TOMORROW starts here.

CISCO

Cisco live!

# IOS Service Discovery Gateway Simplify Mobile Device Deployments in Enterprise Networks

BRKRST-2643

Ralph Schmieder

Technical Marketing Engineer

CCIE #9680 R&S / Security

# Session Abstract

Have you ever experienced problems with service discovery on Apple devices when they reside on other subnets? Not seeing your Apple TV or printer? Fear not! Service Discovery Gateway is here to the rescue! With the proliferation of mobile devices, tablets and smartphones (also BYOD) in enterprise networks users might fail to discover services like printers, displays, and media servers among others. This is a major problem faced by many enterprise networks today and is especially acute in education and healthcare networks. Cisco is introducing a new solution in IOS and IOS XE for converged wireless and wired access that allows users to discover services overcoming those existing boundaries to unleash the true potential of BYOD. This session will introduce Cisco's new solution for enterprise-wide service discovery enhancing the Zeroconf protocol family that is widely used especially in Apple products.

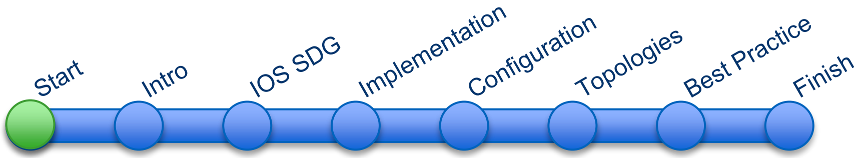
# Session Objectives

At the End of This Session, Participants Should:

- Understand what Service Discovery is
- Understand why this is a problem in todays networks
- Understand how Service Discovery works
- Know about the Service Discovery Gateway and how it addresses the described problem
- Can design and configure a SDG with filters
- Understand the benefit of deploying a SDG in a wired / wireless network and how it enhances the BYOD experience

# Agenda

- Introduction
- IOS Service Discovery Gateway
- Implementation: How does it work?
- Configuration
- Topology Considerations
- Best Practice Recommendations
- Conclusion



Start

Intro

IOS SDG

Implementation

Configuration

Topologies

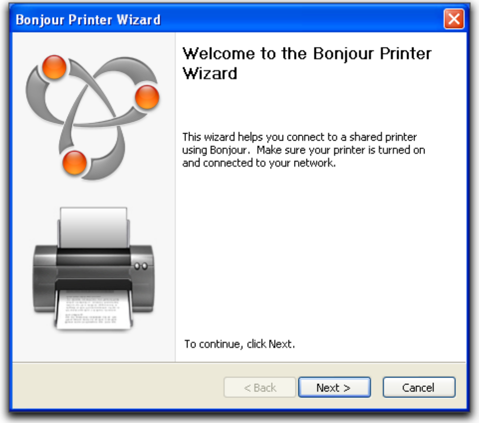
Best Practice

Finish

# Introduction

# What is this about?

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



Bonjour Printer Wizard

Welcome to the Bonjour Printer Wizard

This wizard helps you connect to a shared printer using Bonjour. Make sure your printer is turned on and connected to your network.

To continue, click Next.

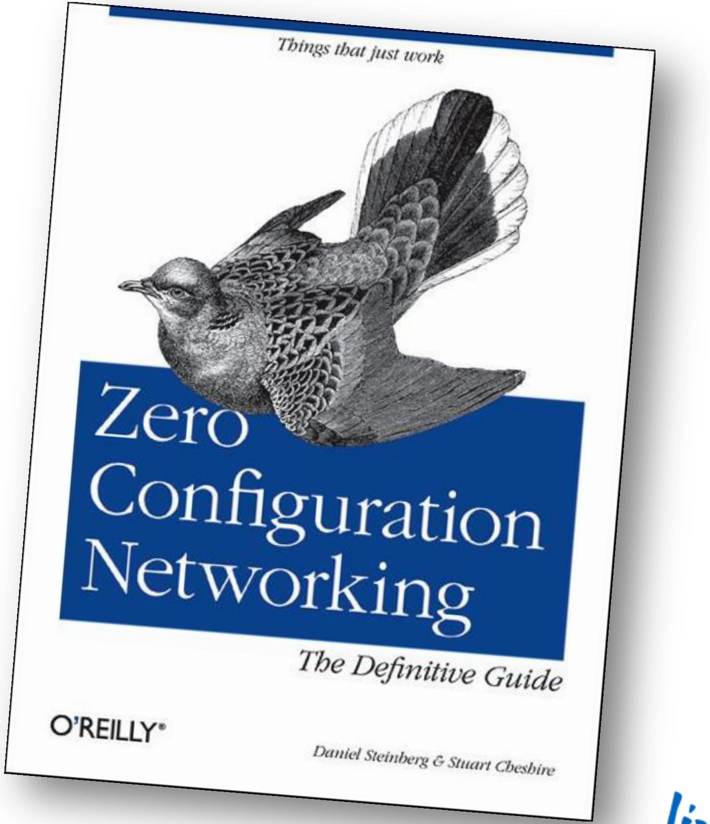
# “Bonjour technologies do not work in a scalable, sustainable fashion between different IP subnets”

Educause Higher Ed Wireless Networking Admin Group Petition —761 Signatures

# 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/


Things that just work
Zero Configuration Networking
The Definitive Guide
O'REILLY®
Daniel Steinberg & Stuart Cheshire

# 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

# 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"

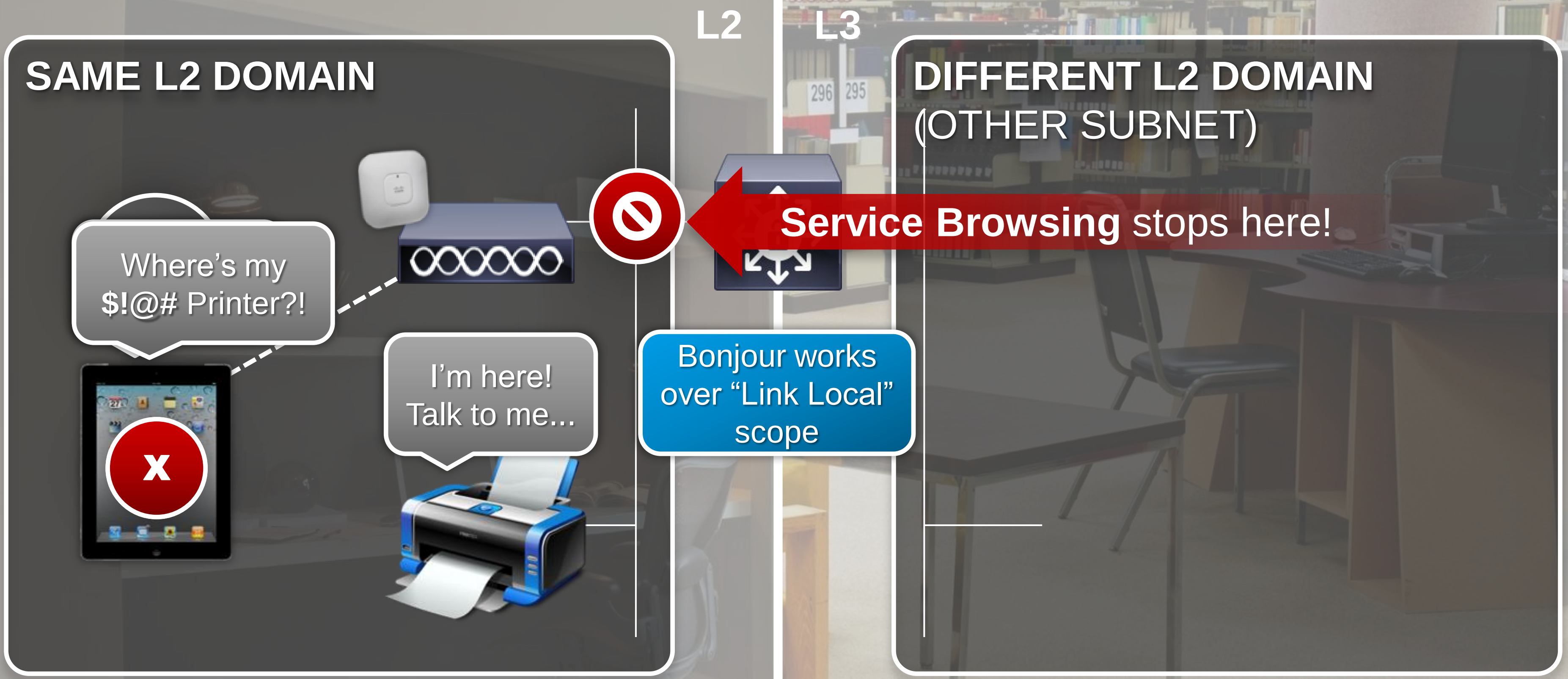
## Dynamically find resources like Printers or Displays

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

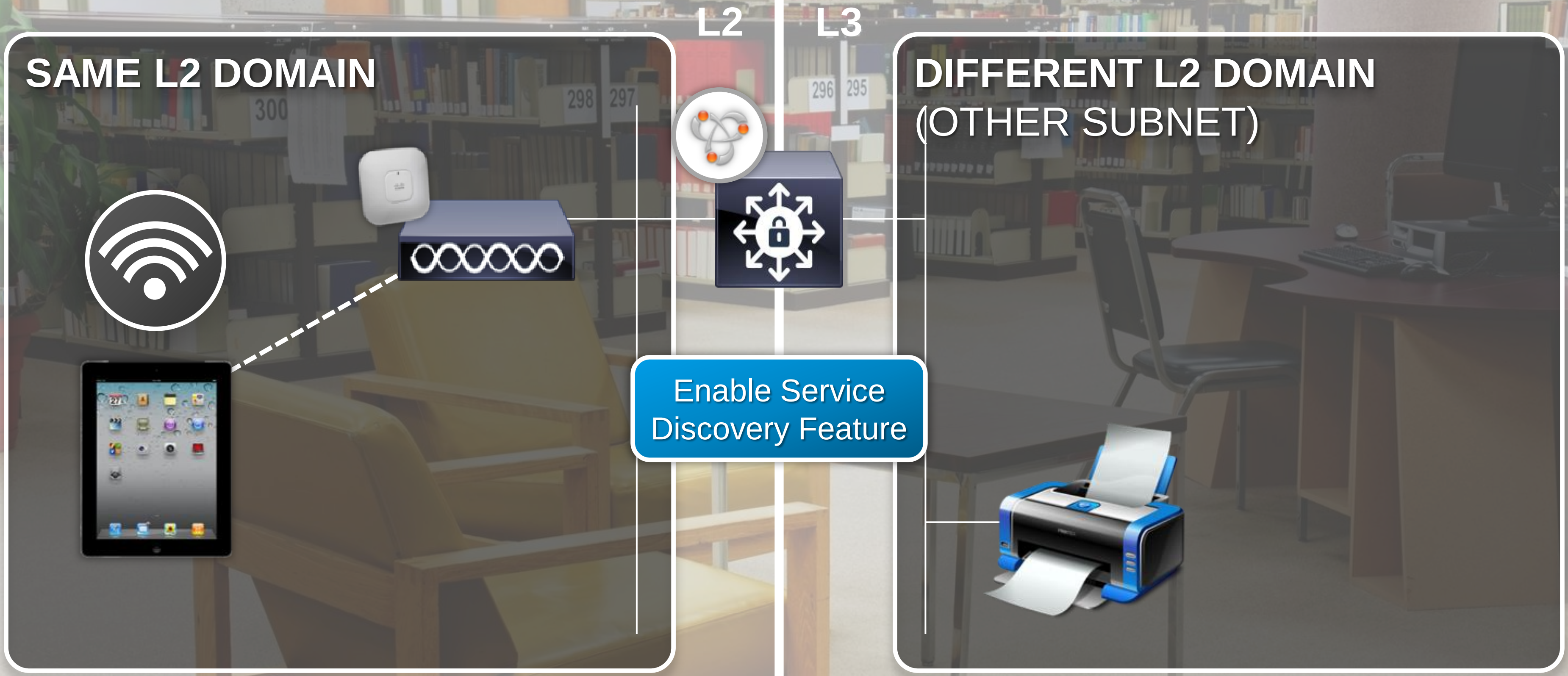
## RFC says it should be IP address family agnostic

