



Autonomic Control Plane

A “Virtual Out Of Band Channel”

Alvaro Retana (aretana@cisco.com)

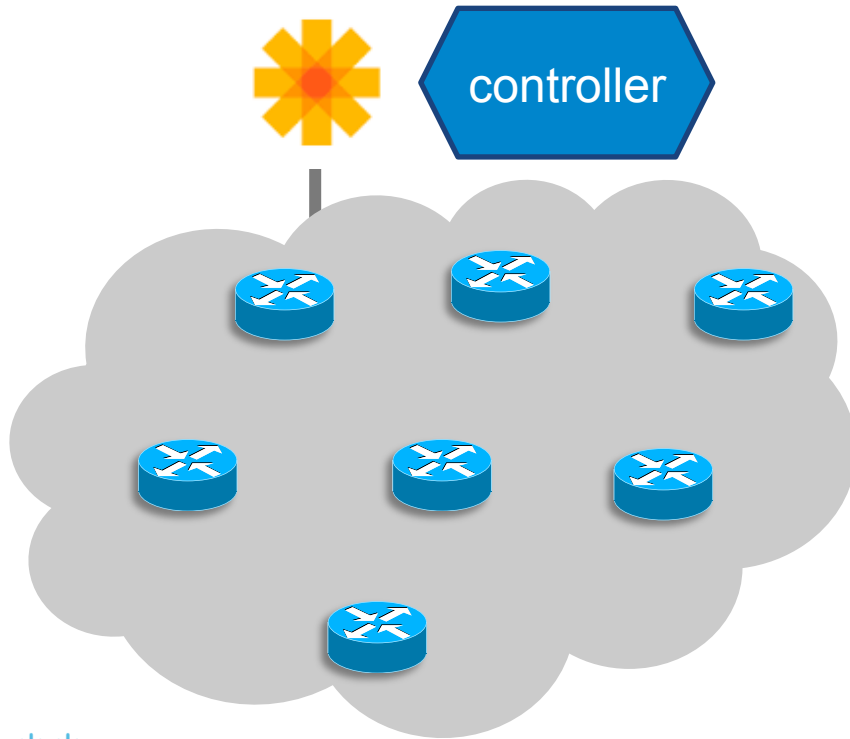
Distinguished Engineer, Cisco Services

We all know:

SDN Will Save The World

Yes, but...

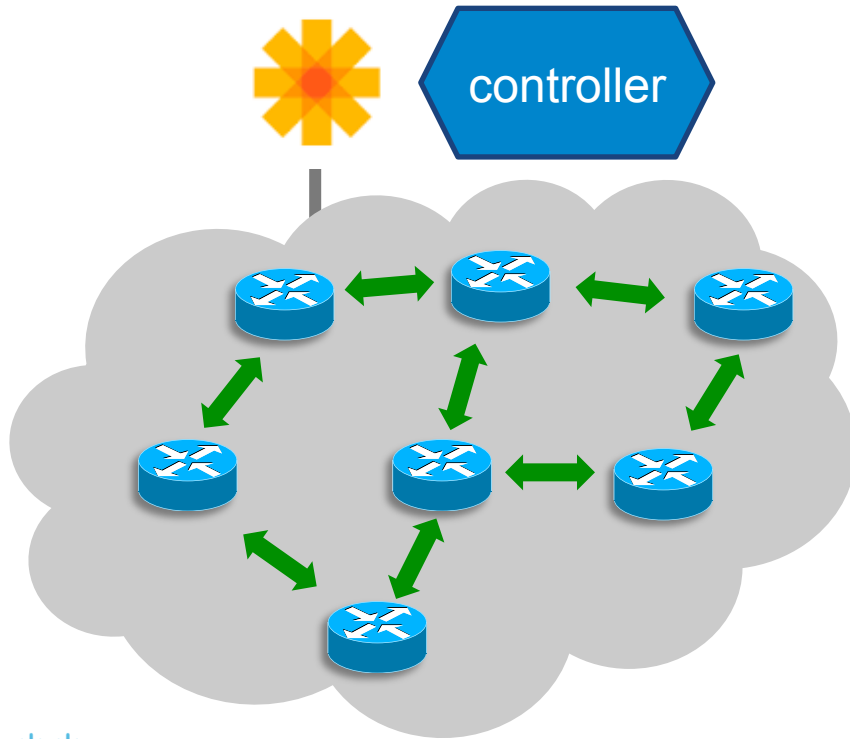
SDN – Unanswered Questions...



How does a Controller:

- Discover network elements?
- Enrol them securely?
(without pre-staging?)
- Reach them consistently?

SDN – Unanswered Questions...

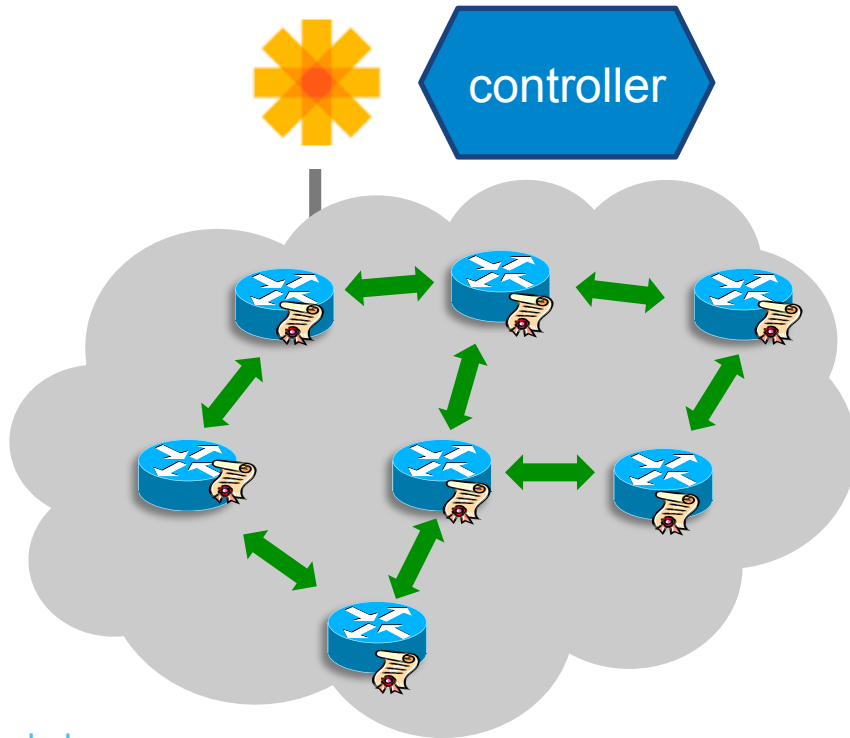


How does a Controller:

- Discover network elements?
 - Autonomic discovery
- Enrol them securely?
(without pre-staging?)

- Reach them consistently?

