

INTUITIVE

Cisco *live!*
June 10-14, 2018 • Orlando, FL



Designing ISE for Scale & High Availability

Craig Hys, Principal Engineer
BRKSEC-3699



Cisco *live!*

#CLUS



INTUITIVE

Session Abstract

Cisco Identity Services Engine (ISE) delivers context-based access control for every endpoint that connects to your network. **This session will show you how to design ISE to deliver scalable and highly available access control services for wired, wireless, and VPN from a single campus to a global deployment.**

Focus is on design guidance for distributed ISE architectures including high availability for all ISE nodes and their services as well as strategies for survivability and fallback during service outages. Methodologies for increasing scalability and redundancy will be covered such as load distribution with and without load balancers, optimal profiling design, and the use of Anycast.

Attendees of this session will gain knowledge on how to best deploy ISE to ensure peak operational performance, stability, and to support large volumes of authentication activity. Various deployment architectures will be discussed including ISE platform selection, sizing, and network placement.

ISE Sessions @Live Orlando 2018

You Are Here

Sunday

TECSEC-2672
*Identity Services Engine
2.4 Best Practices*
Jesse Dubois,
Eugene Korneychuk,
Kevin Redmon,
Vivek Santuka
Monday 9:00-6:00

Monday

BRKSEC-2059
*Deploying ISE in a
Dynamic Environment*
Clark Gambrel
Monday 1:30-3:30

Wednesday

BRKSEC-3697
Advanced ISE Services, Tips & Tricks
Craig Hyps, Wednesday 8:00-10:00

BRKCOC-2018
*Inside Cisco IT: How Cisco Deployed ISE and
Group Based Policies throughout the Enterprise*
Raj Kumar, David Iacobacci
Wednesday 8:30-10:00

BRKSEC-2464
*Lets get practical with your network security
by using Cisco ISE*
Imran Bashir, Wednesday 10:30-12:00

BRKSEC-2695
*Building an Enterprise Access Control
Architecture using ISE and Group Based Policies*
Imran Bashir, Wednesday 1:30-3:30

Thursday

BRKSEC-3699
*Designing ISE for Scale & High
Availability*
Craig Hyps
Thursday 8:00-10:00

BRKSEC-2038
*Security for the Manufacturing
Floor - The New Frontier*
Shaun Muller
Thursday 10:30-12:00

BRKSEC-2039
*Cisco Medical Device
Segmentation*
Tim Lovelace, Mark Bernard
Thursday 1:00-2:30

Important: Hidden Slide Alert

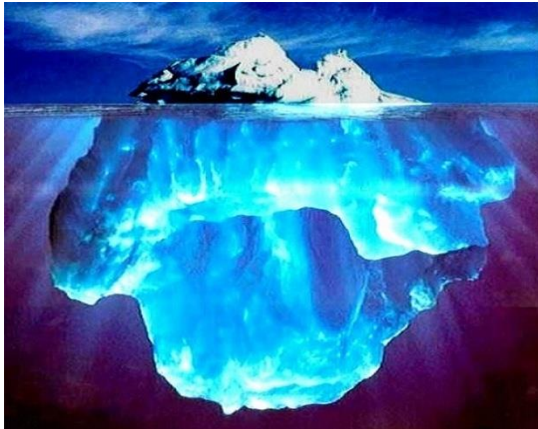


Look for this “For Your Reference”
Symbol in your PDF’s

There is a tremendous amount of
hidden content, for you to use later!



For Your
Reference



~500 +/- Slides in
Session Reference PDF

Available on
ciscolive.com

BRKSEC-3699 - Designi

Documents

 Session Presentation

 Session Reference

View Session

 Session Video

Cisco Webex Teams

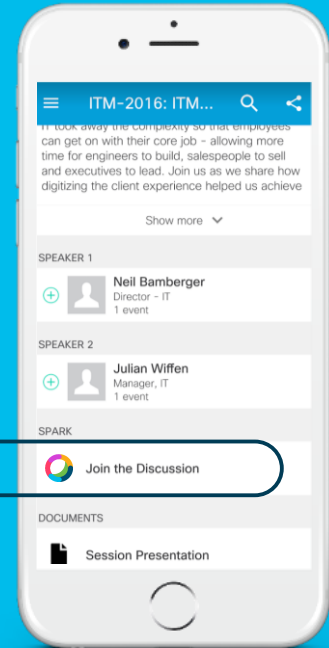
Questions?

