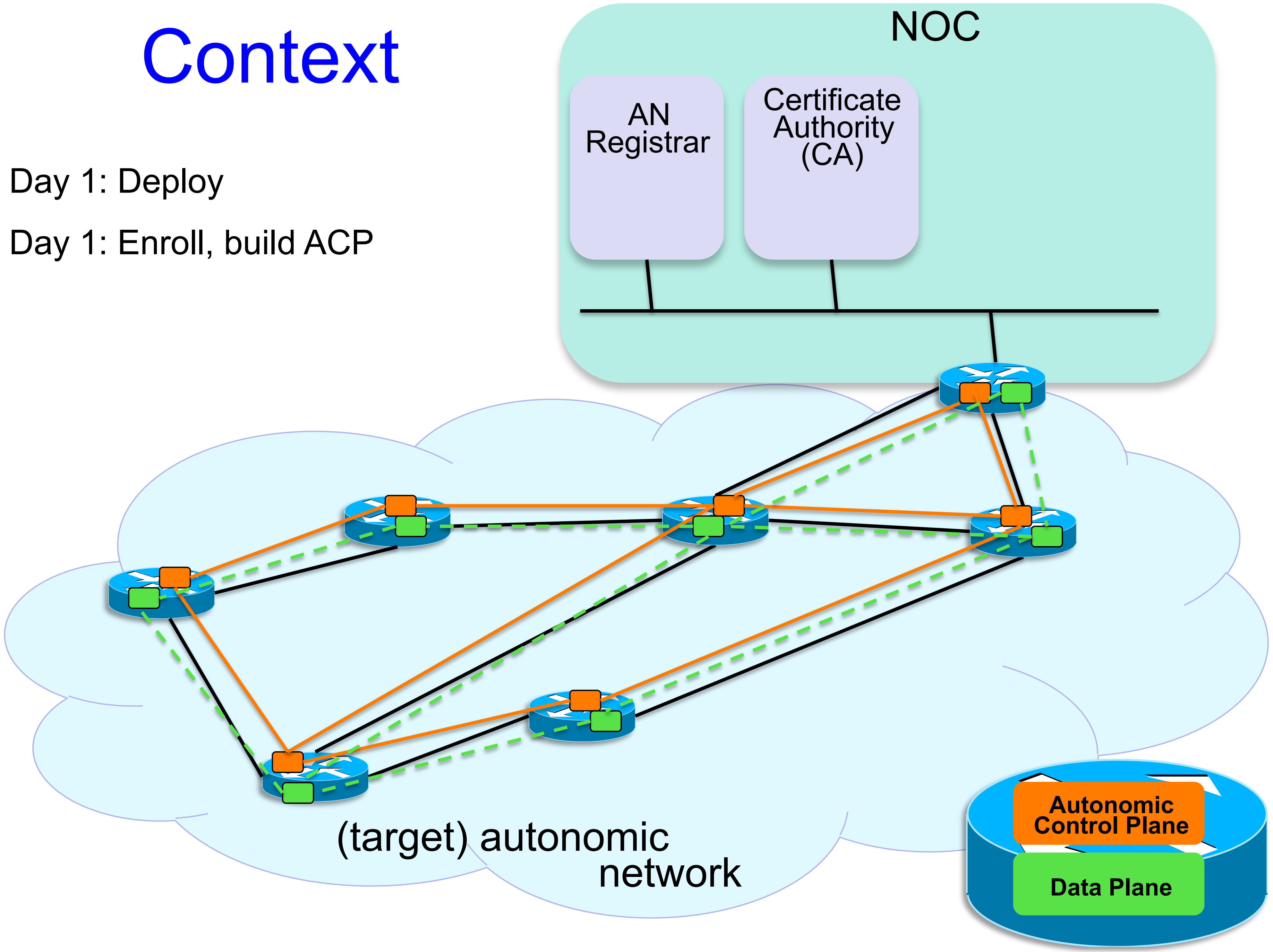

Management applications (e.g., TMN)
Signalling applications (e.g., ASON)
Other applications (e.g., software download)
Management communications
Signalling communications
Other communications
DCN
G.7712-Y.1703(10)_F6-1