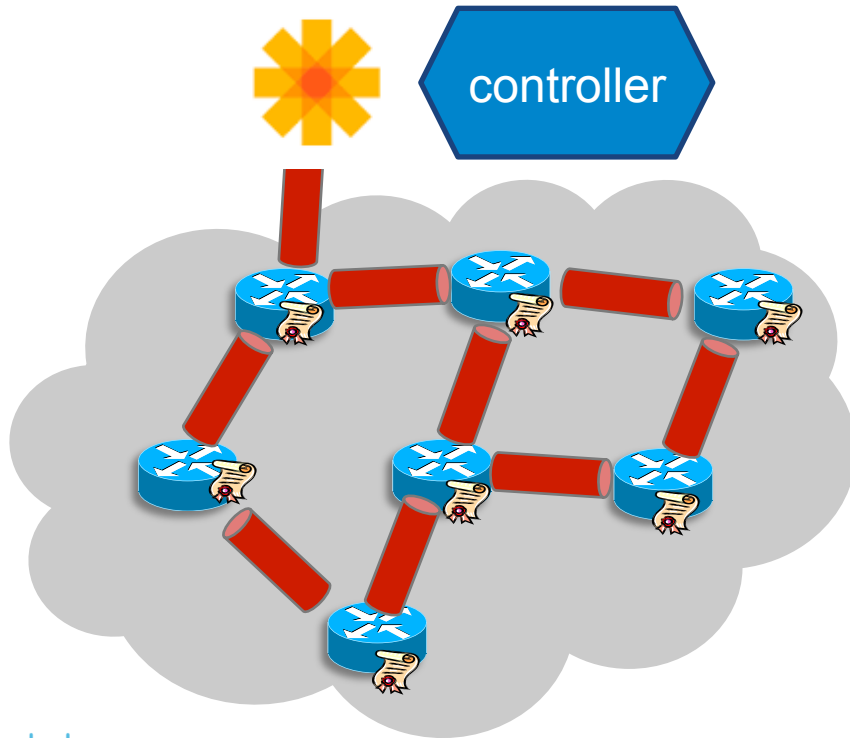
SDN – Unanswered Questions...



How does a Controller:

- Discover network elements?
 - Autonomic discovery
- Enrol them securely?
(without pre-staging?)
 - Secure bootstrap process
 - → Domain certificates
- Reach them consistently?

SDN – Unanswered Questions...

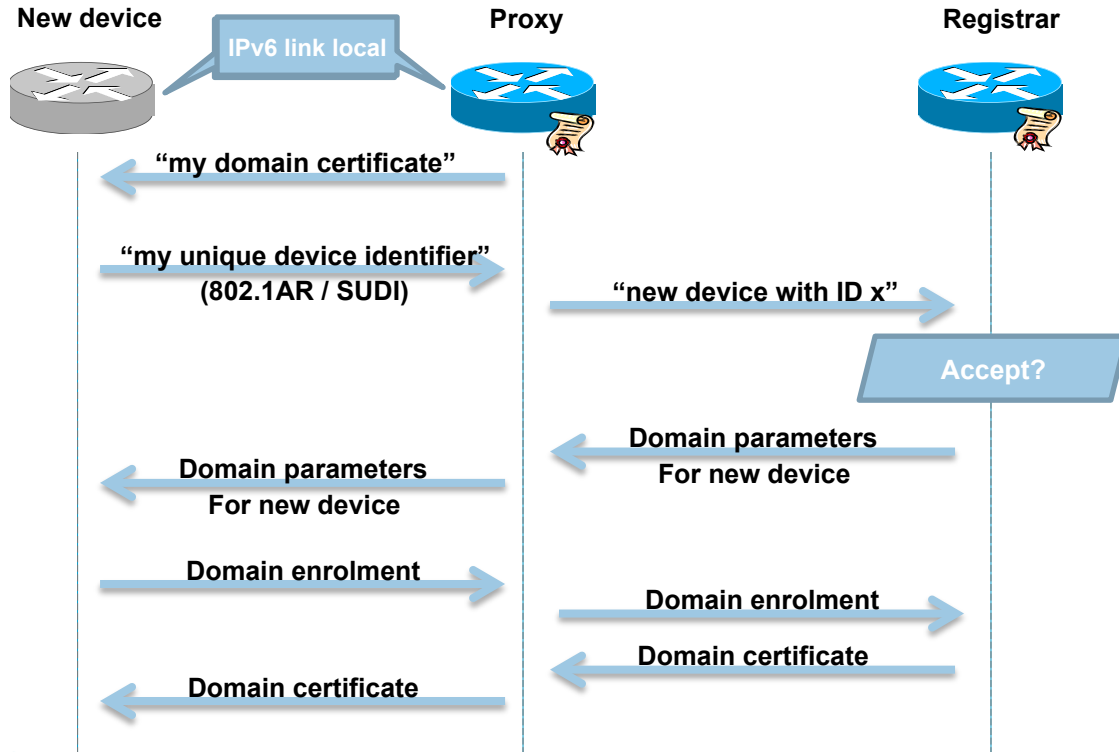


How does a Controller:

- Discover network elements?
 - Autonomic discovery
- Enrol them securely? (without pre-staging?)
 - Secure bootstrap process
 - → Domain certificates
- Reach them consistently?
 - Autonomic Control Plane
 - Independent of the data plane!

