



Voice of the Engineer

Deep Dive Series: Profiling

Voice of the Engineer

Solutions approach to partner training








- Partner Enablement through series of WebEx Training Sessions
- Basics are introductory sessions open to AM, SE, FE
- Deep Dives are Field Engineer focus
 - Deployment information from the Experts for the Experts
- Recordings and Slides will be Archived on the Partner Community
- Voice of the Engineer – Deep Dives
 - <https://communities.cisco.com/docs/DOC-30977>
- Voice of the Engineer – Basics
 - <https://communities.cisco.com/docs/DOC-30718>

Voice of the Engineer – Deep Dives

<https://communities.cisco.com/docs/DOC-30977>

- Identity Services Engine (ISE)
 - ✓ TrustSec & ISE Overview - 9/25/12
 - ✓ AAA, 802.1X, MAB - 10/9/12
 - ✓ ISE Profiling – 10/23/12
 - ✓ Web Auth, Guest & Device Registration – 11/6/12
 - ✓ Bring Your Own Device & EAP Chaining – 11/20/12
 - ✓ Posture & Security Group Access – 12/4/12
 - ✓ **Troubleshooting & Best Practices (Submit requests in survey) – 12/18/12**
- <http://cisco.cvent.com/events/voice-of-the-engineer-series-security/event-summary-d707f808c5124beb86ff59ebab996589.aspx>
- AnyConnect – Tentative Schedule
 - ✓ AnyConnect VPN – 11/13/12
 - ✓ AnyConnect NAM – 12/11/12
 - ✓ AnyConnect Mobile – 1/8/13
 - ✓ Advanced AnyConnect Configuration – 1/29/13
- Content Security – In Planning

Agenda for Voice of the Engineer

-  TrustSec & ISE Overview
-  AAA, 802.1X, MAB
-   Profiling
-  Web Authentication, Guest & Device Registration
-  Bring your own Device & EAP-Chaining
-  Posture & SGA
-  Troubleshooting & Best Practices

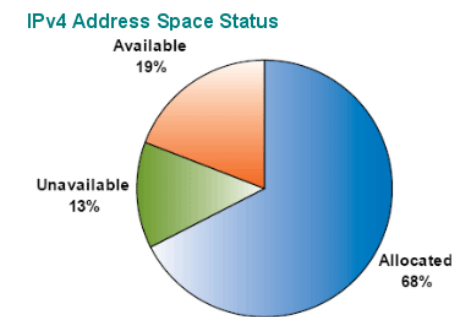
ISE Profiling Services



Agenda

-  Why Profiling?
-  Profiling Policies
-  Probe Overview
-  Enhanced Profiling Features
-  Best Practices - Profiling in a Real Network
-  Monitoring and Reporting

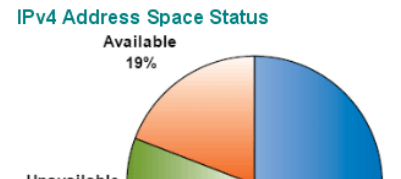
The User to Device Ratio Has Changed



What is all this stuff on my network?!!!



The User to Device Ratio Has Changed



Things are spinning out of control!



ISE Profiling

- What ISE Profiling is:

Dynamic classification of every device that connects to network using the infrastructure.

Provides the context of “What” is connected independent of user identity for use in access policy decisions



PCs	Non-PCs			
	UPS	Phone	Printer	AP

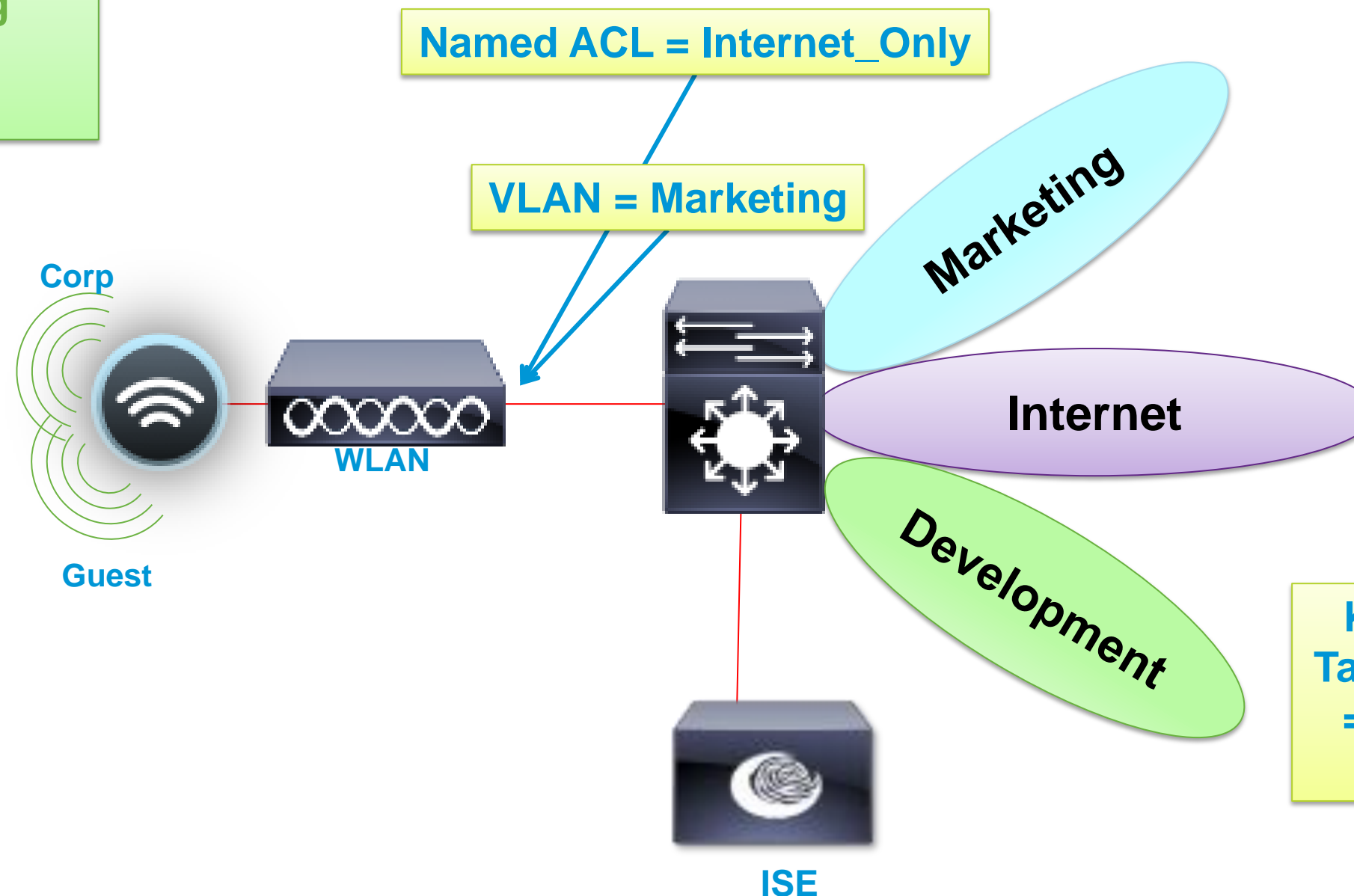
- What Profiling is NOT:

- An authentication mechanism.
- An exact science for device classification.

Profiling User Devices

Differentiated Access Based on Device Type

- How can I restrict access to my network?
- Can I manage the risk of using personal PCs, tablets, smart-devices?



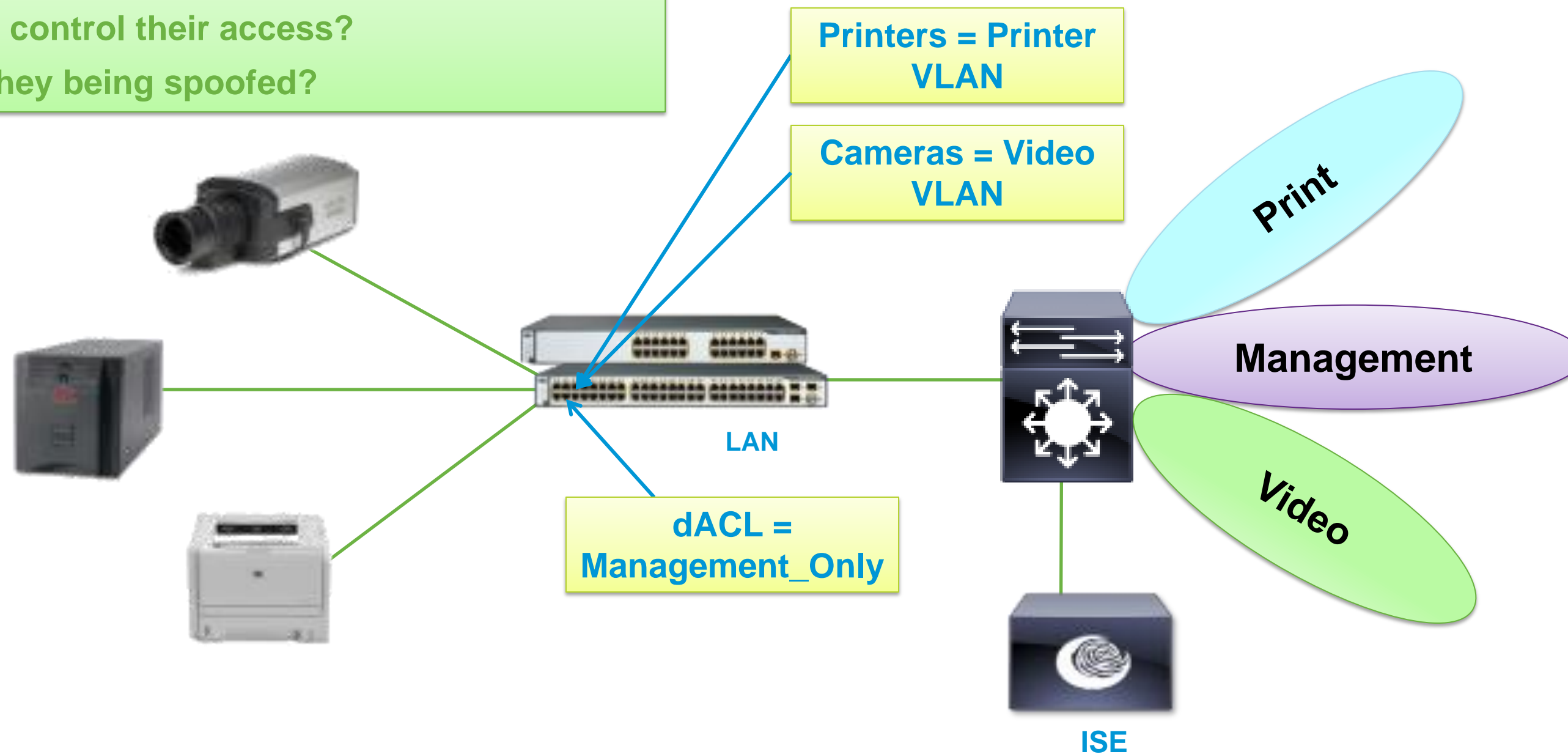
Kathy + Corp Laptop = Full Access to Marketing VLAN

Kathy + Personal Tablet / Smartphone = Limited Access (Internet Only)

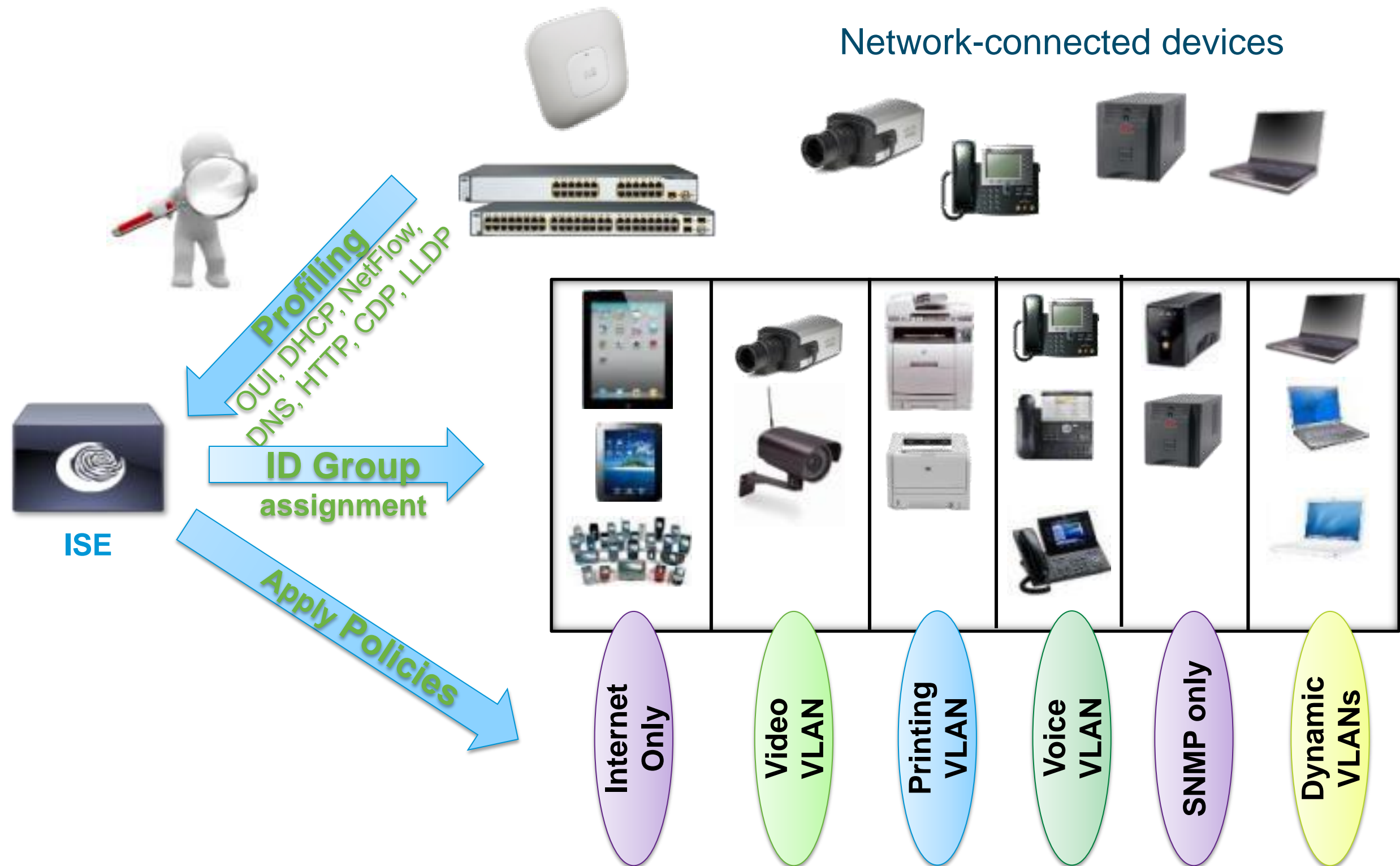
Profiling Non-User Devices

Dynamic Population of MAB Database Based on Device Type

- How do I discover non-user devices?
- Can I determine what they are?
- Can I control their access?
- Are they being spoofed?



ISE Profiler: 3 Steps

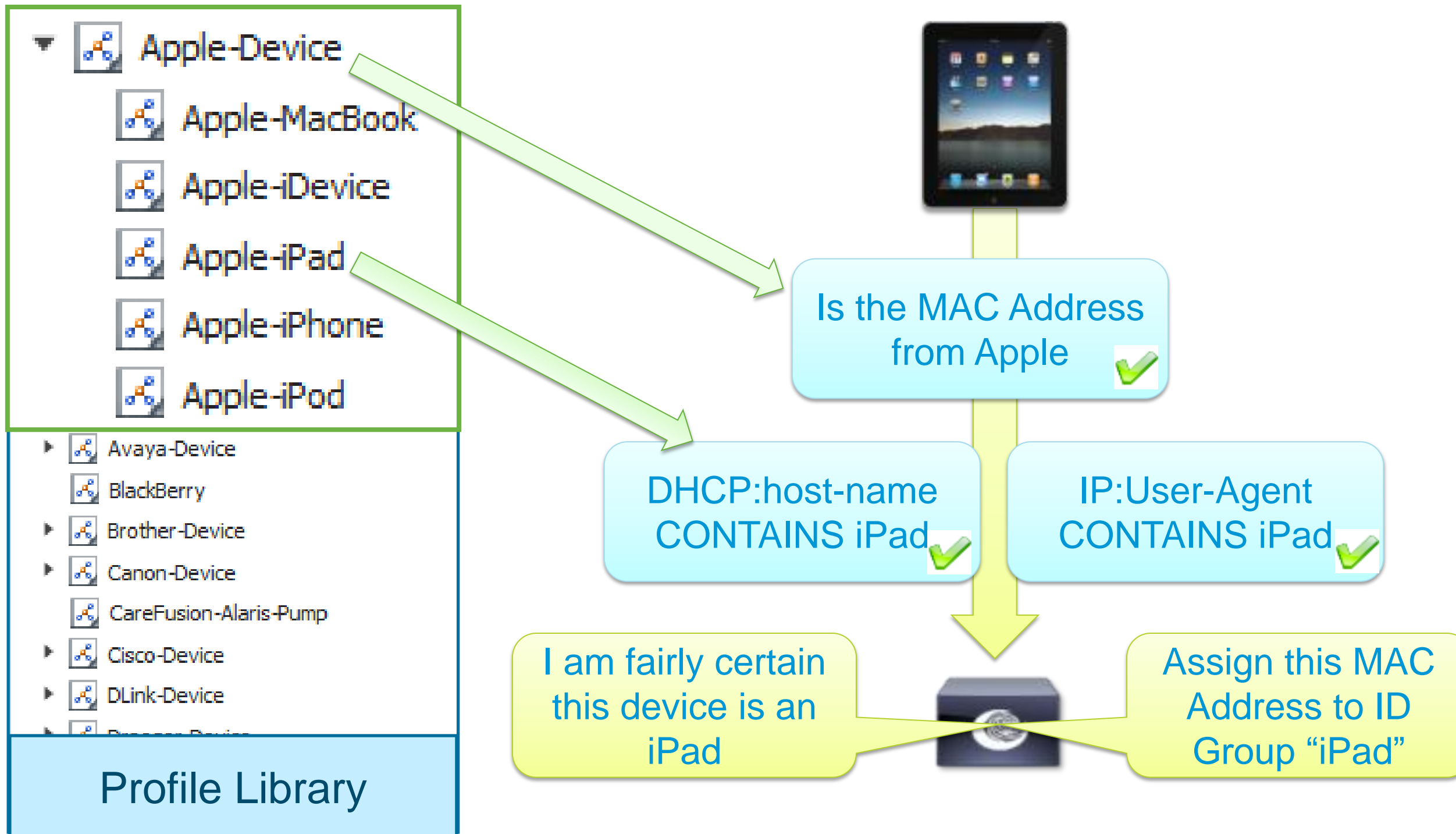


Profiling Policies

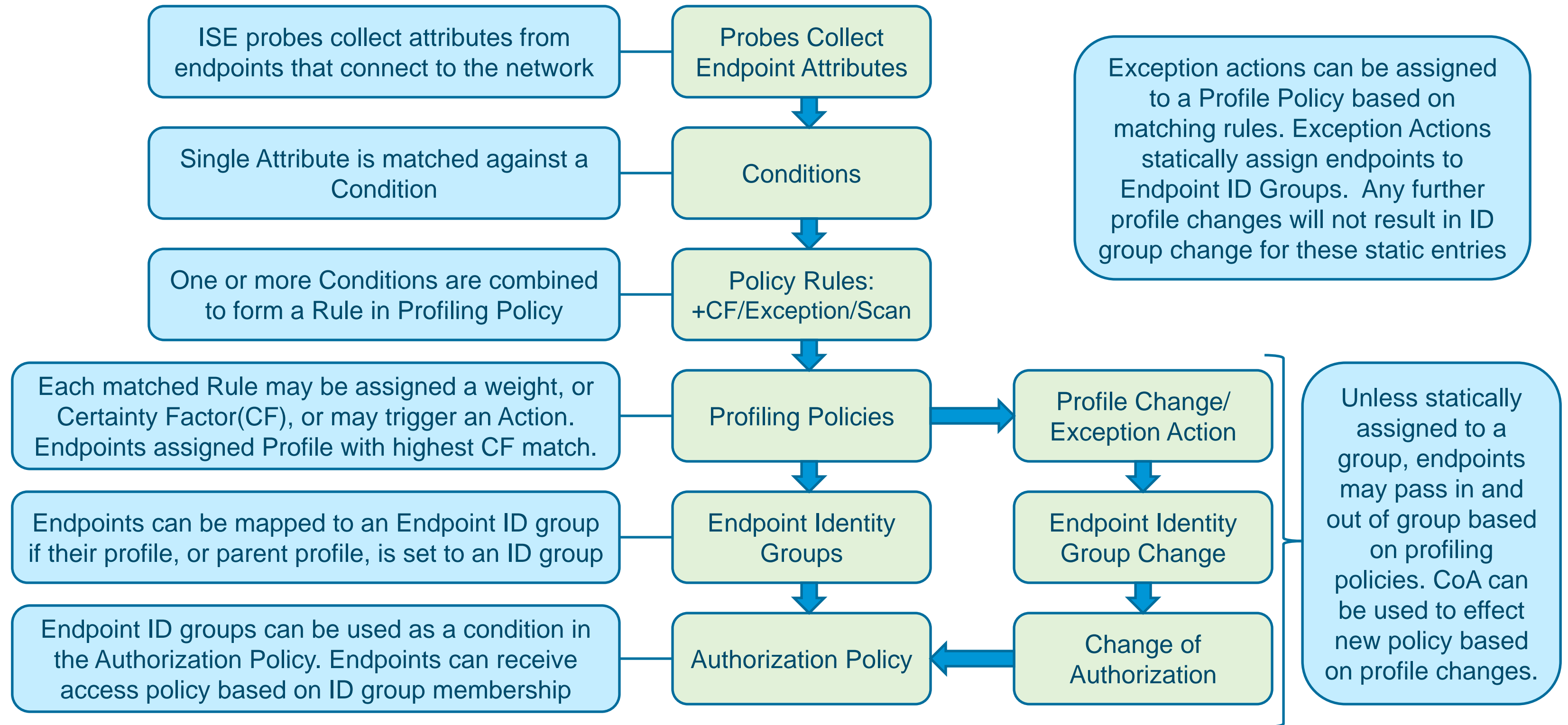


Profiling Policy Overview

Profile Policies Use a Combination of Conditions to Identify Devices



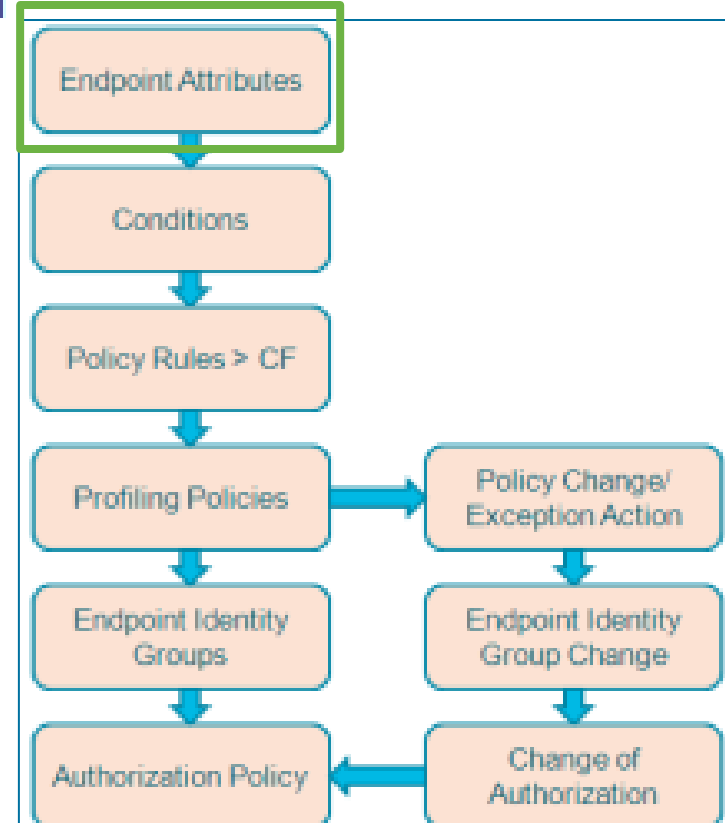
Profiling Policy Architecture and Components



Sample Attributes for Custom Profiler Conditions

RADIUS	SNMP	MAC	DHCP	NMAP	NetFlow	LLDP
Called-Station-ID	hrDeviceStatus	MACAddress	boot-file	161-udp	MAX_TTL	IldpCacheCapabilities
Calling-Station-ID	ifDescr	OUI	client-fqdn	162-udp	MIN_PKT_LNGTH	IldpCapabilitiesMapSupported
CHAP-Challenge	ifIndex	IP	client-identifier	1900-udp	MIN_TTL	IldpChassisId
CHAP-Password	ifOperStatus		device-class	21-tcp	nexthop	IldpManAddress
Class	port		dhcp-class-identifier	22-tcp	OUT_BYTES	IldpPortDescription
Connect-Info	portIfIndex		dhcp-client-identifier	23-tcp	OUT_PKTS	IldpPortId
Digest-Attributes	sysContact		dhcp-message-type	25-tcp	output	IldpSystemCapabilitiesMapEnabled
Digest-Response	sysDescr		dhcp-parameter-request-list	3306-tcp	OUTPUT_SNMP	IldpSystemDescription
EAP-Key-Name	sysLocation		dhcp-requested-address	3389-tcp	prot	IldpSystemName
EAP-Message	sysName		dhcp-user-class-id	443-tcp	PROTOCOL	IldpTimeToLive
NAS-IP-Address	sysObjectID		domain-name	445-tcp	sampling_interval	
NAS-Port	sysUpTime		host-name	445-udp	source_id	
NAS-Port-Id	Vlan	name-servers	500-udp	src_as		
NAS-Port-Type	VlanName	pxe-client-arch	520-udp	SRC_MAC		
Service-Type	vlanPortVlan	pxe-client-machine-id	53-tcp	SRC_MASK		
Framed-IP-Address		pxe-client-network-id	53-udp	SRC_TOS		
		server-identifier	631-udp	SRC_VLAN		
		vendor-class	67-udp	srcaddr		
			68-udp	srcport		
			80-tcp	sys_uptime		
			8080-tcp	tcp_flag		
				TCP_FLAGS		
				operating-system		