- IPv4
- IPv6

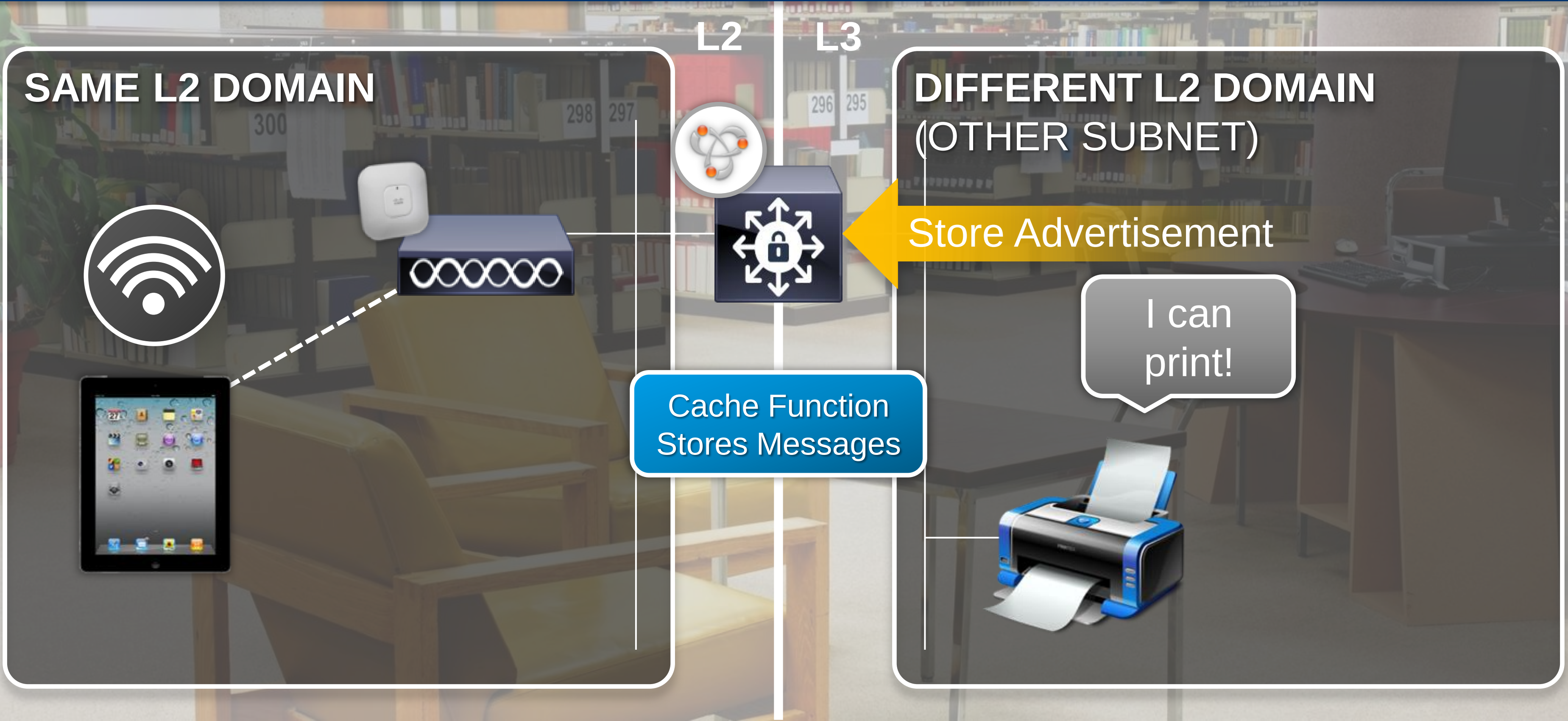
# The Issue Explained


L2
L3
SAME L2 DOMAIN
DIFFERENT L2 DOMAIN
(OTHER SUBNET)
Where's my $!@# Printer?!
I'm here! Talk to me...
x
**Service Browsing** stops here!
Bonjour works over "Link Local" scope

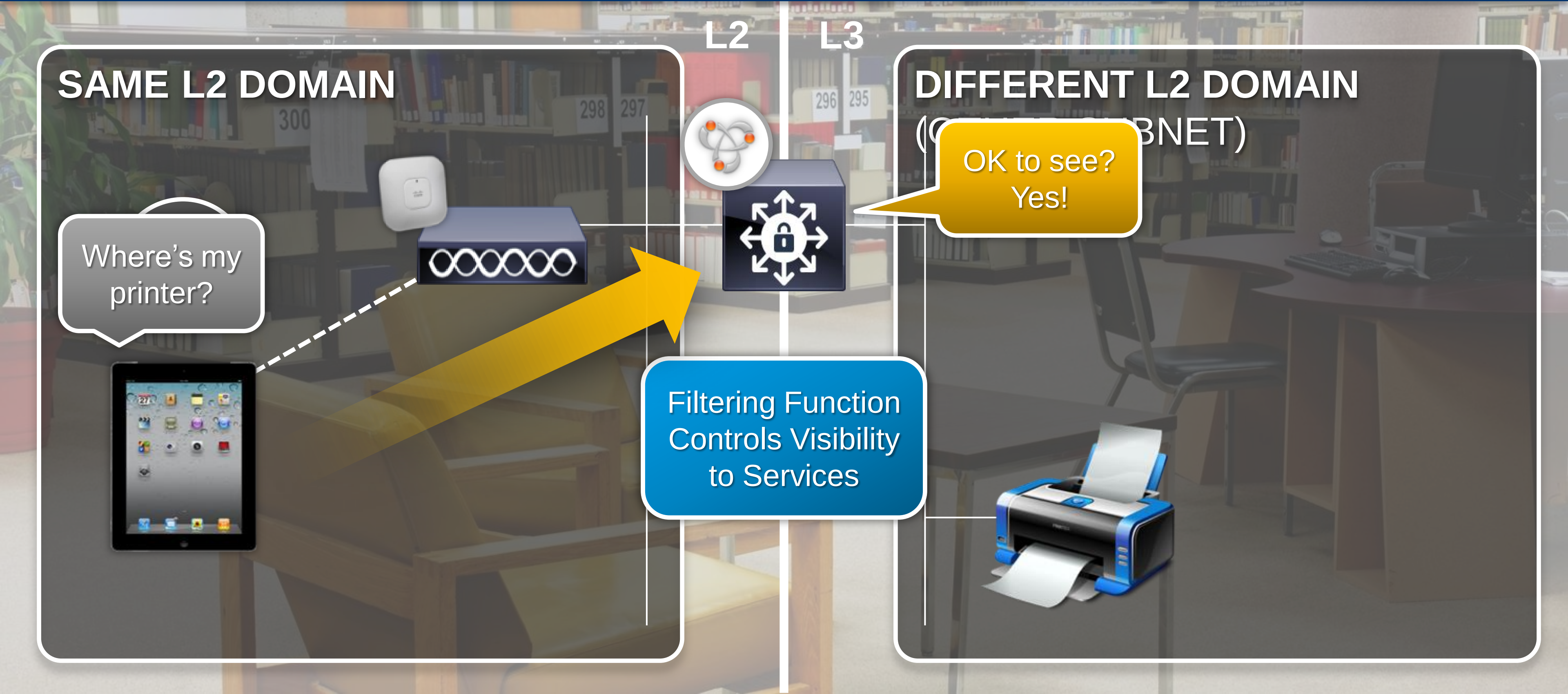
# Cisco Solution in the Network



# Cisco Solution in the Network



# Cisco Solution in the Network



L2

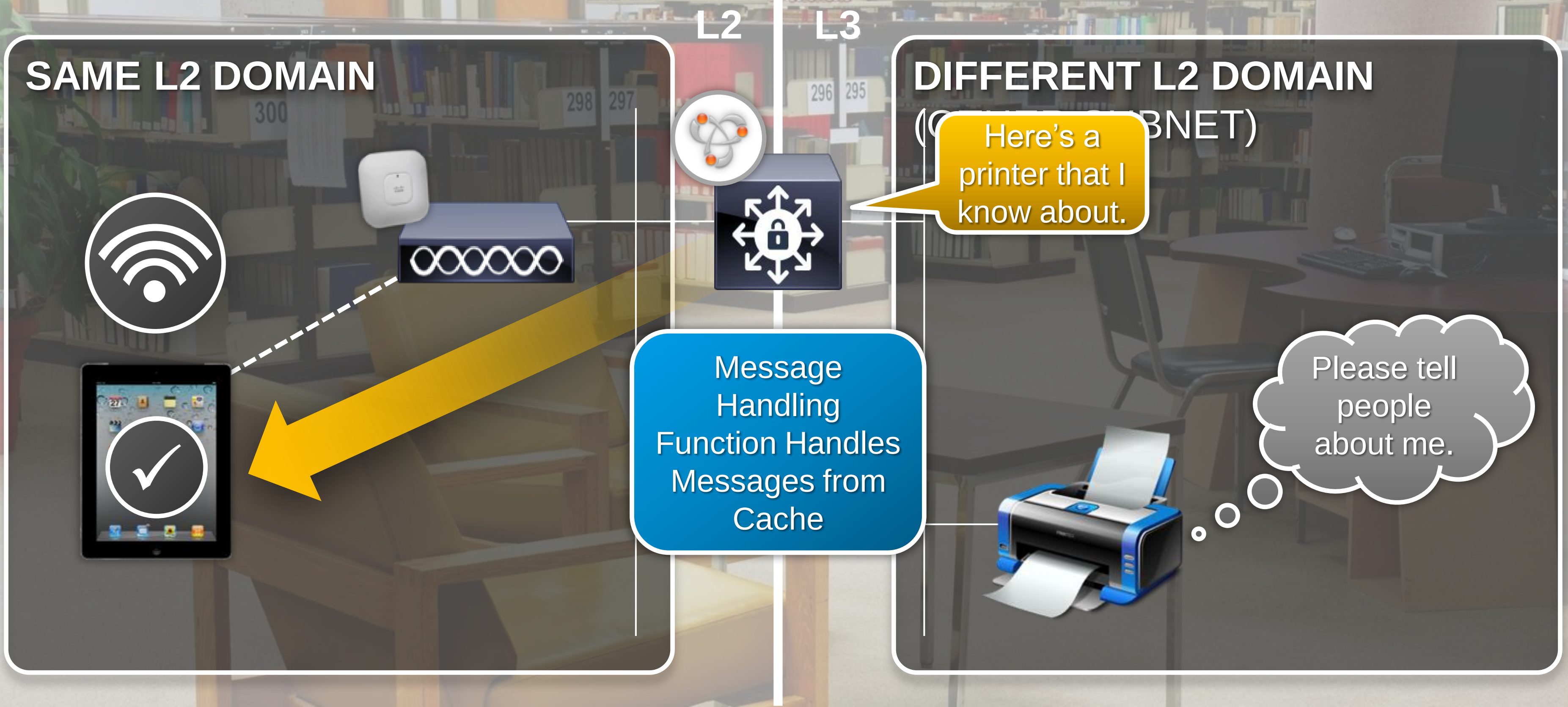
L3

SAME L2 DOMAIN

DIFFERENT L2 DOMAIN
(C[illegible]BNET)

