Cisco TechAdvantage Webinars
Supporting Zeroconf and Apple Bonjour in the Enterprise Using Cisco's Service Discovery Gateway

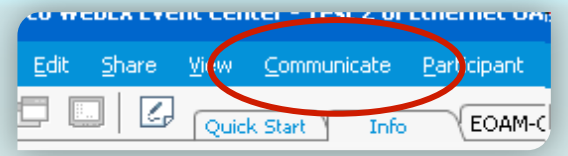
Ralph Schmieder

Amit Dutta

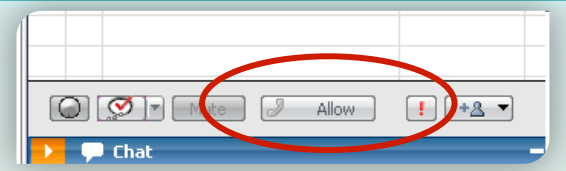
Follow us @GetYourBuildOn

Housekeeping

- Submit questions in Q&A panel and send to "All Panelists"
  Avoid CHAT window for better access to panelists
- For WebEx audio, select COMMUNICATE > Join Audio Broadcast



- For WebEx call back, click ALLOW phone button at the bottom of participants side panel



- Where can I get the presentation?
  Or send email to: ask_techadvantage@cisco.com
- Please complete the post-event survey
- Join us for upcoming TechAdvantage Webinars:
  www.cisco.com/go/techadvantage

Speakers & Panelists Introduction

Speakers

Ralph Schmieder
Technical Marketing Engineer
rschmied@cisco.com

Amit Dutta
Product Manager
amdutta@cisco.com

Panelists

Stephen Orr
Distinguished Systems Engineer
sorr@cisco.com

Tarunesh Ahuja
Technical Engineering Leader
tahujae@cisco.com

David Lapier
Product Marketing Manager
dlapier@cisco.com

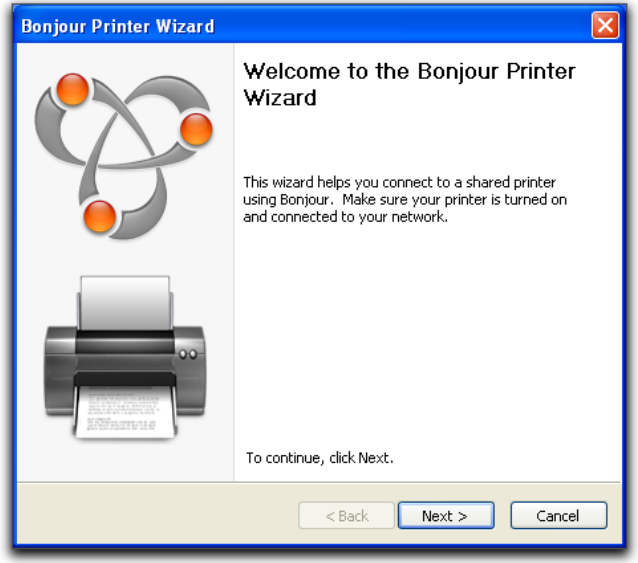
From Home Networks...

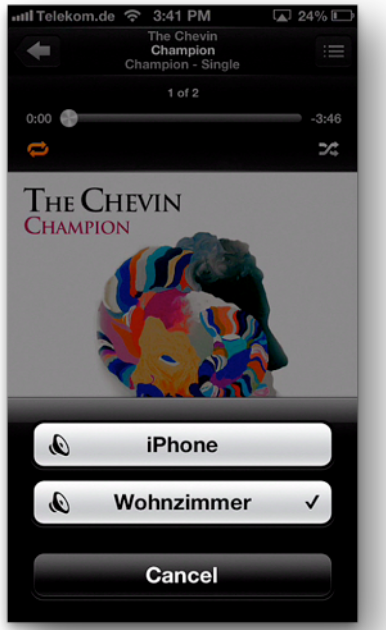
- In Personal Networks
  - There's often no central services available.
  - How do I get an address?
  - How do I easily find my printer?
  - How do I stream music to my music device in the living room?
- Need for ad-hoc IP Connectivity and Service Discovery
  - Addressed by Zeroconf / DNS-SD / Bonjour, LLMNR / UPnP SSDP, DLNA, (ZigBee) to name a few
- Problem solved... Right?

DNS-SD=DNS Service Discovery, LLMNR=Link Local Multicast Name Resolution, UPnP SSDP=Universal Plug and Play Simple Service Discovery Protocol, Digital Living Network Alliance