Use Cisco Webex Teams (formerly Cisco Spark) to chat with the speaker after the session

How

- 1 Find this session in the Cisco Events App
- 2 Click “Join the Discussion”
- 3 Install Webex Teams or go directly to the team space
- 4 Enter messages/questions in the team space

Webex Teams will be moderated by the speaker until June 18, 2018.



cs.co/ciscolivebot#BRKSEC-3699

Where can I get help after Cisco Live?



ISE Public Community

<http://cs.co/ise-community>

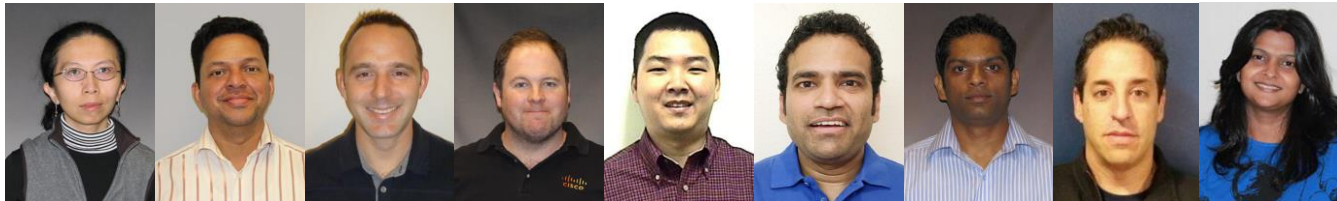
Questions answered by ISE TMEs and other Subject Matter Experts – the same persons that support your local Cisco and Partner SEs!

ISE Compatibility Guides

<http://cs.co/ise-compatibility>

ISE Design Guides



<http://cs.co/ise-guides>



Courtesy
of
Thomas
Howard



Agenda

- Sizing Deployments and Nodes
- Bandwidth and Latency
- Scaling ISE Services
 - RADIUS, Guest, Web Services, Compliance, TACACS+
 - Profiling and Database Replication
 - MnT (Optimize Logging and Noise Suppression)
- High Availability
 - Appliance Redundancy
 - Admin, MnT, and pxGrid Nodes
 - PSN Redundancy with and without Load Balancing
 - NAD Fallback and Recovery 
- Monitoring Load and System Health 



Time Permitting

Sizing Guidance for ISE Nodes

ISE 2.4 Scaling by Deployment/Platform/Persona

Max Concurrent Session Counts by Deployment Model and Platform

- By Deployment

Deployment Model	Platform	Max Active Sessions per Deployment	Max # Dedicated PSNs / PXGs	Min # Nodes (no HA) / Max # Nodes (w/ HA)
	3515	7,500	0	1 / 2
	3595	20,000	0	1 / 2
	3515 as PAN+MNT	7,500	5 / 2*	2 / 7
	3595 as PAN+MNT	20,000	5 / 2*	2 / 7
	3595 as PAN and MNT	500,000	50 / 2	3 / 58
	3595 as PAN and Large MNT	500,000	50 / 4	3 / 58

- By PSN

Max Active Sessions != Max Endpoints; ISE 2.1+ supports 1.5M Endpoints

Scaling per PSN	Platform	Max Active Sessions per PSN
Dedicated Policy nodes (Max Sessions Gated by Total Deployment Size)	SNS-3515	7,500
	SNS-3595	40,000

* Each dedicated pxGrid node reduces PSN count by 1 (Medium deployment only)

Sizing Production VMs to Physical Appliances

Summary

Appliance used for sizing comparison	CPU		Memory (GB)	Physical Disk (GB) **
	# Cores	Clock Rate*		
SNS-3415	4	2.4	16	600
SNS-3495	8	2.4	32	600
SNS-3515	6	2.3	16	600
SNS-3595	8	2.6	64	1,200

* Minimum VM processor clock rate = 2.0GHz per core (same as OVA).