Filtering Function Controls Visibility to Services

# Cisco Solution in the Network



L2

L3

SAME L2 DOMAIN

DIFFERENT L2 DOMAIN

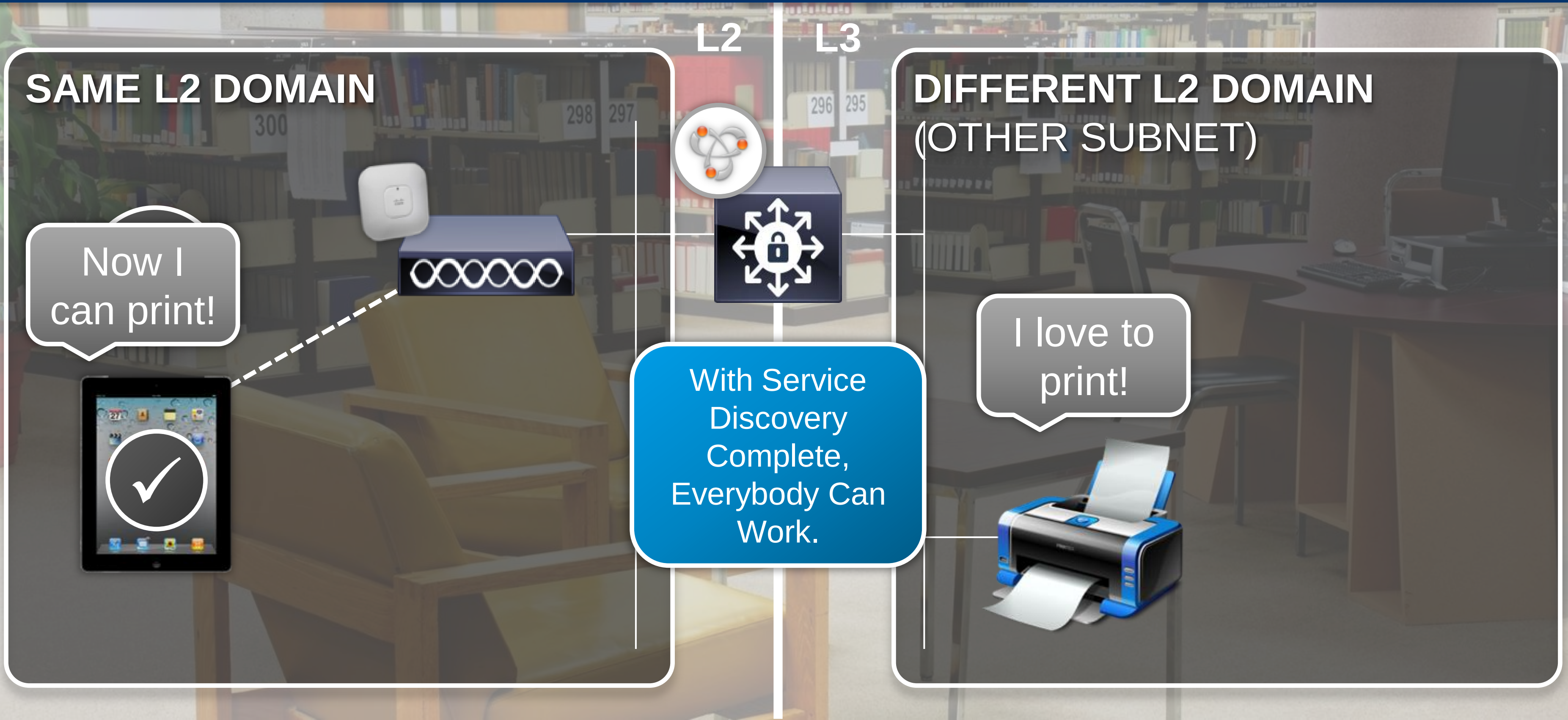
(C BNET)

Here's a printer that I know about.

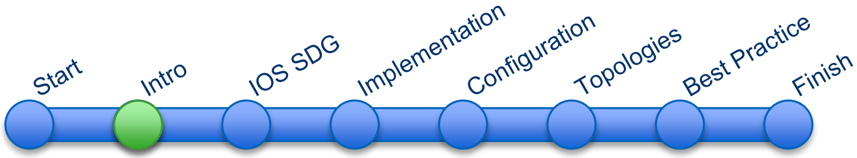
Message Handling Function Handles Messages from Cache

Please tell people about me.

# Cisco Solution in the Network



With Service Discovery Complete, Everybody Can Work.



Start

Intro

IOS SDG

Implementation

Configuration

Topologies

Best Practice

Finish

# Introducing: IOS Service Discovery Gateway

# IOS Cisco Service Discovery Gateway

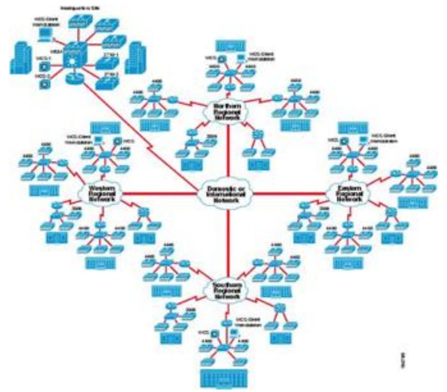
- Enables Zeroconf service discovery across VLANs
  - Easy to manage
  - Designed to scale
  - Transparent to consumer devices
  - IPv4 and IPv6
- Network-wide solution
- Enhances BYOD on the campus
- Can be combined with role-based access control, ‘Better Together’

# Where is this Needed?

Outside your home…

- Wired / Wireless
  - Printers / handheld devices
  - Displays (Apple TVs), …
- Large-Scale Environments
  - Buildings with multiple floors
  - General L2 segregation using VLANs
- Combination of both

&

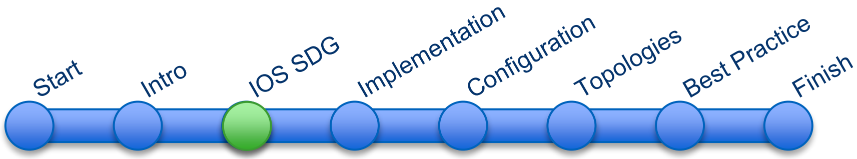

Northern Regional Network
Western Regional Network
Domestic or International Network
Eastern Regional Network
Southern Regional Network

# Service Discovery vs. Access Control

- Service Discovery
  - Is your Phone Book. What is Mr. Printer's number?
  - Can I call Mr. Printer?
- Access Control
  - Phone book needed if known number?
  - Do we allow the phone call?
- Better Together
  - use the phone book for easy lookup (Service Discovery)
  - Use 'caller screening' for security (e.g. ACLs)

# Benefits and Considerations

| Benefits | Considerations |
|---|---|
| **Eliminate Boundaries.** Allow service discovery crossing VLAN boundaries | **Topology Support:** Current implementation supports only one hop (access devices connected to a distribution switch) |
| **Granular application of filters.** On either a global or per-interface basis | **Filtering** per segment**.** Role Based Access will be addressed in a later phase |
| **Control of advertised and consumed services.** Like with ACLs, the visibility of services can be controlled | **No Hierarchy.** Flat namespace implied by protocol specification |
| Supports both **IPv4 and IPv6** | **Endpoints** may have difficulties with longer lists |
| Simultaneous integrated **wired and wireless network support** | |
| **BYOD readiness** – the service is transparent to end devices | |



Start

Intro

IOS SDG

Implementation

Configuration

Topologies

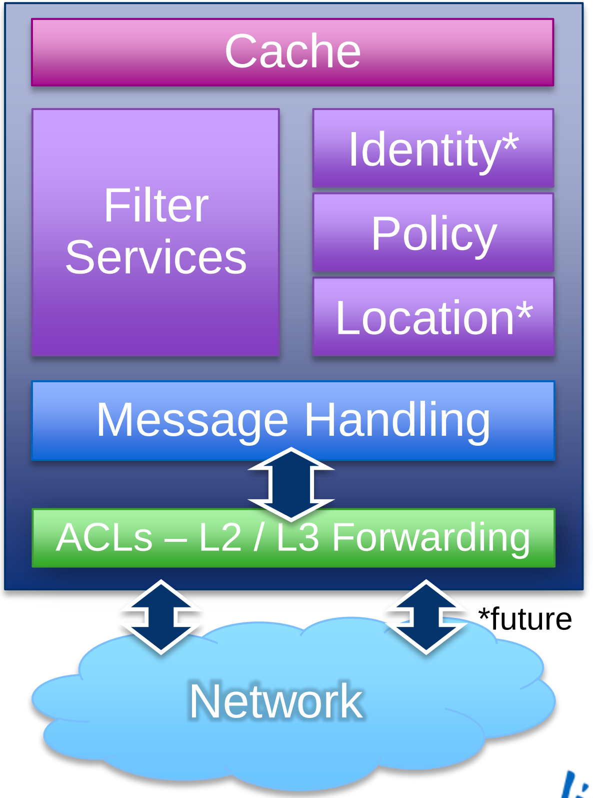
Best Practice

Finish

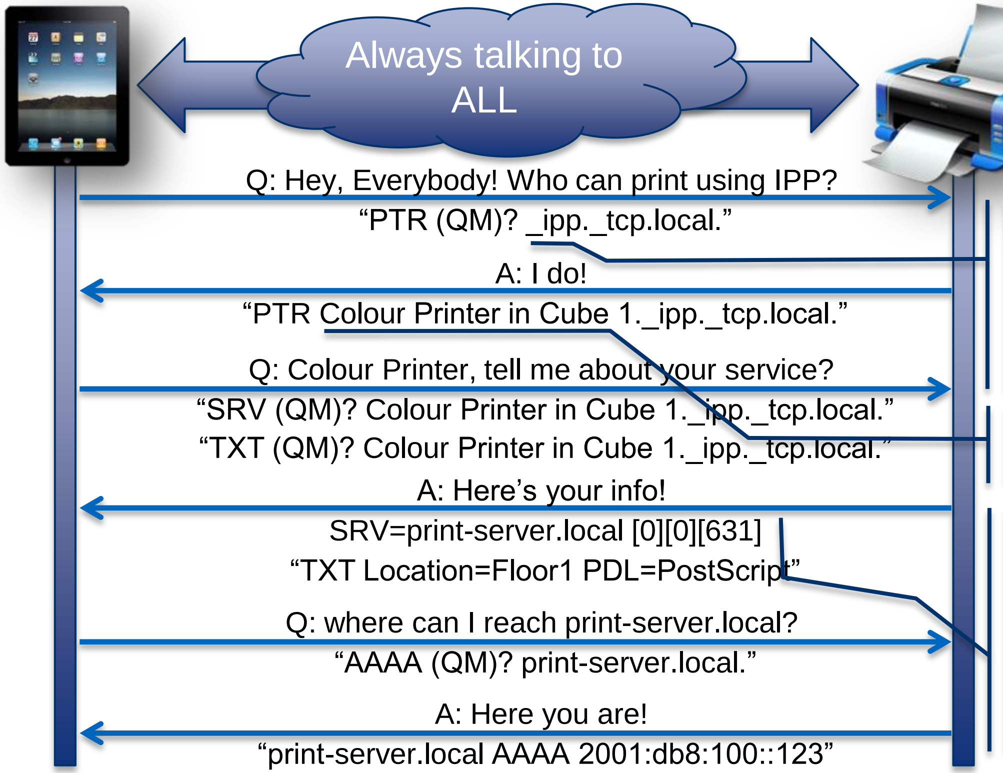
# Implementation

# 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 mDNS
- Process mDNS message-set
  - Includes Proxy functions
- Combination with other technologies
  - RBAC with ACLs / SGTs / SGACLs
  - Unicast / multicast forwarding



# Service Discovery "Conversation"



Q: Hey, Everybody! Who can print using IPP?
"PTR (QM)? _ipp._tcp.local."

A: I do!
"PTR Colour Printer in Cube 1._ipp._tcp.local."

Q: Colour Printer, tell me about your service?
"SRV (QM)? Colour Printer in Cube 1._ipp._tcp.local."
"TXT (QM)? Colour Printer in Cube 1._ipp._tcp.local."

A: Here's your info!
SRV=print-server.local [0][0][631]
"TXT Location=Floor1 PDL=PostScript"

Q: where can I reach print-server.local?
"AAAA (QM)? print-server.local."