To Enterprise Networks

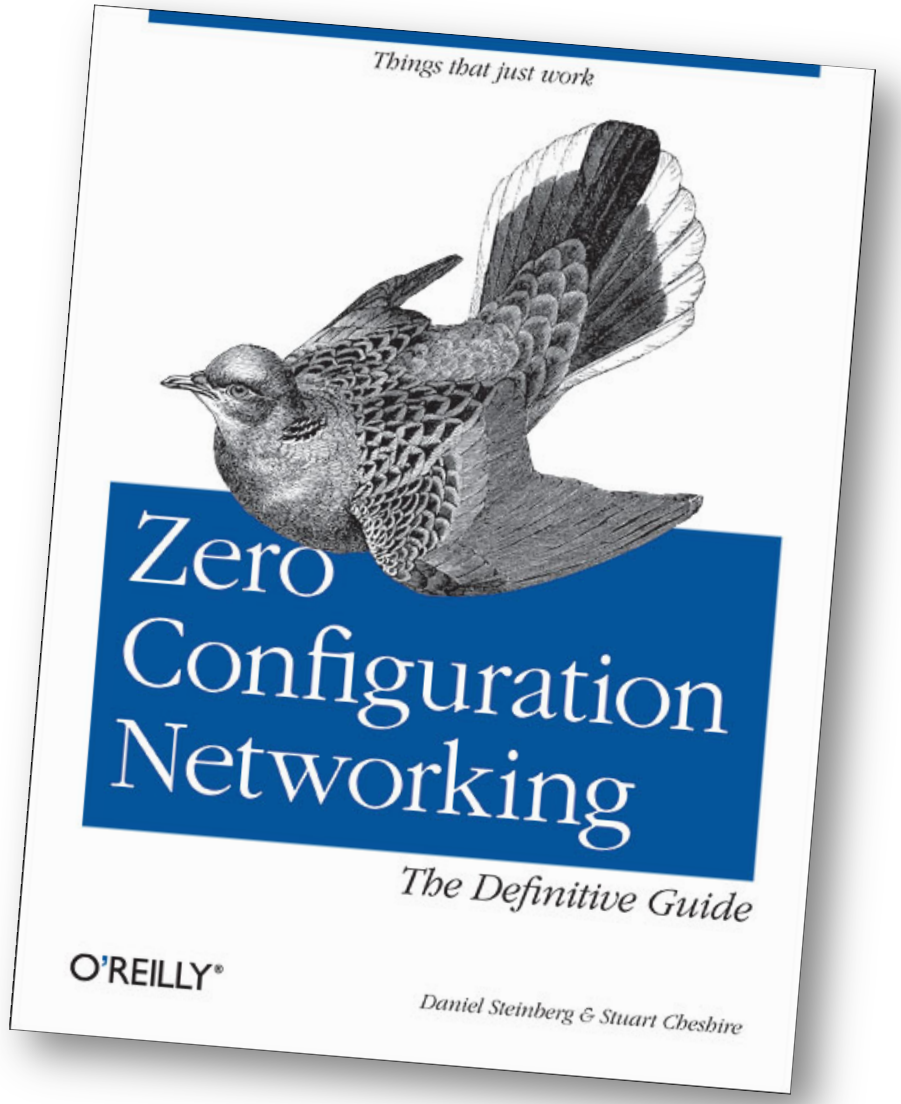
- BYOD: Massive influx of consumer devices to be placed on Enterprise networks
- Consumer devices are typically located within a single Layer 2 domain in the home
- Customer expect to have the same type of services in the Enterprise / Campus but also ***across L3 boundaries***
- Device types include mobile devices (iOS, Android), printers, cameras, PCs etc.





What is Zeroconf?

- *Zero Configuration Networking*
- "**To enable communications of hosts** and services on a network that may not contain configuration services such as DNS and DHCP **without needing a guy in a white lab coat**."
- Three components of the Zeroconf architecture
  1. Addressing
  2. Naming
  3. Discovery
- Available on Safari Books



http://www.zeroconf.org/

Where is Zeroconf available?

Personal Computer Operating Systems

- Windows
- Mac OS X
- Linux

Appliances & Networking

- Printers
- Access Points
- Switches
- Routers

Mobile Devices

- Smartphones
- Tablets
- Android / iOS based

Examples, non-conclusive lists

AV Equipment

- Speakers
- Cameras
- Displays
- AV Receivers

Software

- Applications
- Network Management Software

Small Business Pro
Security Appliance Configuration Utility

http://www.cisco.com/web/sbtg/gui_mockups/sa520w_v1119/bonjourConfig.htm

What is Service Discovery?

A subset of Zeroconf

- DNS-SD defined by RFC 6763 "DNS-Based Service Discovery"
- Typically transported via multicast DNS (mDNS)
- mDNS defined in RFC 6762 "Multicast DNS"

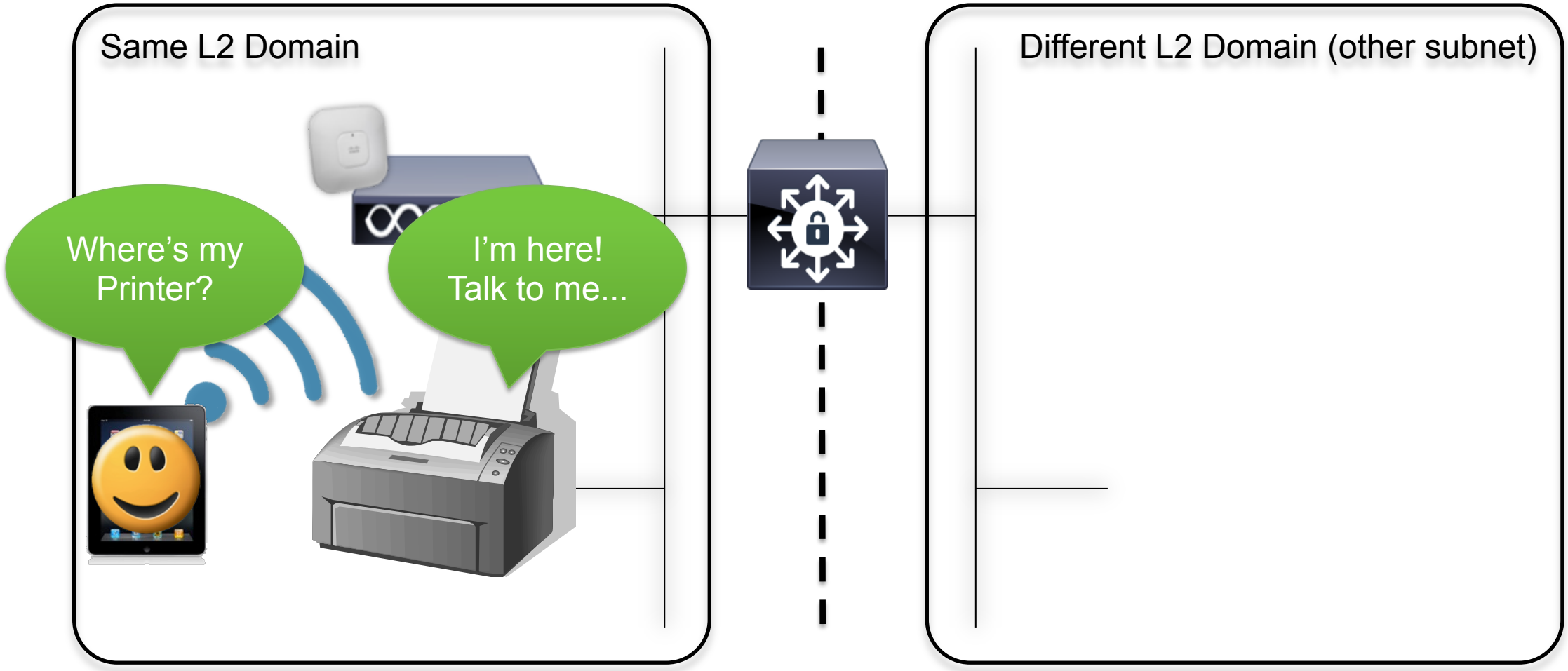
Dynamically find resources like Printers or Displays