Bootstrapping Security

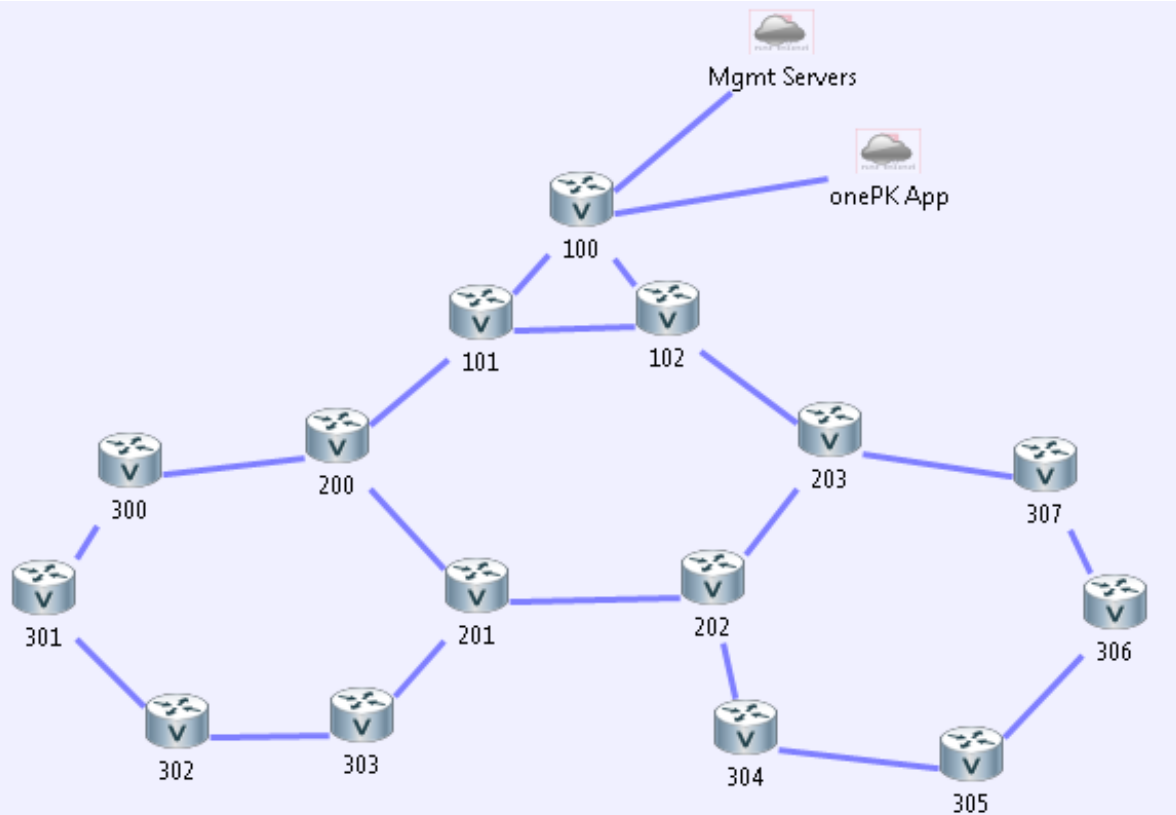
Secure Domain Certificate Enrolment



Fundamental Idea:
Using a secure vendor ID
to bootstrap a domain ID

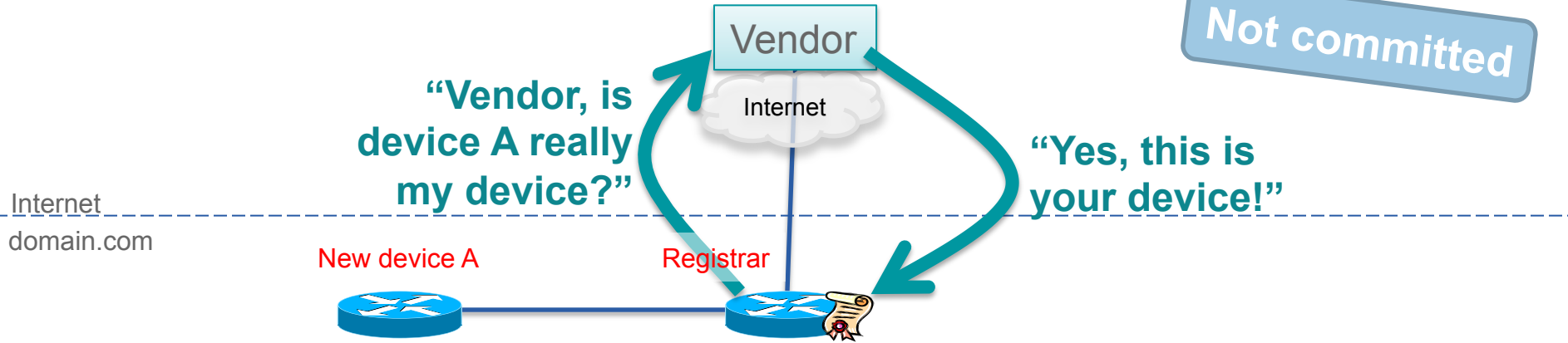
See: <http://tools.ietf.org/html/draft-pritikin-anima-bootstrapping-keyinfrastructures/>

Demo 1: *Secure* Zero-Touch Bootstrap



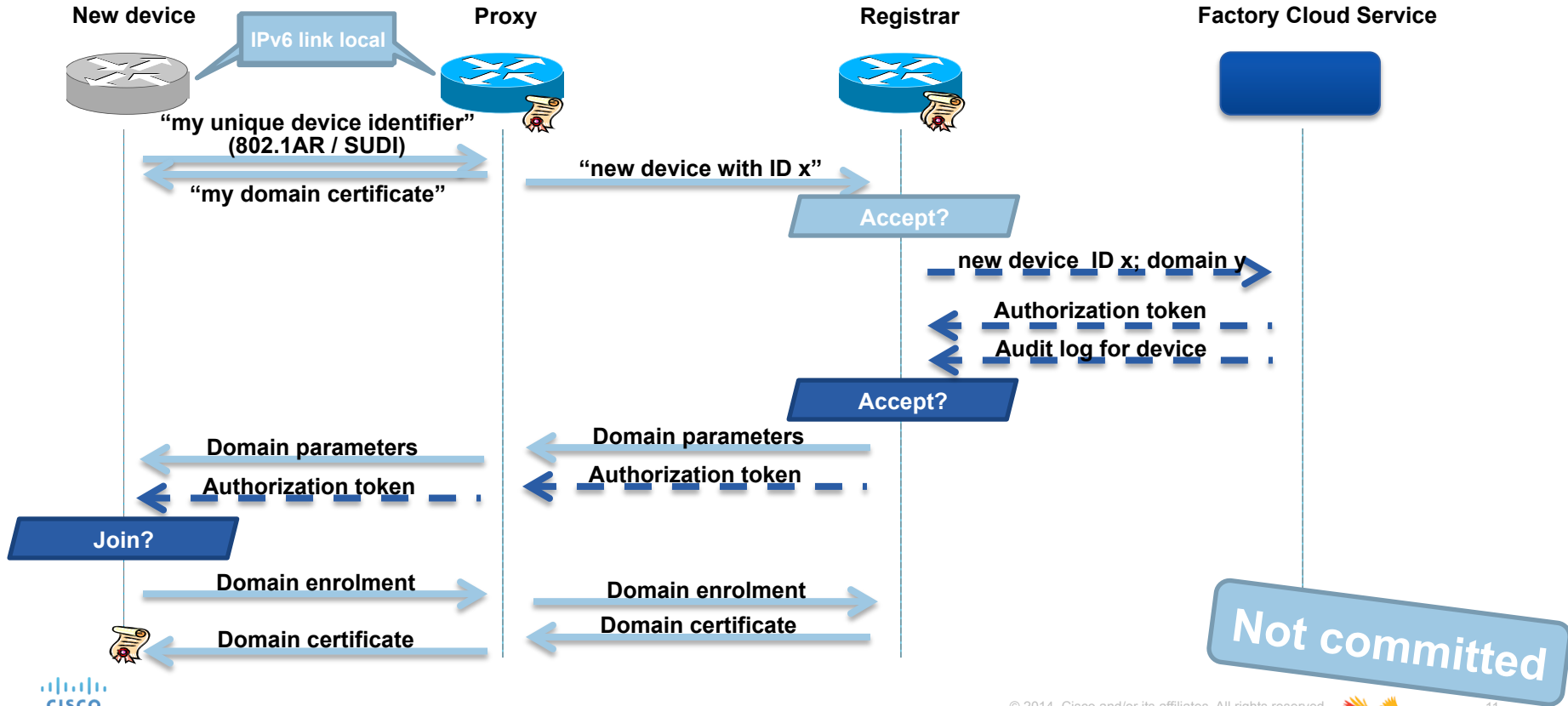
- Minimal config on a central node
- Network bootstraps automatically
- AND: securely!

Would you use Cloud based device identification?