A: Here you are!
"print-server.local AAAA 2001:db8:100::123"

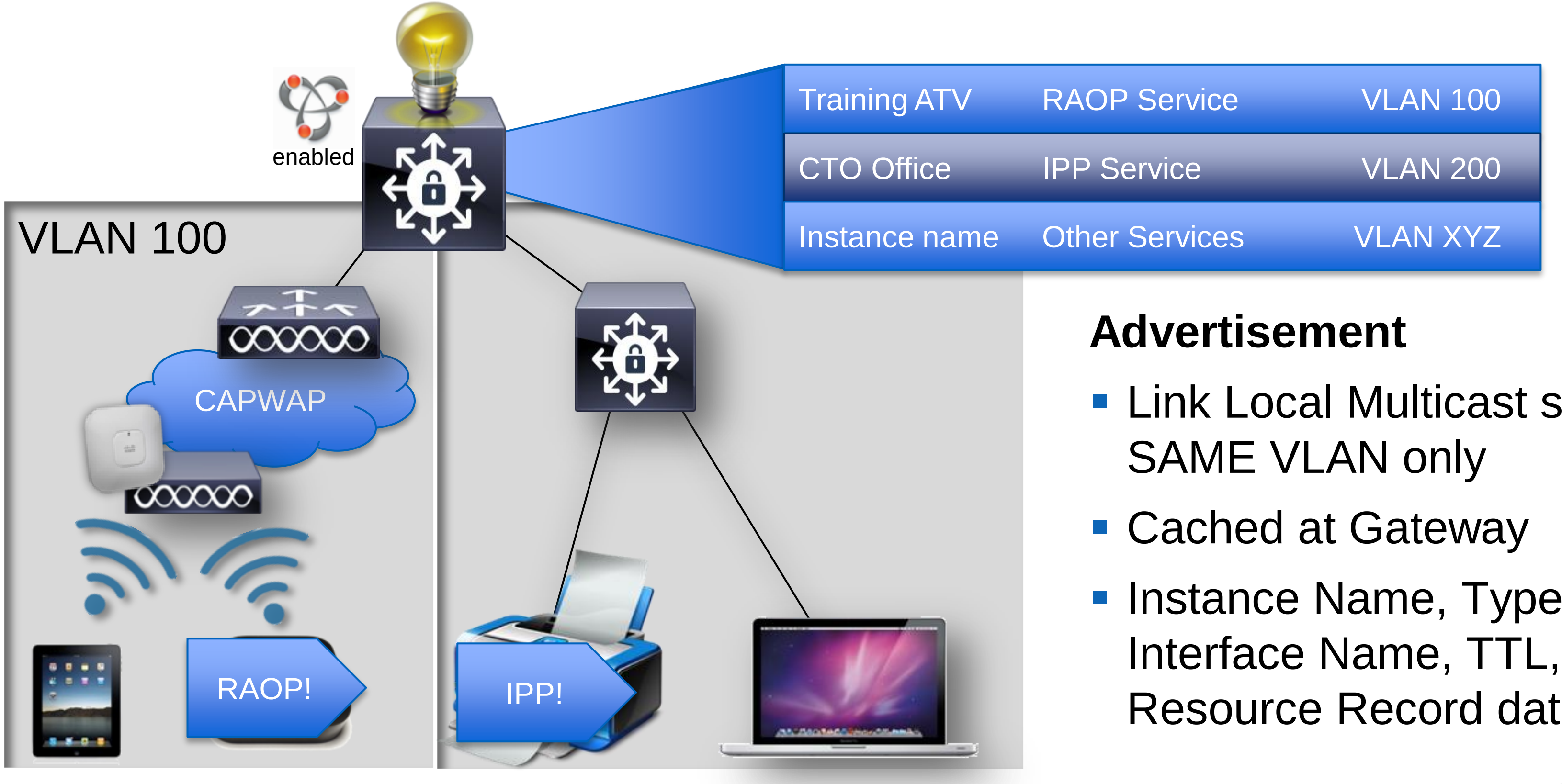
RFC 2782 (DNS SRV Service Types) and RFC 6355 (Service name and Port numbers)

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.

# SDG Demonstration Video #1

# Service Discovery Across Subnets

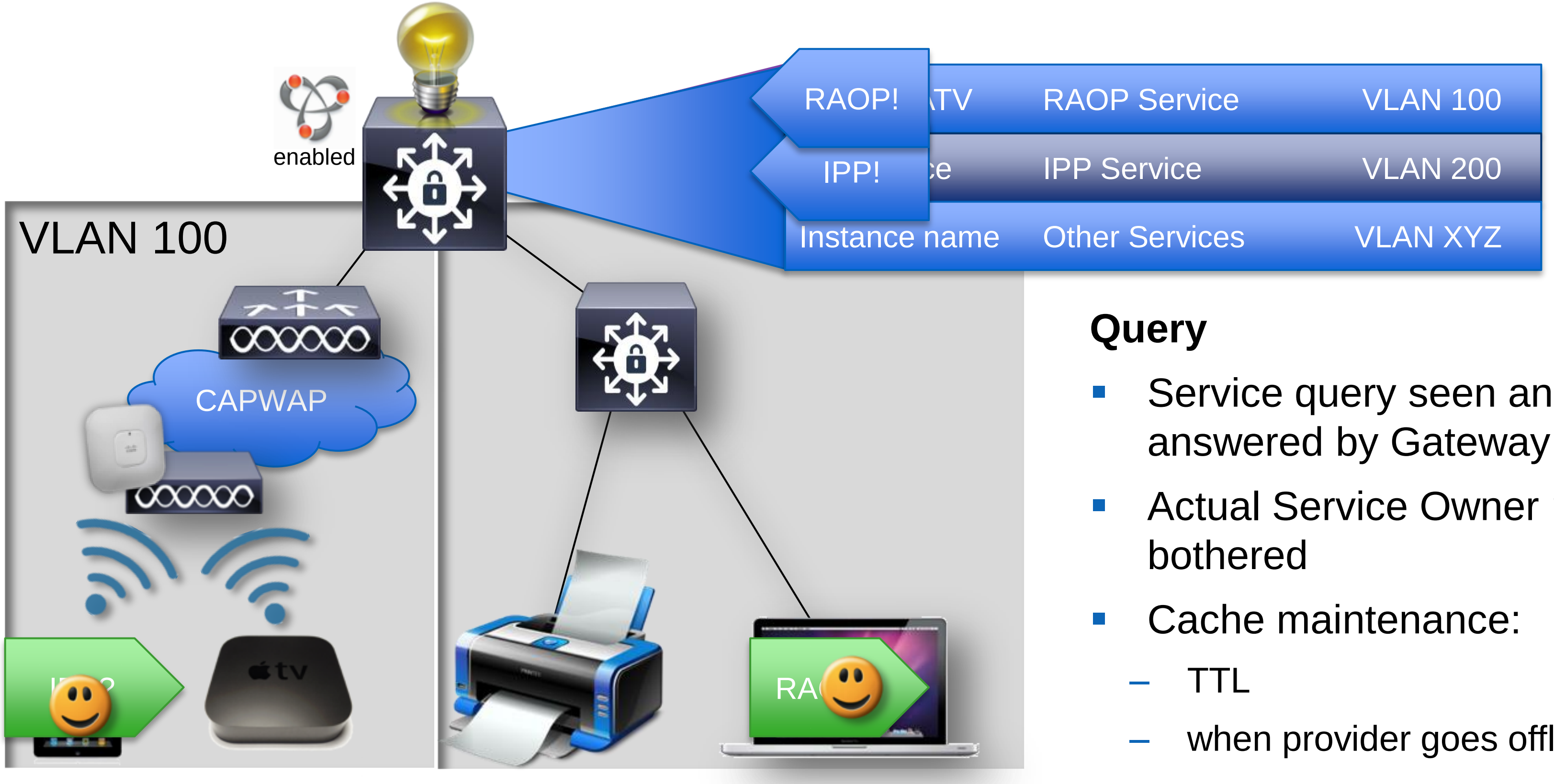


| | | |
|---|---|---|
| Training ATV | RAOP Service | VLAN 100 |
| CTO Office | IPP Service | VLAN 200 |
| Instance name | Other Services | VLAN XYZ |

## Advertisement

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

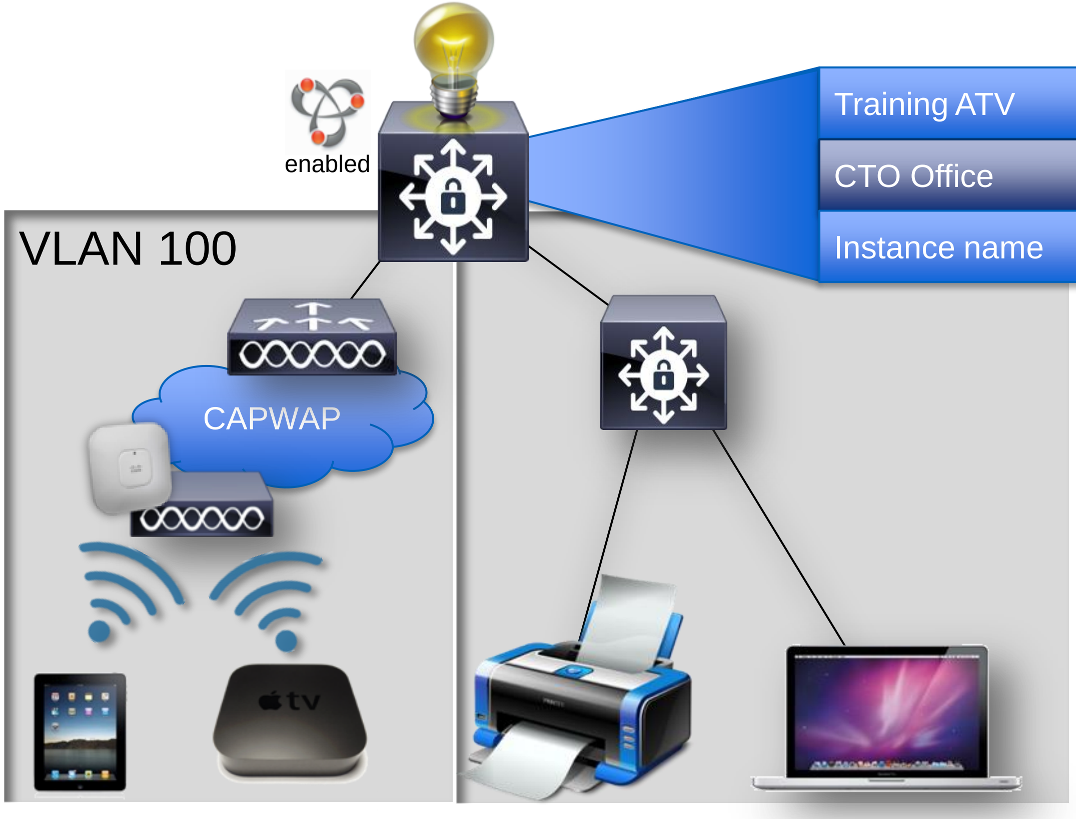
# Service Discovery Across Subnets



## Query

- Service query seen and answered by Gateway
- Actual Service Owner not bothered
- Cache maintenance:
  - TTL
  - when provider goes offline

# Service Discovery Across Subnets



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

**Cache Entry removed when**

- Device disappears / TTL expires
- Service is explicitly removed by Device*

* no example shown

# Service Discovery Gateway for Cisco IOS

- Initial Release Features
  - Gateway service at Layer 3, proxy across Layer 3 boundaries
  - Wired and wireless VLANs
  - mDNS service-based filters on ingress and egress, per VLAN
  - Build cache, cache management
  - Role-Based Access Control (Phase 1)
  - Design target: Support for up to 10,000 services per gateway, no pre-set limit for number of clients per service
- At-a-Glance "What is Zero Configuration Networking?" – CCO (Jul 2013)
  - Includes "What is The Cisco Service Discovery Gateway?"
  - http://www.cisco.com/en/US/partner/products/hw/switches/ps4324/product_at_a_glance_list.html