- Connectivity between distributed "AN" "agents"
  - TBD (not in rev -00)

Context

Day 1: Deploy

Day 1: Enroll, build ACP

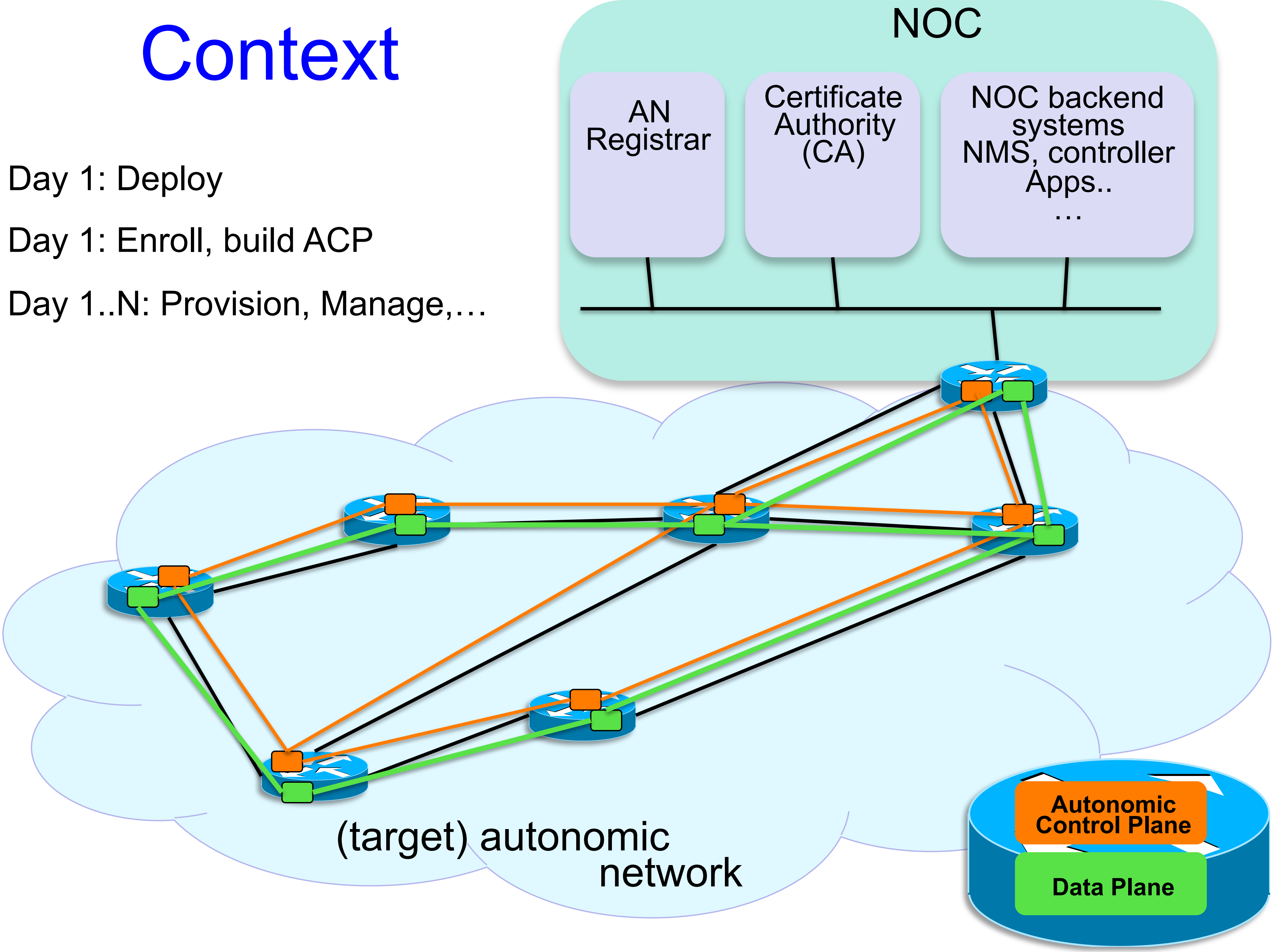


Context

Day 1: Deploy

Day 1: Enroll, build ACP

Day 1..N: Provision, Manage,…


NOC
AN Registrar
Certificate Authority (CA)
NOC backend systems NMS, controller Apps.. …