- No central infrastructure required (no DHCP, no DNS, …)
- Works on link-local only addresses, if need be

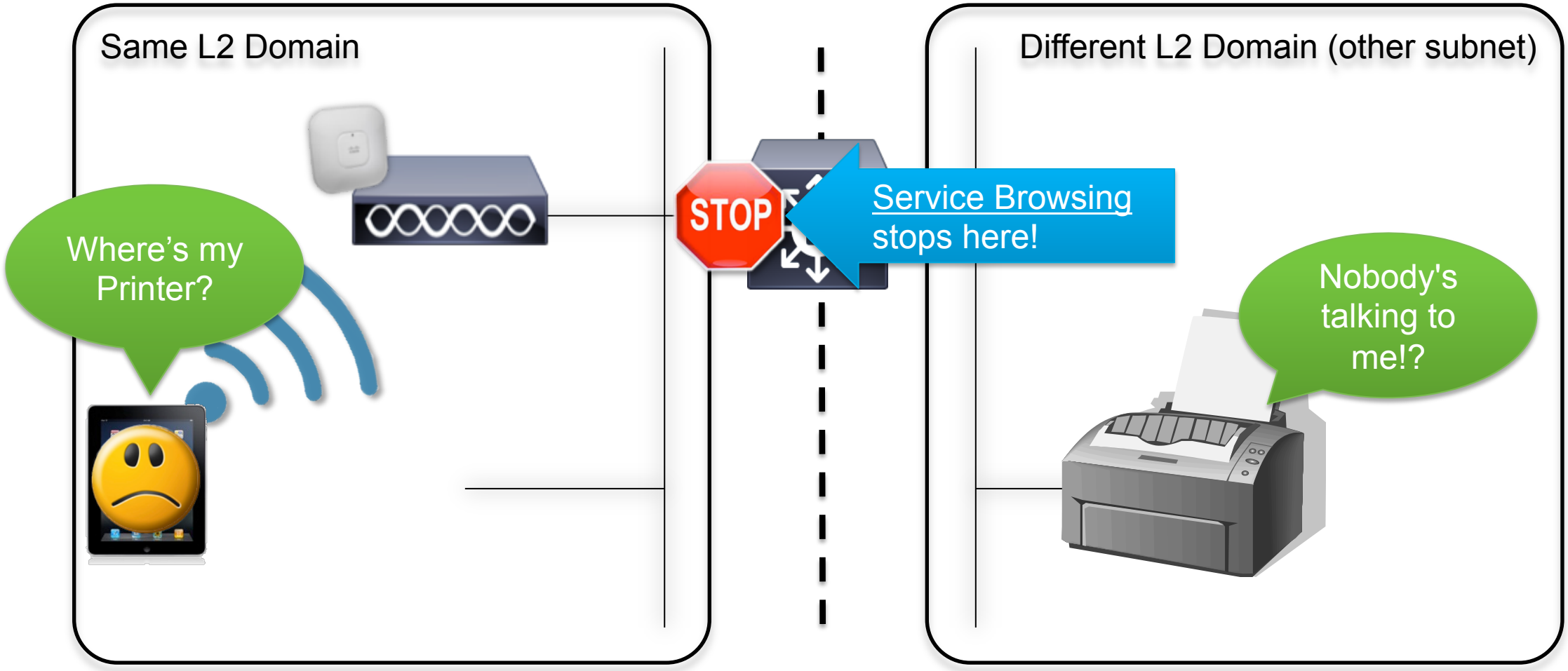
IP address family agnostic

- IPv4
- IPv6

The Need for Service Discovery Gateway



The Need for Service Discovery Gateway (cont.)