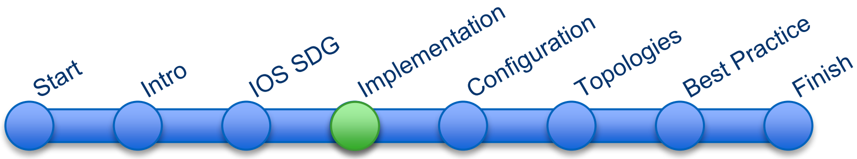
# Service Discovery Gateway for Cisco IOS

## Platform Support

- Catalyst 3k and 4k / Sup7E platforms
  15.2(1)E and 3.5.0E
- Catalyst 3650 and 3850
  3.3.0SE
- Catalyst 5760 Wireless LAN Controller
  3.3.0SE
- Catalyst 6500
  15.1(2)SY
- ISR-G2
  15.4(1)T
- ASR 1000
  3.11S

# Release Documentation

- Catalyst 6500
  - http://www.cisco.com/en/US/docs/ios-xml/ios/ipaddr_dns/configuration/15-sy/dns-15-sy-book_chapter_0100.html
- Catalyst 4500
  - http://www.cisco.com/en/US/docs/ios-xml/ios/ipaddr_dns/configuration/15-e/dns-15-e-book.html
- Catalyst 3650, 3850 and 5760 WLC
  - http://www.cisco.com/en/US/docs/switches/lan/catalyst3850/software/release/3se/multicast/configuration_guide/b_mc_3se_3850_cg_chapter_010100.html
- Catalyst 3750-E, Cisco 3750-X and 3560-X
  - http://www.cisco.com/en/US/docs/ios-xml/ios/ipaddr_dns/configuration/15-e/dns-serv-disc-gtw.html
- ASR 1000
  - http://www.cisco.com/en/US/docs/routers/asr1000/release/notes/asr1k_feats_important_notes_311s.html
- ISR
  - http://www.cisco.com/en/US/docs/ios-xml/ios/ipaddr_dns/configuration/15-mt/Service-Discovery-Gateway.html



Start

Intro

IOS SDG

Implementation

Configuration

Topologies

Best Practice

Finish

# Configuration

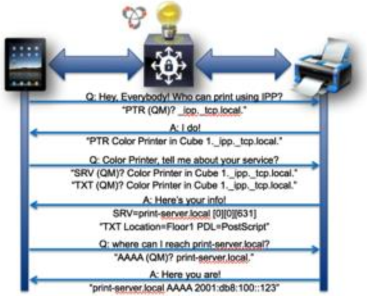
# mDNS Filters

## What is it?

- Filters are like ACLs for mDNS
- Define what service types, message types or instances are allowed to be learned
- Applied globally or on a per-Interface basis
- **Default is Deny!**

## How does it work?

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



Q: Hey, Everybody! Who can print using IPP?
"PTR (QM)? _ipp._tcp.local."

A: I do!
"PTR Color Printer in Cube 1._ipp._tcp.local."

Q: Color Printer, tell me about your service?
"SRV (QM)? Color Printer in Cube 1._ipp._tcp.local."
"TXT (QM)? Color Printer in Cube 1._ipp._tcp.local."

A: Here's your info!
SRV=print-server.local [0][0][631]
"TXT Location=Floor1 PDL=PostScript"

Q: where can I reach print-server.local?
"AAAA (QM)? print-server.local."

A: Here you are!
"print-server.local AAAA 2001:db8:100::123"

```
 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

- First Match, Logical ‘AND’ of Matches
- Use of RegExp for Strings
- Service-Type
  - matches the SRV advertisements and queries
  - "_ipp._tcp" (Printing), "_xmpp._tcp" (Jabber)
- Service-Instance
  - matches the explicit service instance (service name)
  - services instances can use Unicode, White Space etc.
  - “myfånçy printer in røøm 123._ipp._tcp”
- Message-Type
  - Enumeration
  - ‘any’, ‘query’ or ‘announcement’

- Inbound 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 message-type announcement
 match service-type _airplay\._tcp
!
service-list mdns-sd limited permit 30
 match service-type .*
!
```

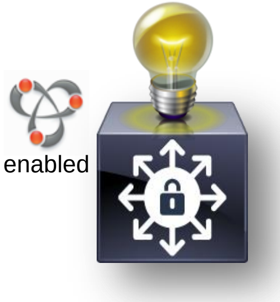
# mDNS Proxy

## What is it?

- Enables mDNS service extension
- Filters define what gets proxied and what not (in / out)
- Interface Filters take Precedence over Global Filters

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

## How does it work?



- Enabled globally
- Can be overridden per Interface

```
interface Vlan100
ip address 172.16.31.4 255.255.255.0
 ipv6 address 2001:DB8:1:100::/64 eui-64
 ipv6 enable
 ipv6 eigrp 100
 service-routing mdns-sd
  service-policy permit-all IN
  service-policy permit-all OUT
end
```

# Active Query

## What is it?

Periodic polling of services

- Keeps cache content fresh
- Globally defined
- Queries on all L3 interfaces

## How does it work?

Ask for services

- Defined using a service-list
- Timer from 60 to 3600 seconds

```
service-list mdns-sd AQ query
 service-type _airplay._tcp
!
service-routing mdns-sd
 service-policy-query AQ 900
!
```

# Redistribution

- Redistribution is **flooding** of *service announcements* (remove / add of services)
- Configured per interface
- **ENABLED:** announcements will be forwarded to other interfaces instantly

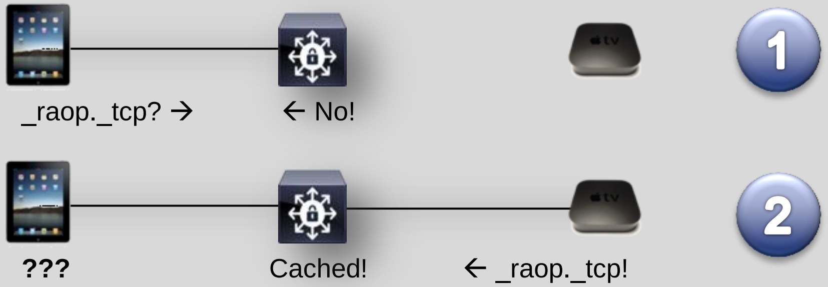
  ***Pro:*** quicker update of client info

  ***Con:*** more announcements / multicasts
- **DISABLED:** only a query by a client will result in a response by the cache

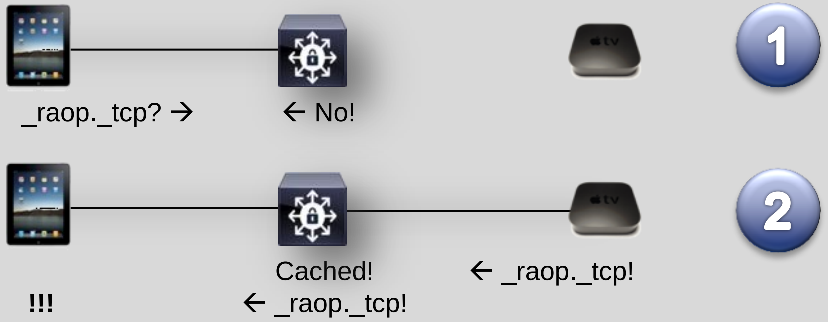
  ***Pro:*** less announcement traffic

  ***Con:*** clients may use outdated information (until it times out) or don't see new services instantly

**without** redistribution:



**with** redistribution:



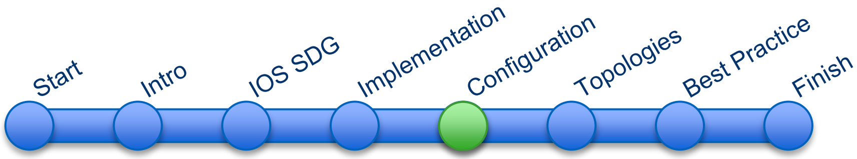
# Redistribution (cont.)

**Best Practice: Don’t turn on Redistribution of Service Announcements**

- **NOT** required to extend services across subnets
- Active Query sufficient most of times
- Can cause Multicast storms
- Should only be enabled if needed
- Control with specific filters (OUT)

Here’s how to turn them on:

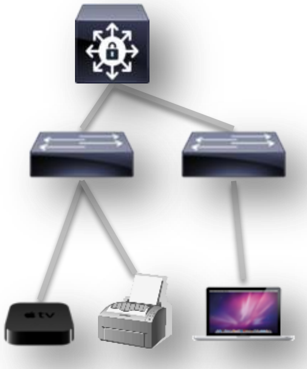
```
interface Vlan100
 [...]
 service-routing mdns-sd
 redistribute mdns-sd
end
```



# Topology Support & Inter-Operability

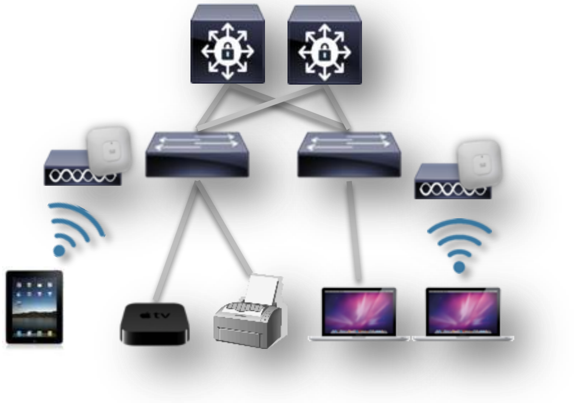
# Topology Thoughts

- Simple, Wired Topology – Check

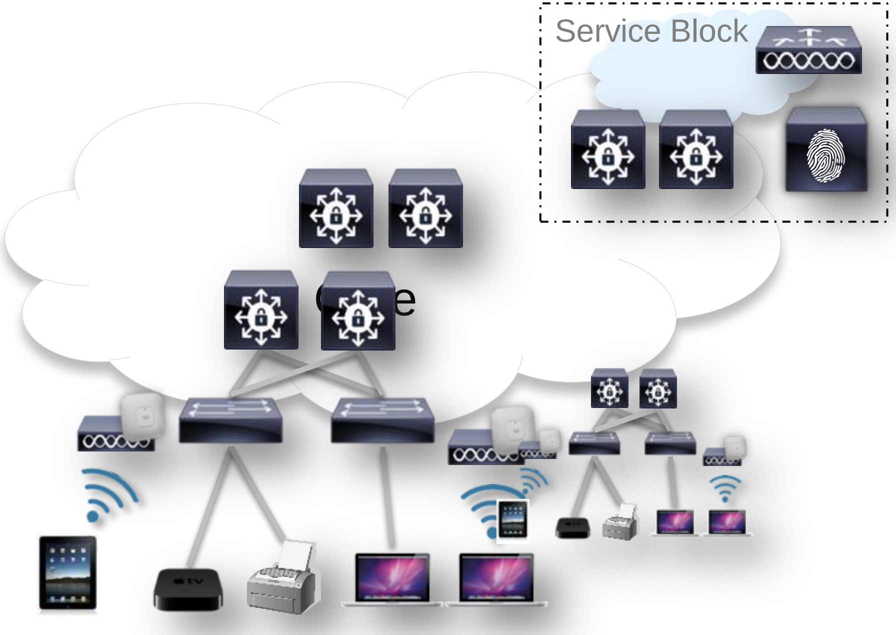


# Topology Thoughts

- Simple, Wired Topology – Check
- Local Wireless – Check
- Redundancy?



# Topology Thoughts



- Simple, Wired Topology – Check
- Local Wireless – Check
- Redundancy?
- Multiple Sites?
- Centralized Wireless?
- etc.