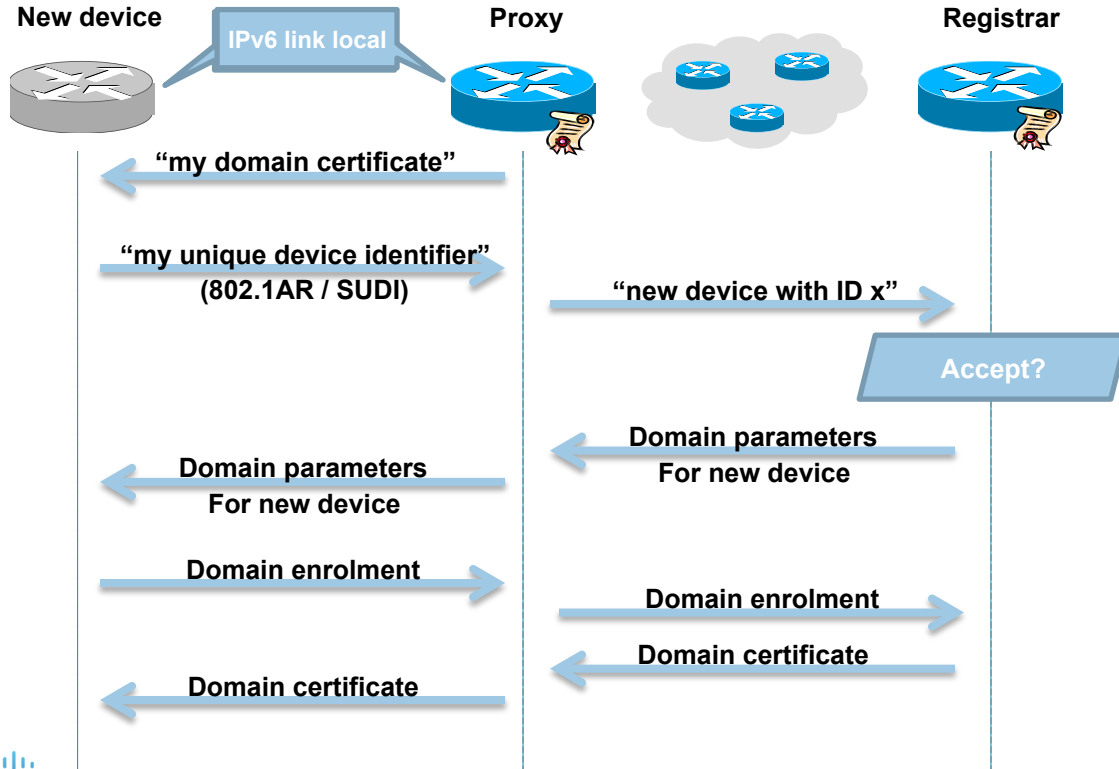
- Vendor validates UDI-customer mapping, based on sales records
- Operator can override on registrar → Control remains with operator

Secure Domain Certificate Enrolment



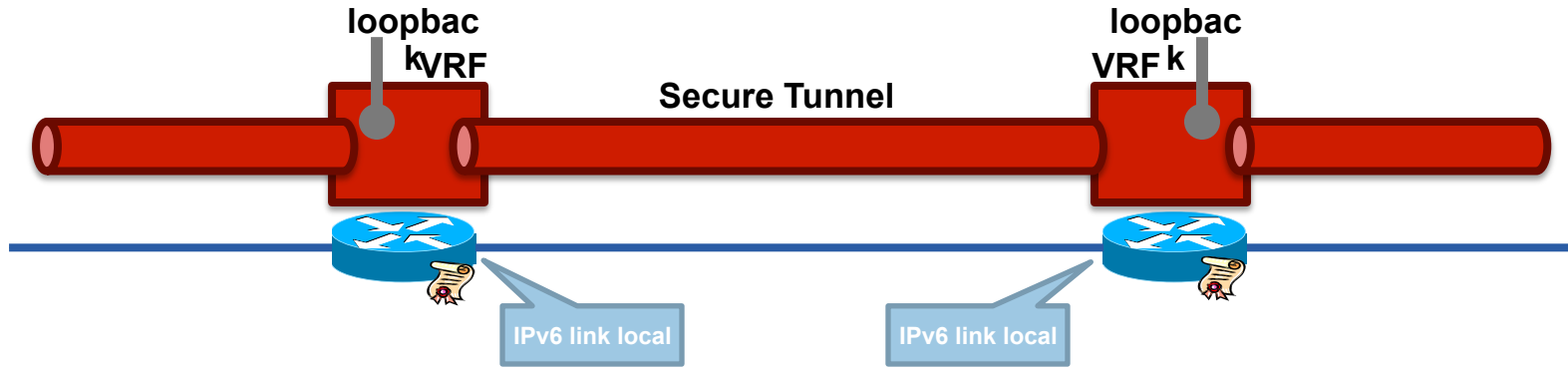
The “Virtual Out Of Band Channel”

Where Is The Catch?



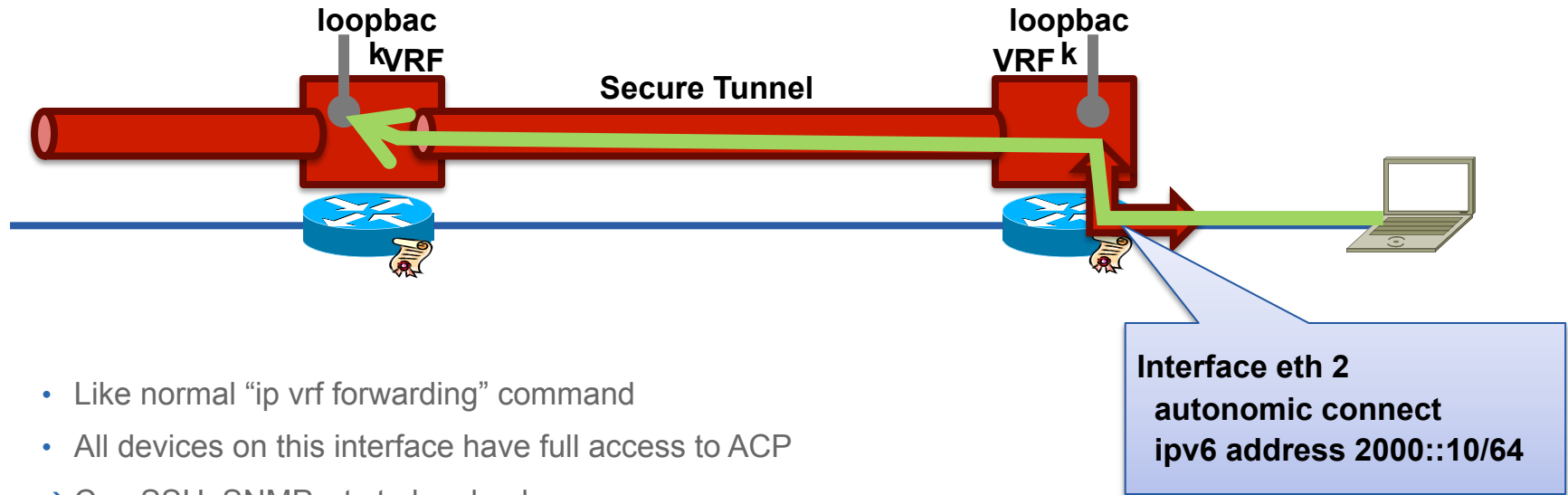
How do nodes communicate without IP addressing?