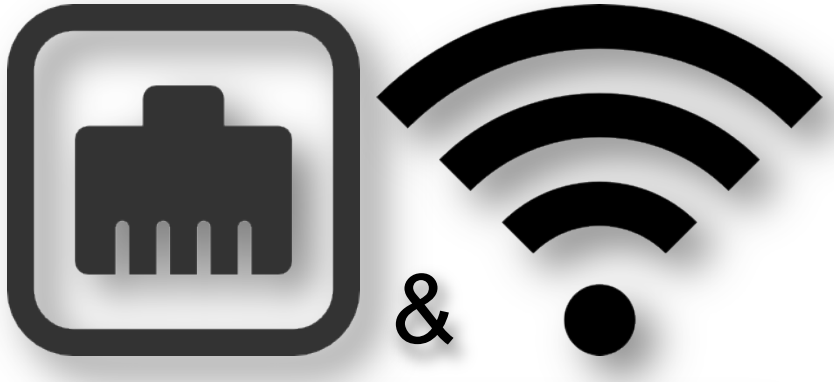


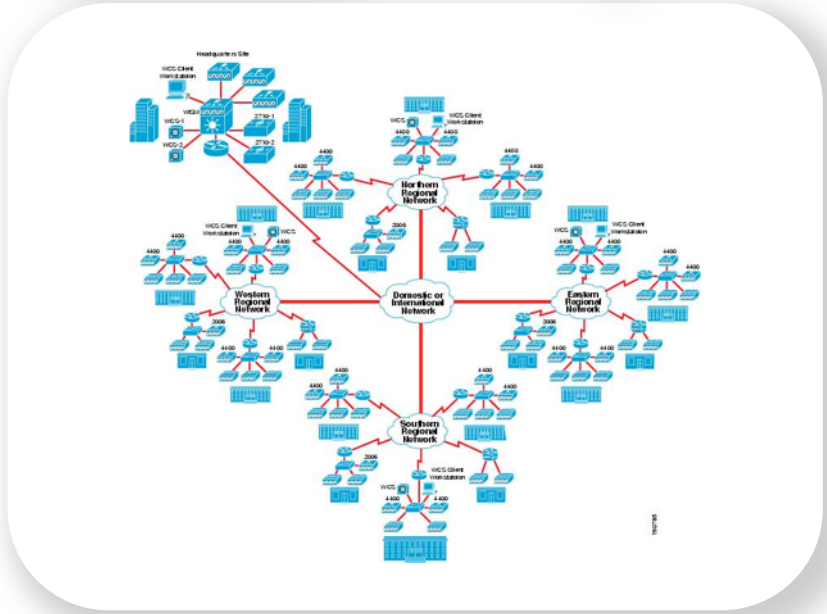
Cisco Service Discovery Gateway

- On IOS (wired & wireless)
- Enables Zeroconf service discovery across VLANs
  - Easy to manage
  - Designed to scale
  - Transparent to consumer devices
  - IPv4 and IPv6
- Network-wide solution
- Enhances BYOD on the campus
- Can be combined with role-based access control, ‘Better Together’

Where is this needed?

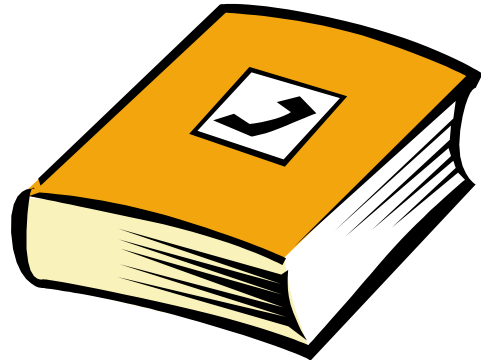
- Typically in wired / wireless scenarios
  - Wired printers / Wireless devices
  - Wired Displays (Apple TVs), Wireless devices
- Large-Scale Environments
  - Buildings with multiple floors
  - General L2 segregation using VLANs
- At first Layer 3 Hop / Distribution Layer
- Think "DHCP helper" for Service Discovery





Service Discovery vs. Access Control

- Service Discovery
  - Is your Phone Book. Tell me, where I can reach Mr. Printer
  - Doesn't necessarily mean that you can actually reach / talk to Mr. Printer
- Access Control
  - Is like caller screening
  - Even if a person is not listed in the phone book, you might call that person because you know the number
  - "I know Mr. Printer is at 1.2.3.4, let's call him even if I don't see him in the phone book"
- Better Together
  - use the phone book for easy lookup (Service Discovery)
  - use the caller screening for security (ACL / SGT / SGACL ...)