** Actual disk requirement is dependent on persona(s) deployed and other factors. See slide on Disk Sizing.

Warning: # Cores not always = # Logical processors / vCPUs due to Hyper Threading

ISE Platform Properties

Minimum VM Resource Allocation

Minimum CPUs	Minimum RAM	Minimum Disk	Platform Profile
2	4	100 GB	EVAL
4	4	200GB	IBM_SMALL_MEDIUM
4	4	200GB	IBM_LARGE
4	16	200GB	UCS_SMALL
8	32	200GB	UCS_LARGE
12	16	200GB	SNS_3515
16	64	200GB	SNS_3595
16	256	200GB	SNS_3595 <large>

- Least Common Denominator used to set platform.
- Example:
4 cores
32GB RAM
= UCS_SMALL

Why Do I Care?

Because memory, max sessions, and other table spaces are based on Persona and Platform Profile

ISE OVA Templates

Summary

OVA Template	CPU			Virtual Memory (GB)	Virtual NICs (GB)	Virtual Disk Size	Target Node Type
	# CPUs	Clock Rate (GHz)	Total CPU (MHz)				
Eval	2	2.3	4,600	8	4	200GB	EVAL
SNS3415	4	2.0	8,000	16	4	200GB	PSN/PXG
						600GB	PAN/MnT
SNS3495	8	2.0	16,000	32	4	200GB	PSN/PXG
						600GB	PAN/MnT
SNS3515	8 12	2.0	12,000	16	6	200GB	PSN/PXG
						600GB	PAN/MnT
SNS3595	8 16	2.0	16,000	64	6	200GB	PSN/PXG
						1.2TB	PAN/MnT

CSCvh71644 - VMware OVA templates for SNS-35xx are not detected correctly...

For 35x5 ISE VMs, HyperThreading is Mandatory

ISE Platform Properties

Verify ISE Detects Proper VM Resource Allocation

- From CLI...

- `ise-node/admin# show tech | begin PlatformProperties`

```
PlatformProperties whoami: root
PlatformProperties show inventory: Process Output:
Profile : UCS_SMALL
Current Memory Size : 16267516
Time taken for NSFAdminServiceFactor
```

- From Admin UI (ISE 2.2 +)
 - Operations > Reports > Diagnostics > ISE Counters > [node] (Under ISE Profile column)

The screenshot shows the ISE Admin UI for 'ISE Counters'. A red box highlights the 'UCS_SMALL' profile name in the top right. A red line connects this box to a red box around 'UCS_SMALL' in the 'Profile' field of the CLI output. Below the filters, a table lists counter attributes and their associated ISE profiles. The 'UCS_SMALL' profile is highlighted in red in the 'ISE Profile' column.

Counter Attribute Threshold		
Attribute Name		ISE Profile
ARP Cache Insert Update Received		UCS_SMALL
DHCP Endpoint Detected		UCS_SMALL
DHCP Skip Profiling		UCS_SMALL

ISE VM Disk Storage Requirements

Minimum Disk Sizes by Persona

- Upper range sets #days MnT log retention
- Min recommended disk for MnT = **600GB**
- Max hardware appliance disk size = 1.2TB
- **Max virtual appliance disk size = 2TB**

CSCvb75235 - DOC ISE VM installation can't be done if disk is greater than or equals to 2048 GB or 2 TB