The Autonomic Control Plane



- Self-forming and self-managing
- Follows network topology
- Not dependent on config or routing table*

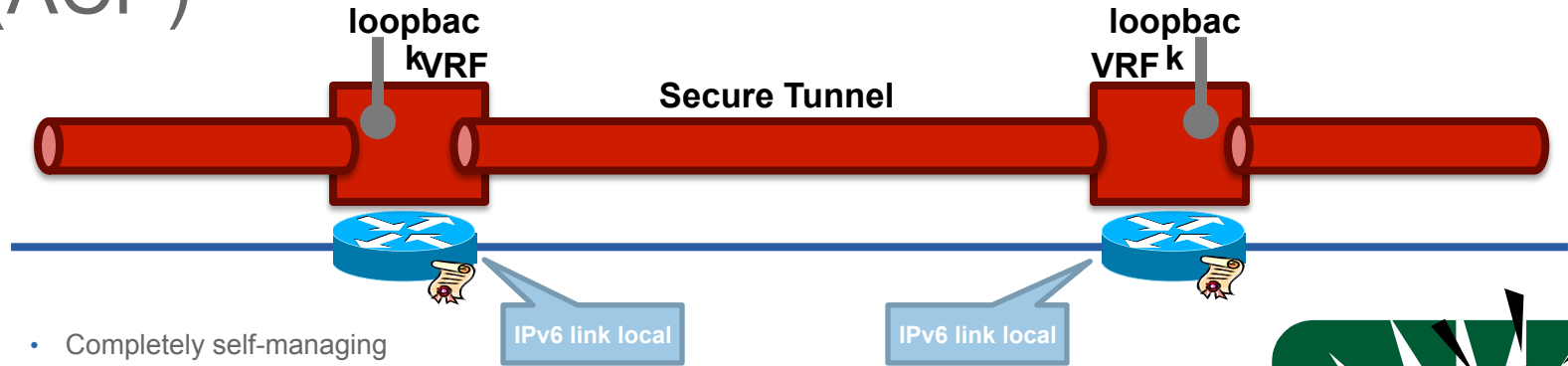
Connecting into the Autonomic Control Plane



- Like normal “ip vrf forwarding” command
- All devices on this interface have full access to ACP
- Can SSH, SNMP, etc to loopbacks

- Long term: Servers will be autonomic devices

Advantages of the Autonomic Control Plane (ACP)

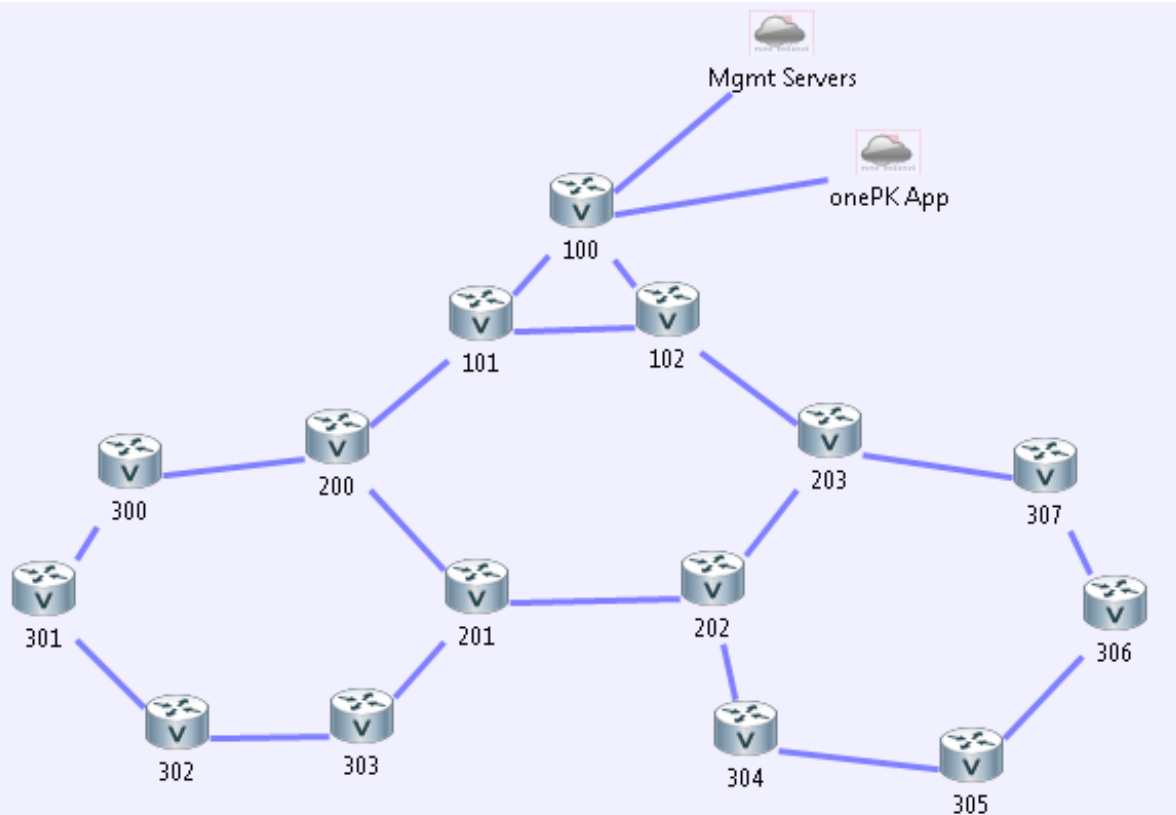


- Completely self-managing
 - No config!
- Secure
 - Separate (VPN) and encrypted (e.g., IPsec)
- Independent of Routing
 - Only depends on link local addresses
- Independent of Configuration
 - Only certificate visible in “sh running”
- Visible
 - Lots of show commands, debugs, etc.