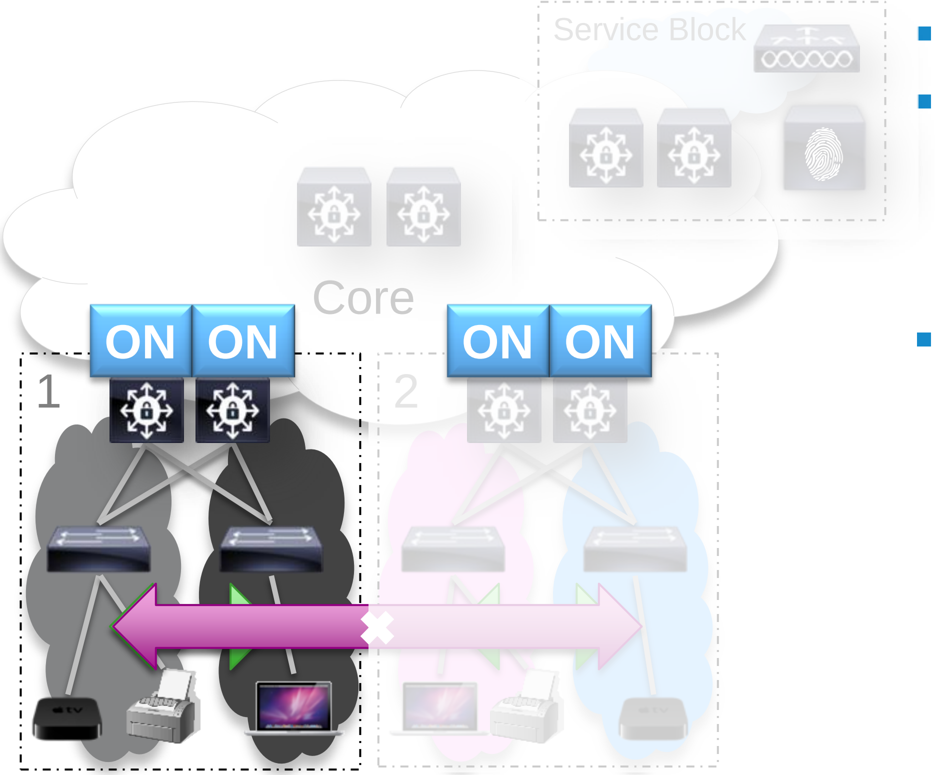
Ramifications of extending a protocol that has been designed for link local use only!

# Topology Thoughts

- Simple, Wired Topology – Check
- Local Wireless – Check
- Redundancy?
- Multiple Sites?
- Centralised Wireless?
- etc.

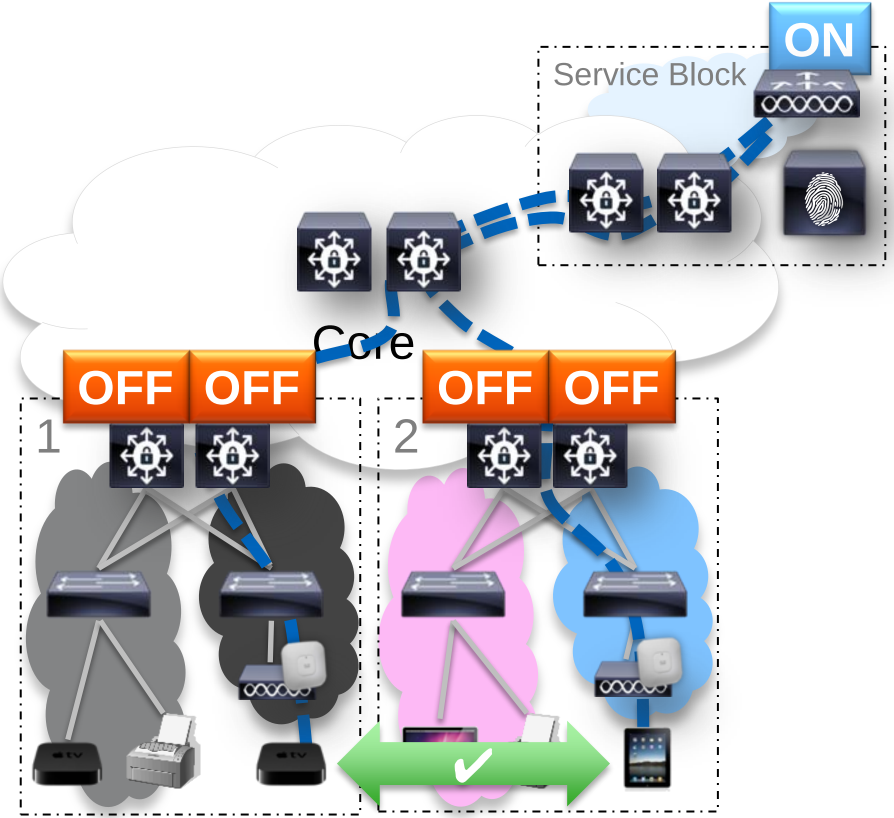
Ramificat col that ha

# Wired Topology



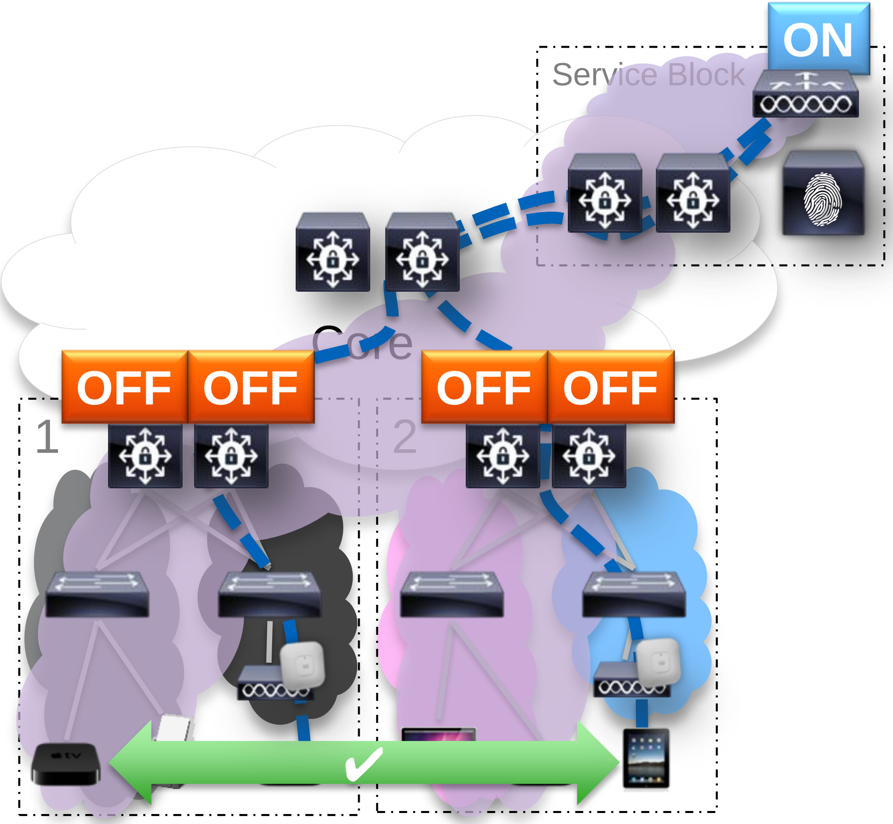
- The **typical** wired use case
- What's working:
  - OK for one distribution block
  - IPv4 / IPv6 agnostic
  - Service filtering (incoming / outgoing)
- What's needed:
  - Extending services across distribution blocks (can I AirPlay to another building?)
  - Name Space Conflict resolution (two Apple TVs having the same name?)

# AireOS Wireless Topology



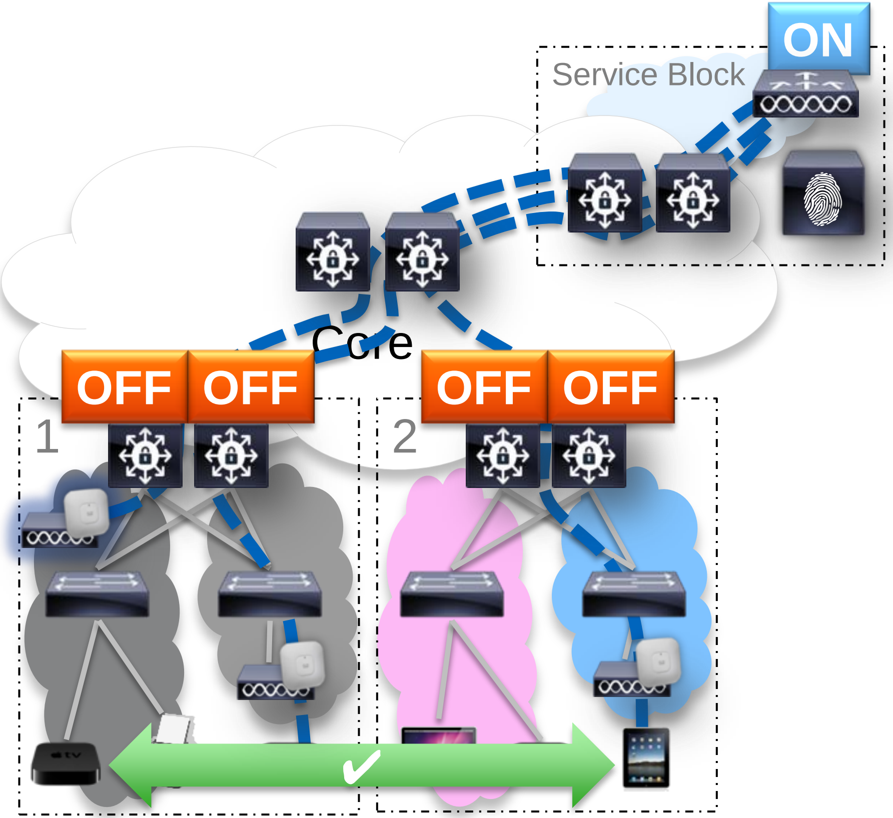
- Centralised Switching for Wireless
- What works:
  - Wireless / Wireless works
  - Cache is central with WLC
  - Wireless overlay, switching vendor agnostic
  - Initial RBAC support
- What's needed:
  - mDNS Proxy Support
  - IPv6 caching of AAAA records
  - Enhanced Filtering
  - Name Conflict Resolution

# AireOS Wireless / Wired Topology



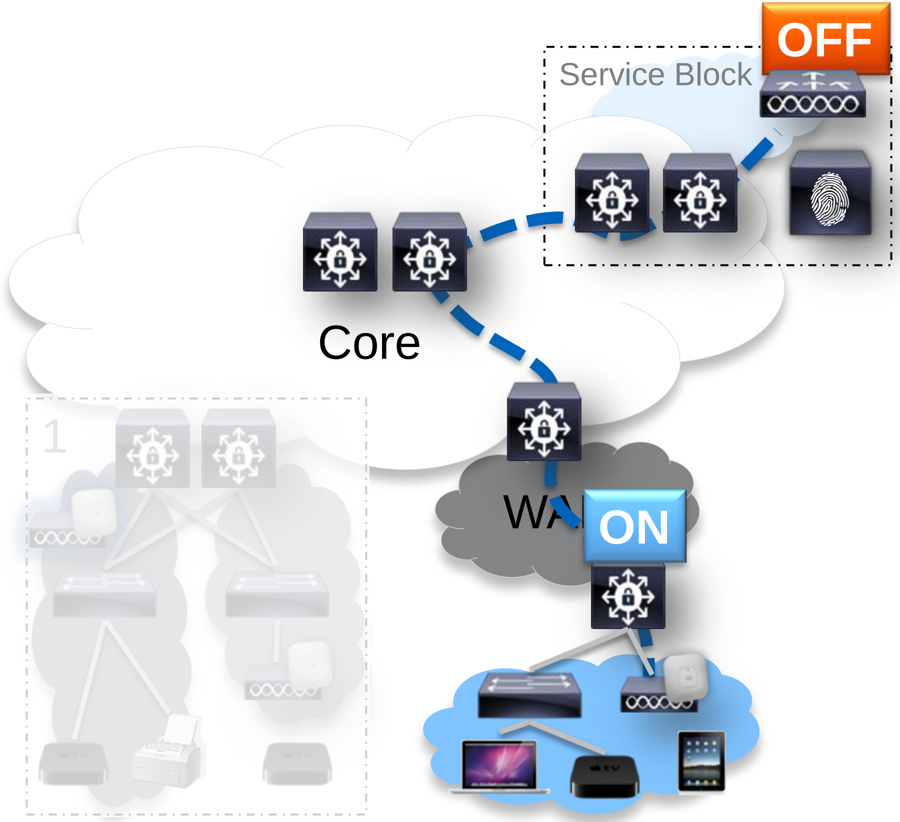
- Centralised Switching for Wireless
- Wired / Wireless needs L2 adjacency
- **Option:** Span services VLAN across domain to make wired devices adjacent
- What works:
  - Wired devices visible to wireless devices
  - Switching vendor agnostic overlay
- What's needed:
  - Campus-spanning VLANs. **Contrary to all best practices and CVDs**