(target) autonomic network
Autonomic Control Plane
Data Plane

Scope

of -00 document

Communication between

- NOC (backend, CA, Registrar)
- OAM/MGMT plane of autonomic devices

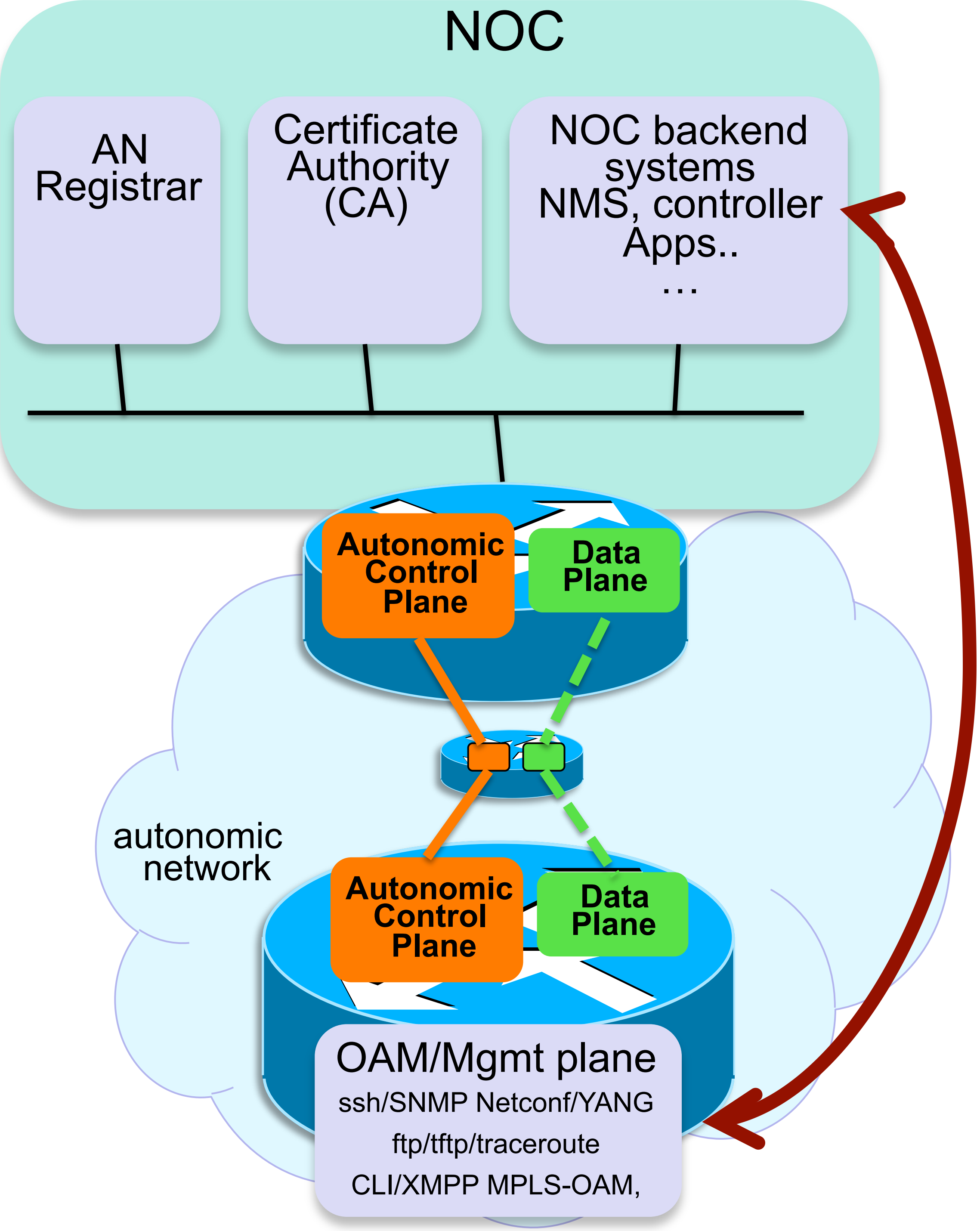
ACP exists/connects as soon as AN device is physcially rechable and enrolled