**Use as a
“Virtual
Out-Of-Band
Channel”**



Demo 2: The Virtual out of Band Channel



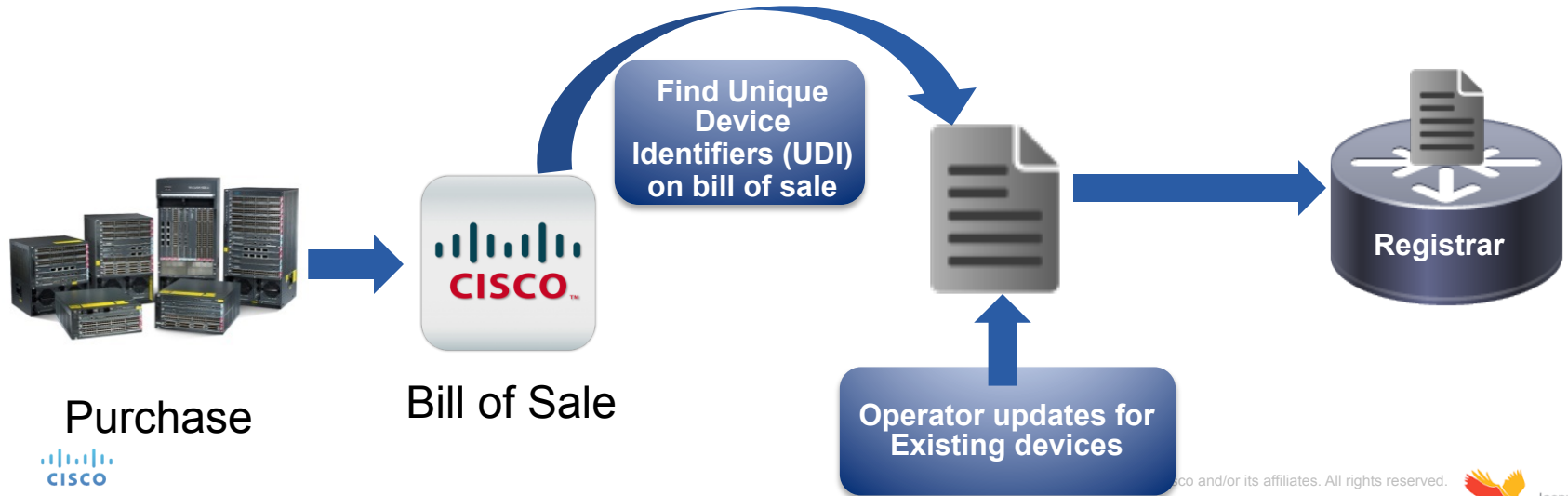
Reachability across the network

- Without addressing
- Without routing

Autonomic Networking Work Flow

Create a Whitelist

- Devices joining the domain must be validated before handing out certificates
- Create a whitelist (text file) of UDIs that are allowed to join
 - Automatically generated by Cisco (from Bill of Sale) for new devices
 - Updated by operator for existing devices
- Load whitelist on the Registrar (manually)



Configure a Registrar

```
Router#configure terminal
```

```
Router(config)#autonomic registrar
```

```
Router(config-registrar)#domain-id cisco.com
```

```
Router(config-registrar)#whitelist disk:whitelist.txt
```

```
Router(config-registrar)#ca url <>
```

```
Router(config-registrar)#no shut
```

Enter Autonomic Registrar Config mode

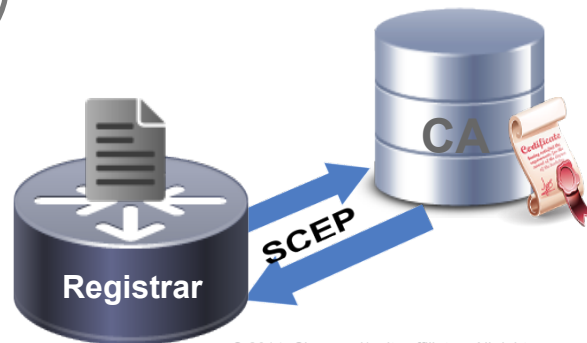
Configure domain-id – any name will do

Specify a local whitelist (Optional)

Specify an external CA's url (Optional)

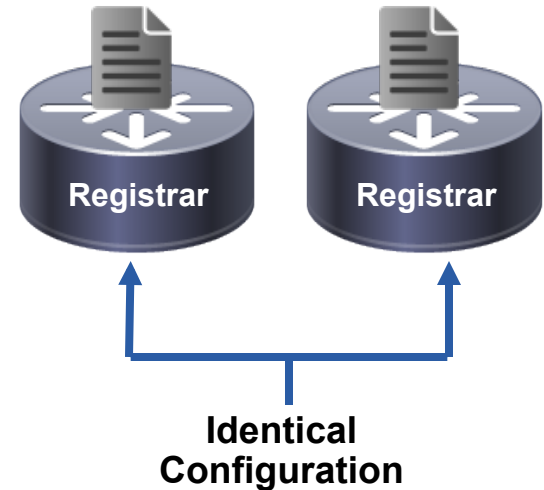
Unshut the Registrar – You're done!

- Registrar also can run an IOS CA locally
- If a whitelist is not used– a deployment window is the recommended alternative



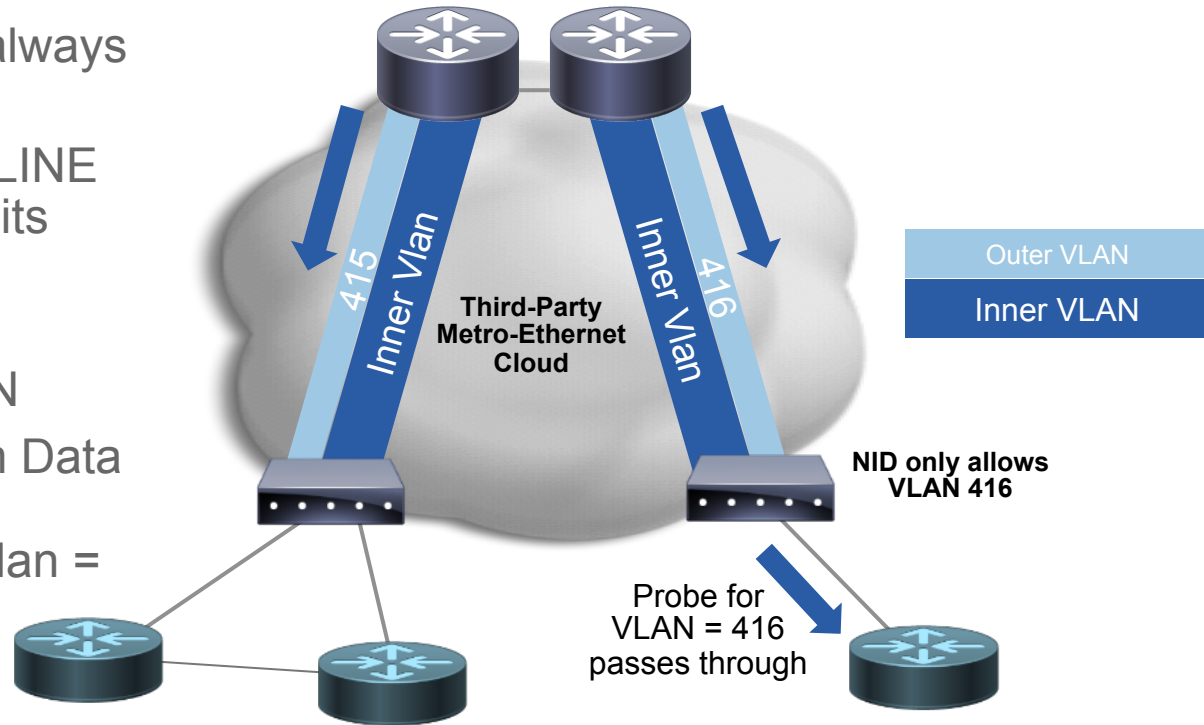
Registrar Redundancy

- A Registrar in an Autonomic domain:
 - validates new devices (whitelist)
 - Hands out domain certificate
- Registrar down → no new devices can join the autonomic domain!
- Good practice to configure multiple registrars
- Registrars can be distributed – no need to be neighbors!