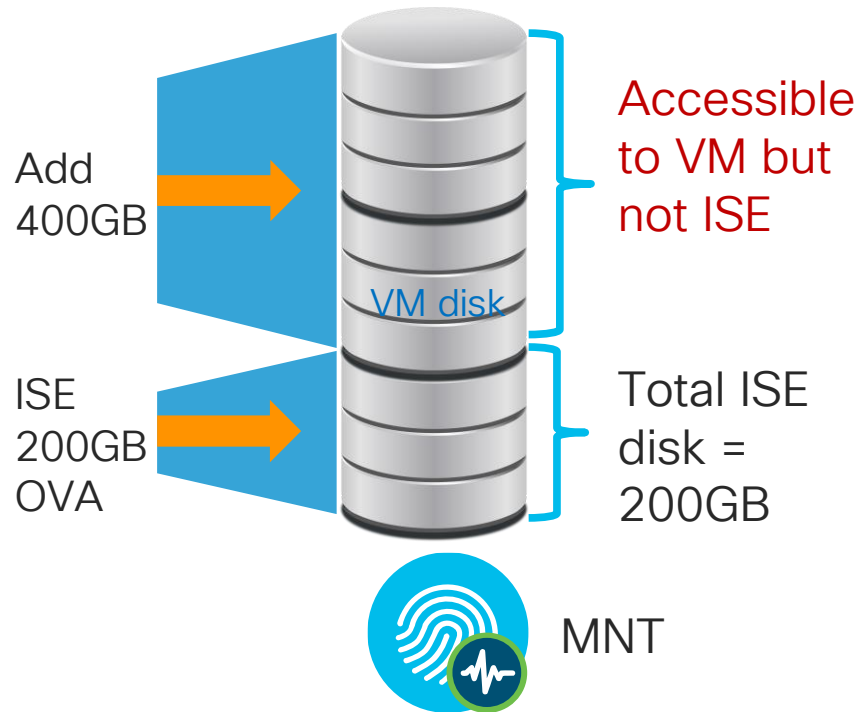
****** Variations depend on where backups saved or upgrade files staged (local or repository), debug, local logging, and data retention requirements.

Persona	Disk (GB)
Standalone	200+*
Administration Only	200-300**
Monitoring Only	200+*
Policy Service Only	200
PAN + MnT	200+*
PAN + MnT + PSN	200+*

VM Disk Allocation

CSCvc57684 Incorrect MnT allocations if setup with VM disk resized to larger without ISO re-image

- ISE OVAs prior to ISE 2.2 sized to 200GB. Often sufficient for PSNs or pxGrid nodes but not MnT.
- Misconception: Just get bigger tank and ISE will grow into it!
- No auto-resize of ISE partitions when disk space added after initial software install
- Requires re-image using .iso
- Alternatively: Start with larger OVA (ISE 2.2)



MnT Node Log Storage Requirements for RADIUS

Days Retention Based on # Endpoints and Disk Size (ISE 2.2)

Total Disk Space Allocated to MnT Node

	200 GB	400 GB	600 GB	1024 GB	2048 GB
5,000	504	1007	1510	2577	5154
10,000	252	504	755	1289	2577
25,000	101	202	302	516	1031
50,000	51	101	151	258	516
100,000	26	51	76	129	258
150,000	17	34	51	86	172
200,000	13	26	38	65	129
250,000	11	21	31	52	104
500,000	6	11	16	26	52

Total Endpoints

ISE 2.2 = 50% days increase over 2.0/2.1
ISE 2.3 = 25-33% increase over 2.2
ISE 2.4 = 40-60% increase over 2.2

Assumptions:

- 10+ auths/day per endpoint
- Log suppression enabled

Based on 60% allocation of MnT disk to RADIUS logging
(Prior to ISE 2.2, only 30% allocations)


RADIUS and TACACS+

MnT Log Allocation

Updated in
ISE 2.2!

- Administration > System > Maintenance > Operational Data Purging

Database Utilization



ise22-pan1.cts.local

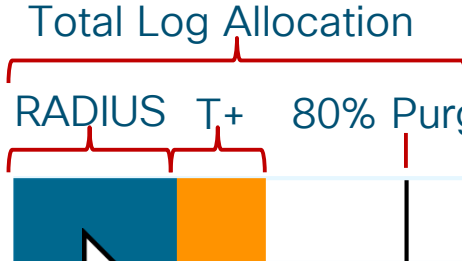
384 GB
Total DB Space

Data Retention Period

RADIUS	<input type="text" value="30"/>	Days
TACACS	<input type="text" value="30"/>	Days

Default Retention reduced from 90 -> 30 days

Total Log Allocation



M&T_PRIMARY
Radius : 67 GB
Days : 24

Operational Data Purging

Purge all data

Purge data older than Days

RADIUS

TACACS

- 60% total disk allocated to both RADIUS and TACACS+ for logging (Previously fixed at 30% and 20%)
- Purge @ 80% (First In-First Out)
- Optional archive of CSV to repository