But potentially slow (hop-by-hope encryption)

Data plane exists only after provisioning

Likely faster than ACP, likely more often not-working (mistakes, failure, during policy change provisioning)

Special case of dual-path end-to-end system



OAM/Mgmt plane
ssh/SNMP Netconf/YANG
ftp/tftp/traceroute
CLI/XMPP MPLS-OAM,

Solution (1)

Network devices OAM supports multi-context (eg: VRF) connectivity.

But not necessarily all desired path policies (not an issue in first phases).

Registrar:

Needs ACP connectivity for enrollment of AN devices.

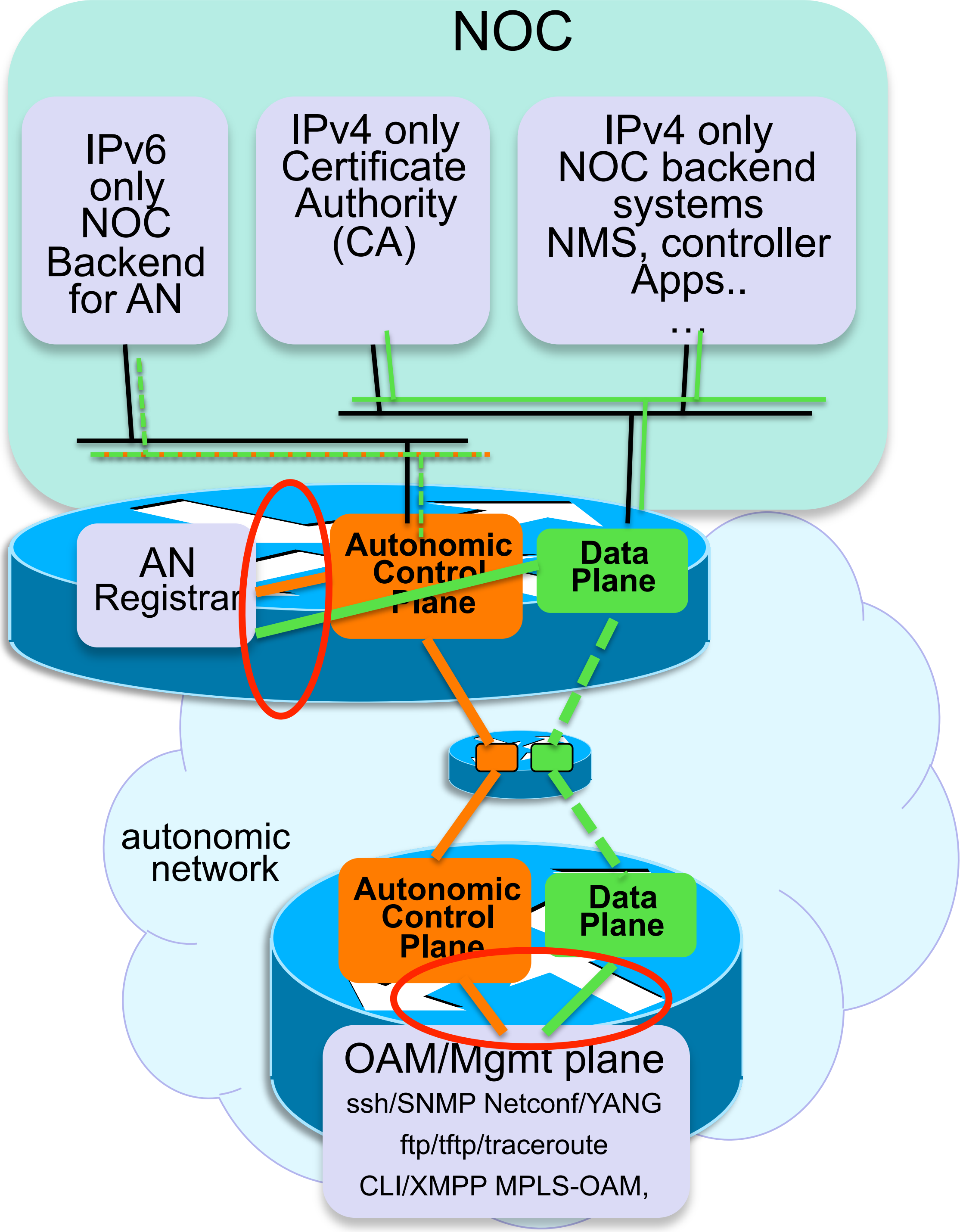
Needs CA connectivity (likely data-plane).

