
TOMORROW starts here.
cisco
Cisco live!

Enterprise SDN - APIC Enterprise Module

BRKRST-2641

Adam Radford

CSA

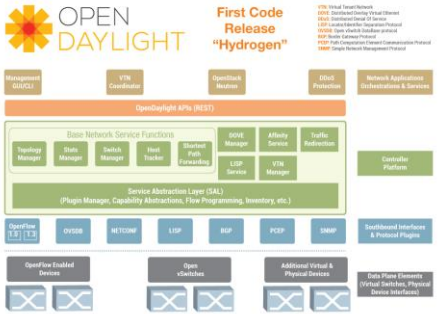
Cisco live!

Today's IT Model - Complex, Not Fast Enough

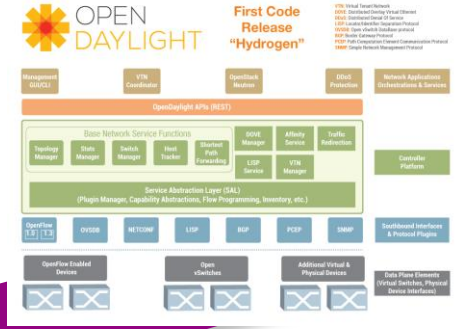
Box by Box

Manual Configuration

Initial Discussion…



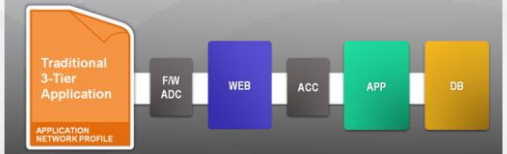
More Maturity



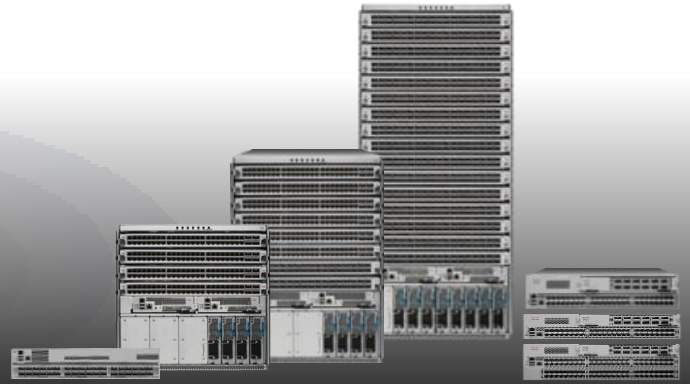
What is APIC-DC?

OPEN RESTFUL APIS
CENTRALISED POLICY MODEL
OPEN SOURCE

CONTROLLER



POLICY MODEL



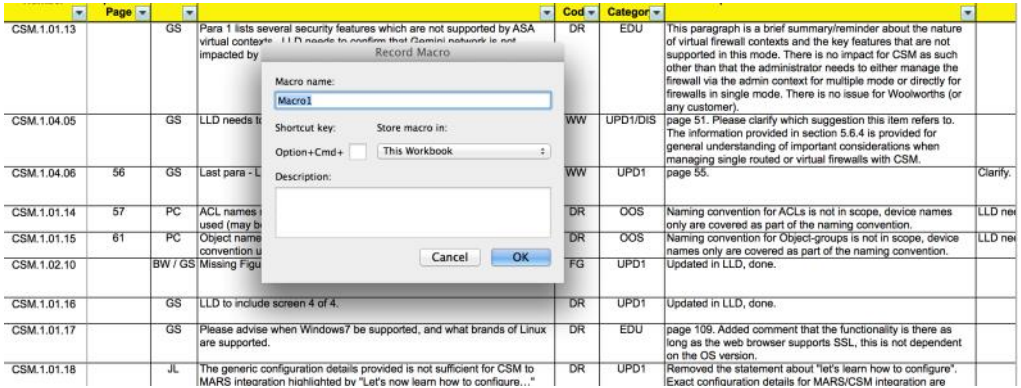
NEXUS 9500 and 9300

ACI

What is Policy?

WHAT

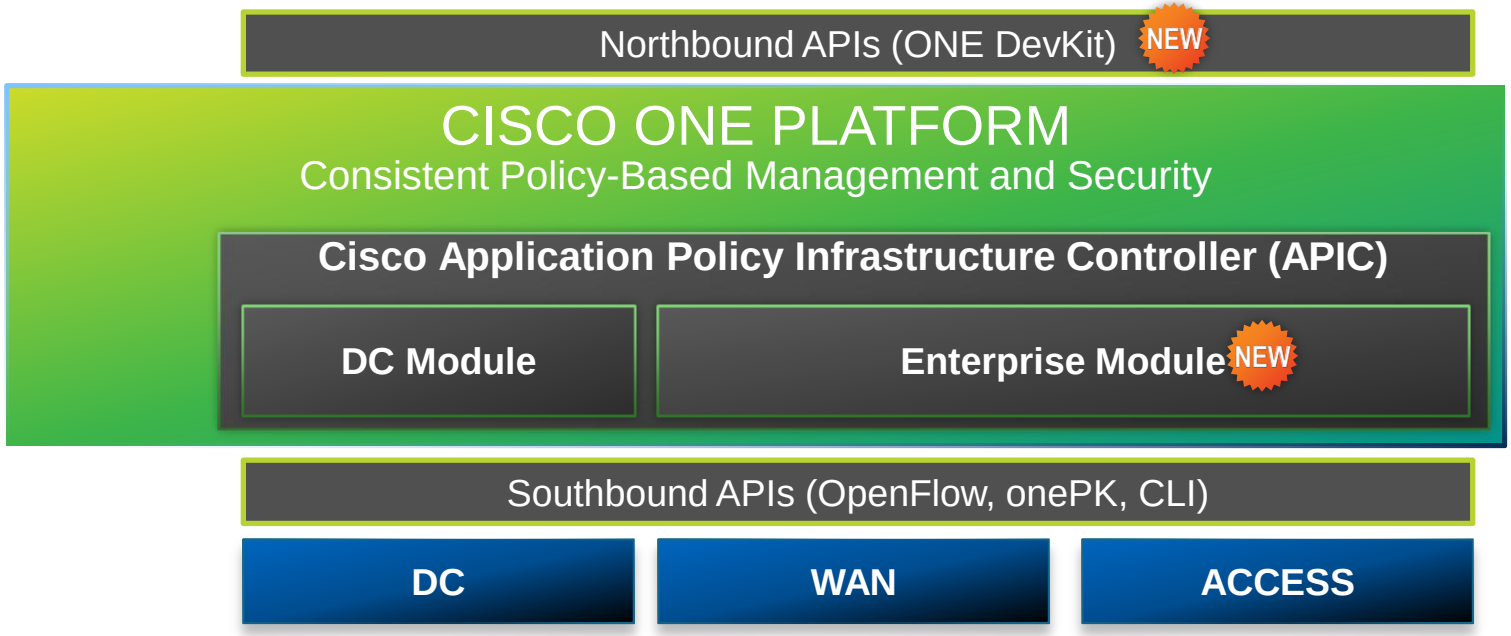
We have tried this before (and failed)?