▼ Purge data Now

Purge all data

Purge data older than Days

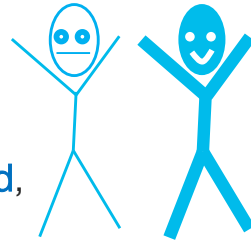
RADIUS

TACACS

BRKSEC-3699 © 2018 Cisco and/or its affiliates. All rights reserved. Cisco Public 19

ISE VM Disk Provisioning Guidance

- Please! No Snapshots!
 - **Snapshots NOT supported**; no option to quiesce database prior to snapshot.
- VMotion supported but storage motion not QA tested.
 - **Recommend avoid VMotion** due to snapshot restrictions.
- Thin Provisioning supported
 - **Thick Provisioning highly recommended**, especially for PAN and MnT)
- No specific storage media and file system restrictions.
 - For example, VMFS is not required and NFS allowed *provided* storage is supported by VMware and meets ISE IO performance requirements.



IO Performance Requirements:

- Read 300+ MB/sec
- Write 50+ MB/sec

Recommended disk/controller:

- 10k RPM+ disk drives
 - Supercharge with SSD !
- Caching RAID Controller
- RAID mirroring
 - Slower writes using RAID 5*

*RAID performance levels:

<http://www.datarecovery.net/articles/raid-level-comparison.html>

<http://docs.oracle.com/cd/E19658-01/820-4708-13/appendixa.html>

ISE VM Provisioning Guidance

- Use reservations (built into OVAs)
- Do not oversubscribe!

Customers with VMware expertise may choose to disable resource reservations and over-subscribe, but do so at own risk.

Introducing “Super” MnT

For Any Deployment where High-Perf MnT Operations Required

- Virtual Appliance Only option in ISE 2.4
 - Requires Large VM License
- 3595 specs + 256 GB
 - 8 cores @ 2GHz min (16000+ MHz)
= 16 logical processors
 - 256GB RAM
 - Up to 2TB* disk w/ fast I/O
- Fast I/O Recommendations:
 - Disk Drives (10k/15k RPM or SSD)
 - Fast RAID w/Caching (ex: RAID 10)
 - More disks (ex: 8 vs 4)

MnT



* CSCvb75235 - DOC ISE VM installation can't be done if disk is greater than or equals to 2048 GB or 2 TB

ISE 2.4 MnT -- Fast Access to Logs and Reports

Identity Services Engine Home Context Visibility Operations Policy Administration Work Centers

RADIUS Threat-Centric NAC Live Logs TACACS Troubleshoot Adaptive Network Control Reports

Live Logs Live Sessions

Misconfigured Supplicants 0 Misconfigured Network Devices 0 RADIUS Drops 2880 Client Stopped Responding 480 Repeat Counter 0

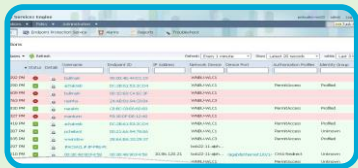
Refresh Never Show Latest 50 records Within Last 30 minutes