Initially most easily put into AN network device.

NOC Backend/CA

Assume IPv4 only NOC today.

Pass ACP unencrypted/native to the New IPv6 only NOC devices/VMs/ apps.



Solution (2)

Once NOC can be Dual-Stack:

IPv6 could simply provide access to ONLY the ACP, and IPv4 ONLY to the data-plane

Requires NOC-edge AN router to put an interface into two different routing contexts for IPv4/IPv6

Use DNS names to help select right address depending on purpose of NOC/OAM action:

Device-acp:

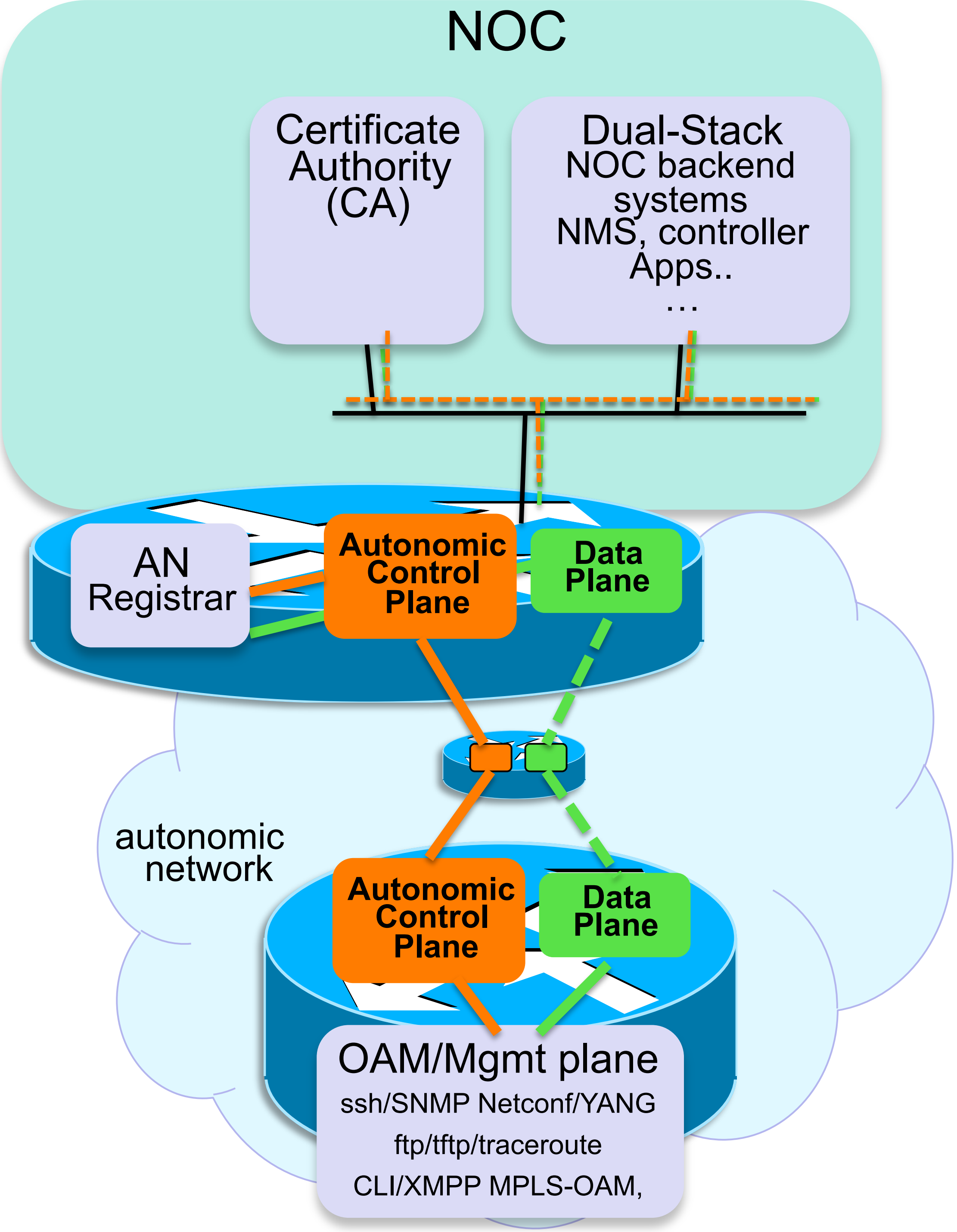
IPv6 only == only ACP

Device-ipv4:

IPv4 only == test data plane reachability

IPv4 + IPv6 = ACP or data plane.

Not a sufficient solution to work with a network that wants an IPv6 data plane



Solution (3)

To leverage ACP in a v6-data-plane or dual-stack data plane network:

Edge IPv6 routing function to select path for IPv6 packet: via data-plane or ACP.

Can be separate router (workaround) or edge-function in AN edge device.