Partial Listing



ISE – Profiling Attribute Collection

Endpoints

Edit Create Delete

Endpoint Profile

- Apple_iPad
- Apple_iPad
- Cisco-Access-Point
- Cisco-IP-Phone-7945
- Cisco-WLC-2100-Series
- ISE-Appliance
- Linux-Workstation
- Microsoft-Workstation
- Windows7-Workstation
- Xerox-Device

Endpoint List > 10	DestinationIPAddress	NetworkDeviceGroups	Device Type#All Device Types, Location#All Locations
* MA	DestinationPort	NetworkDeviceName	wlc
* Policy A	Device IP Address	OUI	D-LINK INTERNATIONAL PTE LIMITED
Static A	Device Type	PolicyVersion	chaddr 1c:bd:b9:d7:9f:9e
* Identity Group A	EapAuthentication	PostureAssessmentSta	ciaddr 10.1.50.100
Static Group A	EapTunnel	PostureStatus	cisco-av-pair audit-session-id=3d64010a00000002956bbf4d
Attribute List	EndPointMACAddress	Pragma	client-fqdn 00:00:00:57:69:6e:37:2d:50:43:2e:64:65:6d:6f:2e:1
ADDomain	EndPointPolicy	Proxy-Connection	dhcp-class-identifier MSFT 5.0
AcsSessionID	EndPointProfilerServer	RequestLatency	dhcp-client-identifier 01:1c:bd:b9:d7:9f:9e
Airespace-Wlan-I	EndPointSource	Response	dhcp-message-type 5
AuthState	Framed-IP-Address	SelectedAccessService	dhcp-parameter-request-list 1, 15, 3, 6, 44, 46, 47, 31, 33, 121, 249, 43, 252
AuthenticationIde	Host	SelectedAuthenticationI	dhcp-requested-address 10.1.50.100
AuthenticationMe	IdentityAccessRestricted	SelectedAuthorizationP	domain-name demo.loc
AuthorizationPolic	IdentityGroup	Service-Type	flags 0x0000
CPMSessionID	IdentityPolicyMatchedRule	StaticAssignment	giaddr 10.1.50.6
Called-Station-ID	Location	StaticGroupAssignmen	hlen 6
Calling-Station-ID	MACAddress	Timestamp	hops 0
Content-Length	MatchedPolicy	Total Certainty Factor	host-name Win7-PC
Content-Type	MessageCode	User-Agent	htype Ethernet (
Cookie	NAS-IP-Address	User-Name	ip 10.1.50.10
Description	NAS-Identifier		op BOOTREF
	NAS-Port		secs 0
	NAS-Port-Type		yiaddr 0.0.0.0




Sample Device Attributes

```

graph TD
    A[Endpoint Attributes] --> B[Conditions]
    B --> C[Policy Rules > CF]
    C --> D[Profiling Policies]
    D --> E[Endpoint Identity Groups]
    E --> F[Authorization Policy]
    G[Policy Change/Exception Action] --> H[Endpoint Identity Group Change]
    H --> I[Change of Authorization]
    I --> F
    
```

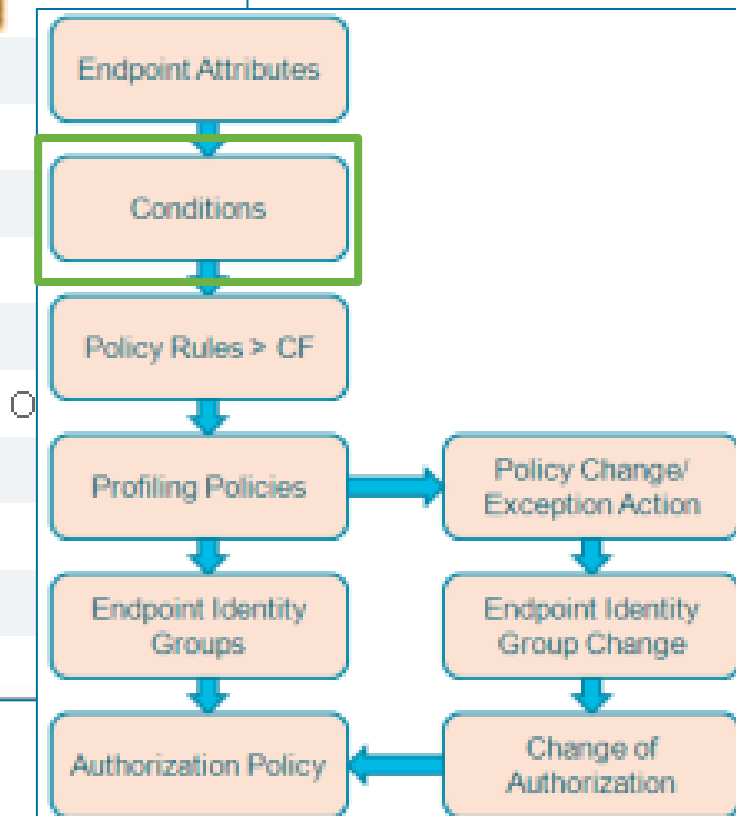
Profiler Conditions Library

Any Combination of These Conditions Could be Use in Your Policies

Conditions		
 Edit	 Create	 Delete
<input type="checkbox"/> Profiler Check Name	Expression	Description
<input type="checkbox"/> AndroidRule1Check1	User-Agent CONTAINS Android	AndroidRule1Check1
<input type="checkbox"/> AndroidRule1Check2	host-name CONTAINS android	AndroidRule1Check2
<input type="checkbox"/> Apple-DeviceRule1Check1	OUI CONTAINS Apple	Apple-DeviceRule1Check1
<input type="checkbox"/> Apple-MacBookRuleCheck1	User-Agent CONTAINS Macintosh	Apple-MacBookRuleCheck1
<input type="checkbox"/> Apple-MacBookRuleCheck2	User-Agent CONTAINS Mac OS	Apple-MacBookRuleCheck2
<input type="checkbox"/> Apple-iPadRule1Check1	User-Agent CONTAINS iPad	
<input type="checkbox"/> Apple-iPadRule2Check2	host-name CONTAINS iPad	Apple-iPadRule2Check2
<input type="checkbox"/> Apple-iPhoneRule1Check1	User-Agent CONTAINS iPhone; U; CPU iPho	Apple-iPhoneRule1Check1
<input type="checkbox"/> Apple-iPhoneRule2Check1	host-name CONTAINS iPhone	Apple-iPhoneRule2Check1
<input type="checkbox"/> Apple-iPodRule1Check1	User-Agent CONTAINS iPod; U; CPU iPhone	Apple-iPodRule1Check1
<input type="checkbox"/> Apple-iPodRule3Check3	User-Agent CONTAINS iPod; U;	Apple-iPodRule3Check3
<input type="checkbox"/> Applera-Check	OUI EQUALS Applera Holding B.V. Singapore	Check for Applera Holding B.V. Singapore O
<input type="checkbox"/> Aruba-APRule1Check1	dhcp-class-identifier EQUALS ArubaAP	Aruba-APRule1Check1
<input type="checkbox"/> Aruba-DeviceRuleCheck1	OUI CONTAINS ARUBA NETWORKS	Aruba-DeviceRuleCheck1
<input type="checkbox"/> Avaya-DeviceRuleCheck1	OUI CONTAINS Avaya	Avaya-DeviceRuleCheck1
<input type="checkbox"/> Avaya-DeviceRuleCheck2	Check for Avaya IP Phone	

Conditions are defined by single matching attribute

Policy > Policy Elements > Conditions > Profiling



Profiler Policies

The image shows a screenshot of the Profiler Policy configuration interface. A callout box at the top right shows a flowchart of the policy processing logic: Endpoint Attributes -> Conditions -> Policy Rules > CF -> Profiling Policies -> Endpoint Identity Groups -> Authorization Policy. A secondary path branches from Profiling Policies to Policy Change/Exception Action -> Endpoint Identity Group Change -> Change of Authorization.

The main configuration area shows a policy named "Apple-iPad" with a description "Policy for Apple iPads". The "Minimum Certainty Factor" is set to 20. The "Exception Action" is set to NONE. The "Network Scan (NMAP) Action" is set to NONE. The "Create Matching Identity Group" option is selected. The "Parent Policy" is set to "Apple-Device".

Below the main configuration, there are two rules:

- Rule 1: If Condition: Apple-iPadRule2Check2 Then: Certainty Factor Increases 20
- Rule 2: If Condition: (Apple-iPadRule1Check1_AND Apple-MacBo... Then: Certainty Factor Increases 20

Three callout boxes provide details for the conditions used in the rules:

- Parent Policy Conditions Details:** Name: Apple-DeviceRule1Check1, Description: Apple-DeviceRule1Check1, Expression: MAC:OUI CONTAINS Apple
- Conditions Details (Rule 1):** Name: Apple-iPadRule2Check2, Description: Apple-iPadRule2Check2, Expression: DHCP:host-name CONTAINS iPad
- Conditions Details (Rule 2):** A table showing the expression breakdown for the second rule:

Name	Expression	Operator
Apple-iPadRule1Check1	IP:User-Agent CONTAINS iPad	AND
Apple-MacBookRuleCheck2	IP:User-Agent CONTAINS Mac OS	
Apple-iPadRule1Check3	IP:User-Agent CONTAINS AppleWebKit	

A green callout box at the bottom left states: "Select this option to create a matching Identity group", pointing to the "Create Matching Identity Group" option in the configuration.

Mapping Profiles to Identity Groups

Rule Name	Identity Groups	Other Conditions	Permissions
S5 IP Phones	Cisco-IP-Phone		Cisco_IP_Phones
S5 smartphones - tablets	AndroidORApple-iPadORApple-iPhone	Radius:Service-Type EQUALS Framed	internet_only
S5 Camera	cisco-camera		PermitAccess

Identity groups directly used as a policy condition

Endpoint Identity Groups

Edit Create Delete

Name	Description
<input type="checkbox"/> Android	Identity Group for Profile: Android
<input type="checkbox"/> Apple-iPad	Identity Group for Profile: Apple-iPad
<input type="checkbox"/> Apple-iPhone	Identity Group for Profile: Apple-iPhone
<input type="checkbox"/> Blacklist	Blacklist Identity Group
<input type="checkbox"/> Cisco-AP-Aironet-3500	Identity Group for Profile: Cisco-AP-Aironet
<input type="checkbox"/> Cisco-IP-Phone	Identity Group for Profile: Cisco-IP-Phone
<input type="checkbox"/> Profiled	Profiled Identity Group
<input type="checkbox"/> Unknown	Unknown Identity Group
<input type="checkbox"/> Workstation	Identity Group for Profile: Workstation
<input type="checkbox"/> cisco-camera	Identity Group for Profile: cisco-camera

Profiler Policy

* Name: Apple-iPad

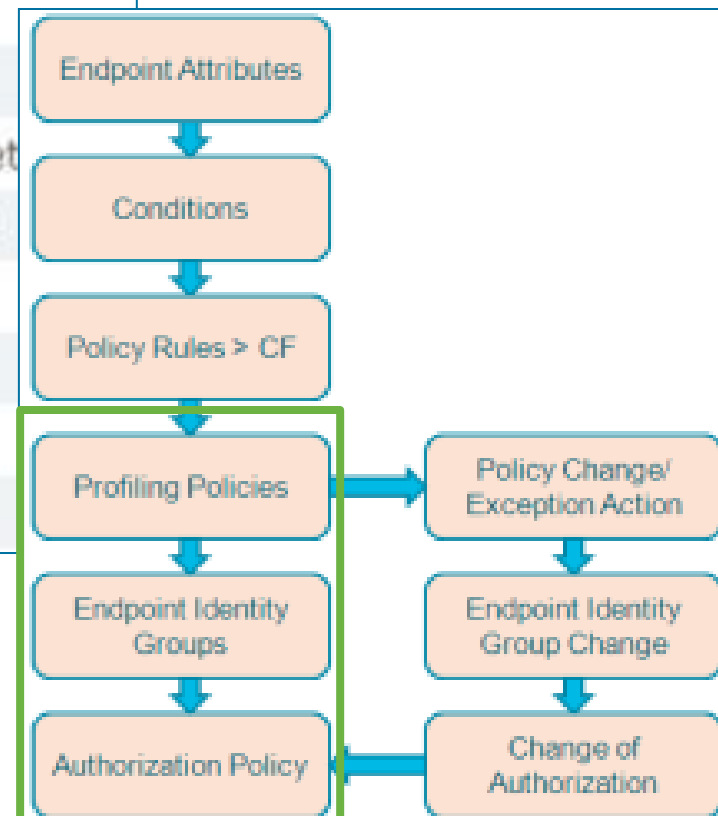
Policy Enabled:

* Minimum Certainty Factor: 20

* Exception Action: NONE

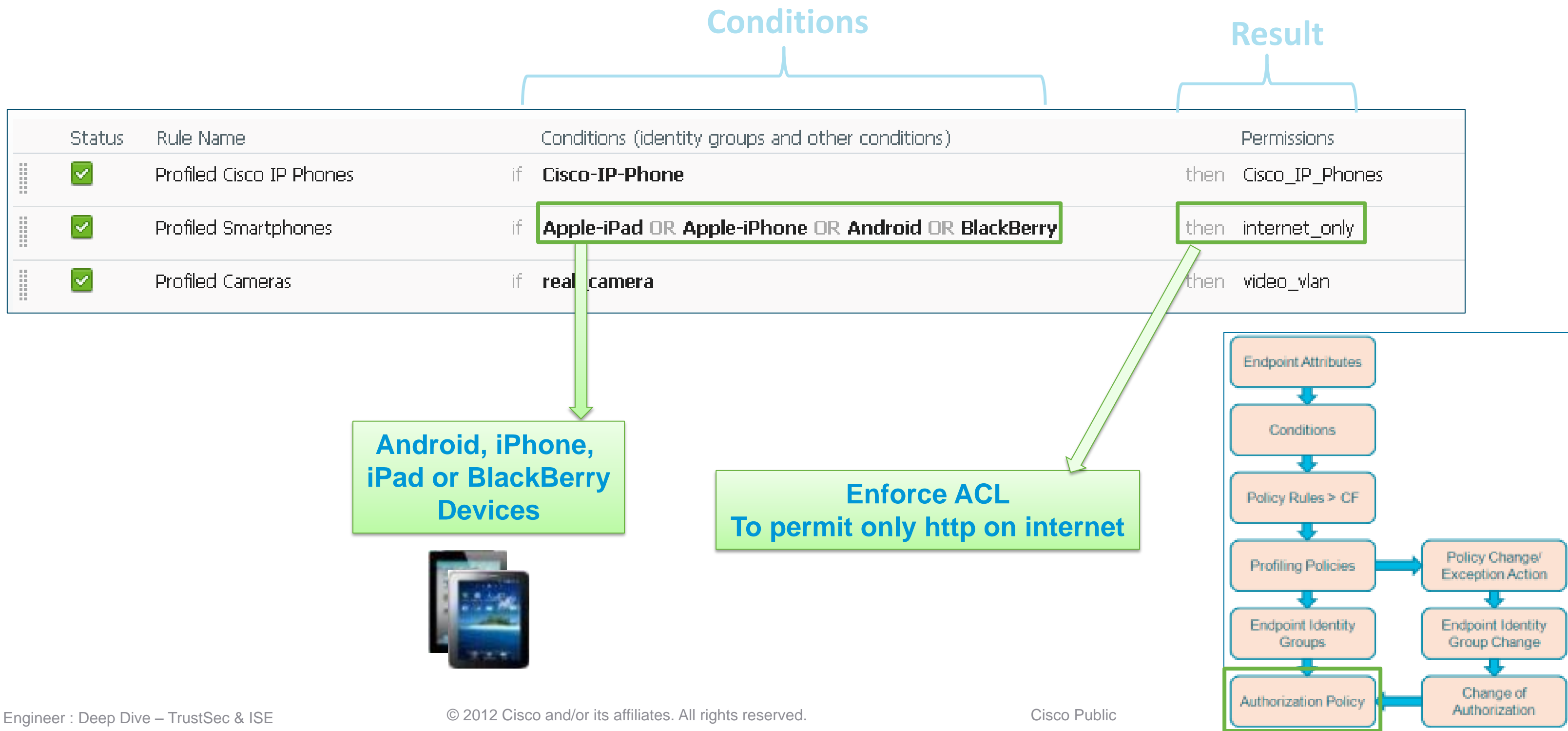
* Network Scan (NMAP) Action: NONE

Create Matching Identity Group



Using Profiles in Authorization Rules

Identity Groups are Defined as Conditions in Authorization Rules



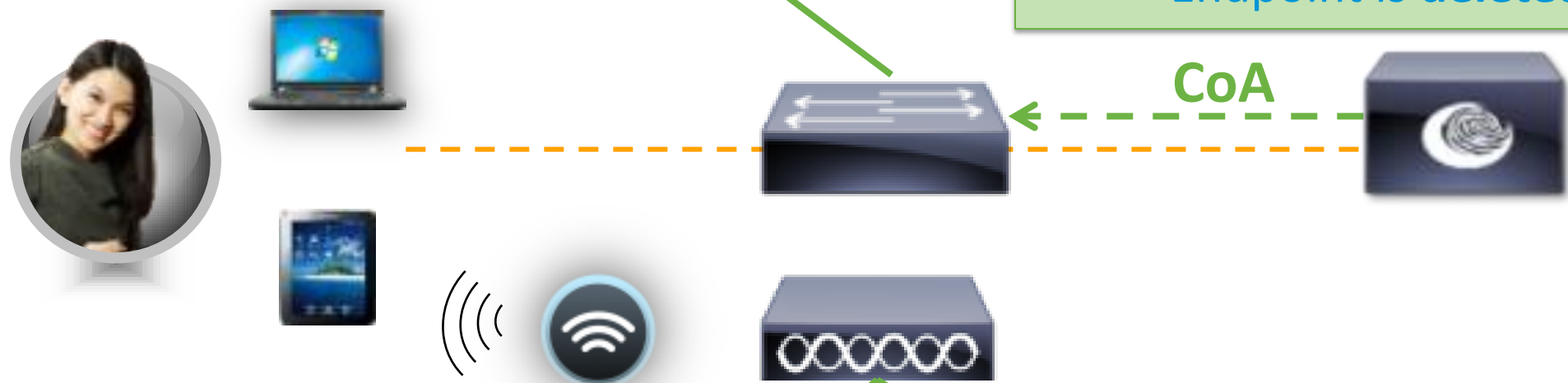
Profiling CoA

Allows ISE to Actively Enforce Policy Over Connected Endpoints

CoA is triggered dynamically for following profile transitions:

- Endpoint is **profiled for the 1st time**.
- Endpoint is **statically assigned with a new Policy**
- Endpoint is **deleted from ISE DB**.

```
aaa server radius dynamic-author
client 10.100.7.20 server-key xxxxxxxx
```



RADIUS Authentication Servers > Edit

Server Index	1
Server Address	10.100.7.20
Shared Secret Format	ASCII
Shared Secret	...
Confirm Shared Secret	...
Key Wrap	<input type="checkbox"/> (Designed for FIPS)
Port Number	1812
Server Status	Enabled
Support for RFC 3576	Enabled

WLANs > Edit (screenshot edited to fit)

General Security QoS Advanced

Allow AAA Override Enabled

NAC

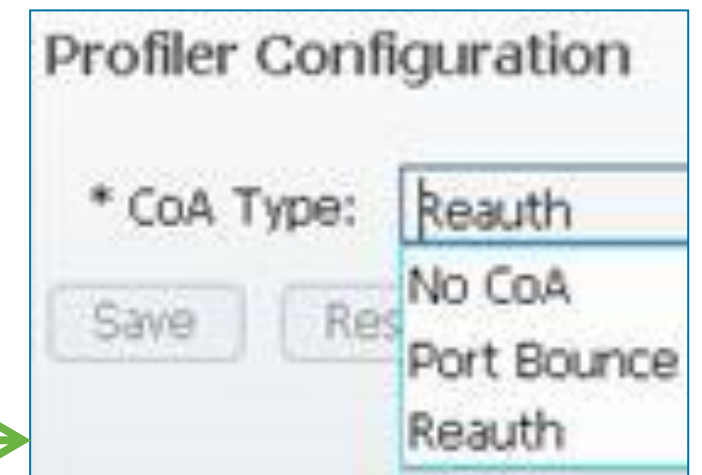
NAC State Radius NAC

CoA and Profiling Exceptions

Profile Transitions

- **Default Exception Actions** (Policy > Policy Elements > Results > Profiling > Exception Actions)

<input type="checkbox"/>	Profiler Action Name ▲	Description
<input type="checkbox"/>	EndpointDelete	When endpoint is deleted or reassigned to the unknown profile.
<input type="checkbox"/>	FirstTimeProfile	When an endpoint profile changes from unknown to known for the first time.
<input type="checkbox"/>	StaticAssignment	When an endpoint has connected to the network and is now statically assigned.



Profiler Configuration

* CoA Type: Reauth

Save Res

No CoA
Port Bounce
Reauth

Type of CoA sent for these events configured under global settings:

Administration → System → Settings → Profiling



- Predefined Exceptions are not configurable and cannot be assigned to a Profile. Administrator may define additional Exception Actions for use in Profiler Policy to trigger CoA and static Profiler Policy assignment.
- **NEW to 1.1.1!** CoA sent on any profile transition that results in change to endpoint access per Authorization Policy. (Based on change of ID Group where ID Group used in Authorization Policy).

Profiler Exception Policy Example

Draeger-M300 Heart Monitor – Default Profile

- Example of default profile

Profiler Policy List > Draeger-M300

Profiler Policy

* Name	<input type="text" value="Draeger-M300"/>	Description	<input type="text" value="Policy for Draeger M300 Medical devices"/>
Policy Enabled	<input checked="" type="checkbox"/>		
* Minimum Certainty Factor	<input type="text" value="20"/>	(Valid Range 1 to 65535)	
* Exception Action	<input type="text" value="NONE"/>		
* Network Scan (NMAP) Action	<input type="text" value="NONE"/>		
	<input type="radio"/> Create Matching Identity Group		
	<input checked="" type="radio"/> Use Hierarchy		
* Parent Policy	<input type="text" value="Draeger-Device"/>		

Rules

If Condition Then

Profiler Exception Policy Example

Create New Profiler Exception

- Add New Exception
- Go to **Policy > Policy Elements > Results > Profiling > Exception Actions**

Profiler Exception Action List > **Draeger-M300**

Profiler Exception Action

* Name	<input type="text" value="Draeger-M300"/>	Description	<input type="text" value="Static Policy Assignment for medical devices - no additional CoA"/>
COA Action	<input type="checkbox"/> Force COA		
* Policy Assignment	<input type="text" value="Draeger-M300"/>		

- In this example, action statically assigns endpoint to policy “Draeger-M300”, but NO CoA will be sent.

Profiler Exception Policy Example

Define Rule Conditions to Trigger Exception

- Add Condition(s) to trigger Exception Action

The screenshot displays the 'Rules' configuration page in Cisco ISE. It shows two rule entries. The first rule is 'If Condition Draeger-M300-Dst-Port Then Certainty Factor Increases 20'. The second rule is 'If Condition Conditions Then Certainty Factor Increases 0'. The 'Conditions' rule is expanded to show a table of conditions:

Condition Name	Expression	Logic	Settings
Draeger-M300-PortC	Draeger-M300-PortCheck1	OR	Settings
Draeger-M300-PortC	Draeger-M300-PortCheck2	OR	Settings
Draeger-M300-PortC	Draeger-M300-PortCheck3		Settings

- In this example, conditions that trigger Exception are identical to those used to match profile.