	Page			Cod	Categor	
CSM.1.01.13		GS	Para 1 lists several security features which are not supported by ASA virtual contexts. LLD needs to confirm that Gemini network is not impacted by	DR	EDU	This paragraph is a brief summary/reminder about the nature of virtual firewall contexts and the key features that are not supported in this mode. There is no impact for CSM as such other than that the administrator needs to either manage the firewall via the admin context for multiple mode or directly for firewalls in single mode. There is no issue for Woolworths (or any customer).
CSM.1.04.05		GS	LLD needs t	WW	UPD1/DIS	page 51. Please clarify which suggestion this item refers to. The information provided in section 5.6.4 is provided for general understanding of important considerations when managing single routed or virtual firewalls with CSM.
CSM.1.04.06	56	GS	Last para - L	WW	UPD1	page 55. Clarify.
CSM.1.01.14	57	PC	ACL names used (may b	DR	OOS	Naming convention for ACLs is not in scope, device names only are covered as part of the naming convention. LLD ne
CSM.1.01.15	61	PC	Object name convention u	DR	OOS	Naming convention for Object-groups is not in scope, device names only are covered as part of the naming convention. LLD ne
CSM.1.02.10		BW / GS	Missing Figu	FG	UPD1	Updated in LLD, done.
CSM.1.01.16		GS	LLD to include screen 4 of 4.	DR	UPD1	Updated in LLD, done.
CSM.1.01.17		GS	Please advise when Windows7 be supported, and what brands of Linux are supported.	DR	EDU	page 109. Added comment that the functionality is there as long as the web browser supports SSL, this is not dependent on the OS version.
CSM.1.01.18		JL	The generic configuration details provided is not sufficient for CSM to MARS integration highlighted by "Let's now learn how to configure..."	DR	UPD1	Removed the statement about "let's learn how to configure". Exact configuration details for MARS/CSM integration are

A.....n

One Platform



Physical and Virtual

Common Policy Engine

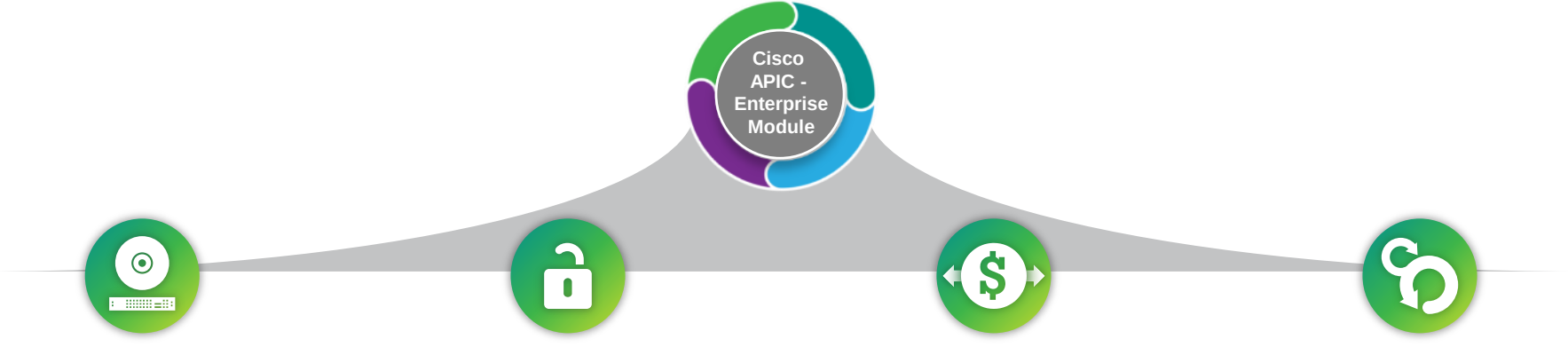
Network Wide Security and Services

Investment Protection

Flexible Licensing NEW

Cisco APIC - Enterprise Module

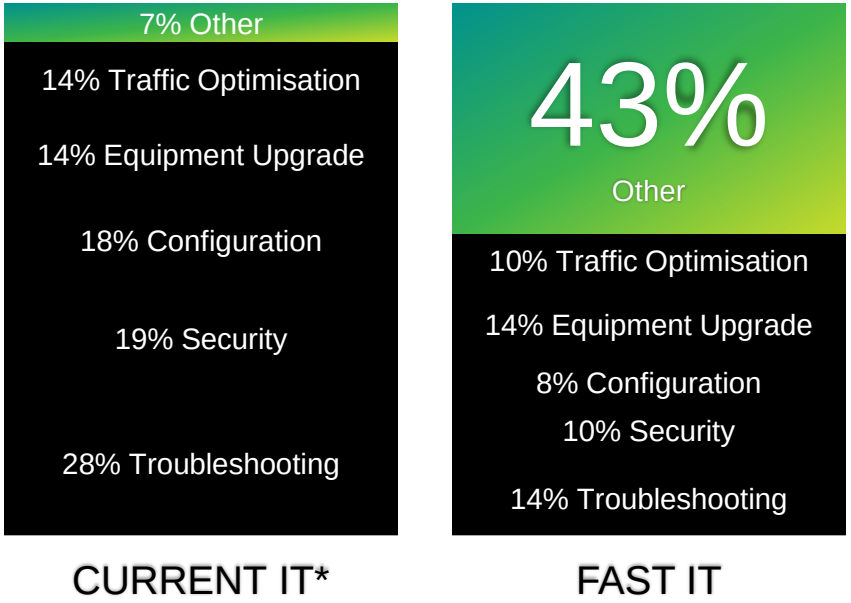
Network Abstraction and Automation



Masking Network Complexity, Exposing Network Intelligence

Cisco APIC - Enterprise Module

Average Time Spent by Network Administrator



36%

More Time Available for Business Innovation

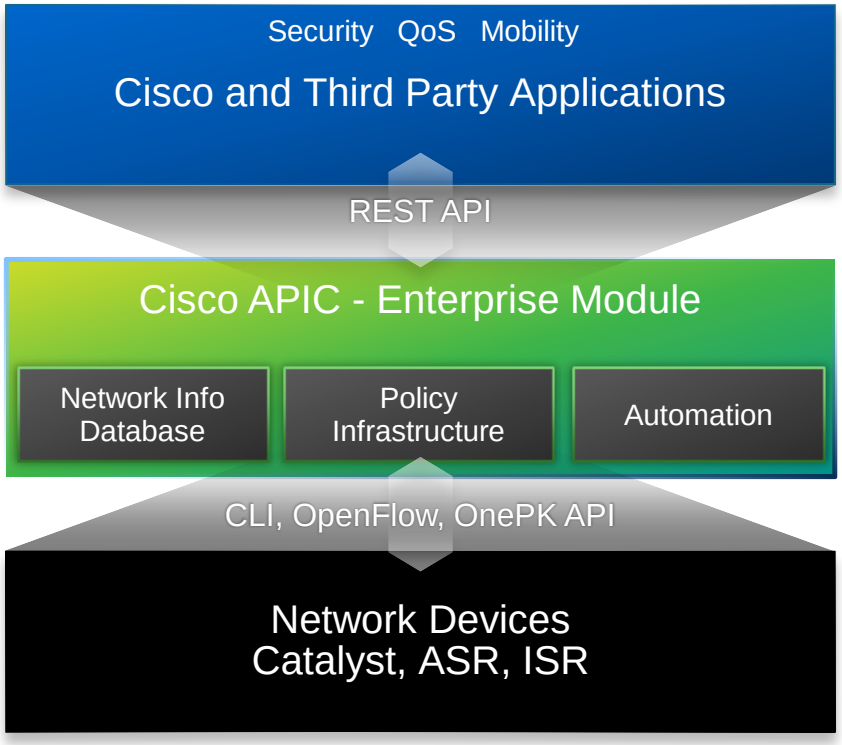
36%

Total Network Operations Time Savings

Reducing IT Operations Time, Creating More Time for IT Innovation

*Source: Forrester Commissioned Study

Cisco APIC - Enterprise Module Architecture



Exposes Network Intelligence

For Business Innovation

Abstracts Network Devices to Mask Complexity

Treat Network as a System

Cisco APIC - Enterprise Module: Initial Deployment Scenarios

Security Automation

Network-Wide Rapid Threat Detection and Mitigation (Sourcefire)