# AireOS Wireless / Wired Topology



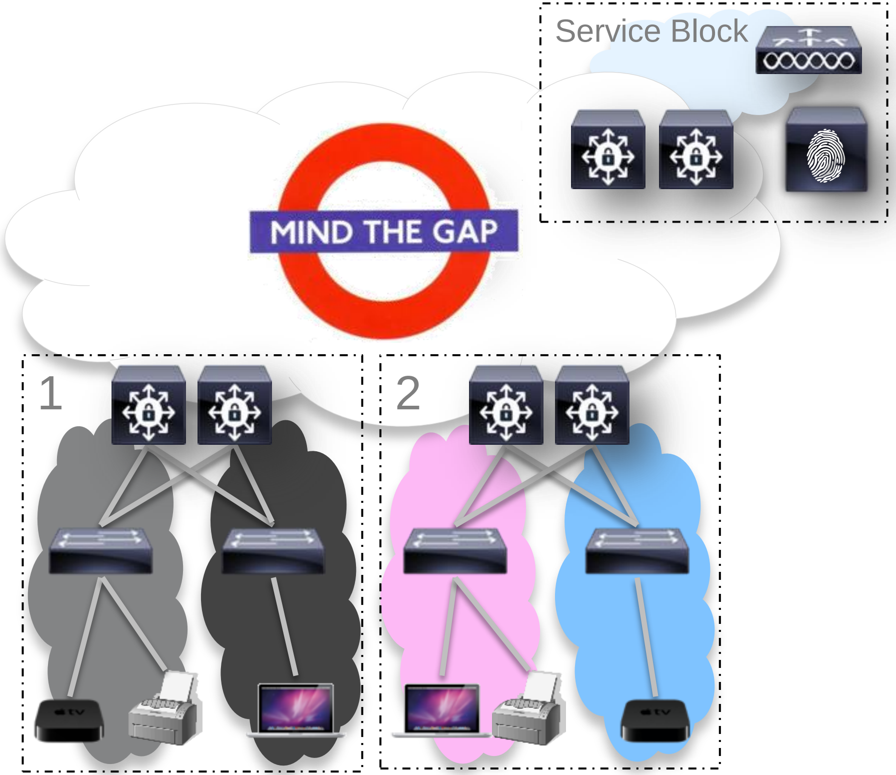
- Centralised Switching for Wireless
- Wired / Wireless needs L2 adjacency
- **Option:** Snooper AP to pick up mDNS traffic and hauls it back to WLC via CAPWAP
- Must be a trunk port
- It's a One-Way-Street (wired → wireless)
- What works:
  - Wired devices visible to wireless devices
  - Vendor agnostic overlay
- What's needed:
  - Additional of APs & licenses

# FlexConnect in the Branch



- Local Switching for Wireless
- No services discoverable outside branch
- What works:
  - mDNS information handled by SDG on switch or router / ISR
  - Otherwise, same characteristics as 'Wired only' scenario
  - 'Sweet Spot' for SDG
- What's needed:
  - SDG deployment in the branch

# Mind the Gap



Potential Pitfalls

- Naming conflicts
- Inconsistent Cache content

Possible Approach

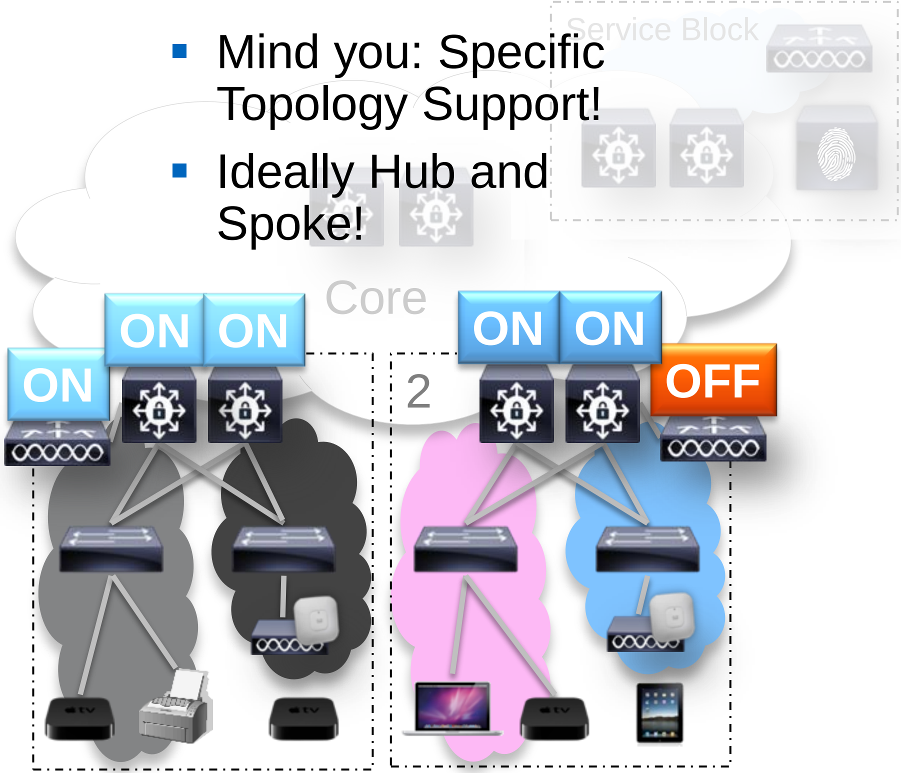
- Enable SDG on all L3 devices
- ‘Active Query’ only for specific services
- Filter unnecessary services
- Strictly Hub-and-Spoke

Alternatively

- Wide Area Bonjour (not dynamic, manual effort)

# Mixed IOS / AireOS Wireless / Wired Topology

- Mind you: Specific Topology Support!
- Ideally Hub and Spoke!



## Centralised Switching for Wireless

| AireOS / IOS | ON | OFF |
|---|---|---|
| ON | 👎 Relies on active queries to sync cache content<br>👎 No AAAA records from AireOS<br>👎 Two caches to configure<br>👎 Inconsistent filter mechanism & capabilities | 👍 mDNS works as defined as in RFC<br>👍 Multiple WISMs in 6k supported<br>👎 Multicast optimi-sation must be off<br>👍 Instant service learning from Wire-less |
| OFF | 👎 No advertisements possible<br>👎 No visibility into different L3 segments<br>👎 Need solution as in previous slides | n/a |

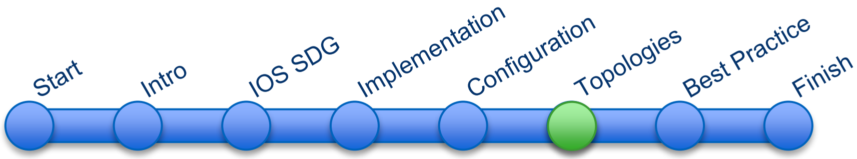
# Mixed IOS / AireOS Wireless / Wired Topology

Service Block
ON

## Centralised Switching for Wireless

| IOS \ AireOS | ON | OFF |
|---|---|---|
| | | s<br>C<br>in 6k<br>ff<br>re- |
| OFF | No advertisements possible<br>No visibility into different L3 segments<br>Need solution as in previous slides | n/a |

**Recommendation:**
In a mixed IOS SDG and AireOS Bonjour Gateway Environment only enable the IOS Service Discovery Gateway.



Start

Intro

IOS SDG

Implementation

Configuration

Topologies

Best Practice

Finish

# Best Practice (and real-life examples)

# What to Allow into the Cache?

## White List Approach

- Allow only services that MUST be extended
- Deny everything else EXCEPT queries (won't work otherwise)

## Be Specific

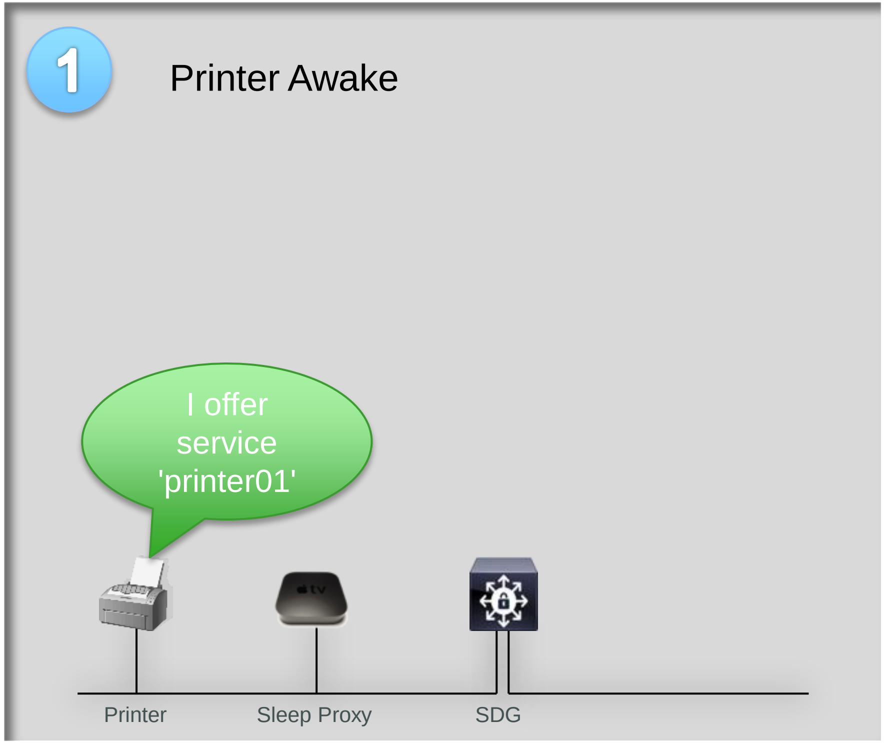
- Denying unwanted or unneeded services helps to keep the chatter down and also is easier on resources (CPU & memory)
- Don't extend Sleep Proxy Services

## Keep Services Fresh

- Devices don't periodically re-announce services
- Cache will **only** forward queries to other interfaces if it has a PTR
- Periodically ask if service is still there

# Quick Detour: Sleep Proxy

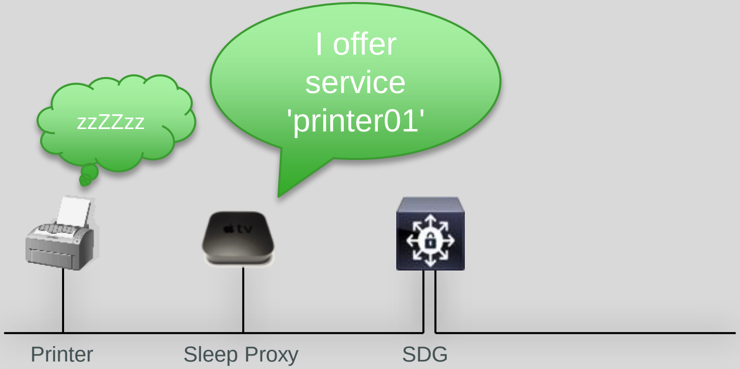
| | |
|---|---|
| **What is it?** | Allows devices to go to sleep while another device responds to service requests for sleeping device. |
| **Why should it be filtered?** | • Split horizon on SDG can limit device visibility.<br>• WoL Packet won't be forwarded, anyway. |
| **Where does it work?** | If device and Sleep Proxy are on the **same** segment. |