Profiler Exception Policy Example

Set Exception Action

- Set action for new rule to “Take Exception Action”
- Set Exception Action to new exception, i.e. Draeger-M300

Profiler Policy List > Draeger-M300

Profiler Policy

* Name Description

Policy Enabled

* Minimum Certainty Factor (Valid Range 1 to 65535)

* Exception Action

* Network Scan (NMAP) Action

Create Matching Identity Group
 Use Hierarchy

* Parent Policy

Rules

...	If Condition	<input type="text" value="Draeger-M300-PortCheck1_OR_Draeger-M30..."/>	+	Then	<input type="text" value="Certainty Factor Increases"/>	<input type="text" value="20"/>
...	If Condition	<input type="text" value="Draeger-M300-PortCheck1_OR_Draeger-M30..."/>	+	Then	<input type="text" value="Take Exception Action"/>	

Create Custom Conditions and Profiler Policy

Profiler Policy

* Name Description

Policy Enabled

* Minimum Certainty Factor (Valid Range 1 to 65535)

* Exception Action

* Network Scan (NMAP) Action

Create Matching Identity Group
 Use Hierarchy

* Parent Policy

Rules

If Condition	<input type="text" value="MAC_OUI_EQUALS_02345__DHCP_dhcp-cla..."/>	+	Then	<input type="text" value="Certainty Factor Increases"/>	<input type="text" value="10"/>
If Condition	<input type="text" value="LLDP_lldpSystemDescription_EQUALS_test"/>	+	Then	<input type="text" value="Certainty Factor Increases"/>	<input type="text" value="10"/>

Profiler Condition List > New Profiler Condition

* Name

* Type

* Attribute Name

* Operator

* Attribute Value

Condition Name	Expression	AND
<input type="text"/>	MAC:OUI <input type="text" value="012345"/>	<input type="text" value="AND"/>
<input type="text"/>	DHCP:dhcp-class-ide <input type="text" value="test"/>	<input type="text" value="AND"/>
<input type="text"/>	IP:User-Agent <input type="text" value="test"/>	<input type="text" value="AND"/>

ISE Profiler Library



~300 (and growing) Pre-built Policies for Device Classification

Endpoint	Vendor	Model	OS	Device	Manufacturer	Model	OS	Device	Manufacturer	Model	OS	Device	Manufacturer	Model
Android	Canon-De	Cisco-DMP	Cisco-IP-PH	DLink-DAP-	HP-Color-L	HP-LaserJ	Lexmark-T	OS_X_Lion-	Samsung-	Xerox-Colo	Xerox-Pha	Xerox-Ph	Xerox-W	Xerox-Workcentre-6505n
Apple-Dev	Canon-MP	Cisco-Devi	Cisco-IP-PH	DLink-Devi	HP-Color-L	HP-LaserJ	Lexmark-T	OS_X_Snow	Samsung-	Xerox-Colo	Xerox-Pha	Xerox-Ph	Xerox-W	Xerox-Workcentre-7120
Apple-Mac	CareFusio	Cisco-IP-C	Cisco-IP-PH	Debian-Wo	HP-Color-L	HP-LaserJ	Lexmark-T	OS_X_Tiger	Samsung-	Xerox-Colo	Xerox-Pha	Xerox-Ph	Xerox-W	Xerox-Workcentre-7132-Multif
Apple-iDev	CentOS-V	Cisco-IP-C	Cisco-IP-PH	Draeger-De	HP-Color-L	HP-LaserJ	Linksys-De	OpenBSD-W	Solaris-Wo	Xerox-Colo	Xerox-Pha	Xerox-Ph	Xerox-W	Xerox-Workcentre-7242
Apple-iPad	Cisco-AIR	Cisco-IP-C	Cisco-IP-PH	Draeger-De	HP-Color-L	HP-LaserJ	LinksysWA	OracleEnter	SonyPS3	Xerox-Colo	Xerox-Pha	Xerox-Ph	Xerox-W	Xerox-Workcentre-7345
Apple-iPho	Cisco-AIR	Cisco-IP-C	Cisco-IP-PH	Draeger-M3	HP-Color-L	HP-LaserJ	Linux-Wo	PCLinuxOS-	Sun-Work	Xerox-Colo	Xerox-Pha	Xerox-Ph	Xerox-W	Xerox-Workcentre-7346
Apple-iPod	Cisco-AIR	Cisco-IP-P	Cisco-IP-PH	Enterasys-D	HP-Device	HP-LaserJ	LinuxMint	Philips-Devi	SymbianO	Xerox-Colo	Xerox-Pha	Xerox-Ph	Xerox-W	Xerox-Workcentre-7428
Applera-D	Cisco-AIR	Cisco-IP-P	Cisco-IP-PH	Fedora-Wo	HP-JetDire	HP-LaserJ	Macintosh	Philips-Intell	Ubuntu-W	Xerox-Colo	Xerox-Pha	Xerox-Ph	Xerox-W	Xerox-Workcentre-7435
Aruba-AP	Cisco-AIR	Cisco-IP-P	Cisco-IP-PH	FreeBSD-W	HP-LaserJe	HTC-Devi	Mandriva-	Polycom-De	VMWare-D	Xerox-Devi	Xerox-Pha	Xerox-Ph	Xerox-W	Xerox-Workcentre-7535
Aruba-Dev	Cisco-AIR	Cisco-IP-P	Cisco-IP-PH	Gentoo-Wo	HP-LaserJe	HTC-Phor	Microsoft-	RICOH-Afici	Vista-Wor	Xerox-Docu	Xerox-Pha	Xerox-Ph	Xerox-W	Xerox-Workcentre-7556
Avaya-Dev	Cisco-AIR	Cisco-IP-P	Cisco-IP-PH	HP-Color-La	HP-LaserJe	IP-Phone	Microsoft-	RICOH-Afici	Windows7	Xerox-Faxc	Xerox-Pha	Xerox-Ph	Xerox-W	Xerox-Workcentre-7675
Avaya-IP-P	Cisco-AIR	Cisco-IP-P	Cisco-IP-PH	HP-Color-La	HP-LaserJe	ISE-Appli	MotorolaD	RICOH-Afici	Windows7	Xerox-Igen	Xerox-Pha	Xerox-Ph	Xerox-W	Xerox-Workcentre-7755
BlackBerry	Cisco-AP-	Cisco-IP-P	Cisco-Rout	HP-Color-La	HP-LaserJe	Konica-De	MotorolaM	RICOH-Afici	Workstati	Xerox-Phas	Xerox-Pha	Xerox-Pr	Xerox-W	Xerox-Workcentre-7775
Brother-D	Cisco-AP-	Cisco-IP-P	Cisco-Swit	HP-Color-La	HP-LaserJe	Konica-Mir	Netgear-D	RICOH-Afici	XBOX360	Xerox-Phas	Xerox-Pha	Xerox-W	Xerox-W	Xerox-Workcentre-M118
Brother-HI	Cisco-AP-	Cisco-IP-P	Cisco-Tele	HP-Color-La	HP-LaserJe	Konica-Mir	NintendoV	RICOH-Afici	Xandros-V	Xerox-Phas	Xerox-Pha	Xerox-W	Xerox-W	Xerox-Workcentre-M20
Brother-HI	Cisco-Acc	Cisco-IP-P	Cisco-WLC	HP-Color-La	HP-LaserJe	Kubuntu-	Nortel-De	RICOH-Devi	Xerox-412	Xerox-Phas	Xerox-Pha	Xerox-W	Xerox-W	Xerox-Workcentre-M20i
Brother-M	Cisco-DM	Cisco-IP-P	Cisco-WLC	HP-Color-La	HP-LaserJe	Lexmark-D	Nortel-IP-	RedHat-Wo	Xerox-700	Xerox-Phas	Xerox-Pha	Xerox-W	Xerox-W	Xerox-Workcentre-M20i
Brother-M	Cisco-DM	Cisco-IP-P	Cisco-WLC	HP-Color-La	HP-LaserJe	Lexmark-P	OS_X-Wo	Router	Xerox-Col	Xerox-Phas	Xerox-Pha	Xerox-W	Xerox-W	Xerox-Workcentre-Pro-133
Canon-Dev	Cisco-DM	Cisco-IP-P	Cisco-WLC	HP-Color-La	HP-LaserJe	Lexmark-T	OS_X_Le	SUSE-Work	Xerox-Col	Xerox-Phas	Xerox-Pha	Xerox-W	Xerox-W	Xerox-Workcentre-Pro-C3545

ISE – Profile Library

- Profiling Policies
 - Android
 - Apple-Device
 - Applera-Device
 - Aruba-Device
 - Avaya-Device
 - BlackBerry
 - Cisco-Device
 - DLink-Device
 - Enterasys-Device
 - HP-Device
 - HTC-Device
 - ISE-Appliance
 - Lexmark-Device
 - Microsoft-Device
 - MotorolaMobile-Device
 - Netgear-Device
 - NintendoWii
 - Nortel-Device
 - SonyPS3
 - SymbianOS-Device
 - VMWare-Device
 - Workstation
 - Xerox-Device

- Apple-Device
 - Apple-MacBook
 - Apple-iPad
 - Apple-iPhone
 - Apple-iPod

- Cisco-Device
 - Cisco-Access-Point
 - Cisco-AP-Aironet-1130
 - Cisco-AP-Aironet-1240
 - Cisco-AP-Aironet-1250
 - Cisco-IP-Phone
 - Cisco-WLC-2100-Series
 - Linksys-Device

- Cisco-Device
 - Cisco-Access-Point
 - Cisco-AP-Aironet-1130
 - Cisco-AP-Aironet-1240
 - Cisco-AP-Aironet-1250
 - Cisco-IP-Phone
 - Cisco-IP-Conference-Station-7935
 - Cisco-IP-Conference-Station-7936
 - Cisco-IP-Conference-Station-7937
 - Cisco-IP-Phone-7902
 - Cisco-IP-Phone-7905
 - Cisco-IP-Phone-7906
 - Cisco-IP-Phone-7910
 - Cisco-IP-Phone-7911
 - Cisco-IP-Phone-7912
 - Cisco-IP-Phone-7940
 - Cisco-IP-Phone-7941
 - Cisco-IP-Phone-7942
 - Cisco-IP-Phone-7945
 - Cisco-IP-Phone-7945G
 - Cisco-IP-Phone-7960
 - Cisco-IP-Phone-7961
 - Cisco-IP-Phone-7962
 - Cisco-IP-Phone-7965
 - Cisco-IP-Phone-7970
 - Cisco-IP-Phone-7971
 - Cisco-IP-Phone-7975
 - Cisco-IP-Phone-7985
 - Cisco-IP-Phone-9971
 - Cisco-WLC-2100-Series
 - Linksys-Device

Profiling Design Considerations

- General Profile Design Planning

1. Identify endpoints requiring device classification (authorization based on profile attributes)

2. Determine required attributes

Most popular endpoints have pre-built profiles. Determine requirements by reviewing default ISE profiles (Profile X contains conditions A, B, and C). Which data/probes are used to collect that data?

Can often determine profiling requirements for similar endpoints types by reviewing existing profiles.

If no existing profile, then temporarily enable probes, collect attributes, and see what device offers.

Some devices may require traffic analysis to determine unique attributes for OUI, DHCP options, User Agent, TCP/UDP ports, or DNS naming

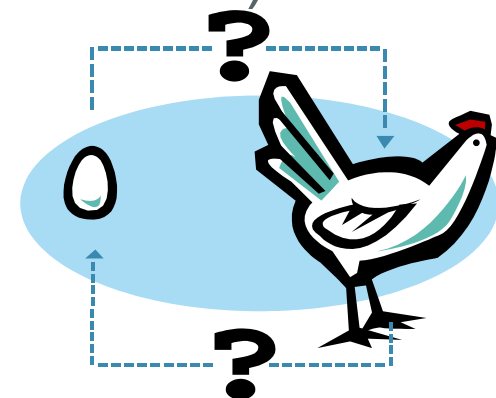
3. Determine best option from available methods to collect required profile data

- Access Device Configuration:

Profile Timing – impacted by MAB/802.1X order and deployment mode (auth open vs closed)

Do access policies allow collection of attributes needed to match policy conditions? →

- Exception Policies may be required to override dynamic ID group assignments.



Determining Required Profile Attributes

Which Data Should I Collect to Match a Specific Profile Policy?

Profiler Policy List > Apple-iPod

* Name Description

Policy Enabled

* Minimum Certainty Factor (Valid Range 1 to 65535)

* Exception Action

Create Matching Identity Group

Use Hierarchy

* Parent Policy

Rules

- If Condition
- If Condition

Conditions Details

Name **Apple-iPodRule1Check1**

Description **Apple-iPodRule1Check1**

Expression **IP:User-Agent CONTAINS iPod; U; CPU iPhone OS**

Determining Required Profile Attributes

Profile Conditions Reveal Specific Probes and Attributes

<input type="checkbox"/>	AndroidRule1Check1	User-Agent CONTAINS Android	
<input type="checkbox"/>	AndroidRule1Check2	host-name CONTAINS android	
<input type="checkbox"/>	Apple-DeviceRule1Check1	OUI CONTAINS Apple	
<input type="checkbox"/>	Apple-MacBookRuleCheck1	User-Agent CONTAINS Macintosh	
<input type="checkbox"/>			S Mac OS
<input type="checkbox"/>	HP-DeviceRule2Check1	OUI CONTAINS Hewlett	
<input type="checkbox"/>	HP-JetDirect-Printer-Check	dhcp-class-identifier CONTAINS JetDirect	S iPad
<input type="checkbox"/>	HTC-DeviceRule1Check1	OUI EQUALS HTC Corporation	S AppleWebKit
<input type="checkbox"/>	ISE-ApplianceCheck	cdpCachePlatform CONTAINS ISE	S iPad
<input type="checkbox"/>	Kubuntu-WorkstationRule1Check1	User-Agent CONTAINS Kubuntu	
<input type="checkbox"/>	Lexmark-DeviceRule1Check1	OUI CONTAINS Lexmark	S iPhone
<input type="checkbox"/>	Lexmark-Printer-E260dnRule1Check1	dhcp-class-identifier CONTAINS Lexmark E	S iPhone: U: CPU iPh

Profiling Policy Plan



Profiling Policy / Requirements Example:

Device Profile	Unique Attributes	Probes Used	Collection Method
Cisco IP Phone	OUI	RADIUS	RADIUS Authentication
	CDP	SNMP Query	Triggered by RADIUS Start
IP Camera	OUI	RADIUS	RADIUS Authentication
	CDP	SNMP Query	Triggered by RADIUS Start
Printer	OUI	RADIUS	RADIUS Authentication
	DHCP Class Identifier	DHCP	IP Helper from local L3 switch SVI
POS Station (static IP)	MAC Address	RADIUS (MAC Address discovery)	RADIUS Authentication
	ARP Cache for MAC to IP mapping	SNMP Query	Triggered by RADIUS Start
	DNS name	DNS	Triggered by IP Discovery
Apple iPad/iPhone	OUI	RADIUS	RADIUS Authentication
	Browser User Agent	HTTP	Authorization Policy posture redirect to central Policy Service node cluster
	DHCP Class Identifier + MAC to IP mapping	DHCP	IP Helper from local L3 switch SVI
Device X	MAC Address	RADIUS (MAC Address discovery)	RADIUS Authentication
	Requested IP Address for MAC to IP mapping	DHCP	RSPAN of DHCP Server ports to local Policy Service node
	Optional to acquire ARP Cache for MAC to IP mapping	SNMP Query	Triggered by RADIUS Start
	Port # traffic to Destination IP	NetFlow	NetFlow export from Distribution 6500 switch to central Policy Service node

Probe Overview



Select Profiling Probes

ISE Probes

- ISE Profiler can use various probes to identify devices. It may not be easy to choose which ones to use:

RADIUS HTTP DHCPSPAN

DHCP SNMP Query NetFlow

DNS NMAP SNMP Trap

The screenshot shows the 'Profiling Configuration' tab in the ISE Profiler configuration interface. It lists several probes, each with an unchecked checkbox and a right-pointing arrow icon:

- NETFLOW
- DHCP
- DHCPSPAN
- HTTP
- RADIUS
- Network Scan (NMAP)
- DNS
- SNMPQUERY
- SNMPTRAP

Select Profiling Probes

ISE Probes

Home Operations Policy Administration

System Identity Management Network Resources Guest Management

Deployment Licensing Certificates Logging Maintenance Admin Access Settings

Deployment

ise-mnt-1
ise-pan-1
ise-psn-1
ise-psn-2

1 Edit Node

General Settings Profiling Configuration

Hostname **ise-psn-1**
FQDN **ise-psn-1.cts.local**
IP Address **10.1.100.5**
Node Type **Identity Services Engine (ISE)**

Personas

Administration Role **SECONDARY**

Monitoring Role **SECONDARY**

Policy Service

Enable Session Services ⓘ

Include Node in Node Group **<None>**

Enable Profiling Service

General Set **2** Profiling Configuration

▶ NETFLOW

▶ DHCP

▶ DHCPSPAN

▶ HTTP

▶ RADIUS

▶ Network Scan (NMAP)

▶ DNS

▶ SNMPQUERY

▶ SNMPTRAP

RADIUS Probe

RADIUS Packets Received from Network Access Devices

- Common RADIUS Attributes

User-Name	NAS-IP-Address	NAS-Port	Framed-IP-Address
Calling-Station-Id	Acct-Session-Id	Acct-Session-Time	Acct-Terminate-Cause

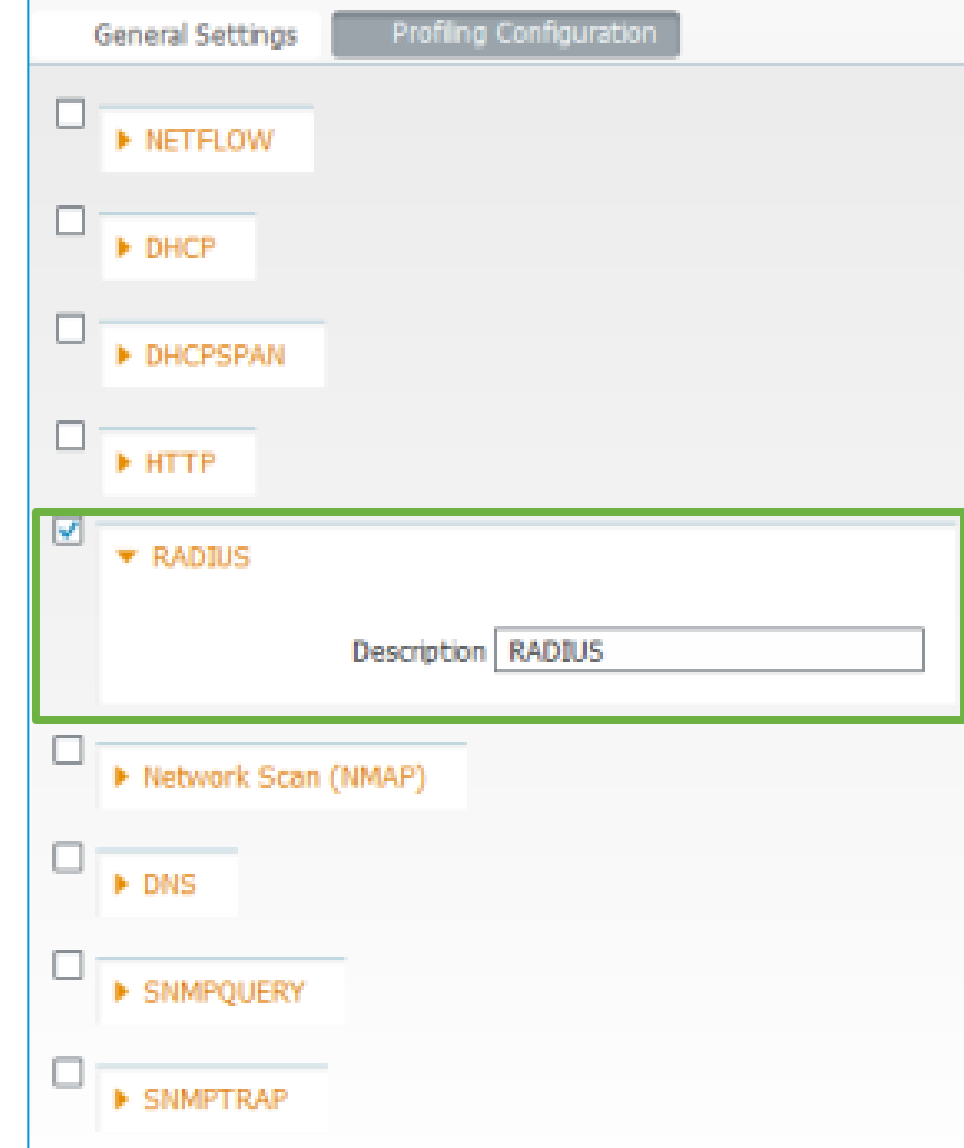
Endpoint IP Address



Dependent on NAD config, but usually Endpoint MAC Address

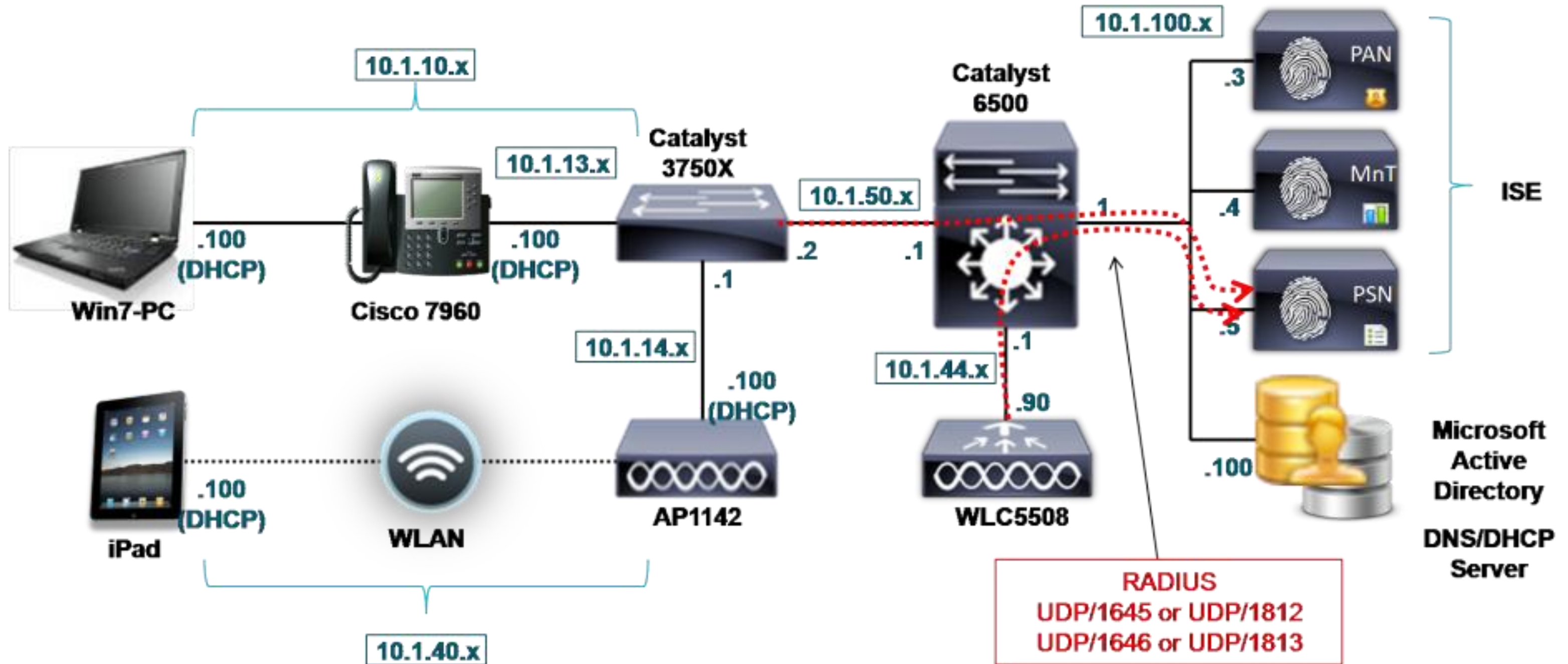
- MAC address -> OUI for NIC vendor classification
- RADIUS Accounting provides MAC:IP binding to support other probes that rely on IP address (DNS, NetFlow, NMAP, and HTTP)
- Sample access switch configuration:
 - Enable RADIUS Auth and Accounting for ISE PSNs enabled for session and profiling services.
 - Include options to send various attributes via RADIUS.

```
aaa authentication dot1x default group radius
aaa authorization network default group radius
aaa accounting dot1x default start-stop group radius
ip radius source-interface xxx
radius-server attribute 6 on-for-login-auth
radius-server attribute 8 include-in-access-req
radius-server attribute 25 access-request include
radius-server host @PSN auth-port 1812 acct-port 1813 key xxx
radius-server vsa send accounting
radius-server vsa send authentication
```



RADIUS Probe

Sample Profiling Topology



SNMP Trap Probe

SNMP Traps Received from Network Access Devices

- SNMP Trap probe intended for use with SNMP Query probe to trigger queries against access device.
- Supports Link Down/Up, MAC Notification, and Informs. (ISE does not currently process WLC traps.)
- NAD config in ISE must be set to accept traps.

SNMP Settings

• SNMP Version

• SNMP RO Community

• Polling Interval seconds

Link Trap Query

MAC Trap Query

- Sample access switch configuration for SNMP Link and MAC Notification traps:

```
interface <Endpoint_Interface>
  snmp trap mac-notification added
  snmp trap mac-notification removed
  mac address-table notification change
  mac address-table notification mac-move
  snmp-server trap-source <Management_Interface>
  snmp-server enable traps snmp linkdown linkup
  snmp-server enable traps mac-notification change move
  snmp-server host @PSN version 2c cisco
```

General Settings Profiling Configuration

NETFLOW

DHCP

DHCPSPAN

HTTP

RADIUS

Network Scan (NMAP)

DNS

SNMPQUERY

SNMPTRAP

Link Trap Query

MAC Trap Query

Interface

Port

Description

SNMP Query Probe

SNMP Polling of Configured Network Access Devices

- **System Query** – Periodic per Polling Interval set in NAD config

Reads the following MIBs: System, cdpCacheEntry, IldpLocalSystemData, IldpRemoteSystemsData, cLApEntry (WLC only), and cldcClientEntry (WLC only)

Polling distributed amongst all PSNs with SNMPQuery probe enabled.

ARP info collected during to build IP ARP Cache table in ISE.

- **Interface Query** – Triggered by SNMP Trap or RADIUS Accting Start for specific interface

- Reads the following MIBs:
 - Interface data (ifIndex, ifDesc, etc)
 - CDP (if Cisco) and LLDP data
 - Session Data (for if_type=Ethernet)
 - Port, VLAN, dot1X data

- **Sample access device configuration:**

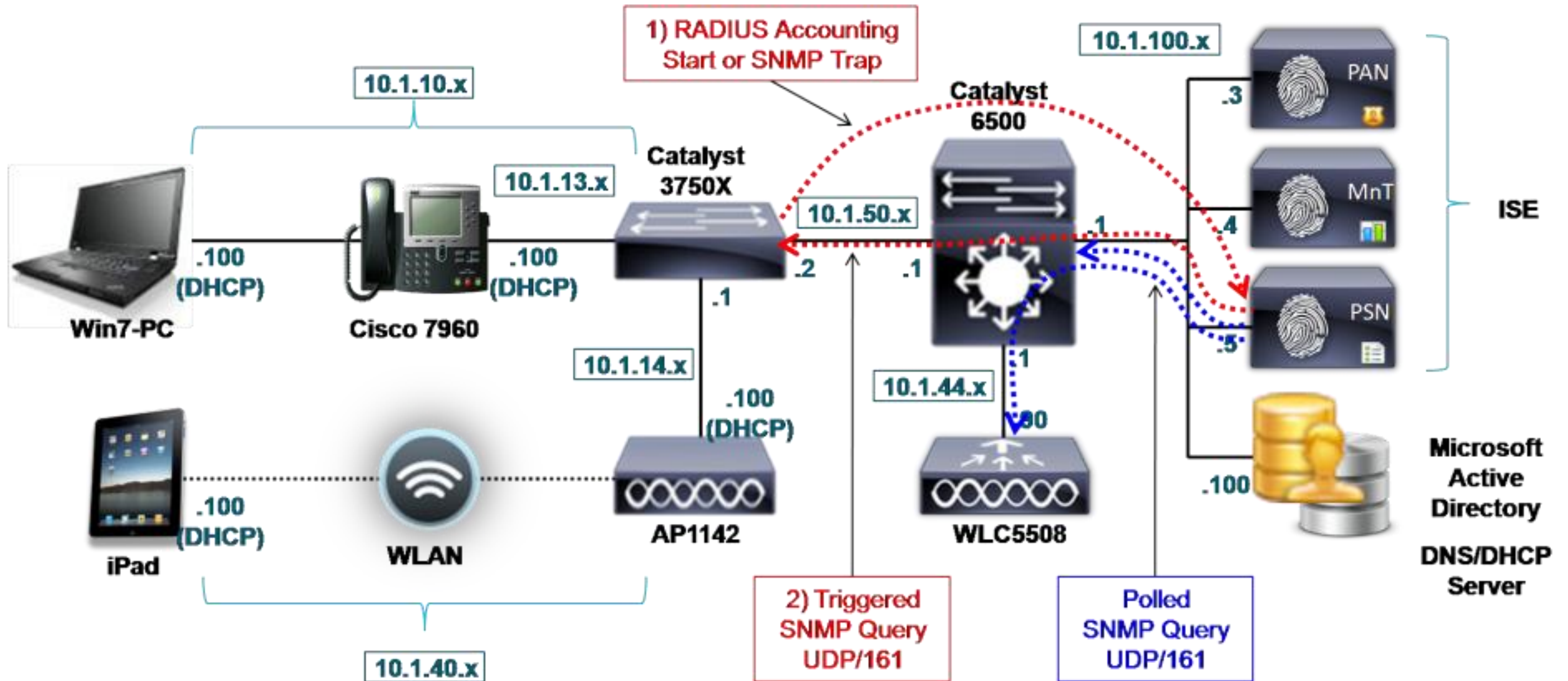
```
snmp-server community ciscoro RO
snmp-server community ciscorw RW
```

Send Interface Query 30 sec after trigger

Select optimal PSN to perform polling; only PSNs enabled for SNMP Query probe will display in list.