ACL Management Automation

QoS Provisioning

Easy QoS

Follow Me QoS

Compliance Assurance

IWAN: Path Optimisation

Automated Performance Routing (PfR) Configuration

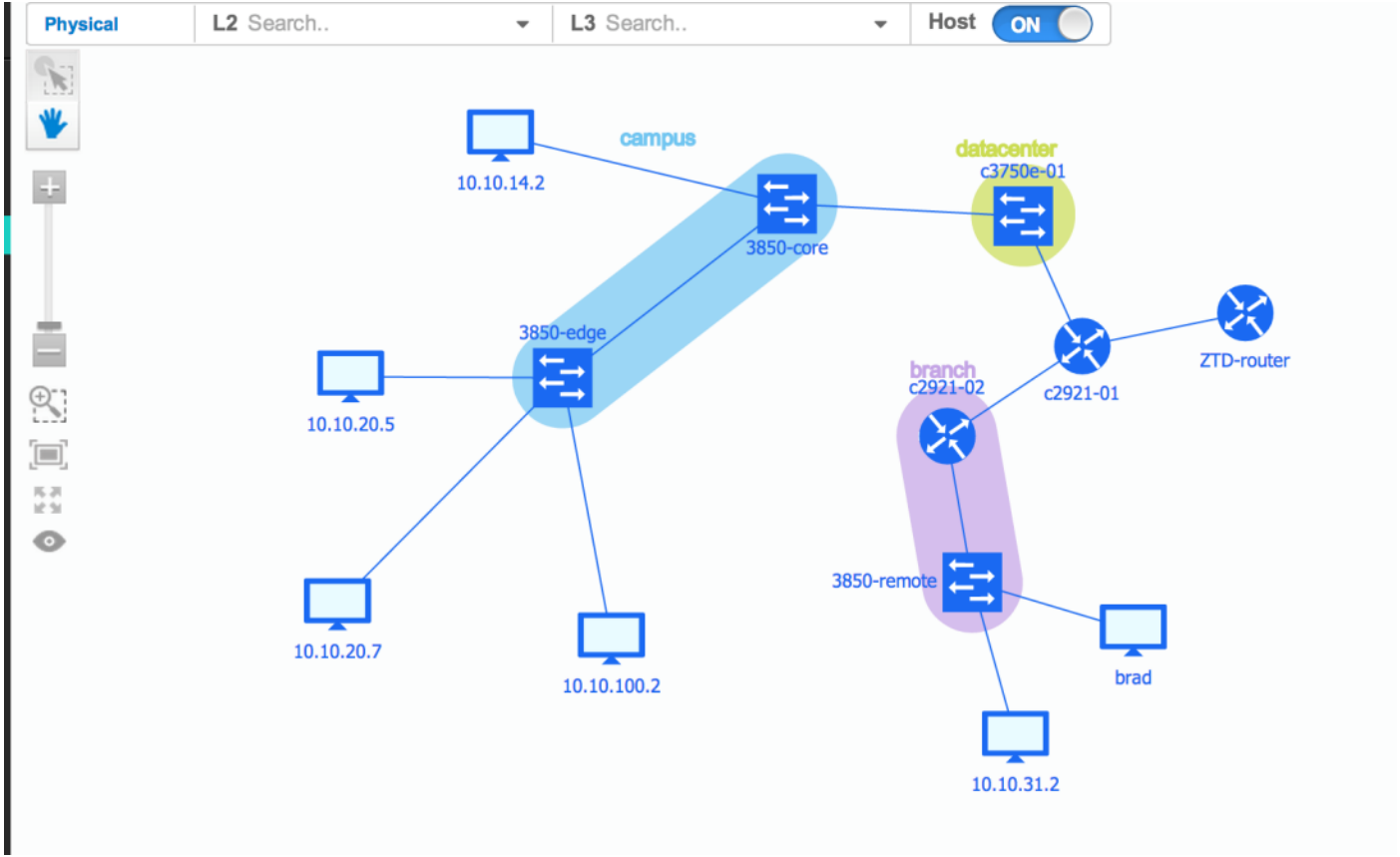
Automated WAN Policy Compliance Assurance

Solving the Most Pressing, Complex and Tedious IT Problems

Inventory

Device Status	Device Name	MAC Address	IP Address	Hosts	IOS/Firmware	Platform	Serial Number	Configuration	Device Role	Location	Tag	Last Updated Time	Update Frequency (seconds)	Number of Updates
Reachable	3850-edge	7C:95:F3:BC:71:64	10.10.4.2	10.10.20.5, 10.10.20.7, 10.10.100.2	03.02.02.SE	WS-C3850-24P	FOC1731X0KN	View	Access	Add	campus	2014-02-16 12:13:18		1146
Reachable	c2921-02	24:B6:57:53:77:E2	10.10.5.2		15.4(20131012:104348)	CISCO2921/K9	FGL154611FF	View	Distribution	branch Office	branch	2014-02-16 12:13:09		1147
Reachable	ZTD-router	50:3D:E5:58:BC:20	10.10.7.2		15.4(1)T	CISCO1941/K9	FGL150425CN	View	Unknown	Add	Add	2014-02-16 12:13:09		1147
Reachable	c3750e-01	00:22:56:CA:B7:C3	10.66.124.133		12.2(58)SE2	WS-C3750E-48TD	FDO1229R0WD	View	Distribution	Add	datacenter	2014-02-16 12:13:14		1147
Reachable	3850-remote	7C:95:F3:BD:2B:64	10.10.6.2	10.10.31.2, 10.10.30.2	03.02.02.SE	WS-C3850-24P	FOC1731X15W	View	Access	branch Office	branch	2014-02-16 12:13:12		1147
Reachable	c2921-01	F8:66:F2:F4:AA:A2	100.1.1.1		15.4(20131012:104348)	CISCO2921/K9	FHK1436F2CC	View	Unknown	Add	Add	2014-02-16 12:13:09		1147
Reachable	3850-core	7C:95:F3:BD:2A:64	10.10.10.110	10.10.14.2	03.02.02.SE	WS-C3850-24P	FOC1731U0WY	View	Access	Head Office	campus	2014-02-16 12:13:13		1147