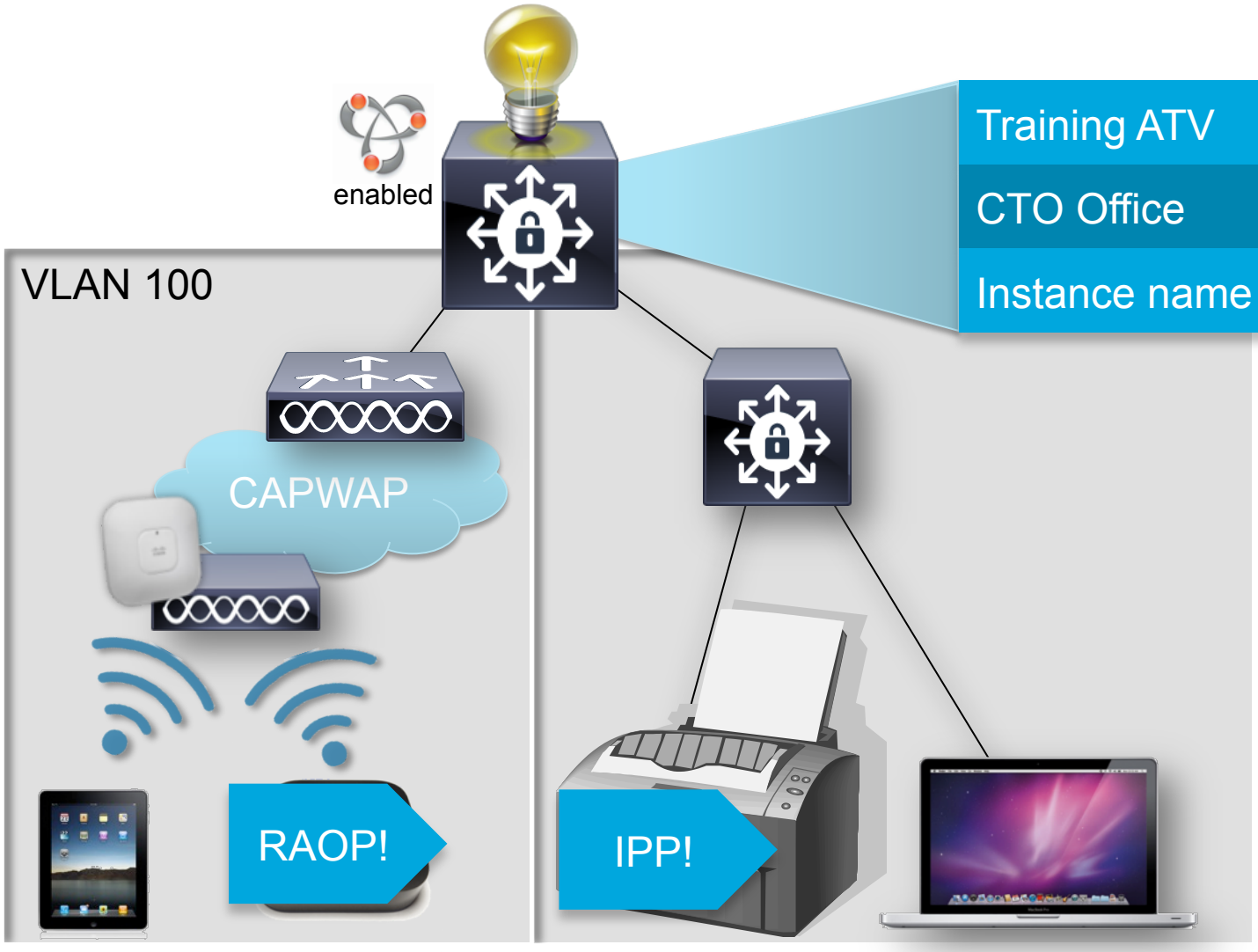


Benefits

- **Boundary elimination.** Service discovery crossing L2 domains
- **Service control**. Like with ACLs, the visibility of services can be controlled
- **Granular Filter Capabilities.** On either a global or per-interface basis
- **Multi-Protocol Support.** IPv4 and IPv6
- **Converged Access.** Wired and wireless network support
- **BYOD readiness.** Provide transparent access to user devices

How does it work?

How does it work?

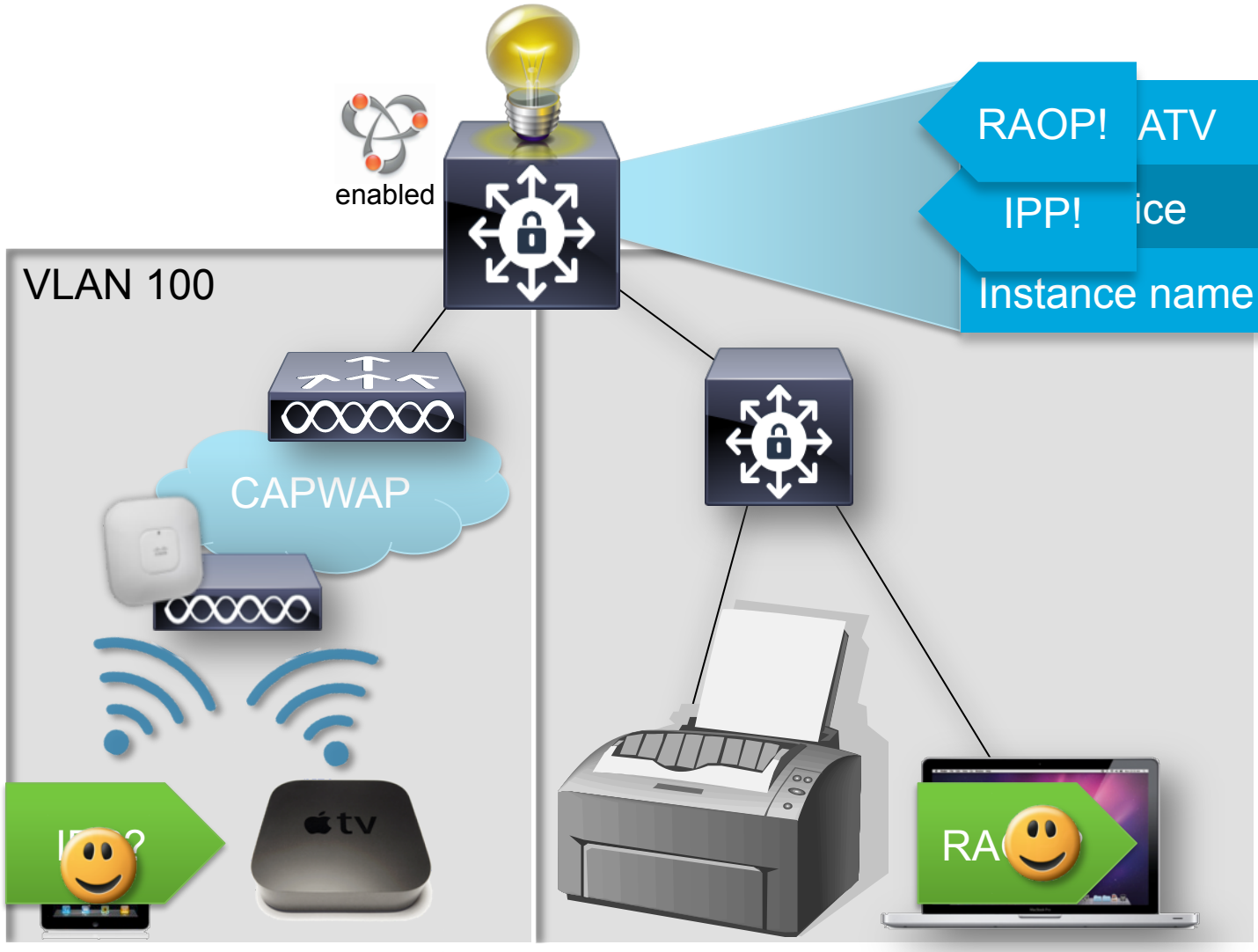


Training ATV	RAOP Service	VLAN 100
CTO Office	IPP Service	VLAN 200
Instance name	Other Services	VLAN XYZ

Advertisement

- Link Local Multicast seen in SAME VLAN only
- Cached at Gateway
- Instance Name, Type, Interface Name, TTL, Resource Record data etc.