Bring up Remote Sites: Channel Discovery

- Newly installed device is always passive
- Typically, VLAN based E-LINE services - each NID permits one VLAN
- Channel discovery helps discover the allowed VLAN
- ACP is kept separate from Data plane using QinQ service instance with fixed inner vlan = 4094



Restricting VLAN Ranges with Channel Discovery

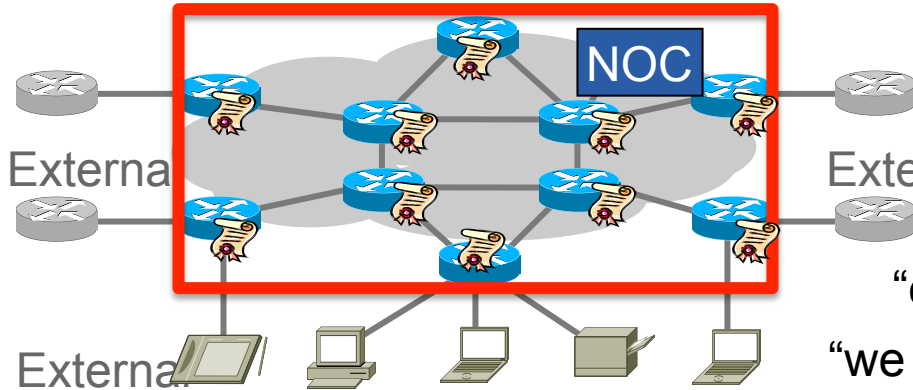
- Intent configured on registrar
- Flooded through network



```
Router#configure terminal
Router(config)#autonomic intent
Router(config-intent)#control-plane
Router(config-intent)#vlan outer 400-420
Router(config-intent)#vlan inner 4092
```

Autonomic Networking Strategy

Possibilities With Domain Certificates



“we can now secure the network automatically”

“bring up OSPF automatically”

“... and PIM-SM!”

External “we could enable guestnet, if a policy says so”

“each device knows what to do”

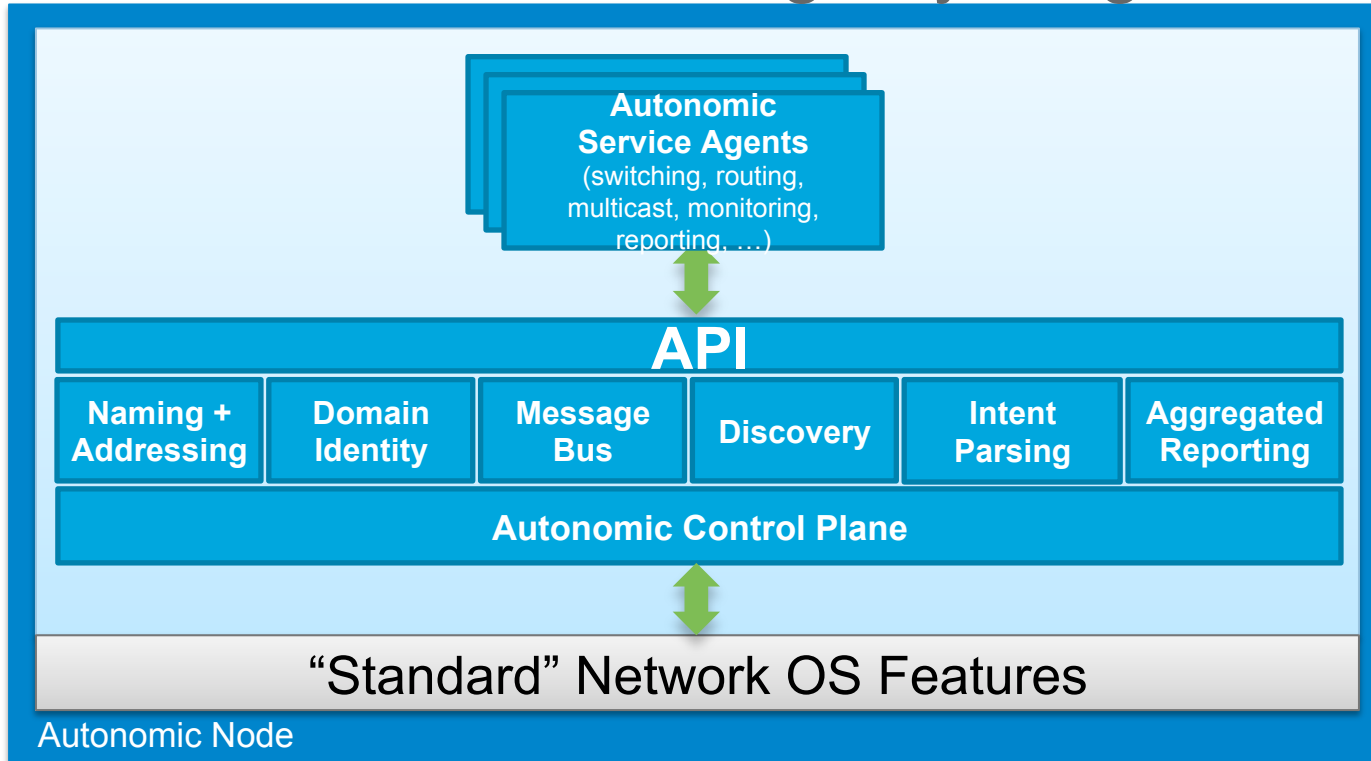
“we can find BGP speakers automatically!”

“... and secure the sessions!”

“the admin can detect unauthorised devices”

“reporting can be aggregated in the network”

Autonomic Networking Layering Model



Autonomic Networking Infrastructure

Please Support Standardisation!

ANIMA Working Group: <http://tools.ietf.org/wg/anima/>

Early work

- A Framework for Autonomic Networking <http://tools.ietf.org/html/draft-behringer-autonomic-network-framework>
- Making the Internet Secure by Default <http://tools.ietf.org/html/draft-behringer-default-secure>

NMRG work

- Autonomic Networking: Definitions and Design Goals <http://tools.ietf.org/html/draft-irtf-nmrq-autonomic-network-definitions>
- Gap Analysis for Autonomic Networking <https://tools.ietf.org/html/draft-irtf-nmrq-an-gap-analysis>