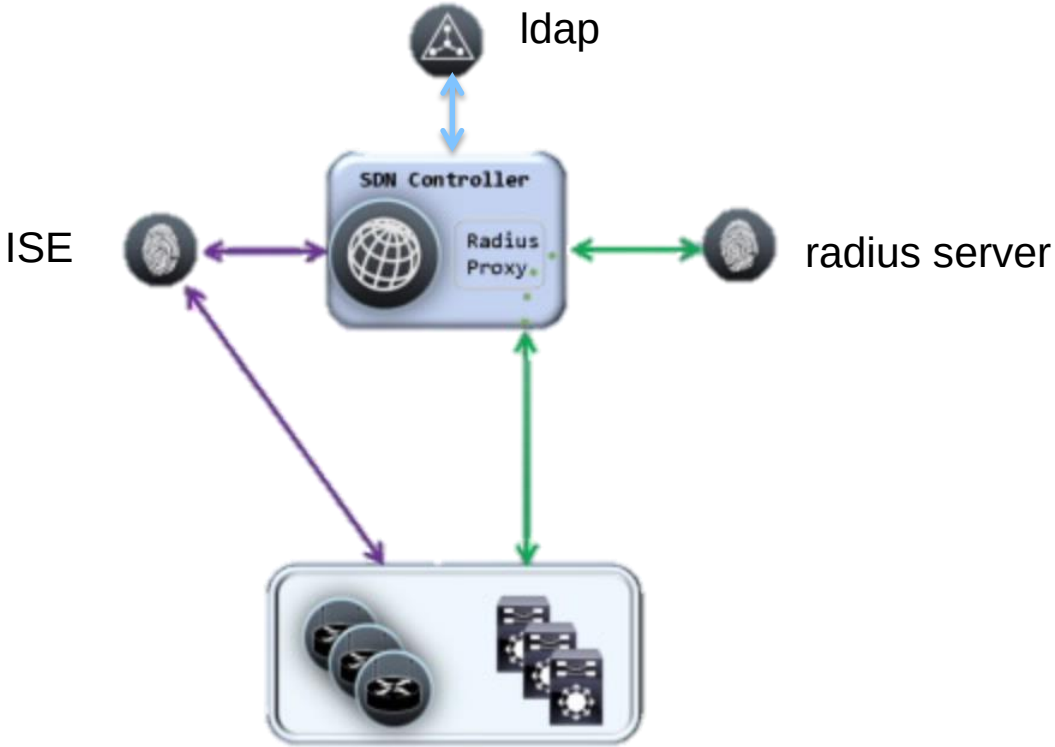
Topology



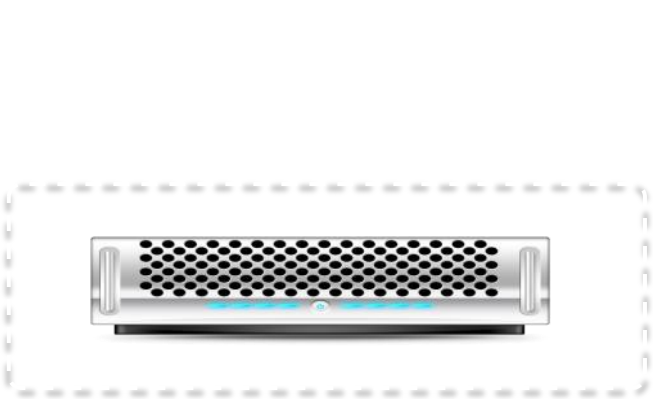


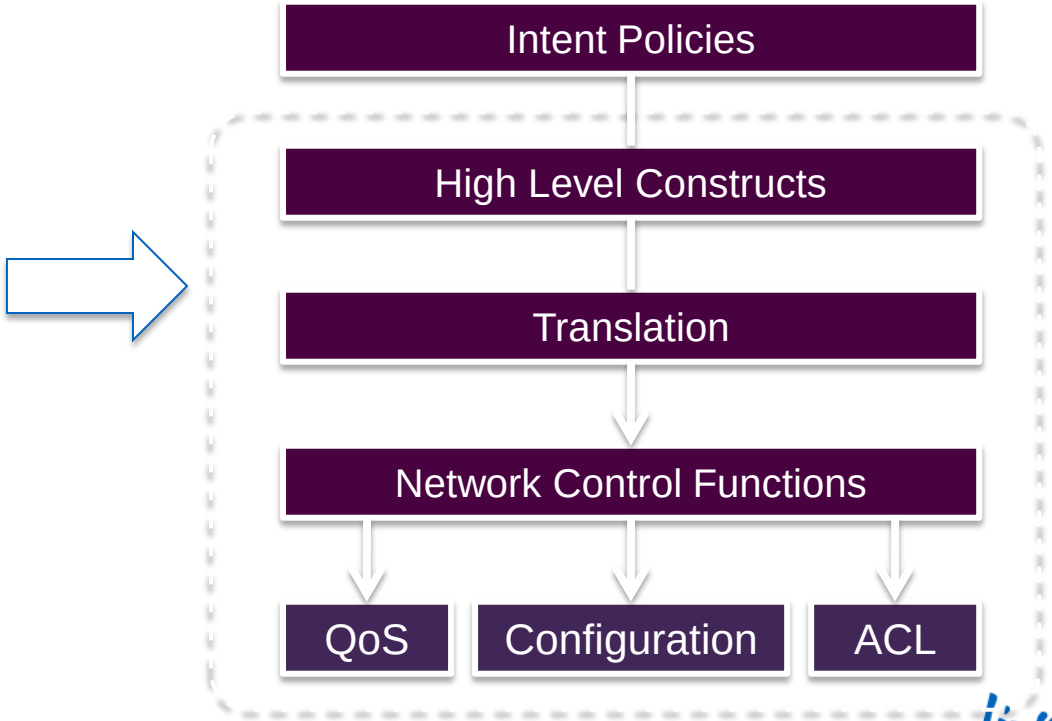

Policy

Controller Deployment

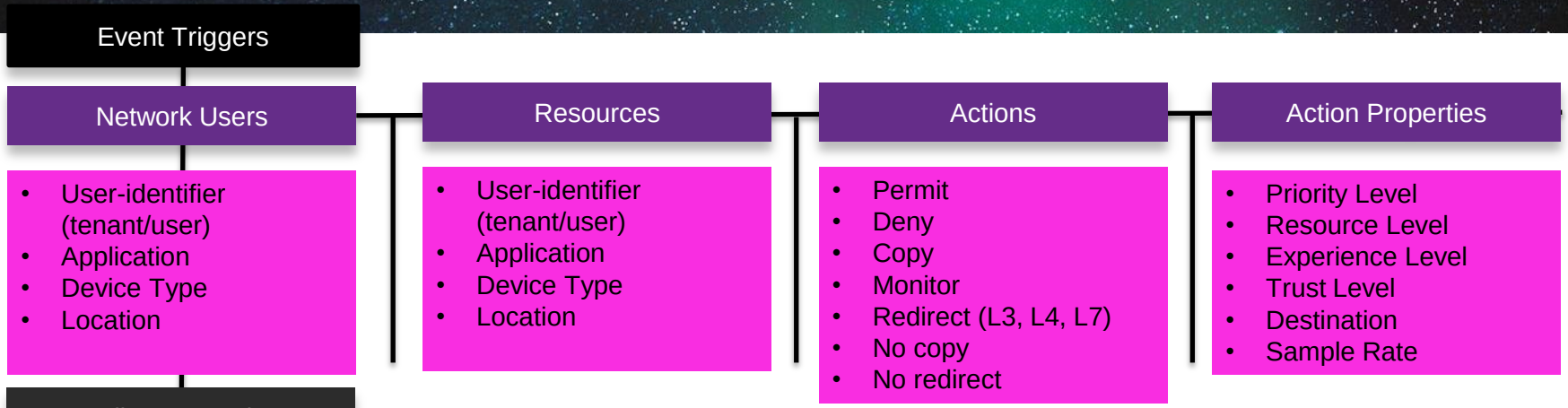


Policy Engine – Business Intent



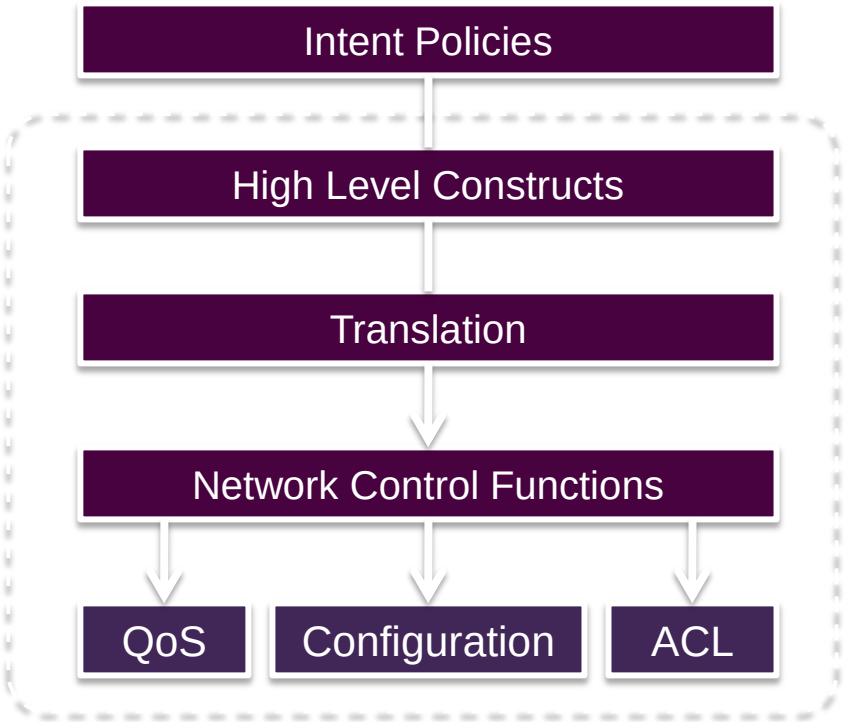


Policy Construct



- High Level Business Intent Policies
- Automatically converted to Network Language
- Conflict Detection and Resolution
- Extensible
- Supports different patterns of policies:
  - **Access Policies**
  - **Source-Destination Directional Policies**
  - **Event – Condition – Action**
  - Includes Collections (Ex: a group of userids, a group of applications, etc.)
  - Choose custom tags for policies
  - Choose multiple attributes in each category