SNMP Query Probe

Sample Profiling Topology



SNMP Query Probe

CDP / LLDP Data Collection

- MIB Data Collected: **CDP**
 - ◆ cdpCacheAddress
 - ◆ cdpCacheCapabilities
 - ◆ cdpCacheDeviceId
 - ◆ cdpCachePlatform
 - ◆ cdpCacheVersion
- Broad Cisco/3rd-party device support
- Sample access switch configuration:

– **CDP:**

```
cdp run
interface <Interface>
  cdp enable
```

– **LLDP:**

```
lldp run
interface <Interface>
  lldp receive
```

LLDP

- ◆ lldpCacheCapabilities
- ◆ lldpCapabilitiesMapSupported
- ◆ lldpChassisId
- ◆ lldpManAddress
- ◆ lldpPortDescription
- ◆ lldpPortId
- ◆ lldpSystemCapabilitiesMapEnabled
- ◆ lldpSystemDescription
- ◆ lldpSystemName
- ◆ lldpTimeToLive

The screenshot shows the 'Profiling Configuration' page with the 'SNMPQUERY' section expanded. The 'SNMPQUERY' section is checked and contains the following configuration fields:

- Retries: 2
- Timeout: 1000
- EventTimeout: 30
- Description: SNMPQUERY

Other sections visible include NETFLOW, DHCP, DHCPSPAN, HTTP, RADIUS, Network Scan (NMAP), DNS, and SNMPTRAP.

Note: Wireless LAN Controllers do not support CDP/LLDP for wireless clients – only CDP on wired connection, so CDP info is not specific to connected wireless endpoints needed for wireless profiling.

DHCP Probes

Collect DHCP Request Attributes from User/Proxy/Helper

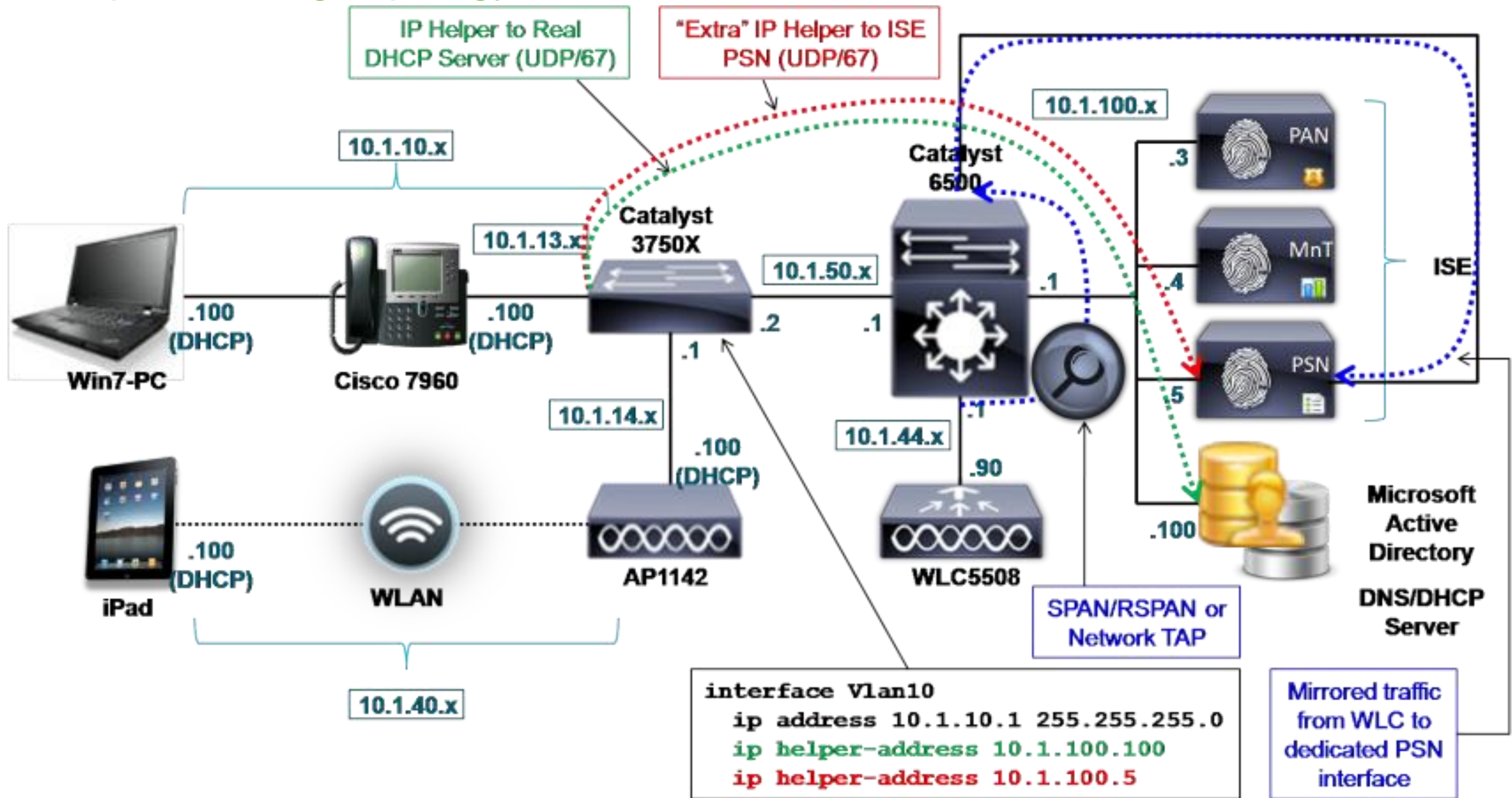
- **DHCP Probe** – Used when PSN interface is destination for DHCP relay traffic.
 - DHCP Proxy also supported, but NAD typically cannot send to more than one target at same time—only after failure or timeout of primary
- **DHCP SPAN Probe** – Captures DHCP packets from a mirrored port such as from SPAN/RSPAN/ERSPAN or network tap
 - Recommend dedicated ISE interface
 - Be sure to enable ISE interface from CLI and make any needed physical connections to SPAN port / tap.
- Sample L3 gateway device configuration:
 - Gateway is the access device if SVI present for client VLAN.

```
interface X (Routed port or VLAN interface)
 ip helper-address @REAL_DHCP_SERVER
 ip helper-address @PSN_Probe_Interface
```

The screenshot shows the 'Profiling Configuration' page in Cisco ISE. It features a sidebar with various protocol categories: NETFLOW, DHCP, DHCPSPAN, HTTP, RADIUS, Network Scan (NMAP), DNS, SNMPQUERY, and SNMPTRAP. The DHCP and DHCPSPAN sections are expanded and highlighted with a green border. The DHCP section is configured with Interface: GigabitEthernet 0, Port: 67, and Description: DHCP. The DHCPSPAN section is configured with Interface: GigabitEthernet 0 and Description: DHCPSPAN. Green arrows point from the text in the slide to these configuration sections.

DHCP Probes

Sample Profiling Topology



Identifying the Machine AND the User

Real Customer Example: Profiling Based on a Custom DHCP Attribute

- One customer decided to modify the DHCP Class Identifier on their Domain Computers
Provided a unique way to profile the device as a Corporate Asset.

- Manual Configuration Example:

```
C:\>ipconfig /setclassid "Local Area Connection" CorpXYZ
```

Windows XP IP Configuration
DHCP ClassId successfully modified for adapter "Local Area Connection"

[http://technet.microsoft.com/en-us/library/cc783756\(WS.10\).aspx](http://technet.microsoft.com/en-us/library/cc783756(WS.10).aspx)

- GPO Script Configuration Example:

- 1 - Create a GPO which has the necessary IPCONFIG command in a startup script
- 2 - Create a Domain Local group called something like 'Laptop Computer Accounts' and add all the laptop computer accounts
- 3 - Modify the GPO by removing the 'Authenticated Users' from the permissions list
- 4 - Add the 'Laptop Computer Accounts' group to the permissions list and assign 'Read' and 'Apply Group Policy' permissions.
- 5 - Link the GPO to the domain root (or the highest level OU which will encompass all computer accounts)

Profiler Policy List > New Profiler Policy

Profiler Policy

* Name: CorpXYZ Description: Look for Custom DHCP User-Class-ID

Policy Enabled:

* Minimum Certainty Factor: 10 (Valid Range 1 to 65535)

* Exception Action: NONE

* Network Scan (NMAP) Action: NONE

Create Matching Identity Group
 Use Hierarchy

* Parent Policy: NONE

Rules

If Condition: DHCP_dhcp-user-class-id_EQUALS_CorpXYZ Then: Certainty Factor Increases 15

Submit Cancel

Condition value must be expressed in hex.

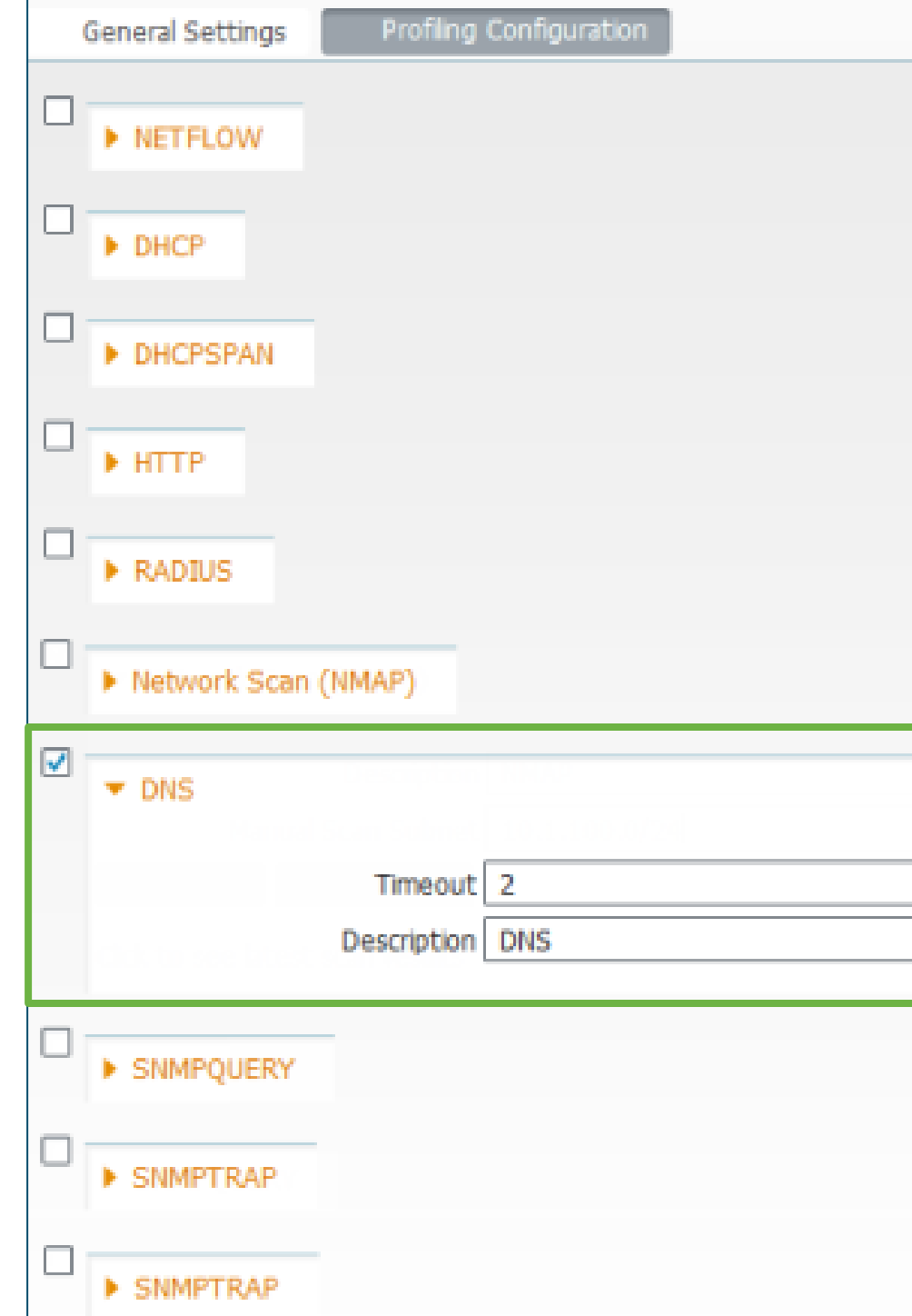
DNS Probe

Collect FQDN of Endpoint via Reverse Name Server Lookup

- If DNS Probe enabled, upon learning IP address of endpoint, reverse DNS lookup performed by PSN against its locally configured name server to retrieve the endpoint FQDN.
- DNS Probe requires IP address for reverse DNS lookup obtained from one of the following sources:
 - RADIUS Probe – “Framed-IP-Address”
 - SNMP Probe – “cdpCacheAddress”
 - DHCP Probes – “dhcp-requested-address”
- DNS Probe requires DNS reverse PTR records! DHCP clients will require DDNS to be configured and enabled on Servers.

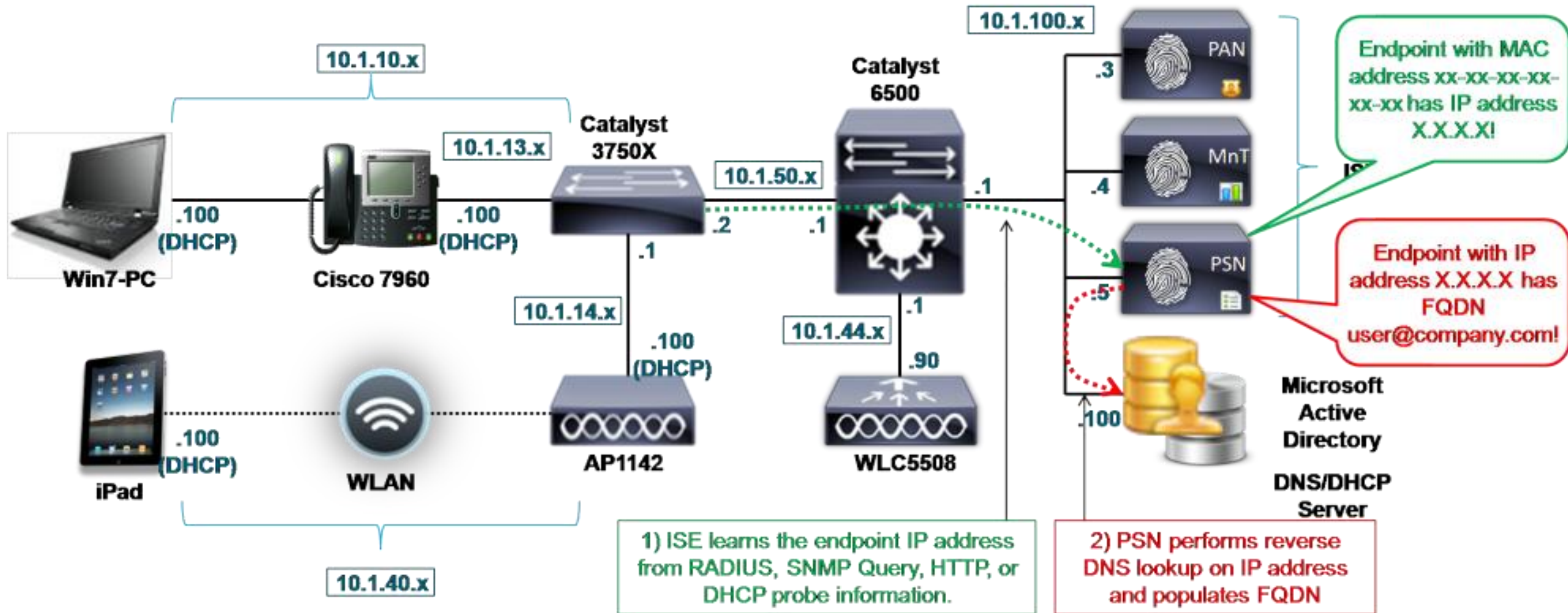
- Sample ISE PSN configuration (CLI):

```
ise-pan-1/admin(config)# ip name-server ?  
<A.B.C.D> Primary DNS server IP address  
<A.B.C.D> DNS server 2 IP address  
<A.B.C.D> DNS server 3 IP address
```



DNS Probe

Sample Profiling Topology



HTTP Probe

Collect HTTP Packet Data from SPAN or URL-Redirects

- **HTTP SPAN Probe** – Captures HTTP User Agent and other HTTP attributes for packets on TCP/80 and TCP/8080
 - Recommend dedicated ISE interface
 - Be sure to enable ISE interface from CLI and make any needed physical connections to SPAN port / tap.
- **URL Redirected Traffic** – HTTP probe can capture traffic sent to PSN via URL Redirection.

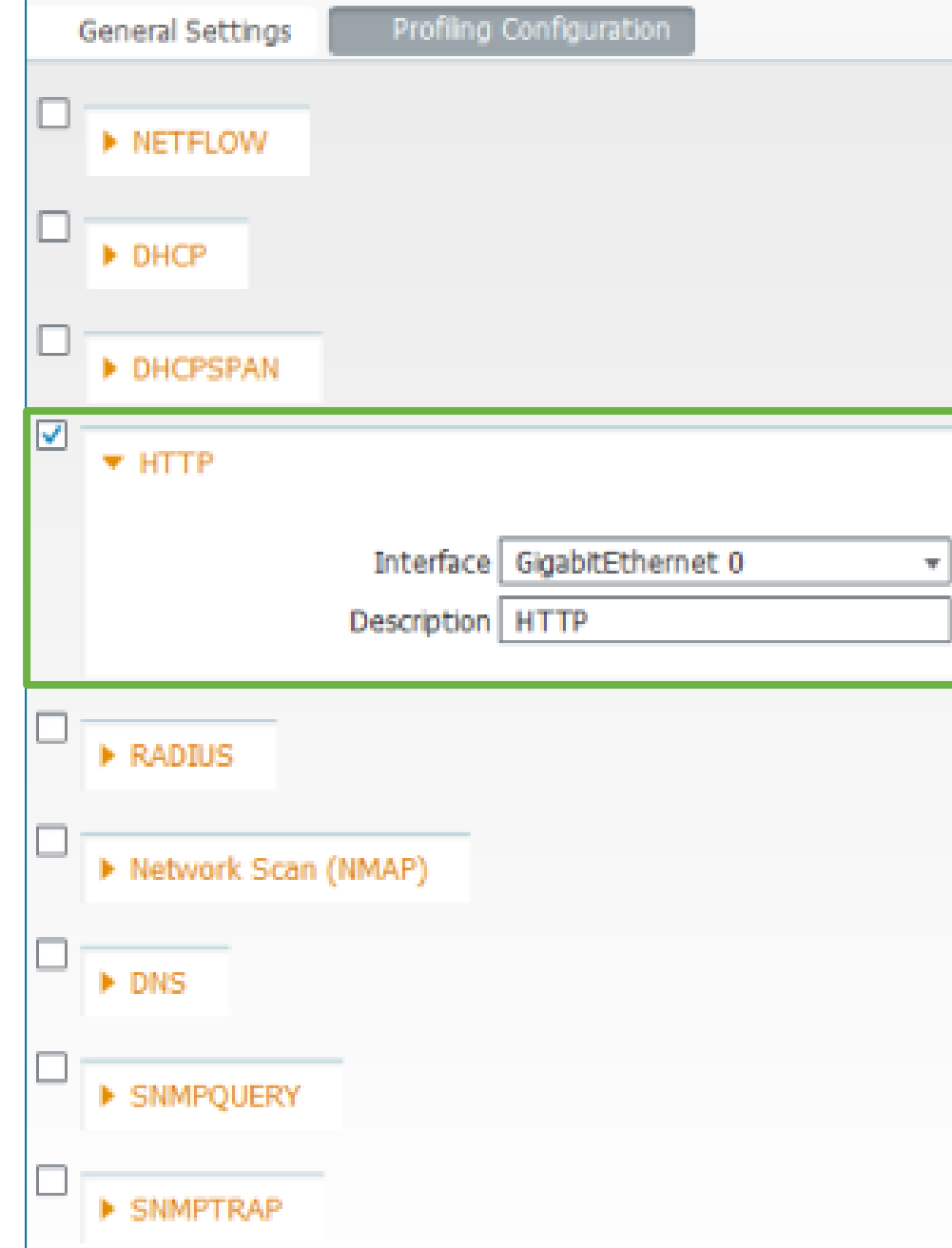
URL Redirected traffic includes LWA, CWA, Client Provisioning, Posture, Native Supplicant Provisioning, and Device Registration WebAuth.

Dedicated interface not required; Probe interface is typically the interface that terminates RADIUS traffic per IP variable substitution of the Redirect URL. URL Redirect example:

```
cisco-av-pair = url-redirect=https://ip:port/guestportal/gateway?sessionId=SessionIdValue&action=cwa
```

- Sample access switch configuration to support http redirects:

```
ip http server
ip access-list extended REDIRECT-ACL
permit tcp any any eq http
```



HTTP Probe

Sample Profiling Topology



NetFlow Probe

Collect NetFlow Export Data from NetFlow-Capable Device

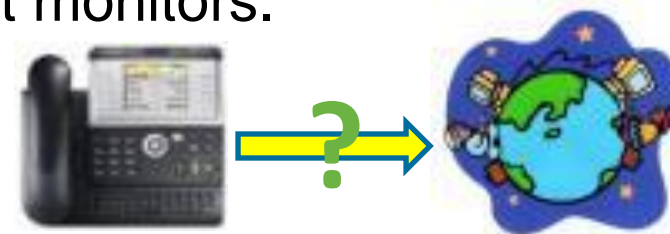
- Key use cases for NetFlow Probe:

Capture flows to match endpoint quintuple traffic = **SRC/DST IP/Port/Protocol**

Classify general purpose hw/sw devices based on the destinations/ports to which they attempt communication.
Ex: Specialized healthcare equipment such as heart monitors.



Match anomalous traffic. Ex: IP Phone attempting to communicate to Internet on TCP port 80.



- Potentially high volumes of data—limit use / filter when possible

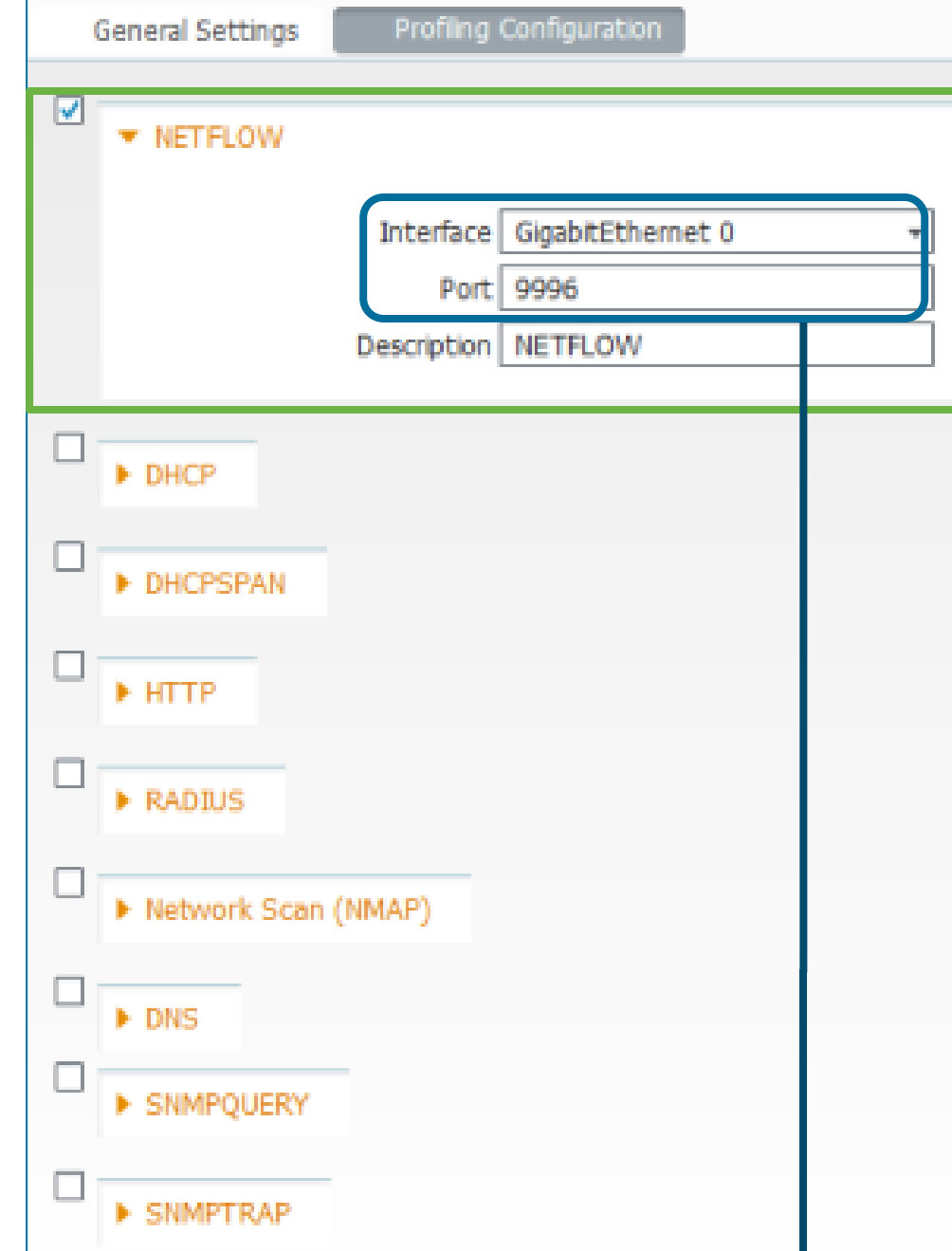
Recommend dedicated ISE interface (enable via CLI and assign IP address for use as the NetFlow export target)

Flexible NetFlow v9 includes numerous enhancements for filters.