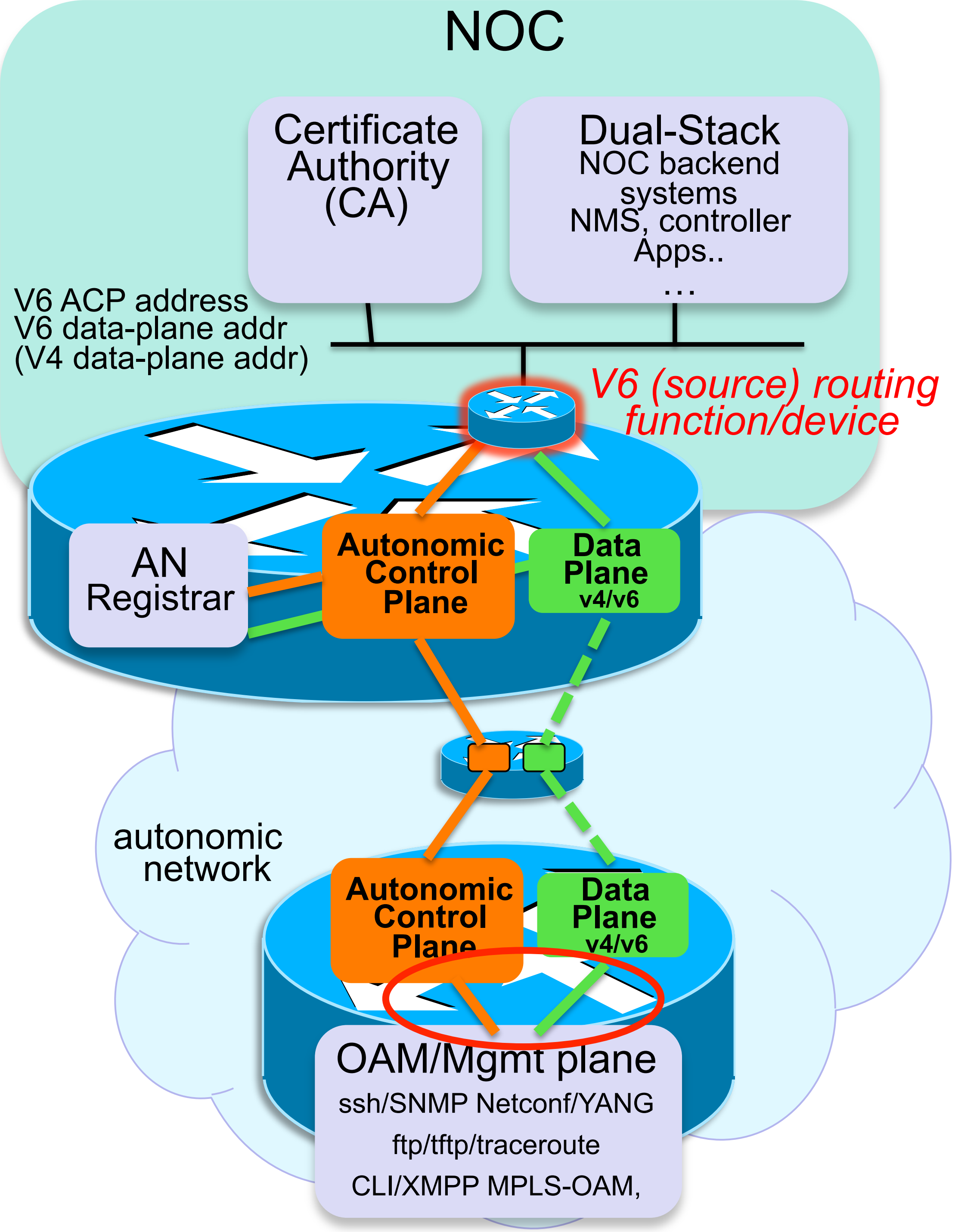
Separate ACP and Data-Plane IPv6 addresses on NOC devices:

No need to inject non-ACP wanted addresses into ACP IPv6 routing.

Leverage “normal” IPv6 host stack policies. Also on AN devices OAM stack:

Select source-IPv6 addr of initiator based on destination address

Select routing context based on source IPv6 addres prefix.



Solution (4)