Give me an Example



UI:: BradWebAccess: Brad Web allow

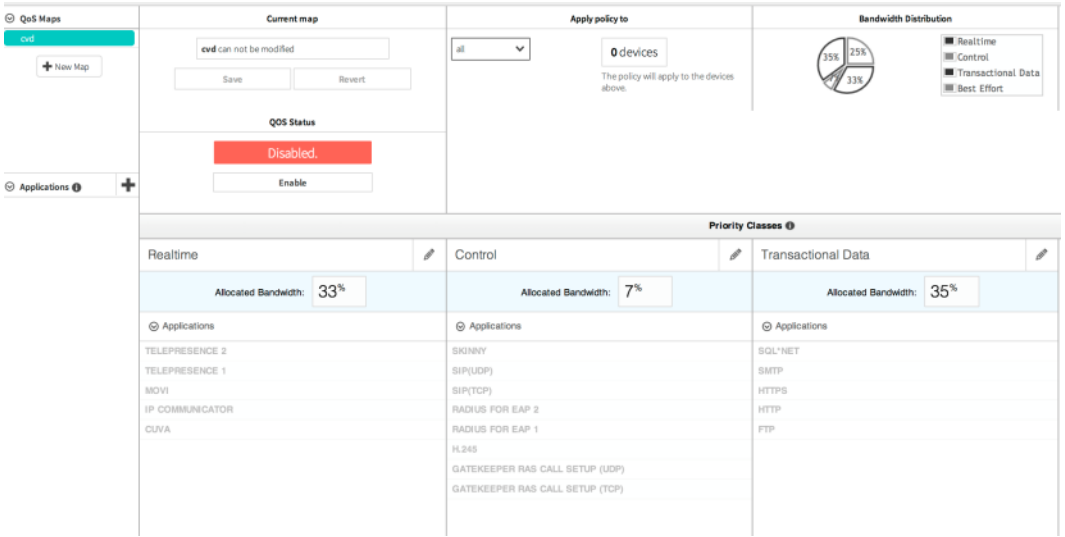
Policy Manager:: Business Policy -> Network Policy

Policy Programmer:: Network Policy-> Network Cmds

Scanner-Service:: Network Commands -> device

Benefits of Centralised Policy

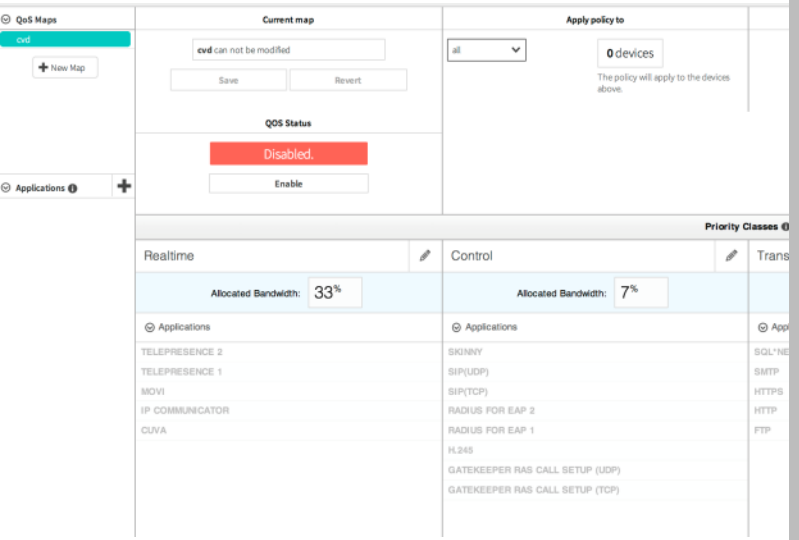
Lets Talk About Easy Qos




```
policy-map EasyQos-Egress
 class REALTIME
   bandwidth remaining percent 33
 class CONTROL
   bandwidth remaining percent 7
 class TRANSACTIONAL-DATA
   bandwidth remaining percent 35
 class BEST-EFFORT
   bandwidth remaining percent 25

interface GigabitEthernet1/0/1
 no switchport
 ip address 10.10.6.2 255.255.255.0
 service-policy output EasyQos-Egress
```