Refresh Reset Repeat Counts Export To Filter

Time	Status	Details	Repeat ...	Identity	Endpoint ID	Endpoint P...	Authenticat...	Authorizati...	Authorizati...	IP Address	Network Device	Device Port	Ide
Jan 26, 2018 11:06:16.262 AM			0	susain	98:5A:EB:8E:FD:16	Apple-Device	Bldg_SJC19...	Bldg_SJC19...	PermitAcces...	10.40.130.16			
Jan 26, 2018 11:05:50.519 AM				jjose2	98:F1:70:33:42:B0						sbgise-bgl13-00...		
Jan 26, 2018 11:05:34.504 AM				INVALID			Building_SJ...	Building_SJ...			WNBU-WLC1		
Jan 26, 2018 11:05:32.821 AM				INVALID			Building_SJ...	Building_SJ...			sjc14-22a-talwar		
Jan 26, 2018 11:05:23.126 AM			0	50:1A:C5:DD:7A:AF	50:1A:C5:DD:7A:AF	Microsoft-W...	Location_NT...	Location_NT...	WLC_NTN...				
Jan 26, 2018 11:05:23.126 AM				50:1A:C5:DD:7A:AF	50:1A:C5:DD:7A:AF	Microsoft-W...	Location_NT...	Location_NT...	WLC_NTN...		NTN-WLC1		Wo
Jan 26, 2018 11:05:11.995 AM				vani	AC:BC:32:AC:7E:23						sjc19-00a-wlc1		
Jan 26, 2018 11:04:54.173 AM			0	kusenapa	DC:EF:CA:4D:41:F	Unknown	Bldg_SJC19...	Bldg_SJC19...	PermitAcces...	10.40.130.46			
Jan 26, 2018 11:04:27.145 AM			0	6C:40:08:92:25:96	6C:40:08:92:25:96	OS_X_EI_C...	Location_BX...	Location_BX...	Guest_Redir...	10.86.103.135			
Jan 26, 2018 11:04:23.999 AM				6C:40:08:92:25:96	6C:40:08:92:25:96	OS_X_EI_C...	Location_BX...	Location_BX...	Guest_Redir...		sampg-bxb22-0...		Wo
Jan 26, 2018 11:04:10.882 AM				INVALID			Building_SJ...	Building_SJ...			sjc14-22a-talwar		
Jan 26, 2018 11:04:06.040 AM				USERNAMEUSE...	4C:EB:42:C7:31:70		Bldg_SJC19...	Bldg_SJC19...			sjc19-00a-wlc1		
Jan 26, 2018 11:04:04.493 AM				jjose2	98:F1:70:33:42:B0						sbgise-bgl13-00...		
Jan 26, 2018 11:04:03.462 AM			0	vinothra	7C:50:49:63:CC:F0	Apple-iPhone	Bldg_SJC19...	Bldg_SJC19...	PermitAcces...	10.40.130.14			

ISE 2.4 MnT Vertical Scaling Scaling Enhancements

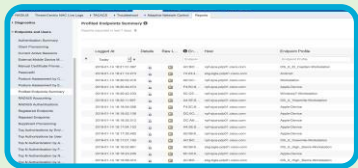
Benefits MnT
on ALL ISE
platforms



Time	Source IP	Destination IP	Source Port	Destination Port	Protocol	Action
01/01/2018 10:00:00	10.10.10.10	10.10.10.10	80	80	HTTP	Success
01/01/2018 10:00:01	10.10.10.10	10.10.10.10	80	80	HTTP	Success
01/01/2018 10:00:02	10.10.10.10	10.10.10.10	80	80	HTTP	Success
01/01/2018 10:00:03	10.10.10.10	10.10.10.10	80	80	HTTP	Success
01/01/2018 10:00:04	10.10.10.10	10.10.10.10	80	80	HTTP	Success
01/01/2018 10:00:05	10.10.10.10	10.10.10.10	80	80	HTTP	Success

Faster Live Log Access

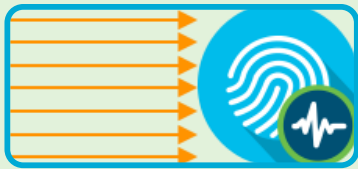
- Run session directory tables from pinned memory
- Tables optimized for faster queries



Report Name	Start Time	End Time	Report Type	Report Status
Network Access Report	2018-01-01 10:00:00	2018-01-01 10:00:00	Network Access	Success
Network Access Report	2018-01-01 10:00:01	2018-01-01 10:00:01	Network Access	Success
Network Access Report	2018-01-01 10:00:02	2018-01-01 10:00:02	Network Access	Success
Network Access Report	2018-01-01 10:00:03	2018-01-01 10:00:03	Network Access	Success
Network Access Report	2018-01-01 10:00:04	2018-01-01 10:00:04	Network Access	Success
Network Access Report	2018-01-01 10:00:05	2018-01-01 10:00:05	Network Access	Success

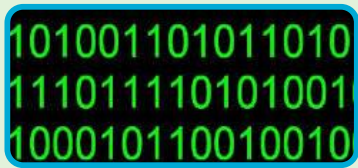
Faster Report & Export Performance

- Report related tables pinned into memory for faster retrieval.
- Optimize tables based on platform capabilities.



Collector Throughput improvement

- Added Multithreaded processing capability to collector.
- Increased collector socket buffer size to avoid packet drops.