Sampled NetFlow may not apply if profile relies on seeing all packets for specific endpoints...What if miss critical flows?

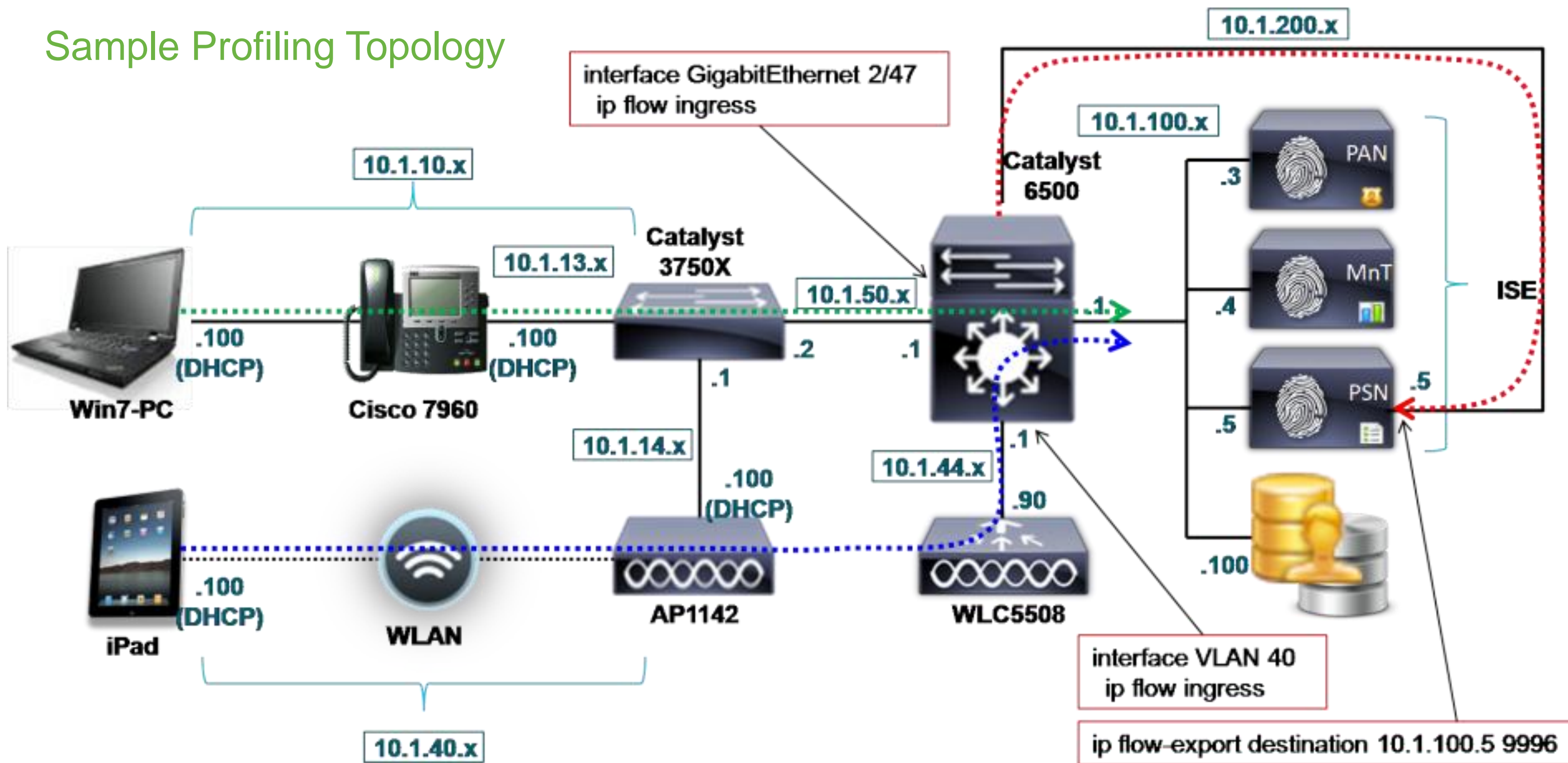
- Example IOS configuration for NetFlow export:

```
ip flow-cache timeout active 1
mls netflow interface
mls flow ip interface-full
ip flow-export source Loopback0
ip flow-export version 9
ip flow-export template timeout-rate 1
ip flow-export destination @ISE-PSN 9996
interface X (Routed port or VLAN interface)
 ip flow ingress
```



NetFlow Probe

Sample Profiling Topology



NMAP Probe

Active Scan Against Endpoints using Network Mapper (NMAP)

- **Network Scan** – On-demand scan against multiple endpoints

From Profiler Configuration page, enter subnet and click **Run Scan**.

Click link to navigate to Endpoints page for results of last scan.

Probe does not need to be enabled for on-demand scan.

- **Endpoint Scan** – Triggered scan of single endpoint

From Endpoint Profile page, select existing NMAP Scan Action

Configure matching condition to initiate Scan Action

Endpoints that match Unknown profile are automatically scanned using **SNMPPortsAndOS-scan**

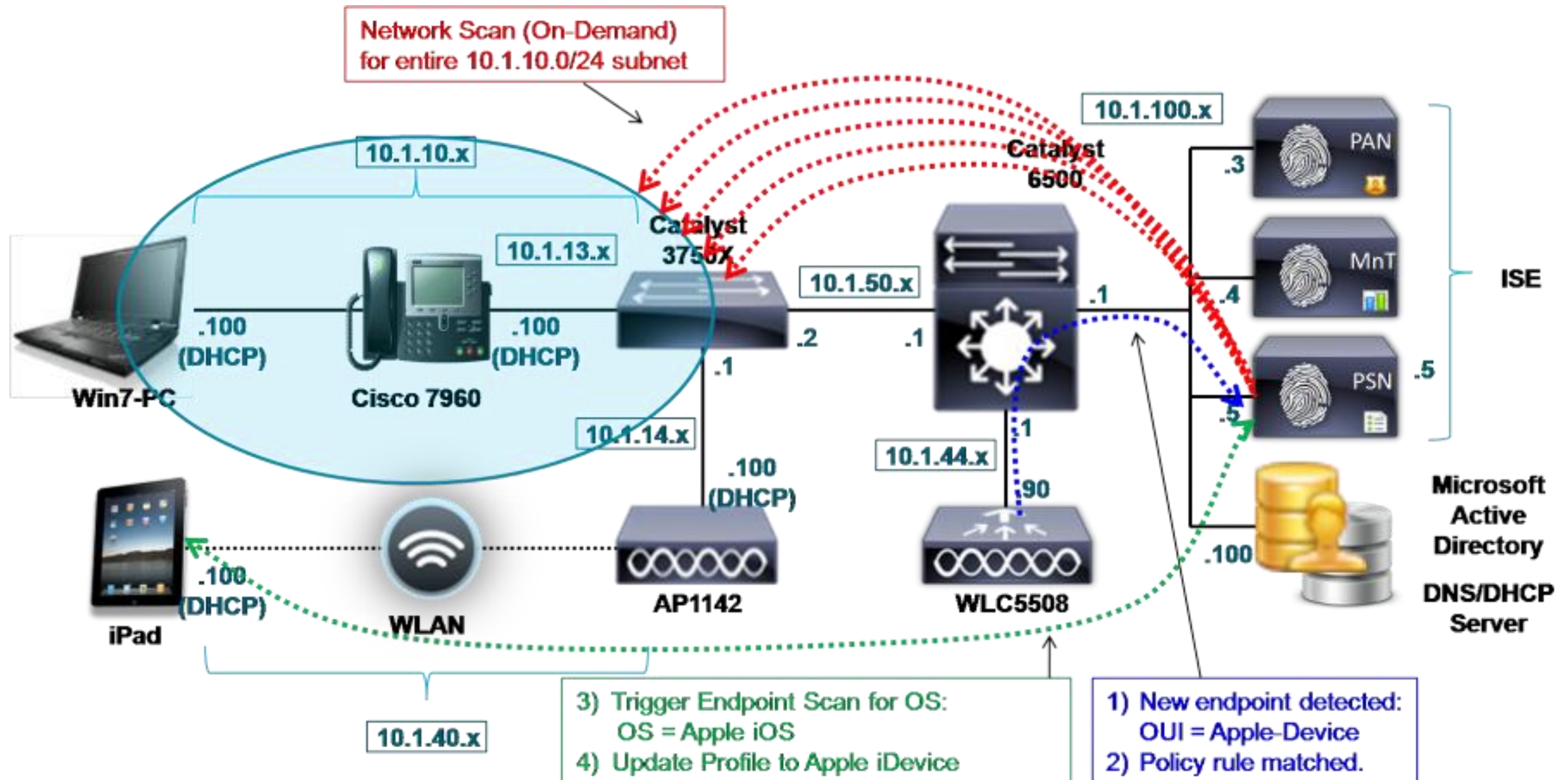
- **Note:** Scan data added to Endpoint database only if real MAC address is known. If endpoints not local to PSN (local ARP), then SNMP may return MAC. Otherwise, other probes required to discover MAC:IP Bindings

- **Caution:** Large network scans can be very time consuming and add heavy load to PSN

The screenshot displays the 'Profiling Configuration' page. At the top, there are two tabs: 'General Settings' and 'Profiling Configuration'. Below the tabs, there is a list of scan actions, each with a checkbox and a right-pointing arrow. The actions listed are: NETFLOW, DHCP, DHCPSPAN, HTTP, RADIUS, Network Scan (NMAP), DNS, SNMPQUERY, and SNMPTRAP. The 'Network Scan (NMAP)' action is selected, indicated by a checked checkbox and a green border around its configuration area. This configuration area includes a 'Description' field with the value 'NMAP', a 'Manual Scan Subnet' field with the value '10.1.100.0/24', and two buttons: 'Run Scan' and 'Cancel Scan'. Below these buttons is a link that says 'Click to see latest scan results'. At the bottom of the screenshot, there is a list of scan actions with checkboxes, including 'Network Scan (NMAP) Action Name', 'CommonPortsAndOS-scan', 'OS-scan', and 'SNMPPortsAndOS-scan'. Blue arrows from the text in the main content point to the 'Run Scan' button, the 'Click to see latest scan results' link, and the 'SNMPPortsAndOS-scan' action in this list.

NMAP Probe

Sample Profiling Topology



NMAP Scan

Manual Scan (On-Demand Scan)

▼ Network Scan (NMAP)

Description
NMAP

Manual Scan Subnet
10.100.7.0/24

Run Scan Cancel Scan

[Click to see latest scan results](#)

Click to see scan results

Endpoint

* MAC Address 00:50:56:4F:AE:6C

* Policy Assignment VMWare-Device

Static Assignment

* Identity Group Assignment Profiled

Static Group Assignment

Attribute List

161-udp snmp

162-udp snmptrap

DeviceRegistrationStatus 0

EndPointPolicy VMWare-Device

EndPointProfilerServer ISE-1-1-ALPHA

EndPointSource NMAP Probe

IdentityGroup Profiled

Latest Network Scan Results Endpoints

Edit

Endpoint Profile	MAC Address	Static Assignment
<input type="checkbox"/> Unknown	E4:1F:13:77:92:AF	false
<input type="checkbox"/> Unknown	E4:1F:13:F1:BD:65	false
<input type="checkbox"/> VMWare-Device	00:0C:29:53:BB:E2	false
<input type="checkbox"/> VMWare-Device	00:0C:29:68:FA:42	false
<input type="checkbox"/> VMWare-Device	00:0C:29:81:7A:99	false
<input type="checkbox"/> VMWare-Device	00:50:56:4E:3E:12	false
<input type="checkbox"/> VMWare-Device	00:50:56:4F:AE:6C	false

Endpoint details

Identities

- Users
- Endpoints
- Latest Network Scan Results

Network Scan (NMAP) in Profiler Policies

Triggered Using Network Scan Option in a Profiler Policy

Profiler Policy List > **Microsoft-Workstation**

Profiler Policy

* Name: Microsoft-Workstation Description

Policy Enabled

* Minimum Certainty Factor: 10 (Valid Range 1-100)

* Exception Action: NONE

* Network Scan (NMAP) Action: CommonPortsAndOS-scan

Parent Policy: CommonPortsAndOS-scan

Rules

If Condition: Microsoft-WorkstationRule2Check1 Then: Certainty Factor Increases 10

If Condition: Microsoft-WorkstationRule1Check1 Then: Certainty Factor Increases 10

If Condition: Microsoft-WorkstationRule1Check1 Then: Take Network Scan Action

If scan detects UDP port 161/162 open, then SNMP Query run against endpoint IP using **public** as default RO community.

Select NMAP Action And Take Network Scan Action

- 161-udp
- 162-udp
- 1900-udp
- 21-tcp
- 22-tcp
- 23-tcp
- 25-tcp
- 3306-tcp
- 3389-tcp
- 443-tcp
- 445-tcp
- 445-udp
- 500-udp
- 520-udp
- 53-tcp
- 53-udp
- 631-udp
- 67-udp
- 68-udp
- 80-tcp
- 8080-tcp
- operating-system

NMAP Actions: Policy > Policy Elements > Results > Profiling > Network Scan Actions

Network Scan Example

Scan Generic Apple Devices to Increase Profiling Fidelity

Profiler Policy List > Apple-Device

Profiler Policy

* Name Description

Policy Enabled

* Minimum Certainty Factor (Valid Range 1 to 65535)

* Exception Action

* Network Scan (NMAP) Action

Create Matching Identity Group

Use Hierarchy

Parent Policy *****NONE*****

Rules

If Condition	<input type="text" value="Apple-DeviceRule1-SCAN"/>	Then	<input type="text" value="Take Network Scan Action"/>
If Condition	<input type="text" value="Apple-DeviceRule1Check1"/>	Then	<input type="text" value="Certainty Factor Increases"/> <input type="text" value="10"/>

Conditions Details

Name **Apple-DeviceRule1Check1**

Description **Apple-DeviceRule1Check1**

Expression **MAC:OUI CONTAINS Apple**

Rule Logic: If detect Apple MAC Address, then perform a network scan for the OS to better determine specific type of Apple device.

Profile Match on Any iDevice

Very Useful for Authorization Policies Based on Matching *any* iPhone / iPad / iPod

Profiler Policy List > **Apple-iDevice**

Profiler Policy

* Name Description

Policy Enabled

* Minimum Certainty Factor (Valid Range 1 to 100)

* Exception Action

* Network Scan (NMAP) Action

Create Matching Identity Group
 Use Hierarchy

* Parent Policy

Rules

If Condition	<input type="text" value="Apple-iOS-NMAP-Rule4Check1"/>	Then	<input type="text" value="Certainty Factor Increases"/>	<input type="text" value="10"/>
If Condition	<input type="text" value="Apple-iOS-NMAP-Rule5Check1"/>	Then	<input type="text" value="Certainty Factor Increases"/>	<input type="text" value="10"/>

Rule Logic: If NMAP detects OS type as either Apple iOS or Apple iPhone OS, then increase CF by 10.

NMAP has determined that device is an iDevice, but specific iDevice type still not confirmed since multiple iDevices can return these same values.

Conditions Details [X]

Name **Apple-iOS-NMAP-Rule4Check1**

Description **NMAP operating-system CONTAINS Apple iOS**

Expression **NMAP:operating-system CONTAINS Apple iOS**

Conditions Details [X]

Name **Apple-iOS-NMAP-Rule5Check1**

Description **NMAP operating-system CONTAINS Apple iPhone OS**

Expression **NMAP:operating-system CONTAINS Apple iPhone OS**

The Probe Avengers

Probes that are Most Effective When They Work as a Team!



- **DNS and NMAP cannot work without an IP Address**
 - **Require IP address** for reverse DNS lookup or NMAP Scan
- **HTTP (SPAN), NetFlow, and NMAP cannot update endpoint without a MAC address**
 - Require MAC - IP binding**
 - Probe data will be added to database only if MAC address is known, otherwise dropped!
 - ARP cache in the profiler service maps IP to MAC addresses.
- **Fellow probes that can provide IP address and IP:MAC binding info:**

RADIUS Probe
Framed-IP-Address

DHCP Probe
dhcp-requested-address

SNMPQuery Probe
ARP table

SNMP Query probe periodically polls all Network Access Devices (configured for polling) for system MIB info including ARP table. May require non-access devices to be configured in ISE if L3 gateway.

Other Probe Contingencies

- **RADIUS Probe**

Framed IP address sent in RADIUS Accounting must be learned via DHCP or IP Device Tracking

- **DHCP Probe**

Assumes all endpoints use DHCP

Static IP on Endpoint? May need to consider alternative probes and methods that do not rely on DHCP conditions or MAC-IP binding.

- **DNS Probe**

Requires Reverse Pointer “PTR” Record to be present in DNS.

- **SNMP Query Probe**

Triggered query requires SNMP Trap or RADIUS probe to alert ISE of new device connection.

Enhanced Profiling Features



Device Sensor

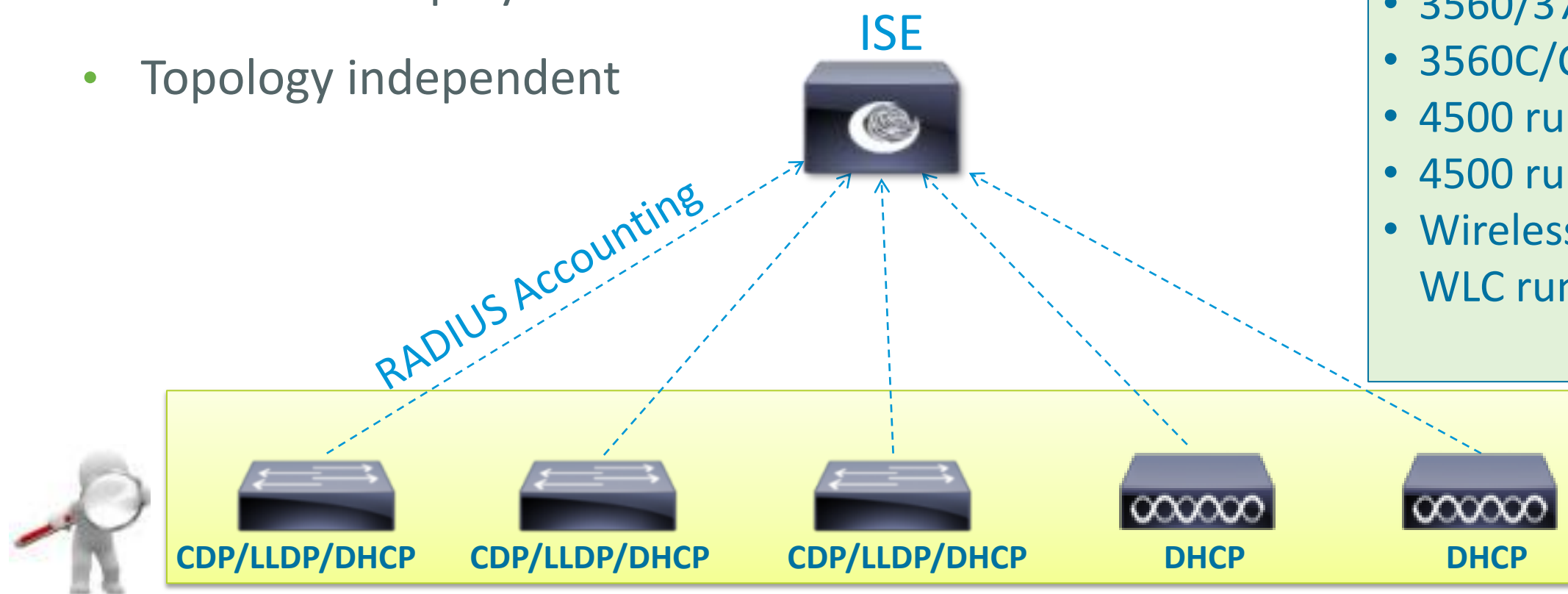
Distributed Probes with Centralized Collection

- Profiling based on **CDP/LLDP, DHCP, HTTP** (WLC only), or **mDNS** (4k only)
- Automatic discovery for most common devices (Printers, Cisco devices, phones)
- Centralized visibility with minimal ISE sensor investment and traffic
- Low touch deployment
- Topology independent

Device Sensor Support

- 3560/3750 running 15.0(1)SE1 (excludes LAN Base)
- 3560C/CG running 15.0(2) SE (excludes LAN Base)
- 4500 running 15.1(1)SG (excludes LAN Base)
- 4500 running IOS-XE 3.3.0SG (excludes LAN Base)
- Wireless Controllers running 7.2.110.0 (DHCP only)
- WLC running 7.3.101.0 (HTTP support added)

Check Release Notes!



Device Sensor Distributed Probes

Device Sensor Data Collection

Enable CDP / LLDP / DHCP

- Access device needs to have services enabled to collect CDP, LLDP, or DHCP
- Sample access switch configurations:

CDP:

- Global: CDP must be enabled (default setting)
- Interface: CDP must be enabled (default setting)

```
cdp run
interface <Interface>
  cdp enable
```

LLDP:

- Global: LLDP must be enabled (disabled, by default)
- Interface: LLDP must be enabled (default setting)

```
lldp run
interface <Interface>
  lldp receive
```

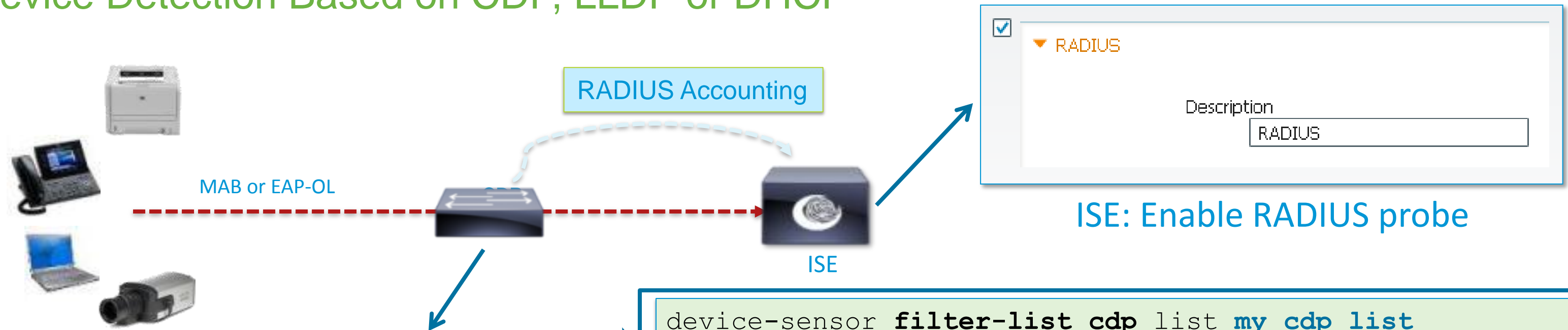
DHCP:

- DHCP Snooping must be enabled globally
- Apply DHCP snooping to each access VLAN

```
ip dhcp snooping
ip dhcp snooping vlan <x,y-z,...>
```


Device Sensor Implementation for Wired

Device Detection Based on CDP, LLDP or DHCP



- 1) Filter DHCP, CDP, and LLDP options/TLVs
- 2) Enable sensor data to be sent in RADIUS Accounting including all changes

```
device-sensor accounting
device-sensor notify all-changes
```

- 3) Disable local analyzer if sending sensor updates to ISE (central analyzer)

```
no macro auto monitor Be aware of CSCtr23701
access-session template monitor
```

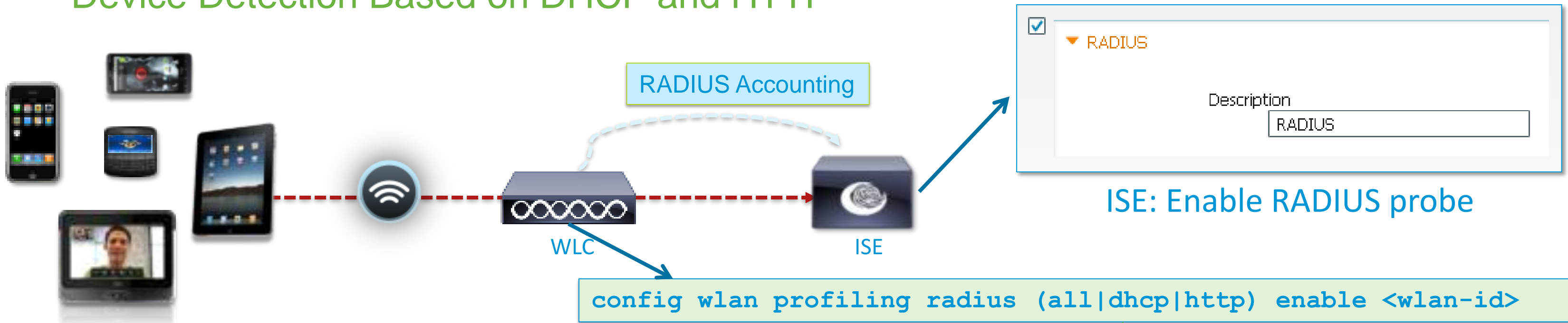
```
device-sensor filter-list cdp list my_cdp_list
  tlv name device-name
  tlv name platform-type
device-sensor filter-spec cdp include list my_cdp_list
```

```
device-sensor filter-list lldp list my_lldp_list
  tlv name system-name
  tlv name system-description
device-sensor filter-spec lldp include list my_lldp_list
```

```
device-sensor filter-list dhcp list my_dhcp_list
  option name host-name
  option name class-identifier
  option name client-identifier
device-sensor filter-spec dhcp include list my_dhcp_list
```

Device Sensor Implementation for Wireless

Device Detection Based on DHCP and HTTP



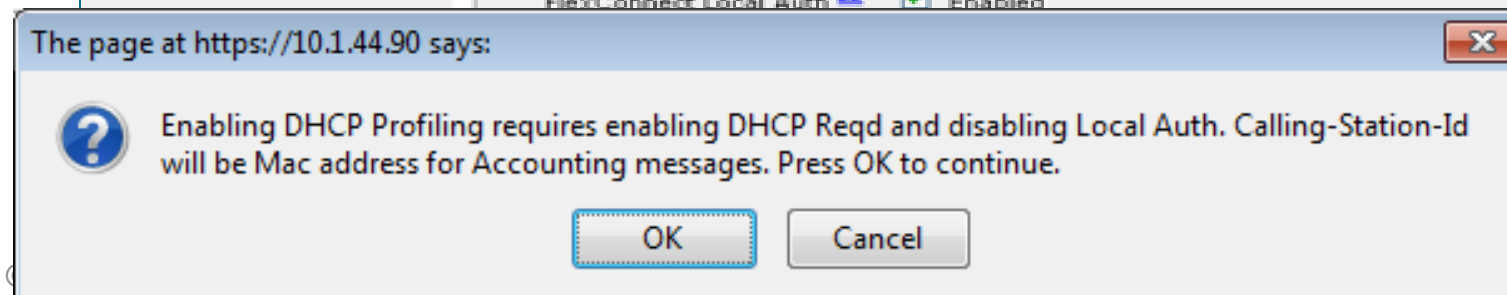
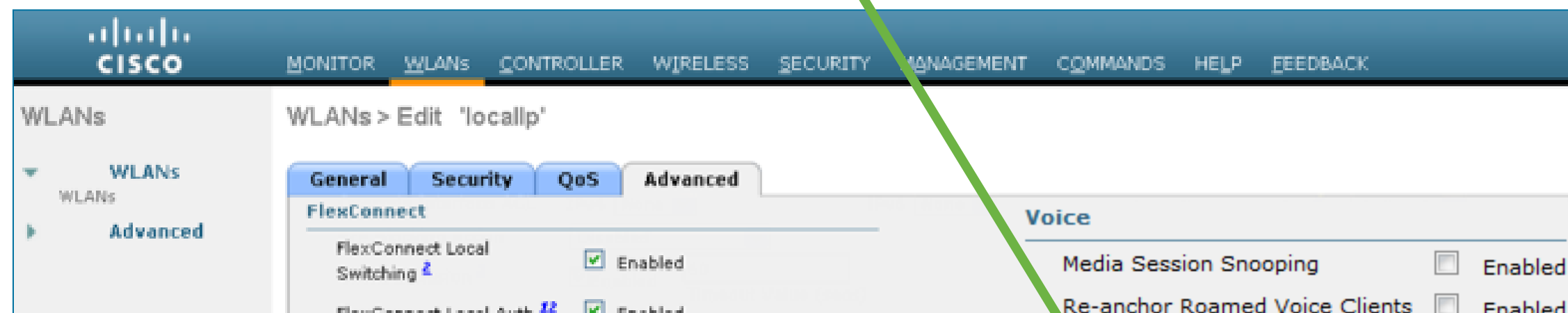
- Enable/Disable device profiling on all the clients that will join the WLAN.