Now the Clever Bit



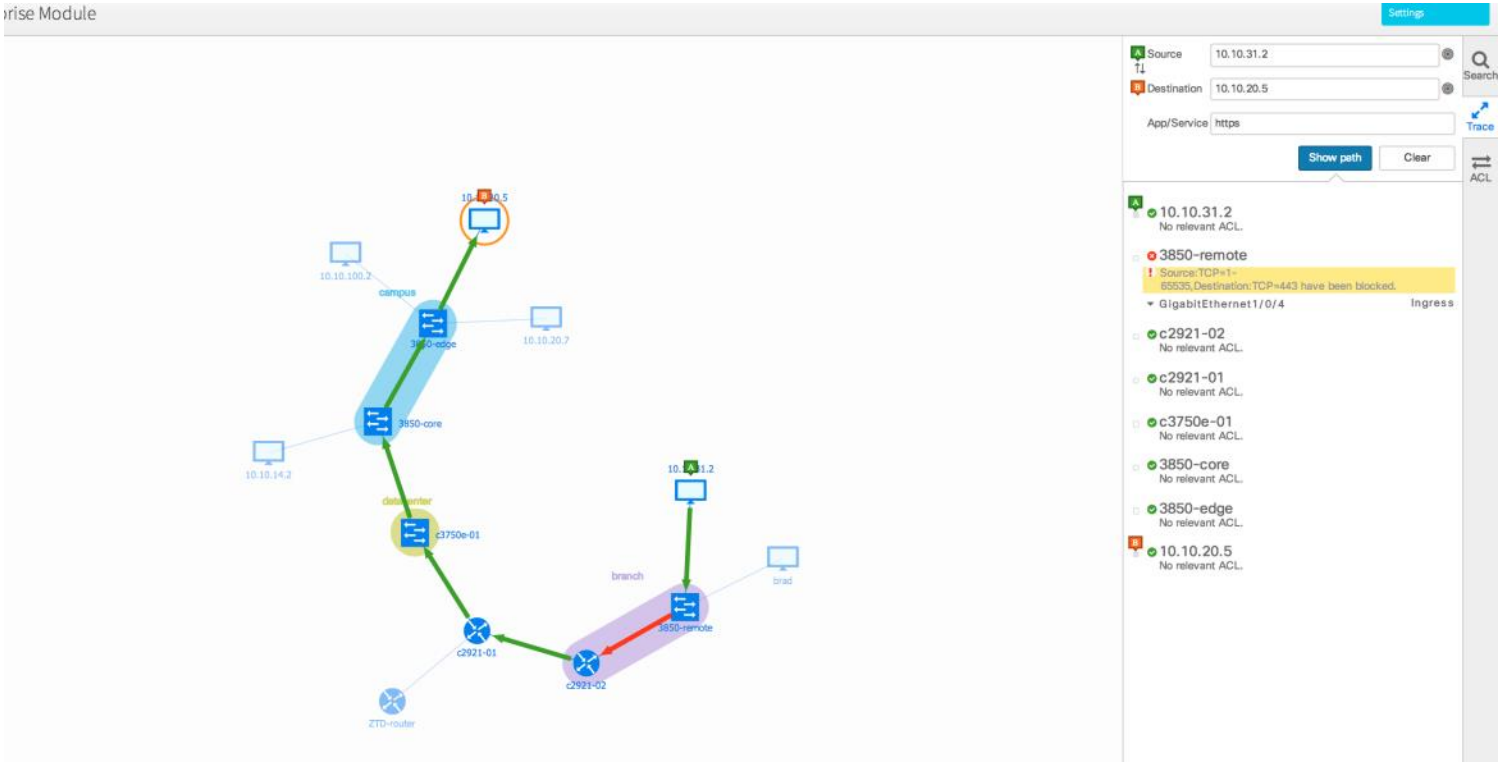

```
class-map match-any User-ClassMap--7367751811899092866
  match access-group name User-Acl—5660381599625002973
class-map match-any User-ClassMap--8740062111854106845
  match access-group name User-Acl—6955512163447700969
class-map match-any User-ClassMap--6899825101577202637
  match access-group name User-Acl—6940214622314956748

policy-map User-PolicyMap--5064108890213890935
 class User-ClassMap--7367751811899092866
   set dscp default
 class User-ClassMap--8740062111854106845
   set dscp default
 class User-ClassMap--6899825101577202637
   set dscp af2

ip access-list extended User-Acl--5660381599625002973
 permit udp any any eq 3689 # itunes
ip access-list extended User-Acl--6955512163447700969
 permit tcp any any range 6881 6999 # bittorrent
ip access-list extended User-Acl--6940214622314956748
 permit tcp any any eq 1914  # xiip
```

Where does this get applied?
Interaction?

Trust Me….