# Quick Detour: Sleep Proxy

| | |
|---|---|
| **What is it?** | Allows devices to go to sleep while another device responds to service requests for sleeping device. |
| **Why should it be filtered?** | • Split horizon on SDG can limit device visibility.<br>• WoL Packet won't be forwarded, anyway. |
| **Where does it work?** | If device and Sleep Proxy are on the **same** segment. |

2 Printer Sleeps, Service now registered with Sleep Proxy

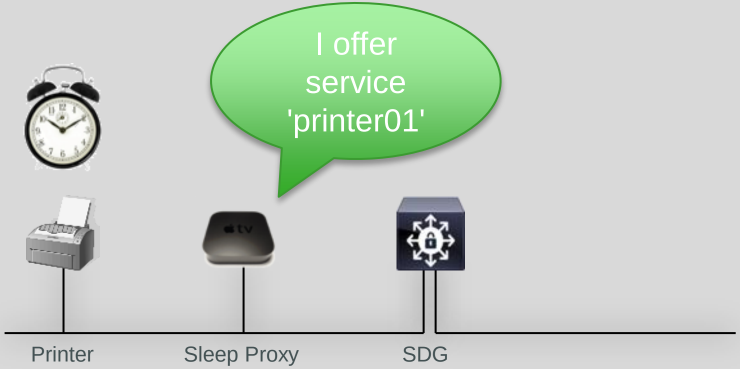


# Quick Detour: Sleep Proxy

| | |
|---|---|
| **What is it?** | Allows devices to go to sleep while another device responds to service requests for sleeping device. |
| **Why should it be filtered?** | • Split horizon on SDG can limit device visibility.<br>• WoL Packet won’t be forwarded, anyway. |
| **Where does it work?** | If device and Sleep Proxy are on the **same** segment. |

3

If service is looked up, Sleep Proxy will respond. If service is accessed, real device will wake up and re-announce the service

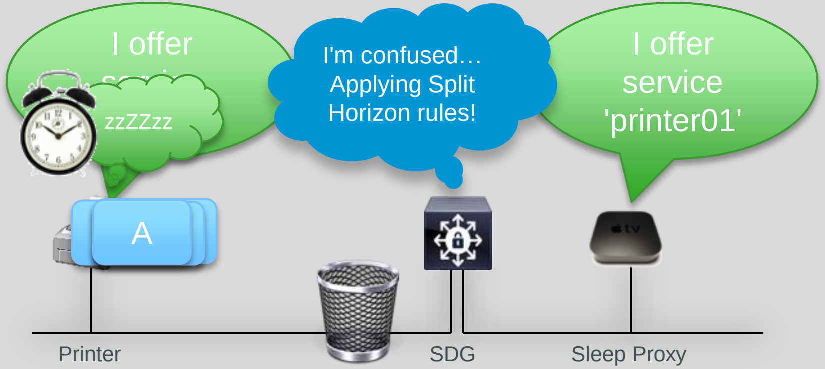


# Quick Detour: Sleep Proxy

| | |
|---|---|
| **What is it?** | Allows devices to go to sleep while another device responds to service requests for sleeping device. |
| **Why should it be filtered?** | • Split horizon on SDG can limit device visibility.<br>• WoL Packet won't be forwarded, anyway. |
| **Where does it work?** | If device and Sleep Proxy are on the **same** segment. |

4

Since the SDG remembers on which interface a service has been learned, it will drop the announcements for A, AAAA, SRV, TXT etc. records from the real device if it still sees the PTR on the Sleep Proxy side.



I offer
zzZZzz
I'm confused… Applying Split Horizon rules!
I offer service 'printer01'
A
Printer
SDG
Sleep Proxy

# Considerations for Filters

| Name | Purpose |
|---|---|
| PERMIT-ALL | Used for OUT-going traffic. No restrictions whatsoever |
| PERMIT-MOST | Used for IN-coming traffic, allows everything **except Sleep Proxy** |
| DENY-ALL | Used for IN-coming traffic, denies everything (esp. service announcements) **except for queries** |
| MIXED | Used for IN-coming traffic, allows specific service announcements, denies all the rest. |

# Filter MIXED Explained

```
service-list mdns-sd mixed permit 10
 match message-type query
!
```

Allow Queries (required)

```
service-list mdns-sd mixed permit 20
 match message-type announcement
 match service-type _ipp._tcp
!
service-list mdns-sd mixed permit 30
 match message-type announcement
 match service-type _universal._sub._ipp._tcp
!
service-list mdns-sd mixed permit 40
 match message-type announcement
 match service-type _airplay._tcp
!
```

Allow specific service announcements (do not include _sleep-proxy._udp)

```
service-list mdns-sd mixed deny 50
!
```

Deny everything else

# Other Filters Explained

```
service-list mdns-sd permit-most deny 10
 match service-type _sleep-proxy._udp
!
service-list mdns-sd permit-most permit 20
!
```

Permit Everything EXCEPT Sleep Proxy

```
service-list mdns-sd permit-all permit 10
!
```

Permit Everything (use for outbound filters only!)

```
service-list mdns-sd deny-all permit 10
 match message-type query
!
service-list mdns-sd deny-all deny 20
!
```

Deny Everything EXCEPT Queries (which are required)

# Active Query Example

```
service-list mdns-sd active-query query
 service-type _universal._sub._ipp._tcp.local
 service-type _ipp._tcp.local
 service-type _airplay._tcp.local
!
```

Query for Services we care for

```
service-routing mdns-sd
 service-policy-query active-query 900
```

Query every 15 minutes

**Note:** .local is automatically appended for strings with only one dot
**Note:** Currently, Active Queries are sent on all L3 Interfaces and are not subject to Filtering.

# Interface Configuration

```
interface GigabitEthernet0/0
 ip address 172.16.33.7 255.255.255.0
 service-routing mdns-sd
  service-policy mixed IN
  service-policy permit-all OUT
!
```

Clients here plus some printers or Apple TVs

```
interface GigabitEthernet0/1
 ip address 172.16.57.1 255.255.255.0
 service-routing mdns-sd
  service-policy permit-most IN
  service-policy permit-all OUT
!
```

Apple TVs, Print Servers here

```
interface GigabitEthernet0/2
 ip address 172.16.58.1 255.255.255.0
 service-routing mdns-sd
  service-policy deny-all IN
  service-policy permit-all OUT
```

Clients only, no learning here

# Complete Configuration

```
Current configuration : 1665 bytes
!
! Last configuration change at 11:01:55 UTC Fri Nov
8 2013
!
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
service compress-config
!
hostname mdns
!
boot-start-marker
boot-end-marker
!
!
logging console emergencies
enable secret 0 cisco
enable password cisco
!
no aaa new-model
!
ip dhcp excluded-address 172.16.57.1 172.16.57.99
ip dhcp excluded-address 172.16.58.1 172.16.58.99
!
ip dhcp pool SERVERS
 network 172.16.57.0 255.255.255.0
 domain-name mdns-sd.lab
 default-router 172.16.57.1
 dns-server 8.8.8.8
!
ip dhcp pool CLIENTS
 network 172.16.58.0 255.255.255.0
 domain-name mdns-sd.lab
 default-router 172.16.58.1
 dns-server 8.8.8.8
!
ip domain-name mdns-sd.lab
ip name-server 8.8.8.8
ip cef
no ipv6 cef
ipv6 multicast rpf use-bgp
!
```

```
!
service-list mdns-sd mixed permit 10
 match message-type query
!
service-list mdns-sd mixed permit 20
 match message-type announcement
 match service-type _ipp._tcp
!
service-list mdns-sd mixed permit 30
 match message-type announcement
 match service-type _universal._sub._ipp._tcp
!
service-list mdns-sd mixed permit 40
 match message-type announcement
 match service-type _airplay._tcp
!
service-list mdns-sd mixed deny 50
!
!
service-list mdns-sd permit-most deny 10
 match service-type _sleep-proxy._udp
!
service-list mdns-sd permit-most permit 20
!
service-list mdns-sd permit-all permit 10
!
service-list mdns-sd deny-all permit 10
 match message-type query
!
service-list mdns-sd deny-all deny 20
!
service-list mdns-sd active-query query
 service-type _universal._sub._ipp._tcp.local
 service-type _ipp._tcp.local
 service-type _airplay._tcp.local
!
service-routing mdns-sd
 service-policy-query active-query 900
!
```

```
interface Ethernet0/0
 description *** (wireless) Clients here plus some printers or aTVs
 ip address 172.16.33.7 255.255.255.0
 service-routing mdns-sd
  service-policy mixed IN
  service-policy permit-all OUT
!
interface Ethernet0/1
 description *** AppleTVs, Print Servers here
 ip address 172.16.57.1 255.255.255.0
 service-routing mdns-sd
  service-policy permit-most IN
  service-policy permit-all OUT
!
interface Ethernet0/2
 description *** Clients only, we don't want to learn anything here
 ip address 172.16.58.1 255.255.255.0
 service-routing mdns-sd
  service-policy deny-all IN
  service-policy permit-all OUT
!
interface Ethernet0/3
 no ip address
 shutdown
!
ip forward-protocol nd
!
no ip http server
ip route 0.0.0.0 0.0.0.0 172.16.33.1
!
control-plane
!
line con 0
 logging synchronous
line aux 0
line vty 0 4
 exec-timeout 0 0
 password cisco
 login
!
end
```

# mDNS Show Commands

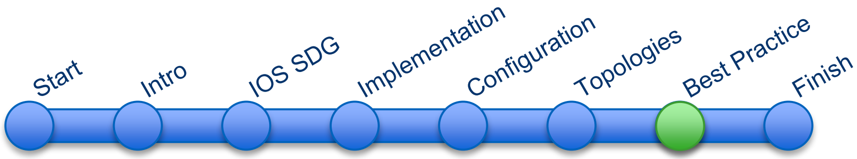
## What it is:

- show cache content
- show requests
- show statistics

```
Router# show mdns cache
mDNS CACHE
==========================================================================================
[<NAME>]                         [<TYPE>][<CLASS>][<TTL>/Remaining] [Accessed] [If-name] [<RR Record Data>]

_ssh._tcp.local                  PTR     IN       4500/4288   9      Vl200   Lab Mac._ssh._tcp
_sftp-ssh._tcp.local             PTR     IN       4500/4288   9      Vl200   Lab Mac._sftp-ssh
_services._dns-sd._udp.local     PTR     IN       4500/4288   1      Vl200   _rfb._tcp.local
_rfb._tcp.local                  PTR     IN       4500/4288   9      Vl200   Lab Mac._rfb._tcp
Lab Mac._ssh._tcp.local          TXT     IN       4500/4288   3      Vl200   (1)''
Lab Mac._sftp-ssh._tcp.local     TXT     IN       4500/4288   3      Vl200   (1)''
Lab Mac._rfb._tcp.local          TXT     IN       4500/4288   3      Vl200   (1)''
```

# SDG Demonstration Video #2



Start

Intro

IOS SDG

Implementation

Configuration

Topologies

Best Practice

Finish

# Conclusion

# Conclusion and Summary

## Services Discovery Gateway:
## IOS-based solution to address a real customer issue!

| | |
|---|---|
| One Architecture for Unified Access | • Wireless and wired connectivity<br>• Pervasively available |
| Manageable BYOD | • Clients operate transparently<br>• IPv6 and IPv4 fully supported<br>• Enhanced with Cisco security solutions |
| Scalable | • No need to redesign your network<br>• Network solution at L3 distribution layer |
| Network Wide Security | • Service filters to control visibility and access<br>• Built-in cache management<br>• Integrates with Access Control |

# 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™