How does it work?

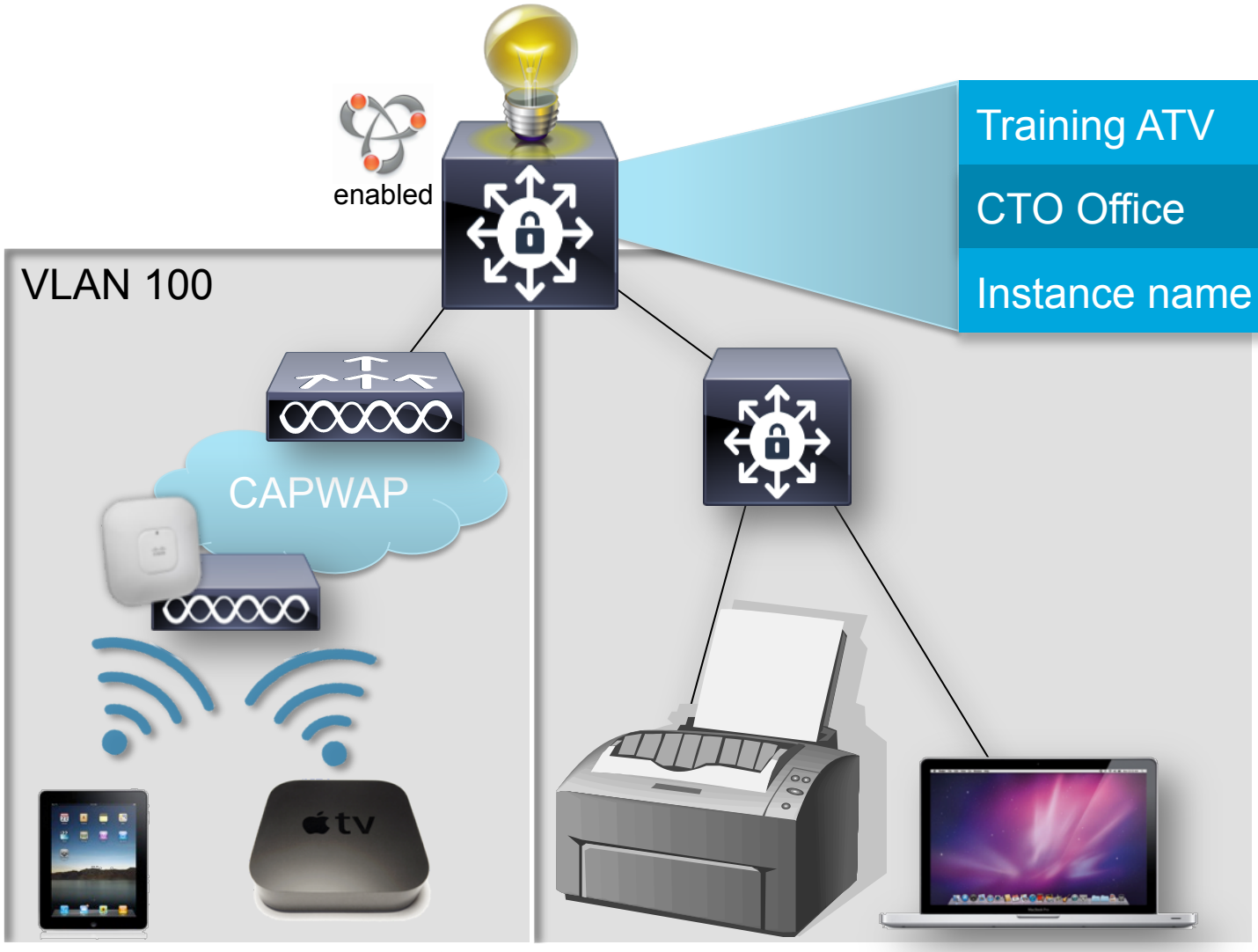


RAOP!	ATV	RAOP Service	VLAN 100
IPP!	ice	IPP Service	VLAN 200
Instance name		Other Services	VLAN XYZ

Query

- Service query seen and answered by Gateway
- Original Device not bothered
- Cache maintenance done on TTL / when device goes offline

How does it work?