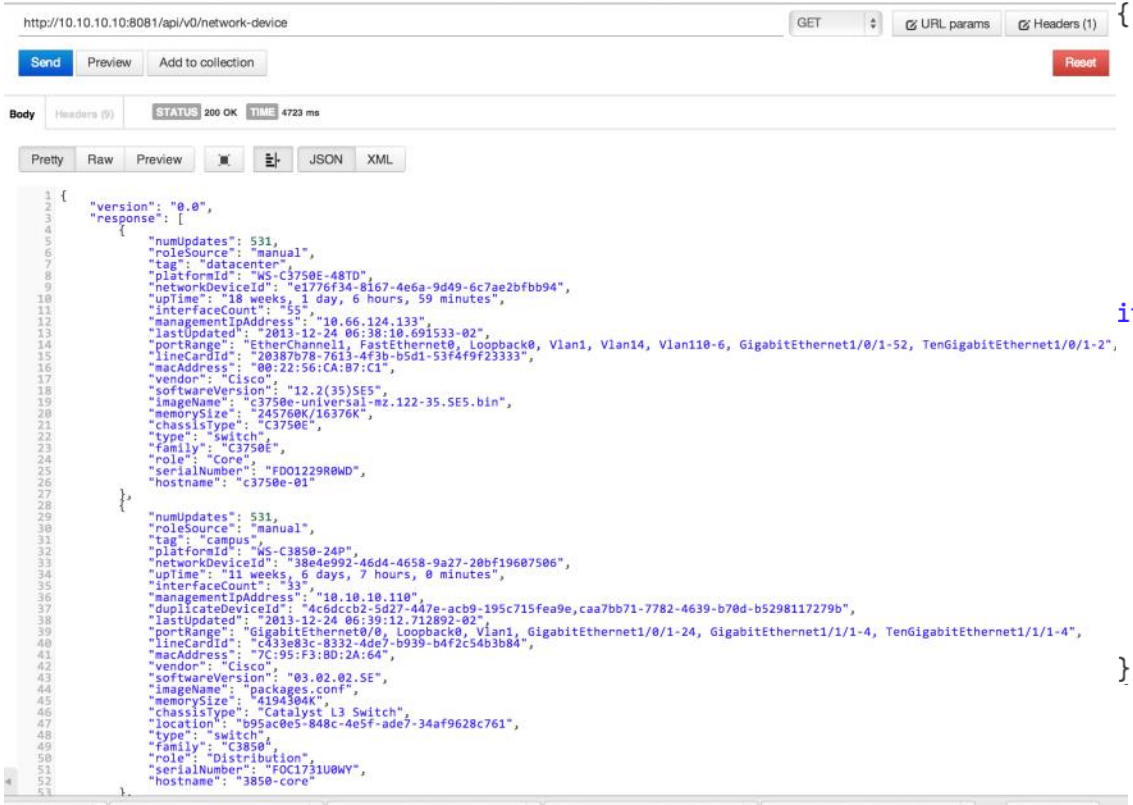





API

Postman

REST CLIENT for Chrome

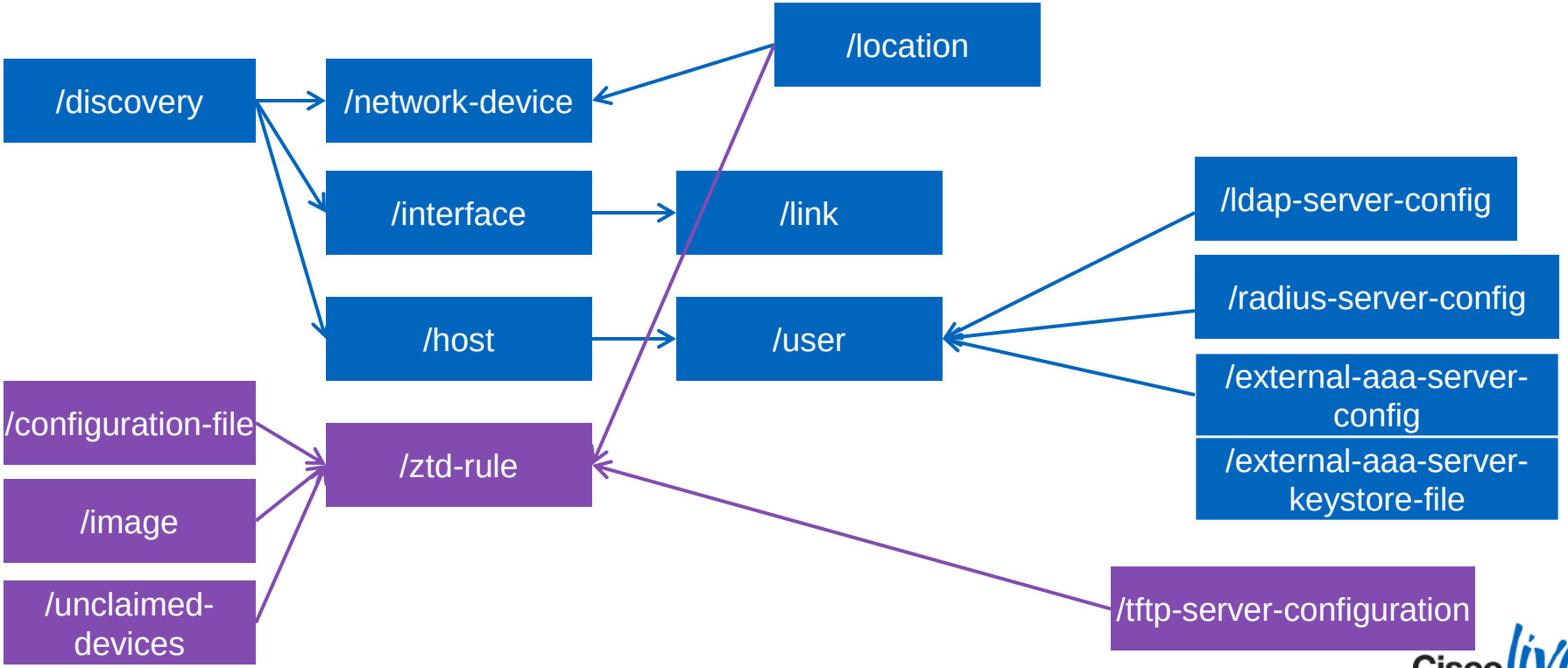



```
{
  "version": "0.0",
  "response": [
    {
      "numUpdates": 531,
      "roleSource": "manual",
      "tag": "datacenter",
      "platformId": "WS-C3750E-48TD",
      "networkDeviceId": "e1776f34-8167-4e6a-9d49-6c7ae2bfbb94",
      "upTime": "18 weeks, 1 day, 6 hours, 59 minutes",
      "interfaceCount": "55",
      "managementIpAddress": "10.66.124.133",
      "lastUpdated": "2013-12-24 06:38:10.691533-02",
      "portRange": "EtherChannel1, FastEthernet0, Loopback0, Vlan1, Vlan14, Vlan110-6, GigabitEthernet1/0/1-52, TenGigabitEthernet1/0/1-2",
      "lineCardId": "20387b78-7613-4f3b-b5d1-53f4f9f23333",
      "macAddress": "00:22:56:CA:B7:C1",
      "vendor": "Cisco",
      "softwareVersion": "12.2(35)SE5",
      "imageName": "c3750e-universal-mz.122-35.SE5.bin",
      "memorySize": "245760K/16376K",
      "chassisType": "C3750E",
      "type": "switch",
      "family": "C3750E",
      "role": "Core",
      "serialNumber": "FDO1229R0WD",
      "hostname": "c3750e-01"
    },
    {
      "numUpdates": 531,
      "roleSource": "manual",
      "tag": "campus",
      "platformId": "WS-C3850-24P",
      "networkDeviceId": "38e4e992-46d4-4658-9a27-20bf19607506",
      "upTime": "11 weeks, 6 days, 7 hours, 0 minutes",
      "interfaceCount": "33",
      "managementIpAddress": "10.10.10.110",
      "duplicateDeviceId": "4c6dccb2-5d27-447e-acb9-195c715fea9e,caa7bb71-7782-4639-b70d-b5298117279b",
      "lastUpdated": "2013-12-24 06:39:12.712892-02",
      "portRange": "GigabitEthernet0/0, Loopback0, Vlan1, GigabitEthernet1/0/1-24, GigabitEthernet1/1/1-4, TenGigabitEthernet1/1/1-4",
      "lineCardId": "c433e83c-8332-4de7-b939-b4f2c54b3b84",
      "macAddress": "7C:95:F3:8D:2A:64",
      "vendor": "Cisco",
      "softwareVersion": "03.02.02.SE",
      "imageName": "packages.conf",
      "memorySize": "4194304K",
      "chassisType": "Catalyst L3 Switch",
      "location": "b95ac0e5-848c-4e5f-ade7-34af9628c761",
      "type": "switch",
      "family": "C3850",
      "role": "Distribution",
      "serialNumber": "FOC1731U0WY",
      "hostname": "3850-core"
    },
```



```
{
    "numUpdates": 531,
    "roleSource": "manual",
    "tag": "campus",
    "platformId": "WS-C3850-24P",
    "networkDeviceId": "1f48372f-894e-4afc-89d3-c144b78
    "upTime": "10 weeks, 5 days, 6 hours, 20 minutes",
    "interfaceCount": "33",
    "managementIpAddress": "10.10.4.2",
    "lastUpdated": "2013-12-24 06:40:14.38939-02",
    "portRange": "GigabitEthernet0/0, Capwap0, Loopback
itEthernet1/1/1-4",
    "lineCardId": "283463d1-4b70-4eaa-aeac-b80604d67331
    "macAddress": "7C:95:F3:BC:71:64",
    "vendor": "Cisco",
    "softwareVersion": "03.02.02.SE",
    "imageName": "packages.conf",
    "memorySize": "4194304K",
    "chassisType": "Catalyst L3 Switch",
    "type": "switch",
    "family": "C3850",
    "role": "Access",
    "serialNumber": "FOC1731X0KN",
    "hostname": "3850-edge"
},
```

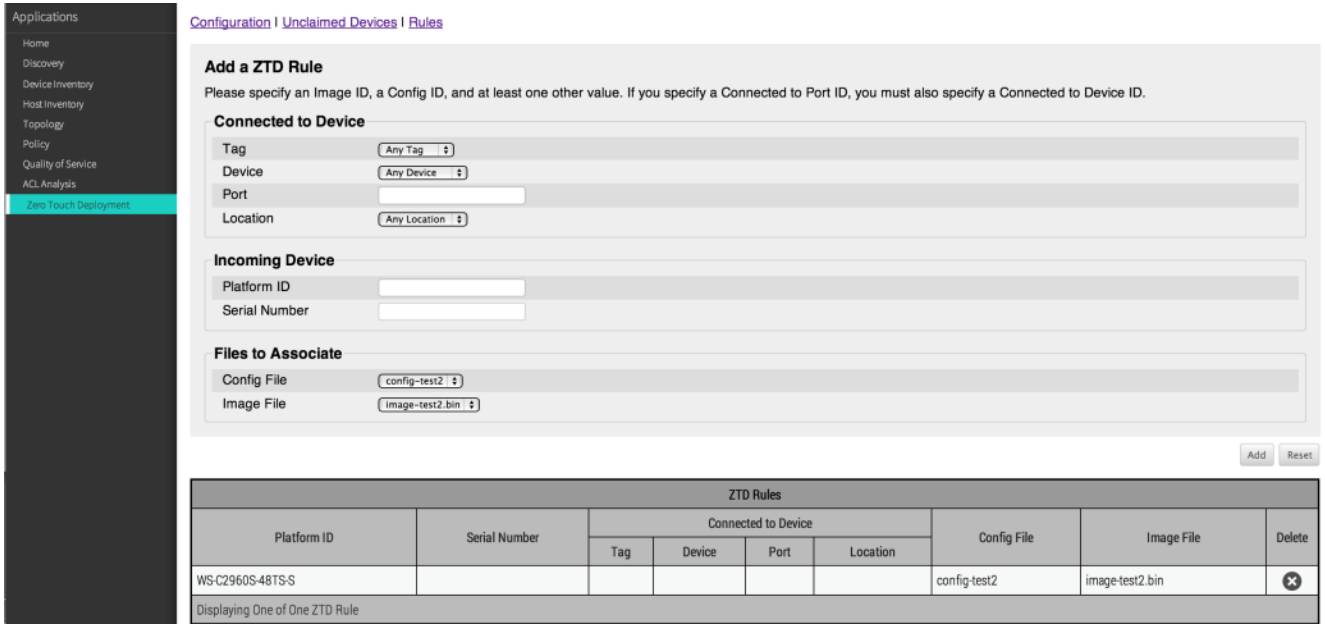
REST API Structure - Setup



General Structure

GET	/noun, /noun/count, /noun/{start}/{end}, /noun/{noun-id}
POST	Returns 409 if duplicate resource, {“response” : “id-of-created-resource”}
PUT	{“response” : “message-about-attributes-that-changed”}
DELETE	404 if fail, {“response” : “message-about-deletion”}