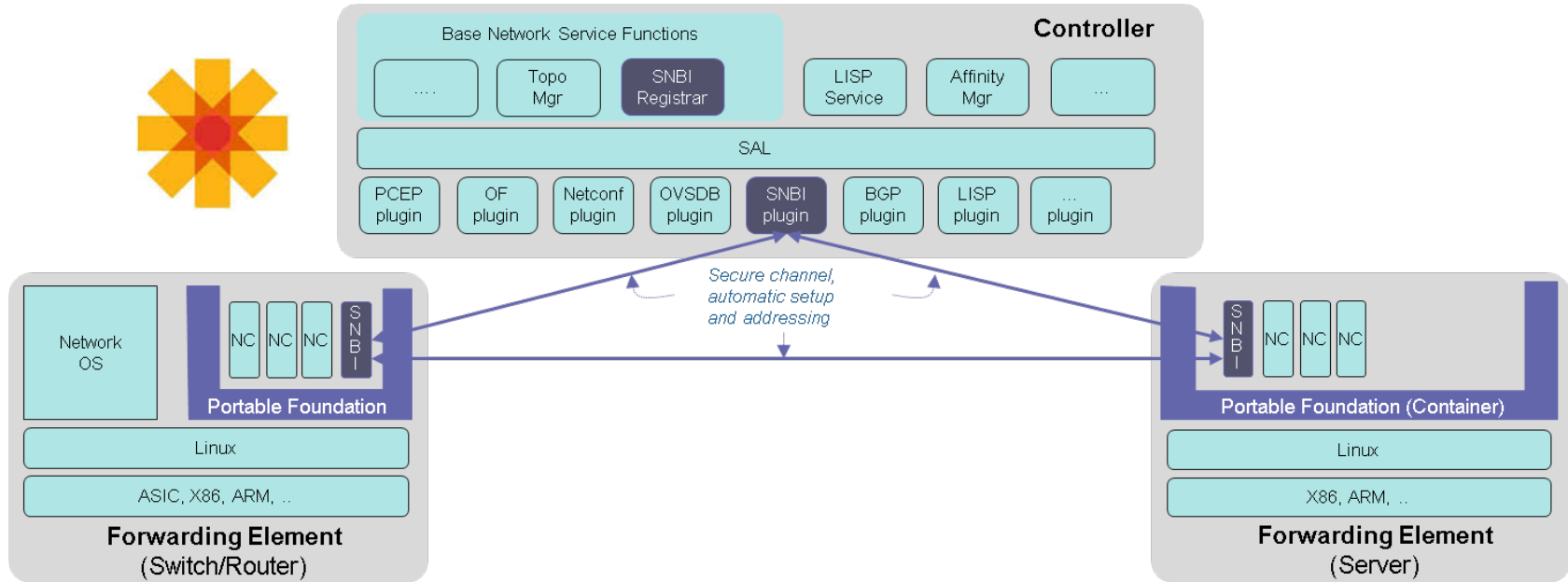
Use case drafts: Those are used to derive requirements for the Autonomic Networking Infrastructure

- Autonomic Networking Use Case for Network Bootstrap <https://tools.ietf.org/html/draft-behringer-autonomic-bootstrap>
- Autonomic Network Stable Connectivity <https://tools.ietf.org/html/draft-eckert-anima-stable-connectivity>
- Autonomic Prefix Management in Large-scale Networks <https://tools.ietf.org/html/draft-jiang-anima-prefix-management>

Solution drafts:

- An Autonomic Control Plane <https://tools.ietf.org/html/draft-behringer-anima-autonomic-control-plane>
- Bootstrapping Key Infrastructures <http://tools.ietf.org/html/draft-pritikin-anima-bootstrapping-keyinfrastructures>
- Bootstrapping Trust on a Homenet (this is in homenet, not ANIMA)
<https://tools.ietf.org/html/draft-behringer-homenet-trust-bootstrap>
- A Generic Discovery and Neg. Protocol for Autonomic Networking <https://tools.ietf.org/html/draft-carpenier-anima-gdn-protocol>

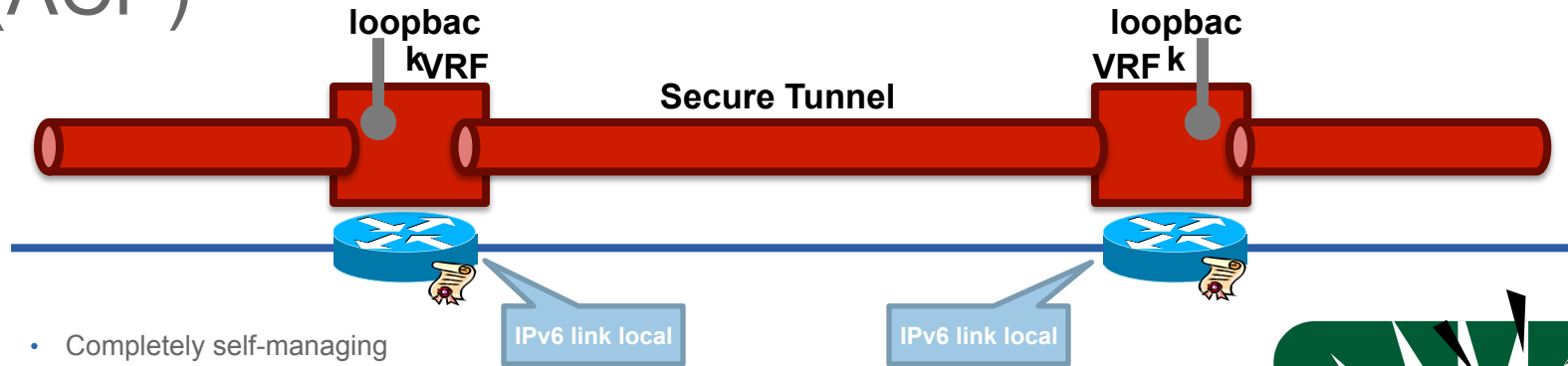
Please get involved: OpenDayLight: Secure Network Bootstrapping Infrastructure (SNBI)



<https://wiki.opendaylight.org/view/SecureNetworkBootstrapping:Main>

Summary

Advantages of the Autonomic Control Plane (ACP)



- Completely self-managing
 - No config!
- Secure
 - Separate (VPN) and encrypted (e.g., IPsec)
- Independent of Routing
 - Only depends on link local addresses
- Independent of Configuration
 - Only certificate visible in "sh running"
- Visible
 - Lots of show commands, debugs, etc.

Use as a
“Virtual
Out-Of-Band
Channel”



Cisco Device Support: SP, Enterprise and IoT

Supported today:

- ASR 901, ASR 901s, ASR 903, ASR 920, ME 3600, ME 3800
- Catalyst 2000, 3000, 4000, NG3k, IE 2000
- Open Source: Secure Network Bootstrap Infrastructure (SNBI; part of OpenDayLight Helium release)

Roadmap

- ASR 9000
- ASR 1000, CSR 1000, ISR-G2, ISR-4000
- (more to come)

References

- www.cisco.com/go/autonomic/
- IEFT Drafts: See earlier slide
- OpenDayLight Project SNBI: <https://wiki.opendaylight.org/view/SecureNetworkBootstrapping:Main>
- Autonomic Networking Configuration Guide, Cisco IOS Release 15S
www.cisco.com/en/US/partner/docs/ios-xml/ios/auto_net/configuration/15-s/an-auto-net-15-s-book.html
- Cisco IOS Autonomic Networking Command Reference
www.cisco.com/en/US/partner/docs/ios-xml/ios/auto_net/command/an-cr-book.html
- **autonomic-team@cisco.com**



CISCO

TOMORROW starts here.