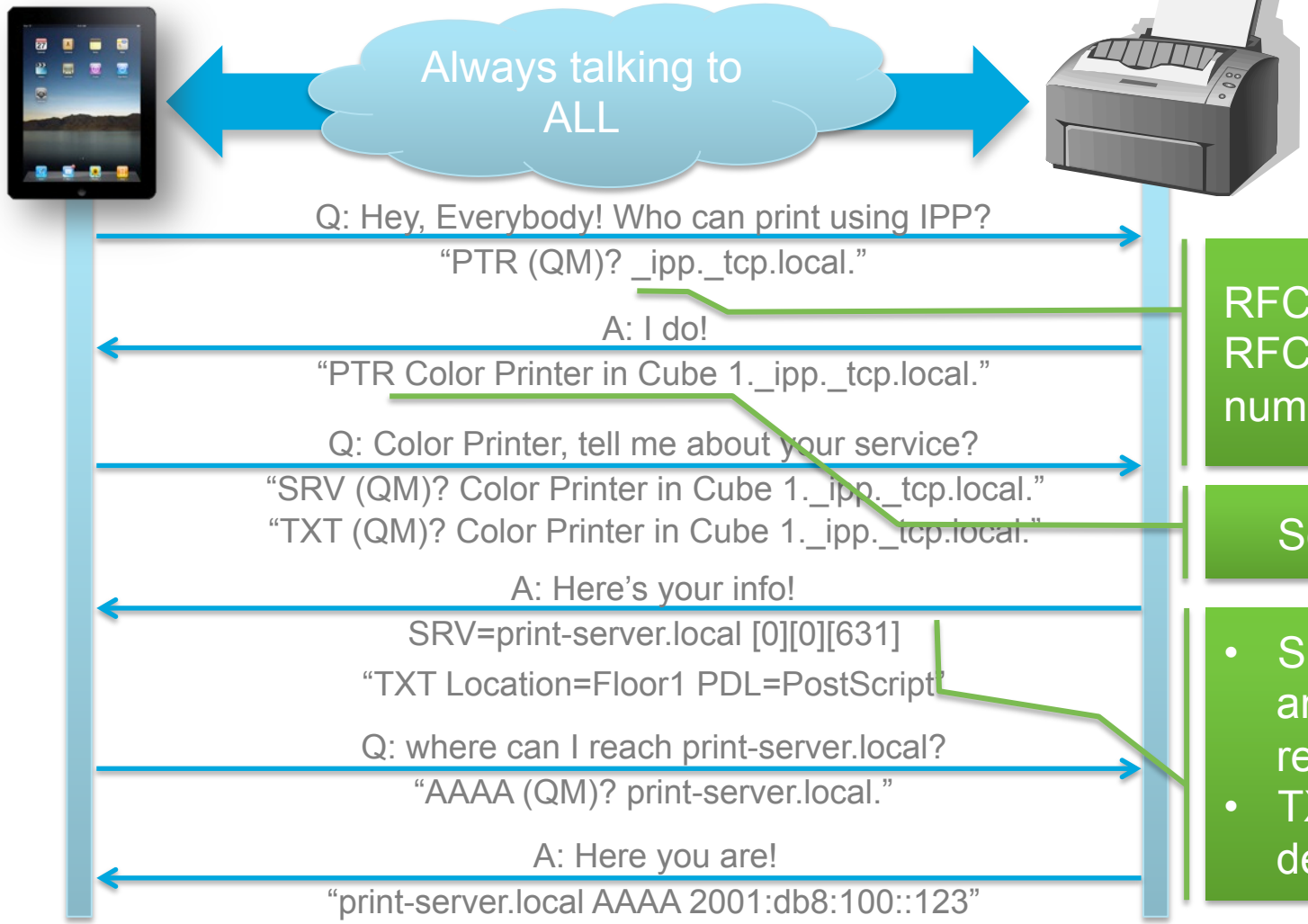


Training ATV	RAOP Service	VLAN 100
CTO Office	IPP Service	VLAN 200
Instance name	Other Services	VLAN XYZ

Cache Entry removed when

- Device disappears when TTL expired
- Service is explicitly removed by Device

Service Discovery in Detail



RFC 2782 (DNS SRV Service Types) and RFC 6355 (Service name and Port numbers)

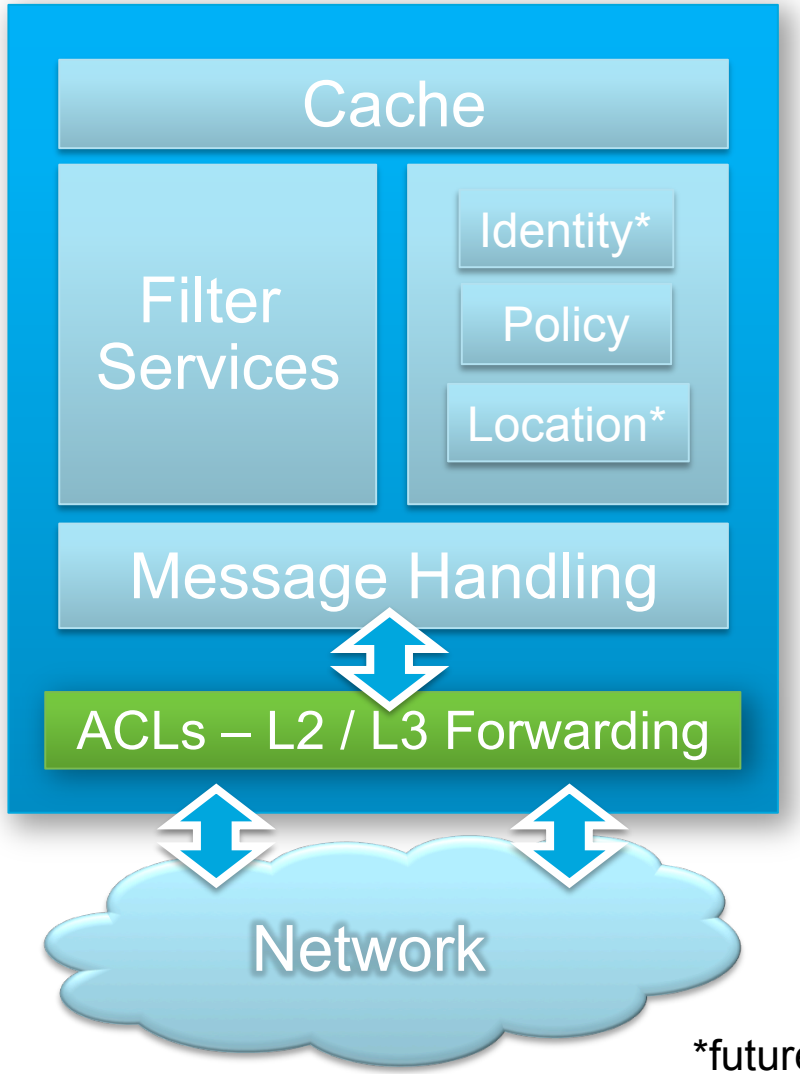
Service Name, Unicode, Descriptive

- SRV record contains the hostname and port where the service can be reached
- TXT record has additional info describing the service.