ZTD



Unclaimed-device

Only if you fail to match a rule

http://10.10.10.10:8081/api/v0/unclaimed-device GET


```
[
    {
        "connectedToMacAddr": "50:3D:E5:58:BC:20",
        "connectedToIpAddr": "10.10.7.5",
        "deviceID": "86197010-ca18-4746-8471-99dd3c577f64",
        "platformID": "WS-C2960-24PC-S",
        "connectedToHostName": "ZTD-router",
        "connectedToPortName": "GigabitEthernet0/1",
        "hostName": "CISCO-ZTD-DEVICE-CISCO",
        "serialNumber": "FOC1417W3G7"
    }
]
```

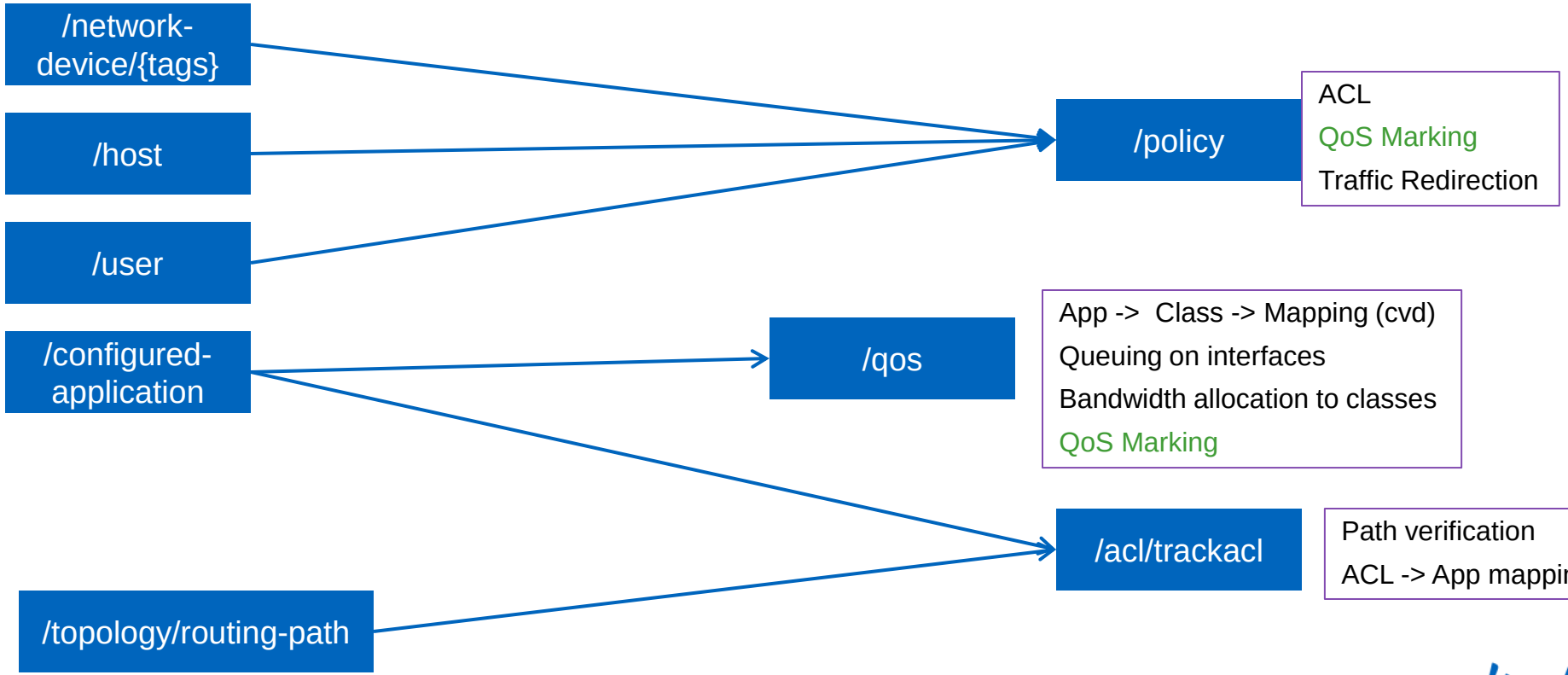
Host

List of devices attached to the network

http://10.10.10.10:8081/api/v0/host GET


```
[{
    "hostId": "88d64ae9-6a5b-4b34-bc36-1e26746d1fec",
    "cdpInformation": IP Phone, # some really interesting implications for policy
    "lldpInformation": null,
    "hostMac": "00:25:4B:CF:0F:20",
    "connectedInterfaceName": "GigabitEthernet1/0/12",
    "numUpdates": 2468,
    "lastUpdated": "2014-01-18 00:13:05.492679-02",
    "connectedNetworkDeviceIpAddress": "10.10.6.2",
    "hostType": "WIRED",
    "vlanId": "30",
    "hostIp": "10.10.30.2",
    "connectedInterfaceId": "321ca21c-02aa-4d2f-9759-27703150fd42",
    "connectedNetworkDeviceId": "88039151-d613-46e9-8e8c-49ea60cc00a5",
    "avgUpdateFrequency": 0,
    "hostName": null
},
```

REST API Structure - Policy



Out of the Box Integration

/api/v0/policy POST
{"actions": ["DENY"], "policyOwner":"admin”, "policyName": "deny_all”, "networkUser": {"userIdentifiers”:["10.10.20.7"]}}

http://10.10.10.10:8081/api/v0/policy POST

{"actions": ["PERMIT”],"policyName": "src-marking”, "policyOwner": "Admin",

"actionProperty": {"priorityLevel": "46"}, "networkUser": {"userIdentifiers”:["10.10.20.5"],"applications”:["80,80,TCP”]} }

Cisco aPI?

POST /discovery/
POST /discovery-frequency/network-device/
POST /discovery-frequency/interface/
POST /discovery-frequency/host/
POST /device-credential/
POST /network-device/location
POST /network-device/tag
POST /link/tag
POST /interface/tag
POST /interface-queue-statistics/
POST /location/
POST /external-aaa-keystore-file/
POST /external-aaa-server-config/
POST /configured-application/
POST /policy/
POST /qos/
POST /qos/policy/scope/{scope}
POST /qos/app-class-map

POST /tftp-server-configuration/
POST /configuration-file/
POST /image/
POST /ztd-rule/
POST /unclaimed-device/device-add/
POST /topology/status/
POST /acl/interfaces/
POST /acl/devices/
POST /acl/trackacls/




Q & A

Complete Your Online Session Evaluation

Give us your feedback and receive a Cisco Live 2014 Polo Shirt!

Complete your Overall Event Survey and 5 Session Evaluations.

- Directly from your mobile device on the Cisco Live Mobile App
- By visiting the Cisco Live Mobile Site www.ciscoliveaustralia.com/mobile
- Visit any Cisco Live Internet Station located throughout the venue

Polo Shirts can be collected in the World of Solutions on Friday 21 March 12:00pm - 2:00pm

Learn online with Cisco Live!

Visit us online after the conference for full access to session videos and presentations.
www.CiscoLiveAPAC.com


CISCO
TM