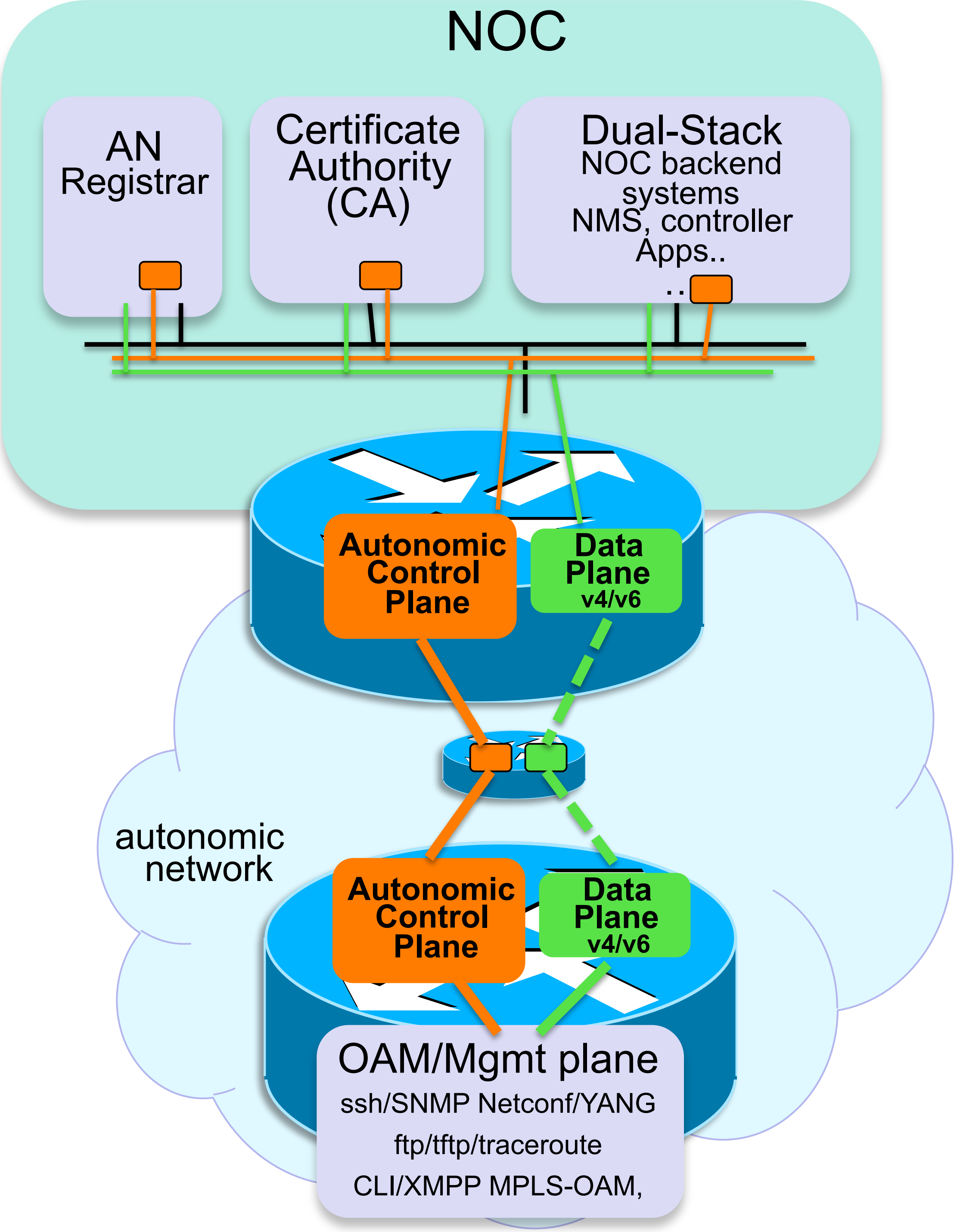
Implement ACP on NOC devices/ Hypervisors

- AN-enrollment, setup of encrypted ACP channel.

Benefits:

- Security all the way into the NOC app
- Leverage AN Certificate on NOC application to also secure OAM messages going across data-plane (TLS/dTLS).
- Eliminates need of “routing function” workaround at edge of AN network. Allows full non-network-device registrar.
- Avoids need for in-network “routing function to route into ACP/data-plane. Now job of the NOC endpoint.

Same policy options as in step 3 with dual IPv6 addresses on NOC device



Solution - more

Bad: Connect IPv4 only NOC systems

- Requires NAT to ACP/IPv6 – should only consider as temporary workaround.

Good: Leverage MP-TCP for OAM connections

- Example:
  - Assume DNS is set up to only have ACP address of AN devices
  - NOC device connects to AN network device via ACP address of device == uses ACP
  - When only ACP is up and running, it will stay on ACP
  - If data-plane running, MP-TCP can negotiate the data-plane addresses, and MP-TCP starts to (also) use data-plane (higher performance.
- Would work with solution step 3 or 4.
- *Need to check what is necessary to set up MP-TCP policies to eg: prefer data-plane over ACP when available.*

Hybrid step 3 / 4:

- NOC device enrolls into AN gets AN certificate, but does not build ACP natively.
- Permits to leverage AN Certificate for TLS/dTLS communication across data-plane.

Thank You