HTTP added in 7.3 – NOTE: CSCuc15636

- DHCP Option 12 (Hostname) and 60 (Vendor Class ID) supported; HTTP – User-Agent only

- DHCP Proxy and Bridged modes supported.

- 7.2.110.0 FlexConnect limits:
 - Standalone APs not supported
 - Local auth w/ local switching not supported



Device Sensor in Action

EndPointMACAddress	00-21-55-D6-01-33
EndPointMatchedProfile	Cisco-IP-Phone-7945
EndPointPolicy	Cisco-IP-Phone-7945
EndPointProfilerServer	ISE-02
EndPointSource	RADIUS Probe
Framed-IP-Address	10.100.15.100
IdentityGroup	Cisco-IP-Phone

```
# show device-sensor cache all
```

```
Device: 0021.55d6.0133 on port GigabitEthernet1/0/1
-----
Proto Type:Name          Len Value
cdp    2:address-type      17 00 02 00 11 00 00 00 01 01 01 CC 00 04 0A 64 0F
      64
cdp    16:power-type       6 00 10 00 06 2E E0
cdp    11:duplex-type      5 00 0B 00 05 01
cdp    25:power-request-type 12 00 19 00 0C 01 33 00 03 00 00 2E E0
cdp    6:platform-type    23 00 06 00 17 43 69 73 63 6F 20 49 50 20 50 68 6F
      6E 65 20 37 39 34 35
cdp    5:version-type     17 00 05 00 11 53 43 43 50 34 35 2E 39 2D 30 2D 33
      53
cdp    4:capabilities-type 8 00 04 00 08 00 00 04 90
cdp    3:port-id-type     10 00 03 00 0A 50 6F 72 74 20 31
cdp    1:device-name      19 00 01 00 13 53 45 50 30 30 32 31 35 35 40 36 30
      31 33 33
dhcp   50:requested-address 6 32 04 0A 64 0F 64
dhcp   54:server-identifier 6 36 04 0A 64 07 64
dhcp   55:parameter-request-list 9 37 07 01 42 06 03 0F 96 23
dhcp   60:class-identifier 40 3C 26 43 69 73 63 6F 20 53 79 73 70 65 6D 73 2C
      20 49 6E 63 2E 20 49 50 20 50 68 6F 6E 65 20 43
      50 2D 37 39 34 35 47 00
dhcp   12:host-name       17 0C 0F 53 45 50 30 30 32 31 35 30 44 36 30 31 33
      33
dhcp   61:client-identifier 9 3D 07 01 00 21 55 D6 01 33
```

Switch Device Sensor Cache

Cisco IP Phone 7945

SEP002155D60133

10.100.15.100

Cisco Systems, Inc. IP Phone CP-7945G

SEP002155D60133

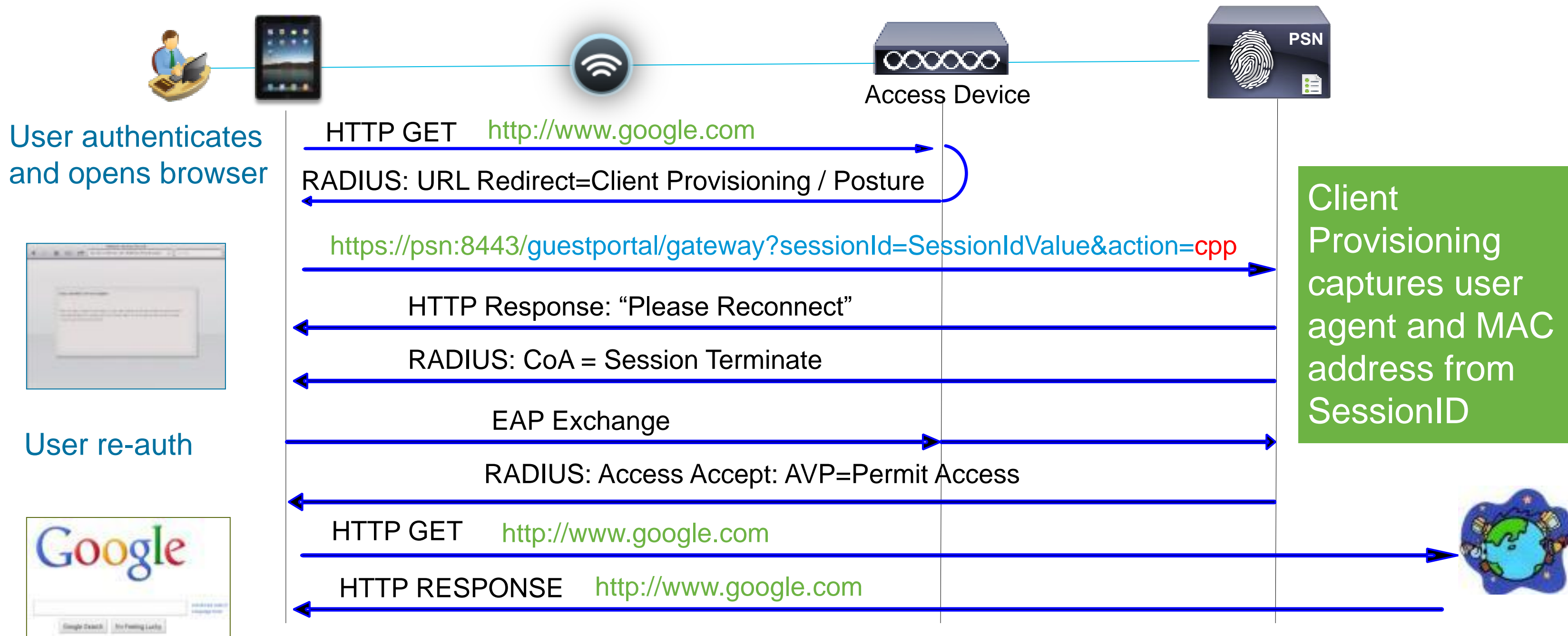
ISE Profiling result

cdpCacheDeviceId	SEP002155D60133
cdpCacheDevicePort	Port 1
cdpCacheDuplex	01:
cdpCachePlatform	Cisco IP Phone 7945
cdpCachePowerConsumption	2e:e0
cdpCacheVersion	SCCP45.9-0-3S

dhcp-class-identifier	Cisco Systems, Inc. IP Phone CP-7945G
dhcp-parameter-request-list	1, 66, 6, 3, 15, 150, 35
dhcp-requested-address	10.100.15.100
dhcp-server-identifier	10.100.7.100
dot1xAuthAuthControlledPortControl	2
dot1xAuthAuthControlledPortStatus	2
dot1xAuthSessionUserName	00-21-55-D6-01-33
host-name	SEP002155D60133

Profiling without Probes

Direct Profiling using **Client Provisioning** (Posture Agent or NSP)



Profile Attributes from Client Provisioning

Administration > Identity Management > Identities > Endpoints

The screenshot shows the configuration page for an endpoint with MAC Address **7C:6D:62:E3:D5:05**. The configuration includes:

- * Policy Assignment:** Apple-iPad
- Static Assignment:**
- * Identity Group Assignment:** Apple-iPad
- Static Group Assignment:**

Attribute List:

EndPointPolicy	Apple-iPad
EndPointProfilerServer	ise-psn-1
EndPointSource	CP
IdentityGroup	Apple-iPad
MACAddress	7C:6D:62:E3:D5:05
MatchedPolicy	Apple-iPad
OUI	Apple, Inc
PolicyVersion	20
StaticAssignment	false
StaticGroupAssignment	false
TimeToProfile	26
Total Certainty Factor	30
User-Agent	Mozilla/5.0 (iPad; CPU OS 5_0_1 like Mac OS X) AppleWebKit/534.46 (KHTML, like Gecko) Version/5.1 Mobile/9A405 Safari/7534.48.3

Callouts and annotations:

- Apple-iPad profiled with 0 probes enabled!** (points to Policy Assignment)
- EndPointSource (Source of last attributes received) = CP (Client Provisioning)** (points to EndPointSource)
- MAC Address retrieved from Calling-Station-ID via SessionID lookup
No IP Address listed for Endpoint; Profiling achieved without MAC-IP Binding** (points to MACAddress)
- User-Agent retrieved from CP and passed to Profiling process** (points to User-Agent)

Buttons: Save, Delete, Reset

Profile Attributes from HTTP Probe Only

Profiling for URL Redirected Flows without Client Provisioning (CPP / NSP)

* MAC Address 00:50:56:A0:0B:3A

* Policy Assignment Windows7-Workstation

Static Assignment

* Identity Group Assignment Microsoft-Workstation

Static Group Assignment

Attribute List

EndPointPolicy	Windows7-Workstation
EndPointSource	HTTP Probe
IdentityGroup	Microsoft-Workstation
MACAddress	00:50:56:A0:0B:3A
MatchedPolicy	Windows7-Workstation
OUI	VMware, Inc.
PolicyVersion	20
StaticAssignment	false
StaticGroupAssignment	false
Total Certainty Factor	60
User-Agent	Mozilla/5.0 (Windows NT 6.1; rv:11.0) Gecko/20100101 Firefox/11.0

Windows 7 Workstation profiled with only HTTP Probe enabled

EndPointSource = HTTP Probe

MAC Address retrieved from Calling-Station-ID via SessionID lookup

User-Agent retrieved from HTTP Probe during Web Auth

Probeless Profiling

Wireless 802.1X with Posture Example

- Employee with iPad connects to corp SSID and logs in using AD account 'employee'
- Device type Unknown, so hit Emp_NonCompliant rule.
- Employee redirected to Client Provisioning/Posture
- OS detection performed to determine CP policy
- User agent captured—iPad not supported for posture agent so ISE send CoA w/session terminate.
- Endpoint user-agent and other data written to db using MAC address from Session ID lookup→Profile=iPad!
- On reconnect, match profile=iDevice and Employee.

Matched AuthC Rule = Dot1X

Authentication Policy

Rule Name	Conditions	Identity Source
MAB	if Wireless_MAB then	Internal Endpoints
Dot1X	If Wireless_802.1X then	AD1
Default	if <no match> then	AD1_Internal

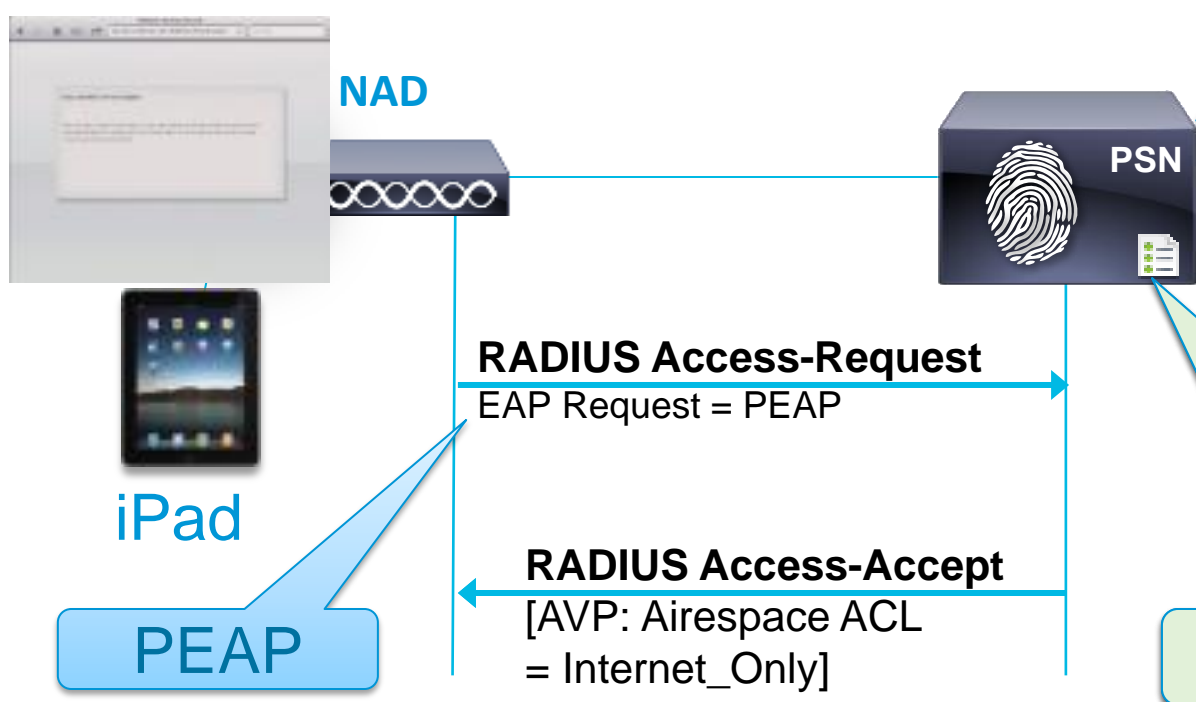
Endpoint Profile = iPad

Authorization Policy

Rule Name	Conditions	Permissions
IP Phones	if Cisco-IP-Phone then	Cisco_IP_Phone
BYOD	if iDevice and Employee then	Internet
Employee	if PC and Employee then	Full_Access
Guest	if Guest then	Internet
Emp_NonCompliant	if Employee and NonCompliant then	Posture
Default	If <no match> then	CWA_Posture

User Agent + MAC Captured

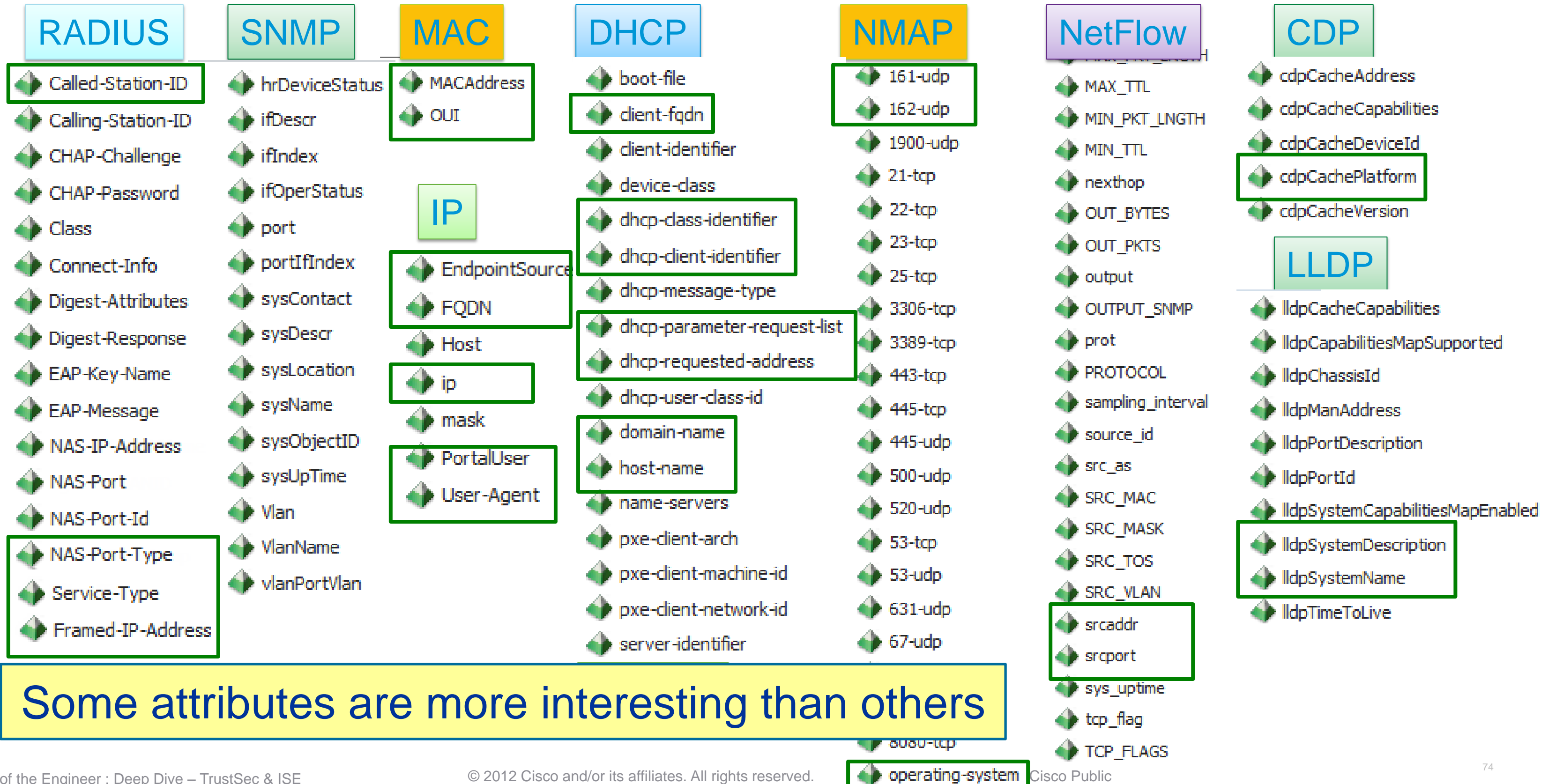
Matched AuthZ Rule = BYOD



Best Practices - Profiling in a Real Network



Sample Attributes Used to Profile Endpoints



Some attributes are more interesting than others

Profiling Probes

Key Attributes and Common Profiling Use Cases

Probe	Key Profiling Attributes	Common Endpoint Profiling Use Cases
RADIUS	Calling-Station-ID Framed-IP-Address	MAC Address -> OUI = Indication of device vendor. Some endpoints can be profiled w/ this attribute alone if vendor only makes specific devices. Ex: 3 rd -party IP phones, mobile devices, game consoles; MAC:IP bindings and probe support.
RADIUS w/Device Sensor	CDP/LLDP/DHCP	See SNMP probe for CDP/LLDP info See DHCP probe for DHCP info
SNMP	MAC Address/OUI CDP/LLDP attributes ARP tables	Valuable for any vendor that leverages CDP/LLDP. For example, Cisco IP phones, cameras, APs. DHCP (See DHCP probe info); MAC Address (see RADIUS probe) Polling of device ARP tables populates ISE MAC:IP bindings.
DHCP	DHCP attributes	Unique Vendor IDs for hardware and software. DHCP fingerprints for OS detection. Hostname/FQDN for common name patterns may indicate OS or device type; Additionally provides MAC:IP Bindings to support other probes.
NMAP	Operating System Common ports Endpoint SNMP data	Operating System detection IF scanning not blocked by network/client FW; Offers classification of endpoints that run SNMP agents like network printers. Good for detecting endpoints that listen on the common UDP/TCP ports.
DNS	FQDN	Value will depend on whether common naming conventions used for hostname/DNS.
HTTP	User-Agent	Operating System detection; some browsers like Chrome may mask actual OS.
NetFlow	Source/Dest IP/Ports/Protocol	Good for detecting mission-specific endpoints with unique traffic patterns or use general purpose hw/sw; May detect anomalous traffic for specific endpoints.

The Unofficial Guide to Probe Selection

Which Probes Apply to My Use Case?

- Relatively and Generally Speaking...

Which probes are the easiest/most difficult to deploy?

Which probes have the least/highest impact to my network?

(in terms of traffic overhead, ISE server load, or additional components to support)

What is the general value that this probe adds to my ability to profile my endpoints?