Implementation Details

Service Discovery Gateway Architecture

- Cache / Directory of available services
- Filter Services
  - Permit / Deny globally -or- on per-interface basis
  - Inbound & outbound filters
  - Service Types and Instances
  - Wildcarding / Regular Expressions
  - ACLs for Service Discovery
- Process Service Discovery message-set
  - Includes Proxy functions
- Combination with other technologies
  - RBAC with ACLs / SGTs / SGACLs
  - Unicast / multicast forwarding



*future

Service Discovery Gateway for Cisco IOS

Initial Release Features

- Gateway service at Layer 3, proxy across Layer 3 boundaries
- Wired and wireless VLANs
- Service-based filters on ingress and egress, per VLAN
- Build cache, distribute only when configured
- Limited Role-Based Access Control
- Service logging
- Design target: Support for up to 14,000 services per switch, no pre-set limit for number of clients per service

Service Discovery Gateway for Cisco IOS – Platforms

- Catalyst 3560, 3750, current 4500 platforms
  15.2E release, target FCS August 2013
- Catalyst 3760 and 3850, Catalyst 5760 Wireless LAN Controller
  Target FCS August-Sept 2013
- Catalyst 6500
  Q3 CY13
- ISR-G2, ASR1000 and ISR 4400 series
  Q4 CY13

Futures are Subject to Change Without Notice

Configuration

Basic Configuration

- Minimal, working configuration shown below
- Allows all services announcements into the cache
- Responds to all service queries with cache content
- Global configuration, applies to all SVI / VLAN interfaces

```
service-list mdns-sd permit-all 10
service-routing mdns-sd
 service-policy permit-all in
 service-policy permit-all out
 redistribute mdns-sd
```

Global vs. Per-Interface

- Enabling Service Discovery Gateway functionality
- Filters define what gets accepted and what not (in / out)
- Interface Filters take precedence over Global Filters

Global Configuration

```
service-routing mdns-sd
  service-policy <service-list> in
  service-policy <service-list> out
  redistribute mdns-sd
!
```

Per-Interface Configuration

```
interface Ethernet0/0
ip address 172.16.31.4 255.255.255.0
 ipv6 address 2001:DB8:1:100::/64 eui-64
 ipv6 enable
 service-routing mdns-sd
  service-policy <service-list> in
  service-policy <service-list> out
!
```

Service Filters

- Filters are like ACLs for services
- Queries, Announcements, Types and Instance names
- Define what should be learned and responded to
- Applied globally or on a per-Interface basis
- **Default action is Deny!**

- match on
  - service-type
  - service-instance
  - message-type
- either deny, permit
- sequenced
- uses regular expression (instance & type)

```
service-list mdns-sd <name> {permit|deny} <sequence_number>
  match message-type {query|announcement|any}
  match service-instance <instance-name>
  match service-type <DNS service type string>
```

Filter Definition / Example

- Service-Type:
  - Uses Regular Expression String
  - matches the SRV advertisements and queries
  - Example are _ipp._tcp (Printing), _xmpp._tcp (Jabber)
- Service-Instance
  - Uses Regular Expression String
  - matches the explicit service instance (a service name)
  - service instances can use Unicode, White Space etc.
  - Example “my fåncy printer in røøm 123._ipp._tcp”
- Message-Type
  - enumeration
  - either ‘any’ or ‘query’ or ‘announcement’
- First Match, Logical ‘AND’ of Matches

Filter denies AirPlay Services, allow all the rest:

```
service-list mdns-sd limited deny 10
 match message-type announcement
 match service-type _raop\._tcp
!
service-list mdns-sd limited deny 20
 match service-type _airplay\._tcp
!
service-list mdns-sd limited permit 30
 match service-type .*
!
```

Service Redistribution

- Redistribution of service announcements (removal of / adding a service)
- Either configured globally or per interface
- **ENABLED:** announcements will be forwarded to other interfaces instantly

  pro: quicker update of client info
  con: more announcements / multicasts
- **DISABLED:** only a query by a client will result in a response by the cache

  pro: less announcement traffic
  con: clients may use outdated information (until it times out) or don't see new services instantly

mDNS Show Commands

- show cache content
- show requests
- show statistics
- show interfaces

```
mDNS CACHE
=================================================================================================
[<NAME>]                          [<TYPE>][<CLASS>] [<TTL>/Remaining] [Accessed] [If-idx] [<RR Record Data>]

_ssh._tcp.local                   PTR     IN      4500/4288   9        2        Lab Mac._ssh._tcp
_sftp-ssh._tcp.local              PTR     IN      4500/4288   9        2        Lab Mac._sftp-ssh
_services._dns-sd._udp.local      PTR     IN      4500/4288   1        2        _rfb._tcp.local
_rfb._tcp.local                   PTR     IN      4500/4288   9        2        Lab Mac._rfb._tcp
Lab Mac._ssh._tcp.local           TXT     IN      4500/4288   3        2        (1)''
Lab Mac._sftp-ssh._tcp.local      TXT     IN      4500/4288   3        2        (1)''
Lab Mac._rfb._tcp.local           TXT     IN      4500/4288   3        2        (1)''
```

Conclusion

Conclusion & Summary

Service Discovery Gateway: IOS-based solution to address real customer pain!

Scalable Architecture	• Network-wide solution at L3 / distribution layer • Wireless and wired connectivity • Built-in cache management and service discovery
Unified Access	• Available for Unified Access, WLCs, Catalyst and WAN / ISRs
Network Wide Security	• Service filters to control visibility and access • Enhanced with Identity Service Policy, ISE, SGT & SGACL
Manageable BYOD	• Clients operate transparently • IPv6 and IPv4 fully supported

Video / Demonstration

- **Thank you!**
- Please complete the post-event survey
- Join us for upcoming webinars:
  Register: www.cisco.com/go/techadvantage

  Follow us @GetYourBuildOn