DDI	D eployment D ifficulty I ndex	Easy	Medium	Difficult
NII	N etwork I mpact I ndex	Low Impact	Medium Impact	High Impact
PVI	P robe V alue I ndex	High Value	Medium Value	Low Value

Probes for Discovery

Best Practice Recommendations for
Discovery Phase
 (NAC/pre-RADIUS deployment):

EDI	Deployment Difficulty Index	Easy	Medium	Difficult
NII	Network Impact Index	Low Impact	Medium Impact	High Impact
PVI	Probe Value Index	High Value	Medium Value	Low Value

Probe	EDI	NII	PVI	Key Profiling Attributes	Notes
RADIUS				N/A	Not applicable since ISE not in auth control plane
RADIUS w/ Device Sensor	2	1	1	CDP/LLDP/DHCP attributes	If network supports Device Sensor, then can leverage RADIUS Accounting independent of auth control plane
SNMPTrap	1	1	1	LinkUp/LinkDown and MAC Notify Traps, Informs	Detect endpoints connections / trigger SNMPQuery probe
SNMPQuery	1	2	1	MAC Address/OUI CDP/LLDP attributes ARP tables	Polling of device ARP tables populates ISE MAC:IP bindings; Be careful of high SNMP Query traffic triggered by excessive RADIUS Accounting updates due to re-auth or Interim Updates.
DHCP (Helper)	2	1	1	DHCP attributes	Provides MAC:IP Bindings; Network impact generally low, but be careful of low DHCP lease timers.
DHCP SPAN	2	3	1	DHCP Attributes	Provides MAC:IP Bindings
NMAP	1	2	2	Operating System Common ports Endpoint SNMP data	SNMP data assumes UDP/161 open and public string. Relative value of NMAP will depend on customer network and whether OS detection is important factor in wired access policy.
DNS	1	1	2	FQDN	Value will depend on whether common naming conventions used
HTTP (Redirect)				N/A	Not applicable since ISE not in auth control plane
HTTP (SPAN)	2	3	2	User-Agent	Consider SPAN of key HTTP chokepoints like server or Internet edge using intelligent SPAN/tap solutions and/or VACL Capture.
NetFlow	3	3	2	Source/Dest IP/Ports/Protocol	Recommended only for specific use cases, not general profiling

Probes for Wired

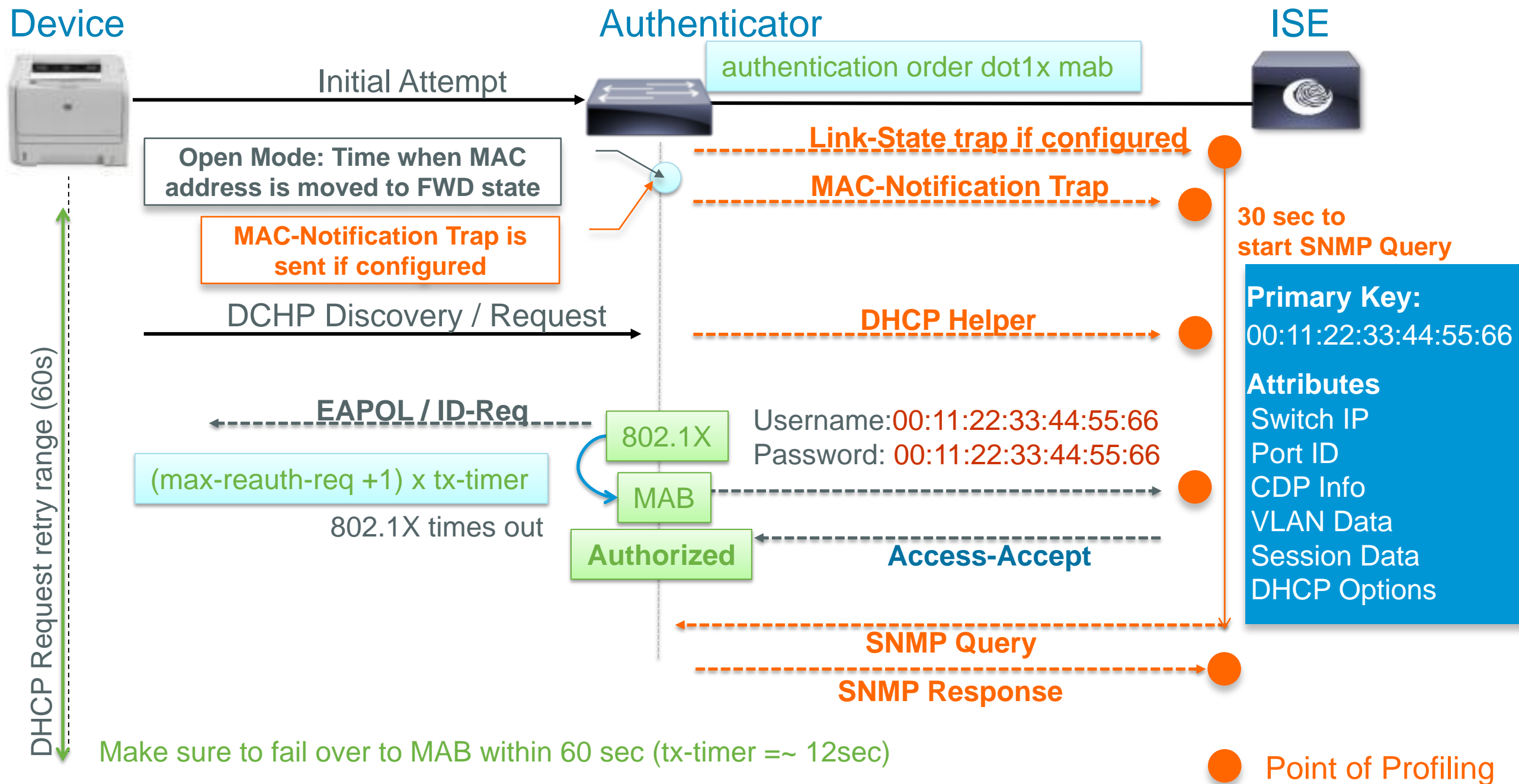
Best Practice Recommendations for ISE Wired Deployment:

EDI	Deployment Difficulty Index	Easy	Medium	Difficult
NII	Network Impact Index	Low Impact	Medium Impact	High Impact
PVI	Probe Value Index	High Value	Medium Value	Low Value

Probe	EDI	NII	PVI	Key Profiling Attributes	Notes
RADIUS	1	1	1	MAC Address (OUI), IP Address, User-Name, Others	Fundamental probe for device detection and enabling other probes
RADIUS w/ Device Sensor	2	1	1	CDP/LLDP/DHCP attributes	If running 3k/4k access switches with Device Sensor support, then this is ideal and optimized method to collect select attributes.
SNMPTrap	1	1	3	LinkUp/LinkDown and MAC Notifications Traps, Informs	Detect endpoints connections / trigger SNMPQuery probe
SNMPQuery	1	2	1	MAC Address/OUI CDP/LLDP attributes ARP tables	Polling of device ARP tables populates ISE MAC:IP bindings; Be careful of high SNMP Query traffic triggered by excessive RADIUS Accounting updates due to re-auth or Interim Updates.
DHCP (Helper)	2	1	1	DHCP attributes	Provides MAC:IP Bindings; Be wary of low DHCP lease timers.
DHCP SPAN	2	3	1	DHCP Attributes	Provides MAC:IP Bindings
NMAP	1	2	2	Operating System Common ports Endpoint SNMP data	SNMP data assumes UDP/161 open and public string
DNS	1	1	2	FQDN	Value will depend on whether common naming conventions used
HTTP (Redirect)	2	1	2	User Agent	Value will depend on relative importance of OS for wired access.
HTTP (SPAN)	2	3	2	User Agent	Consider SPAN of key HTTP chokepoints like Internet edge; Leverage smart SPAN solutions and VACL Capture if possible
NetFlow	3	3	2	Source/Dest IP/Ports/Protocol	Recommended only for specific use cases, not general profiling

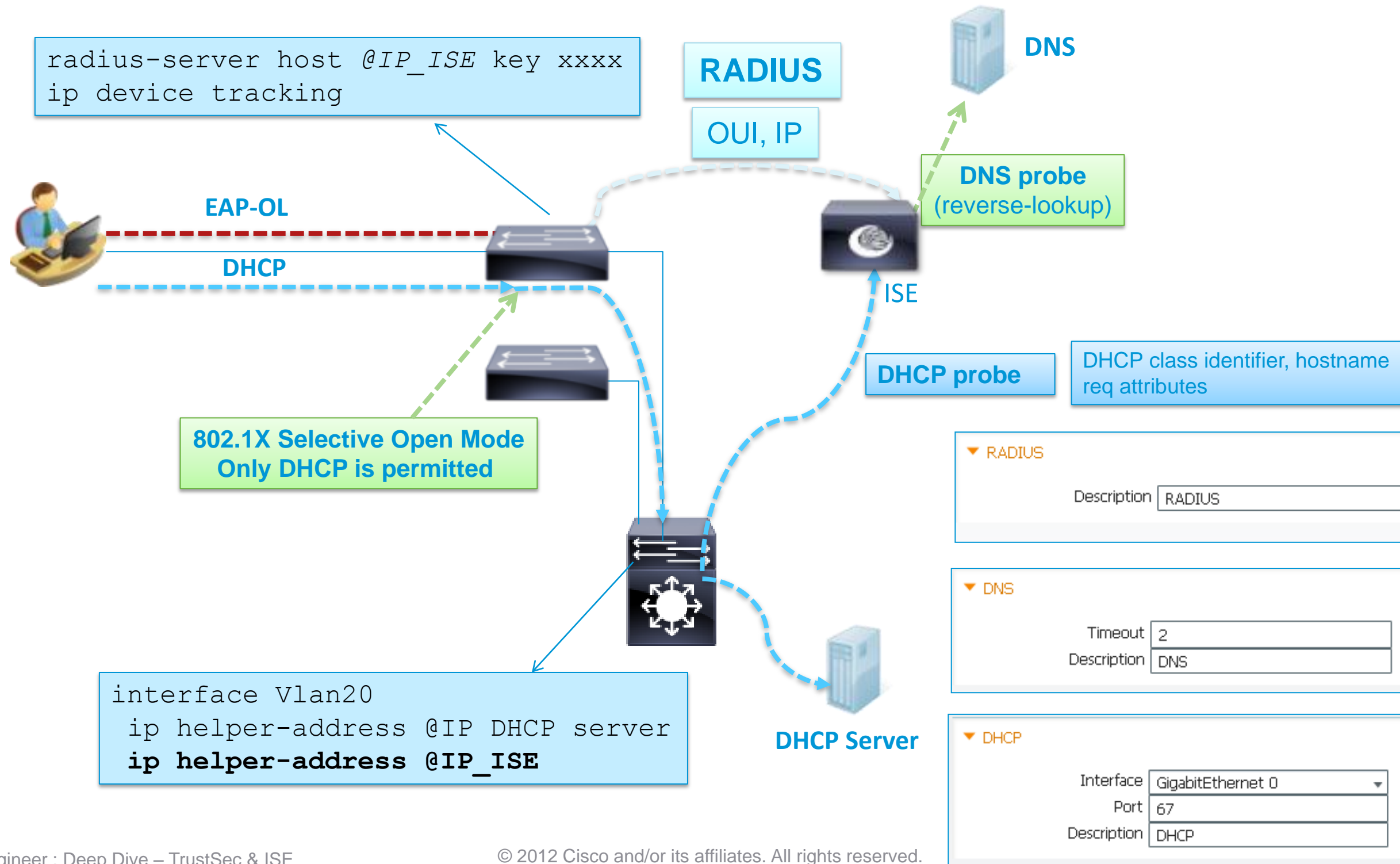
Profiling Flow for a Wired Network

SNMP Query, SNMP Trap, RADIUS, DHCP Helper



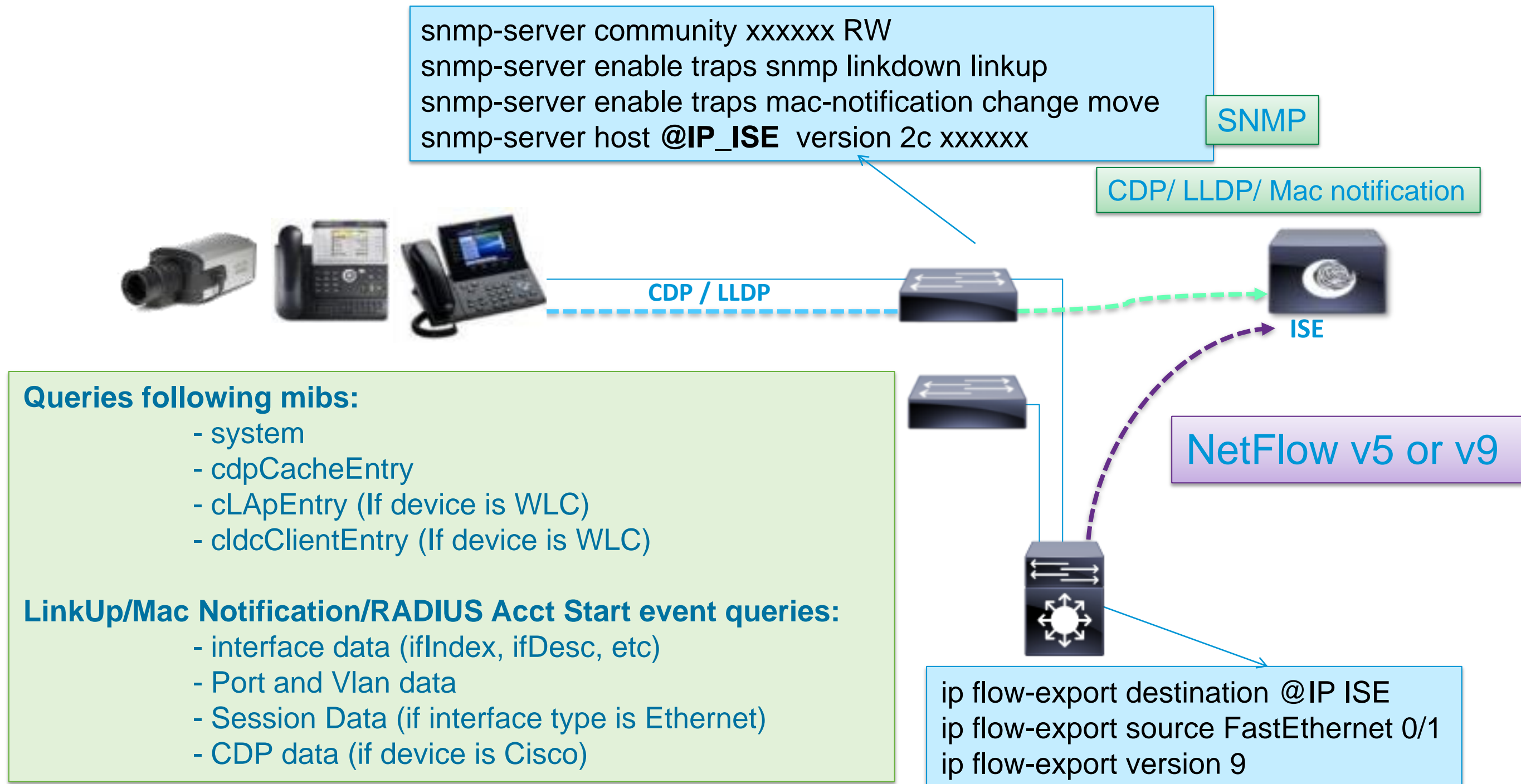
ISE Profiler Probes Implementation

Using Profiling Based on RADIUS, DNS, DHCP in a Wired Network



ISE Profiler Probes Implementation

SNMP/CDP/LLDP, NetFlow



Probes for Wireless

Best Practice Recommendations for ISE Wireless Deployment:

EDI	Deployment Difficulty Index	Easy	Medium	Difficult
NII	Network Impact Index	Low Impact	Medium Impact	High Impact
PVI	Probe Value Index	High Value	Medium Value	Low Value

Probe	EDI	NII	PVI	Key Profiling Attributes	Notes
RADIUS	1	1	1	MAC Address (OUI), IP Address, User-Name, Others	Fundamental probe for device detection and enabling other probes
RADIUS w/ Device Sensor	2	1	1	CDP/LLDP/DHCP attributes	WLC 7.2.110.0 supports Device Sensor which offers optimized delivery of DHCP attributes.
SNMPTrap					WLC traps not currently supported by ISE.
SNMPQuery	1	2	3	MAC Address/OUI IP address	Specific attributes of client wireless connection may offer limited value; Be careful of high SNMP Query traffic triggered by excessive RADIUS Accounting updates due to re-auth or Interim Updates.
DHCP (Helper)	2	1	1	DHCP attributes	Provides MAC:IP Bindings; Be wary of low DHCP lease timers
DHCP SPAN	2	3	1	DHCP Attributes	Provides MAC:IP Bindings
NMAP	1	2	2	Operating System Common ports	OS detection and common ports primary use case. SNMP not common for wireless clients.
DNS	1	1	2	FQDN	Value will depend on whether common naming conventions used
HTTP (Redirect)	2	1	1	User Agent	Common requirement to distinguish mobile device types. HTTP often provides higher fidelity than other methods for OS detection.
HTTP (SPAN)	2	3	1	User Agent	Consider SPAN of key HTTP chokepoints like WLC connections and Internet edge; Optionally use intelligent SPAN/tap options or VACL Capture where available
NetFlow	3	3	2	Src/Dest IP/Ports/Protocol	Recommended only for specific use cases, not general profiling

Wireless Profiling

Best Practices

- Set Calling-Station-ID to MAC Address for non-1X WLANs:
[Security](#) > [AAA](#) > [RADIUS](#) > [Authentication](#)

RADIUS Authentication Servers

Call Station ID Type [u](#) System MAC Address ▼

- Disable DHCP Proxy to allow forwarding of DHCP -> IP Helpers:
[Controller](#) > [Advanced](#) > [DHCP](#)

DHCP Parameters

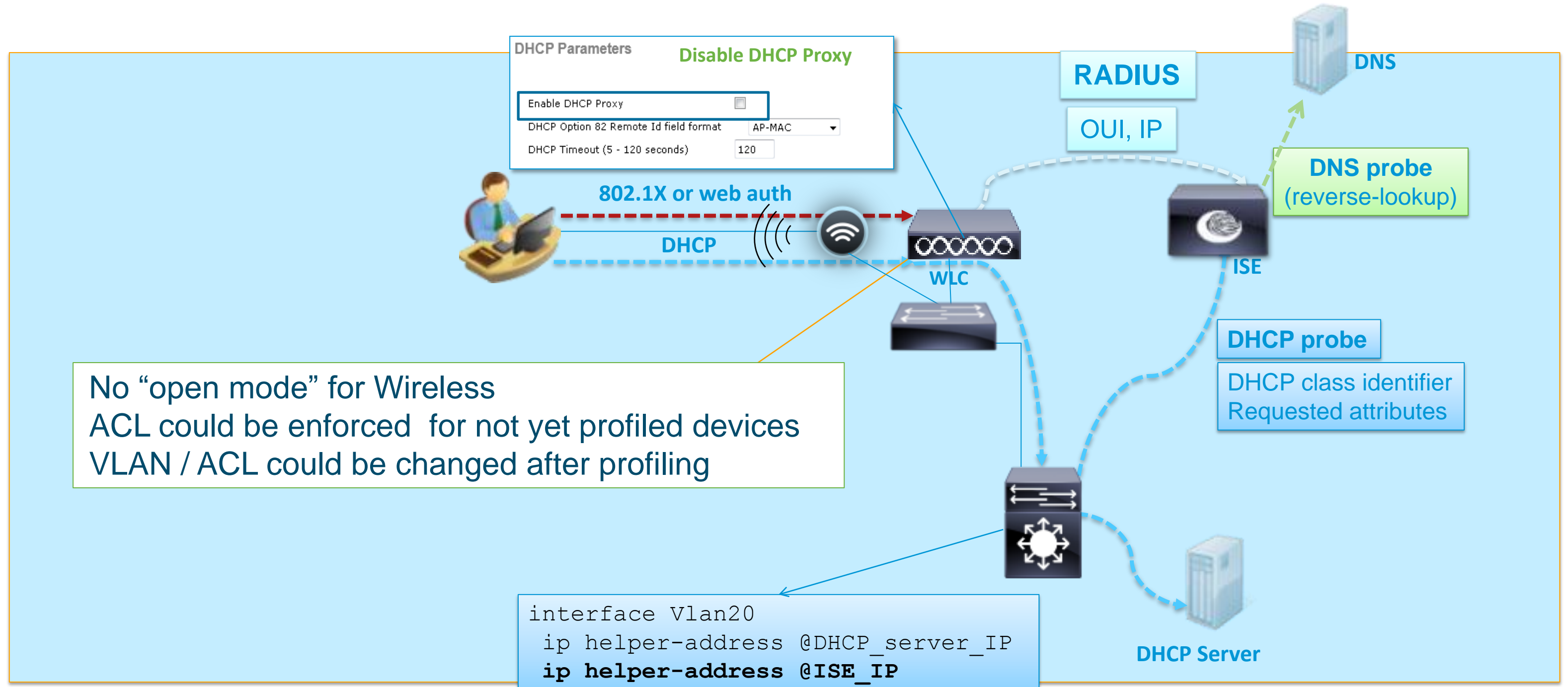
Enable DHCP Proxy

DHCP Option 82 Remote Id field format AP-MAC ▼

DHCP Timeout (5 - 120 seconds) 120

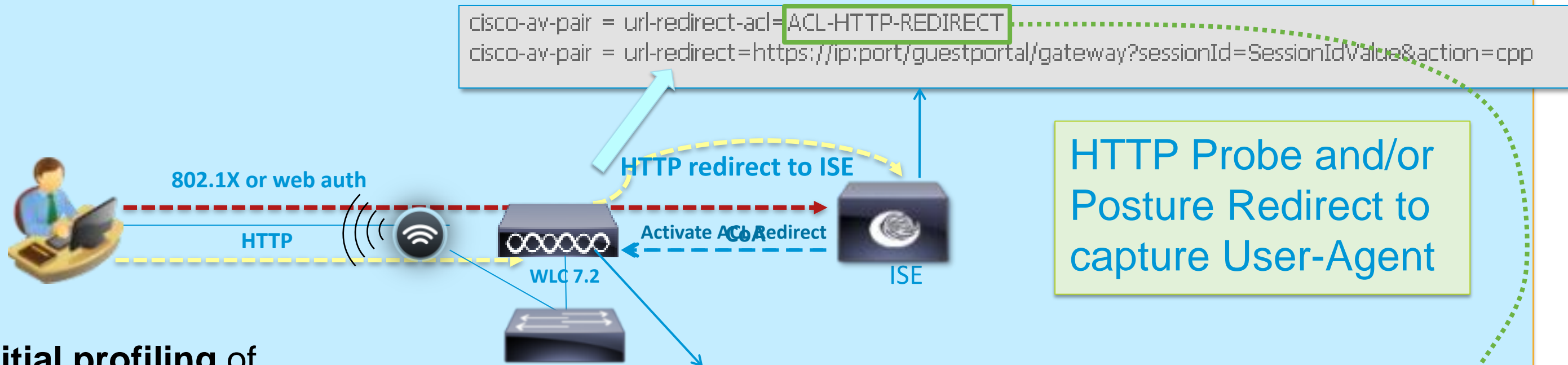
ISE Profiler Probes for Wireless

RADIUS, DNS, DHCP (IP Helper)



ISE Profiler Probes for Wireless

HTTP Best Practice: Use URL Redirect w/Posture and/or HTTP Probe



- Allow the **initial profiling** of HTTP traffic by redirecting to ISE Policy Service node.
- Once profiled, client can bypass redirection through assignment to an ID Group that matches a different Authorization Policy rule.

Access List Name: ACL-HTTP-REDIRECT

Deny Counters: 0

Security > Access Control Lists > ACL-HTTP-REDIRECT

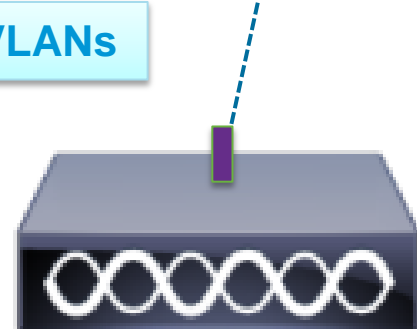
Seq	Action	Source IP/Mask	Destination IP/Mask	Protocol	Source Port	Dest Port	DSCP	Direction	Number of Hits
<u>1</u>	Permit	0.0.0.0 / 0.0.0.0	0.0.0.0 / 0.0.0.0	ICMP	Any	Any	Any	Any	243
<u>2</u>	Permit	0.0.0.0 / 0.0.0.0	0.0.0.0 / 0.0.0.0	UDP	Any	DNS	Any	Inbound	3554
<u>3</u>	Permit	0.0.0.0 / 0.0.0.0	0.0.0.0 / 0.0.0.0	UDP	DNS	Any	Any	Outbound	3447
<u>4</u>	Permit	0.0.0.0 / 0.0.0.0	10.1.100.0 / 255.255.255.248	TCP	Any	Any	Any	Inbound	10536
<u>5</u>	Permit	10.1.100.0 / 255.255.255.248	0.0.0.0 / 0.0.0.0	TCP	Any	Any	Any	Outbound	12850
<u>6</u>	Deny	0.0.0.0 / 0.0.0.0	0.0.0.0 / 0.0.0.0	Any	Any	Any	Any	Any	64292

ISE Profiler Probes for Wireless

URL Redirect / IP Helper Alternative: Use SPAN to Capture HTTP / DHCP Traffic

- SPAN-based probes require a copy of the traffic be sent to ISE
- The SPAN / RSPAN / ERSPAN features are used to send a copy of local switch traffic (VLANs or Ports) to another port on the same or remote switch.

```
monitor session 1 source vlan xx , yy  
monitor session 1 destination interface Gi1/0/24
```



HTTP SPAN Alternative to URL Redirection

DHCPSPAN Alternative to ip helper

▼ DHCPSPAN	
Interface	GigabitEthernet 0
Description	DHCPSPAN
▼ HTTP	
Interface	GigabitEthernet 0
Description	HTTP

SPAN-Based Probes (DHCP, HTTP)

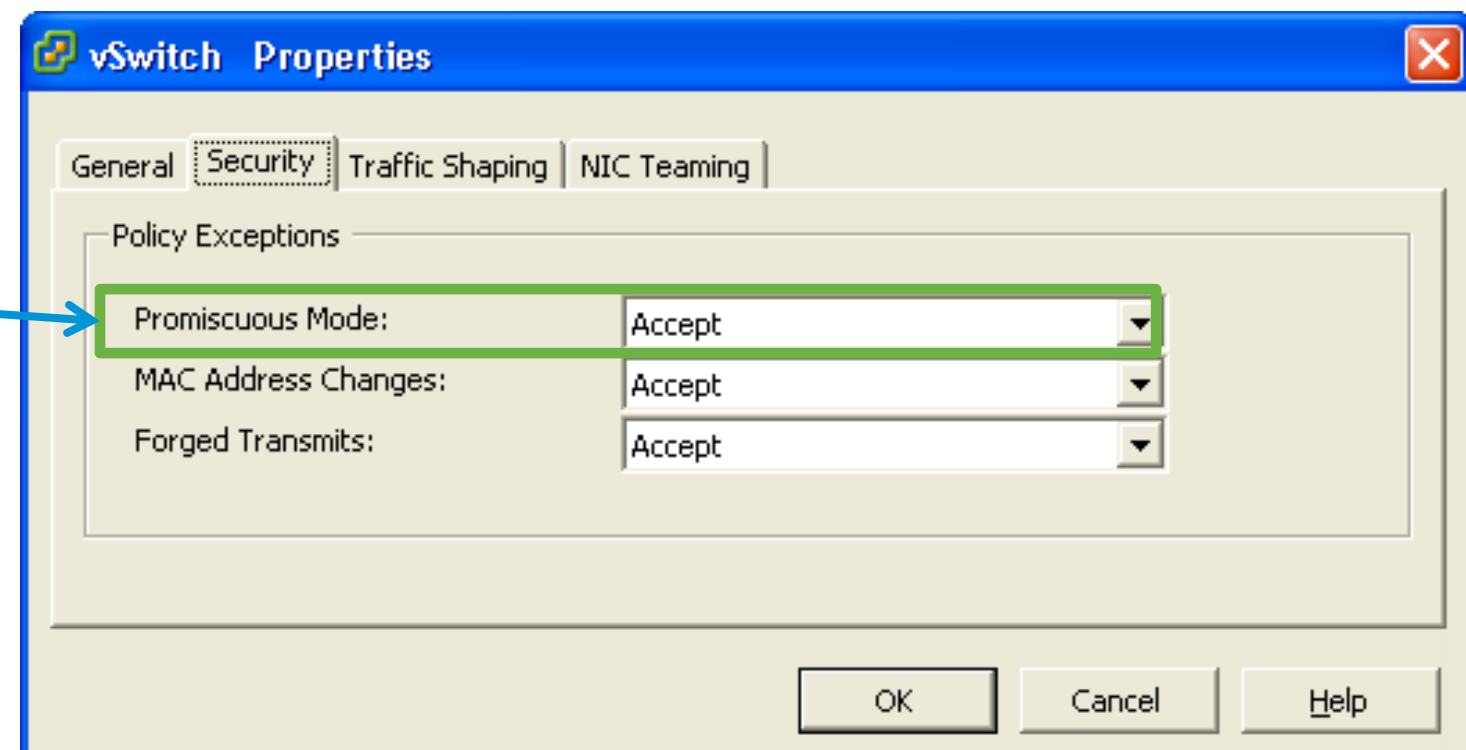
Best Practice Recommendations

- Use dedicated ISE interface (probes supported on all interfaces)

Enable interface from PSN CLI and optionally assign IP address

VMware appliance requires promiscuous mode to be set on the virtual switch/ interface to accept SPAN/mirror traffic.

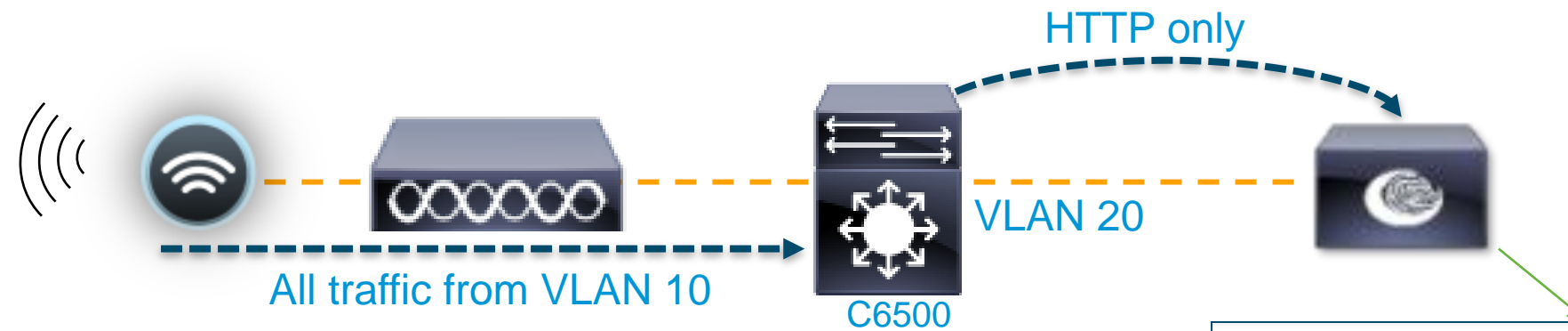
VMware Host > Configuration >
Hardware > Networking >
vSwitch > Security >
Promiscuous Mode: **Accept**
(Default = Reject)



- Use VACL Capture/Redirect with RSPAN to filter traffic to only interesting profile data and to reduce overall data that must be parsed by PSN

VACL Capture (HTTP Example)

Best Practice: Use VACL Capture to Forward only DHCP / HTTP



```
Cat6K(config)#ip access-list extended HTTP_TRAFFIC  
Cat6K(config-ext-nacl)#permit tcp any any eq www
```

```
Cat6K(config)#ip access-list extended ALL_TRAFFIC  
Cat6K(config-ext-nacl)#permit ip any any
```

```
Cat6K(config)#vlan access-map HTTP_MAP 10  
Cat6K(config-access-map)#match ip address HTTP_TRAFFIC  
Cat6K(config-access-map)#action forward capture
```

```
Cat6K(config)#vlan access-map HTTP_MAP 20  
Cat6K(config-access-map)#match ip address ALL_TRAFFIC  
Cat6K(config-access-map)#action forward
```

```
Cat6K(config)#vlan filter HTTP_MAP vlan-list 10
```

```
Cat6K(config)#int fa2/24  
Cat6K(config-if)#switchport capture allowed vlan 10,20  
Cat6K(config-if)#switchport capture
```

▼ HTTP

Interface

Description

Capture HTTP

Forward all other traffic

Applied to VLANs 10

Capture port;
include VLAN 10 traffic routed to VLAN 20

ISE Profiling

General Best Practice Recommendations

- **Use Device Sensors whenever possible to optimize data collection.**
- **Whenever possible, ensure profile data for a given endpoint sent to same PSN;** else potential for excessive updates of endpoint data and contention by multiple PSNs.
- **HTTP Probe:**
 - Use URL Redirects over SPAN to centralize collection and reduce traffic load related to SPAN/RSPAN.
 - In general try to avoid SPAN. If used, look for key traffic chokepoints such as Internet edge or WLC connection; use intelligent SPAN/tap options or VACL Capture to limit amount of data sent to ISE. Also difficult to provide HA for SPAN.
- **DHCP Probe:**
 - Use IP Helpers when possible—be aware that L3 device serving DHCP will not relay DHCP for same!
 - In general try to avoid DHCP SPAN. If used, make sure probe captures traffic to central DHCP Server. HA challenges.
- **SNMP Probe:**
 - Be careful of high SNMP traffic due to triggered RADIUS Accounting updates as a result of high re-auth (low session/re-auth timers) or frequent interim accounting updates.
 - For polled queries, be careful not to set polling interval too low. Be sure to set optimal PSN for polling in ISE NAD config.
 - SNMP Traps primarily useful for non-RADIUS deployments like integration with NAC Appliance
- **NetFlow:** Use only for specific use cases in centralized deployments. Potential for high load on network devices and ISE database (replication).

Monitoring and Reporting



Profiling Monitoring

Real-Time Monitoring

Profiled Endpoint Dashboard

Unique: 1993 (Last 24 Hours)

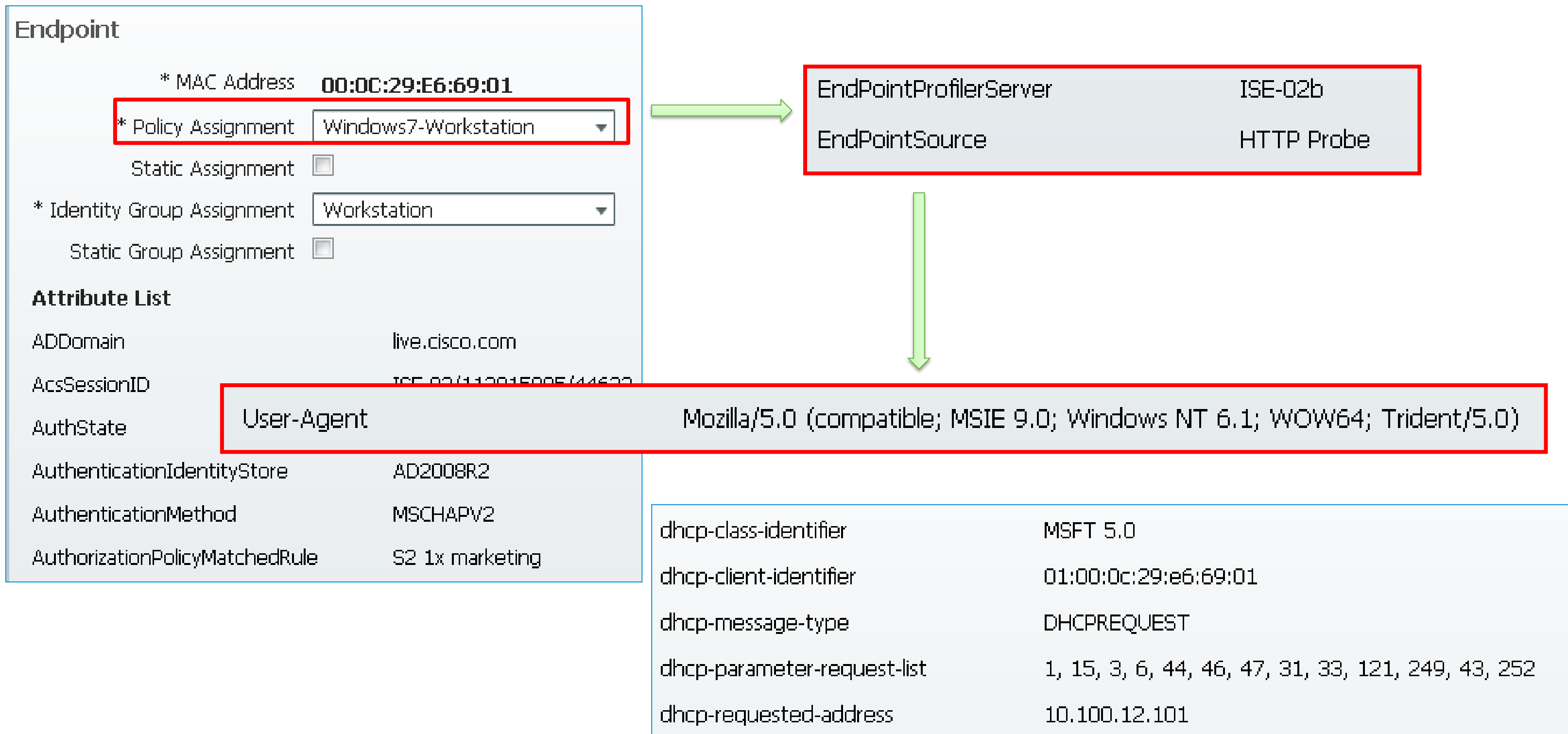
Endpoints

Profiled Endpoint List

Endpoint Profile	MAC Address
<input type="checkbox"/> Cisco-Device	C8:4C:75:85:30:C0
<input type="checkbox"/> Cisco-Device	00:1F:9D:CA:38:40
<input type="checkbox"/> Cisco-Device	00:19:56:D9:29:68
<input type="checkbox"/> Cisco-IP-Phone-7945	00:21:55:D6:00:8D
<input type="checkbox"/> Cisco-IP-Phone-7945	00:21:55:D6:03:08
<input type="checkbox"/> Microsoft-Workstation	00:0C:29:D0:E2:82
<input type="checkbox"/> Microsoft-Workstation	00:24:D7:3A:0E:18
<input type="checkbox"/> Nortel-Device	5C:FF:35:01:F6:DE
<input type="checkbox"/> Unknown	E0:F8:47:53:3D:7D
<input type="checkbox"/> VMWare-Device	00:0C:29:52:3A:DB
<input type="checkbox"/> Windows7-Workstation	F0:DE:F1:0D:59:58
<input type="checkbox"/> Xerox-Device	00:00:00:00:E2:82

Endpoint Detail

All Profiling Attributes Collected about Endpoint



Endpoint Profiler Summary

Detailed Report for Profiler Activity



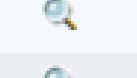
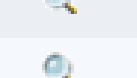
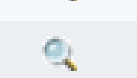
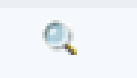
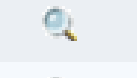
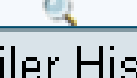

Endpoint > Endpoint Profiler Summary

Showing Page 1 of 1

First Prev Next Last

Generated on December 15, 2011 12:58:10 AM GMT

 [Reload](#)

Logged At		Details	Mac
Dec 15, 2011 12:24 AM		Raw Log	00:18:F8:2D:3C:
Dec 15, 2011 12:24 AM		Raw Log	58:94:6B:3F:7F:
Dec 15, 2011 12:24 AM		Raw Log	00:21:55:D6:01:
Dec 15, 2011 12:24 AM		Raw Log	00:24:D7:2C:9A:
Dec 15, 2011 12:24 AM		Raw Log	00:24:D7:A0:8F:
Dec 15, 2011 12:24 AM		Raw Log	00:50:56:4F:AE:
Dec 15, 2011 12:28 AM		Raw Log	C8:4C:75:85:99:
Dec 15, 2011 12:24 AM		Raw Log	00:16:41:E2:CB:
Dec 15, 2011 12:24 AM		Raw Log	00:1F:3C:B9:DA:

Profiler History

Day	Endpoint policy
Dec 15, 2011 12:24 AM	Windows7-Workstation
Dec 8, 2011 3:14 PM	Windows7-Workstation
Dec 8, 2011 3:14 PM	Windows7-Workstation
Dec 8, 2011 3:13 PM	Microsoft-Workstation
Nov 17, 2011 4:15 PM	Microsoft-Workstation

Endpoint > Endpoint Profiler Detail

Generated on December 15, 2011 1:01:25 AM GMT

Endpoint Session time : Not Applicable

Endpoint Details

Endpoint Static Assignment :
 Endpoint Source :
 Endpoint OUI : Wistron InfoComm (Kunshan)Co
 Endpoint Host Name :
 Endpoint Subnet :
 Endpoint NAD Address : 10.100.7.1
 Endpoint VLAN : 14
 Endpoint FQDN :
 Endpoint Nameserver :
 Endpoint Property : CPMSessionID=07070707000001940E08049E
 StaticAssignment=false
 MacName=quest

Profiler Summary

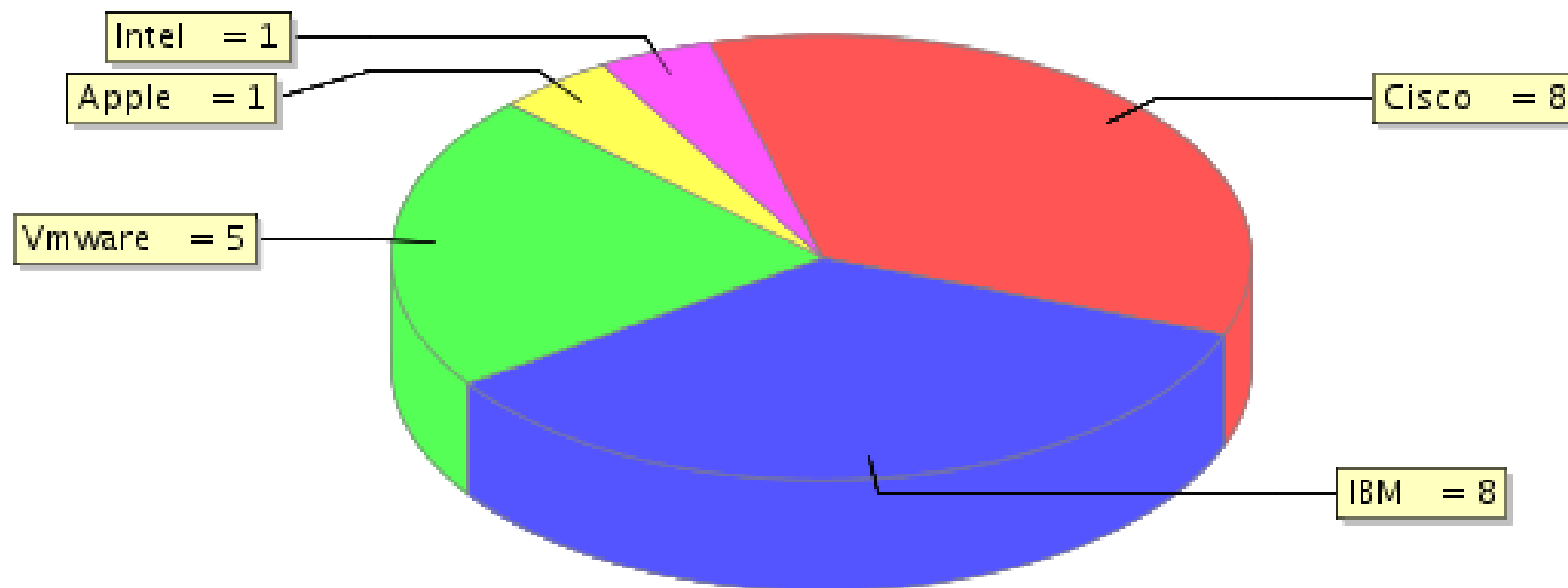
Logged At : Dec 15, 2011 12:24 AM
 Server : ISE-01
 Event : Profiler is triggering Change Of Authorization Request
 Endpoint MAC Address : F0:DE:F1:00:FE:20
 Endpoint Policy : Windows7-Workstation
 Matched Rule :
 Certainty Metric :
 Endpoint Matched Policy : Windows7-Workstation
 Endpoint Action Name :
 Identity Group : Workstation

NCS Prime Reporting

Client Summary By Vendor

Vendor	Average Number of Sessions	Maximum Number of Clients	Average Number of Clients	Total Session Time (Hours)	Total Traffic (MB)	% of Sessions	% of Clients	% of Session Time	% of Traffic
Cisco	16	9	8	236.62	0.0	37.21	34.78	30.91	0.0
IBM	15	9	8	314.98	0.0	34.88	34.78	41.15	0.0
Vmware	6	5	5	209.93	0.0	13.95	21.74	27.43	0.0
Apple	5	2	1	3.75	0.88	11.63	4.35	0.49	100.0
Intel	1	1	1	0.17	0.0	2.33	4.35	0.02	0.0

Clients by Vendor

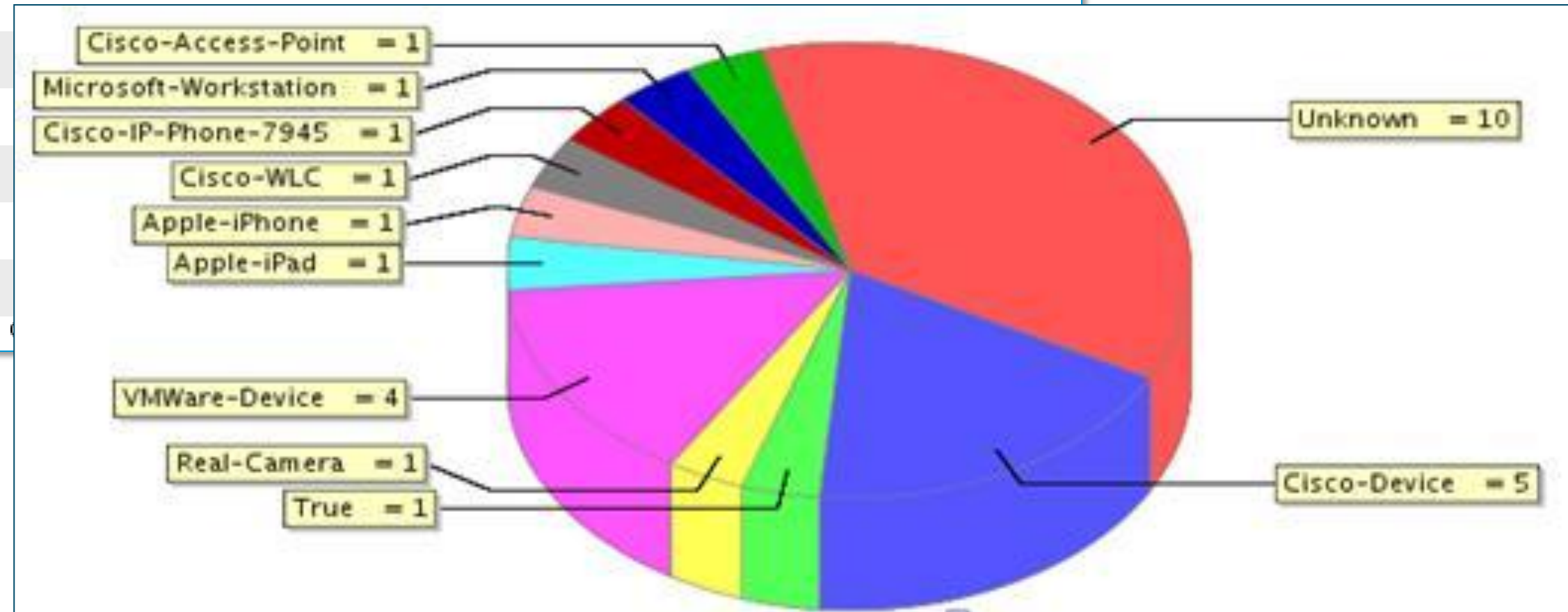


NCS Prime Reporting

Client Summary by Endpoint Type

Endpoint Type	Average Number of Sessions	Maximum Number of Clients	Average Number of Clients	Total Session Time (Hours)	Total Traffic (MB)	% of Sessions	% of Clients	% of Session Time	% of Traffic
Unknown	17	14	10	325.53	0.0	29.82	37.04	42.53	0.0
Cisco-Device	9	5	5	42.0	0.0	15.79	18.52	5.49	0.0
True	5	1	1	17.82	0.0	8.77	3.7	2.33	0.0
Real-Camera	5	1	1	20.0	0.0	8.77	3.7	2.61	0.0
VMWare-Device	5	4	4	155.88	0.0	8.77	14.81	20.36	0.0

Apple-iPad	4	1	1
Apple-iPhone	4	1	1
Cisco-WLC	3	1	1
Cisco-IP-Phone-7945	2	1	1
Microsoft-Workstation	2	2	1
Cisco-Access-Point	1	1	1



Support Resources

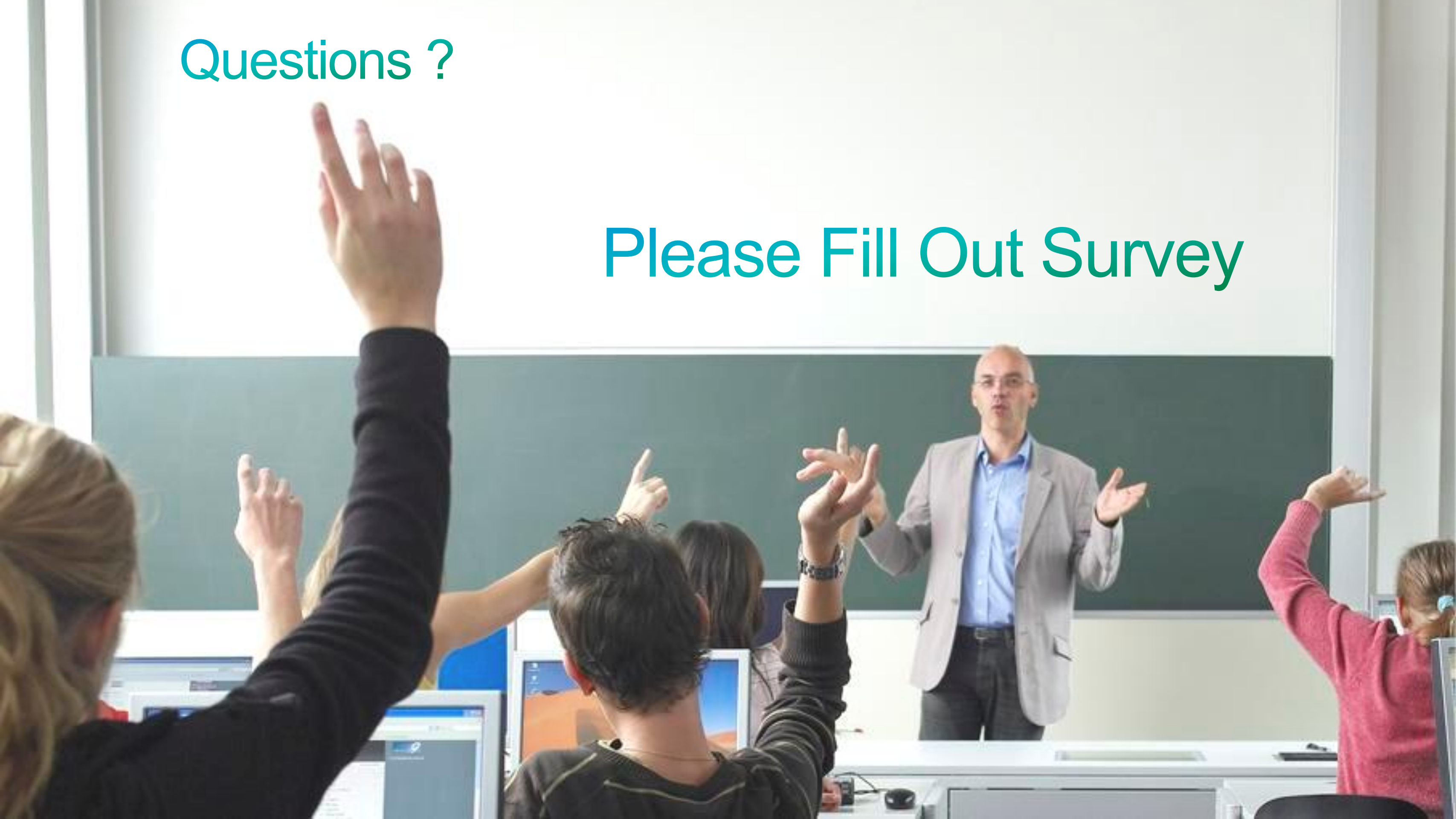
- ISE Product - <http://www.cisco.com/go/ise>
- TrustSec - <http://www.cisco.com/go/trustsec>
- ISE 1.1.1 Demos

<https://communities.cisco.com/community/partner/borderlessnetworks/security?view=video>

- dCloud BYOD Hosted Demos – <http://www.cisco.com/go/byoddemo>
- Free NFR Lab Software for Partners (1.1.1 Available)
Cisco Marketplace - \$35 VMware image, perpetual license, 20 endpoints
<http://cisco.mediuscorp.com/ise>
- PDI Helpdesk - Webpage: <http://www.cisco.com/go/pdihelpdesk>
- Program-related questions: pdihd-bn@cisco.com
- **Your Cisco PDM and CSE**

Questions ?

Please Fill Out Survey



Cisco ISE ATP Resources

- ISE ATP Portal: <http://ciscosecurityatp.com/>
- Cisco Partner ISE Resources: <http://cisco.com/go/isepartner>
- ISE ATP HLD Webinar: <https://communities.cisco.com/docs/DOC-27689>
- ISE HLD Help Alias (US): ise_hld_help@cisco.com
- ATP requirements and guidelines for ISE:
http://www.cisco.com/web/partners/partner_with_cisco/channel_partner_program/resale/atp/ise.html
- Sales Acceleration Center (SAC) for HLD submissions: sac-support@cisco.com
- SAMPG Partner Team:
Sheila Rone srone@cisco.com
Phuong Nguyen pvnguyen@cisco.com

Additional Training

- ISE Security Basics - <https://communities.cisco.com/docs/DOC-30718>
- ISE Best Practices VoD - Security Express - Replays and Presentations
<https://communities.cisco.com/docs/DOC-18350>
- 802.1X Training on PEC
<http://tools.cisco.com/pecx/login?URL=searchOffering%3FcourseId=00028869>
<http://tools.cisco.com/pecx/login?URL=searchOffering%3FcourseId=00028870>
<http://tools.cisco.com/pecx/login?URL=searchOffering%3FcourseId=00028851>
- Team MIDAS Wireless ISE and BYOD classes
Tech Sessions: <http://cisco.cvent.com/d/ccqs4s>
Hands-On Lab Sessions: <http://cisco.cvent.com/d/kcqs43>
Lab Guide: <https://communities.cisco.com/docs/DOC-30944>

Voice Of the Engineer – Security Basics

<https://communities.cisco.com/docs/DOC-30718>

- ISE Registration

<http://cisco.cvent.com/events/security-basics-ise/event-summary-7c9587527cea465fb40e76a08d9d28e3.aspx>

- ASA Registration

<http://cisco.cvent.com/events/security-basics-asa/event-summary-47f2d80478f141a28cea9c5df3f4e2dd.aspx>

Date	Time (Eastern)	Topic
9/12	2:00 - 3:00	ISE Overview
9/26	2:00 - 3:00	ASA Overview
10/10	11:00 - 12:00	ISE Overview
10/24	11:00 - 12:00	ASA Overview
11/7	2:00 - 3:00	ISE Overview
11/28	2:00 - 3:00	ASA Overview
12/5	11:00 - 12:00	ISE Overview
12/12	11:00 - 12:00	ASA Overview