Major Data Reduction

- Remove detailed BLOB data > 7 days old (beyond 2.3 reductions)
- Database optimizations resulting in up to 80% efficiencies

Flash Removal (ISE 2.4)

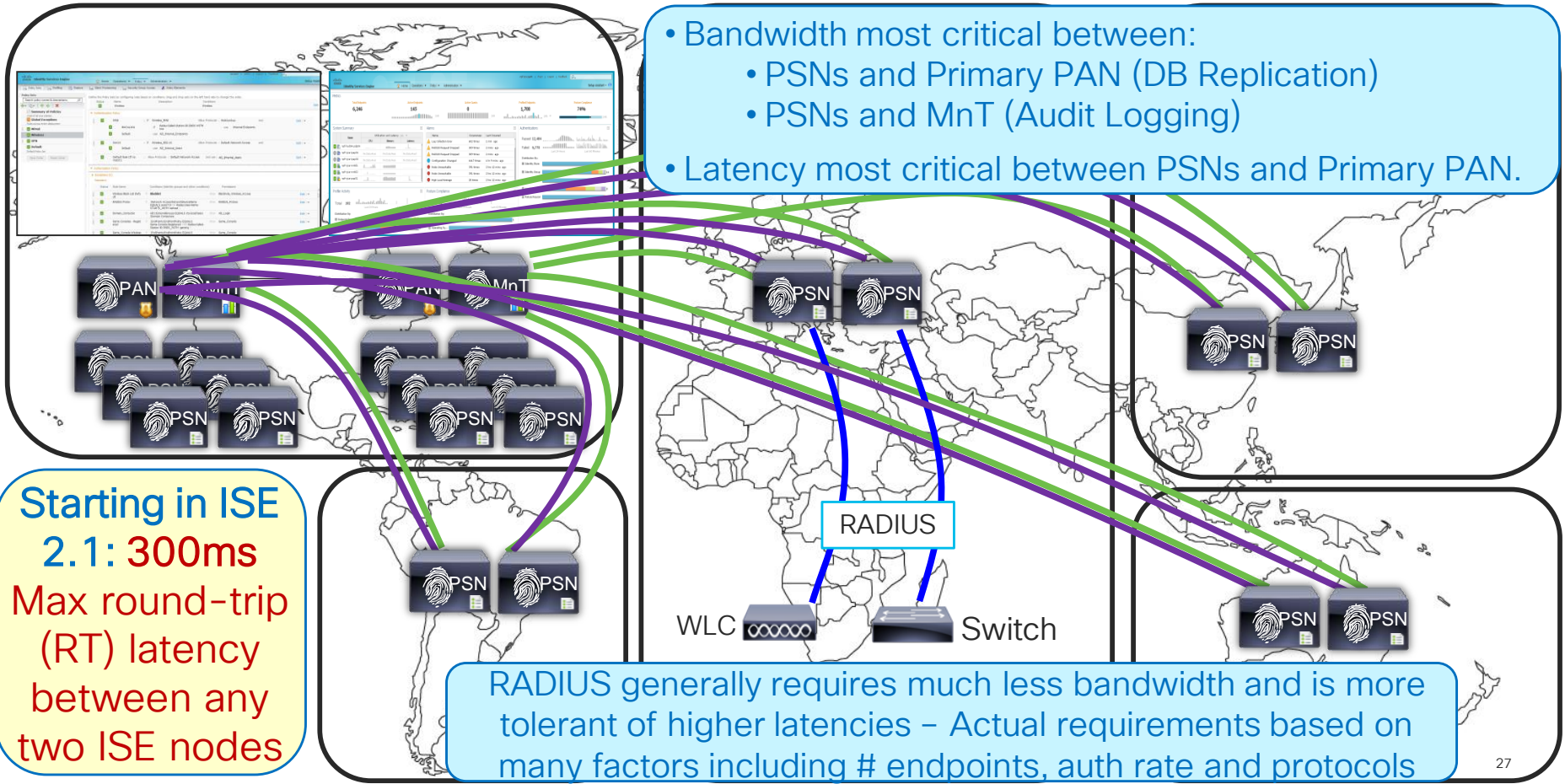
And no Yahoo! User Interface Library (YUI)

- “No Flash”
- C’mon, you mean just a little bit of flash, right?
- No. I’m Saying No Flash! There is no Flash in this product!



Bandwidth and Latency

Bandwidth and Latency

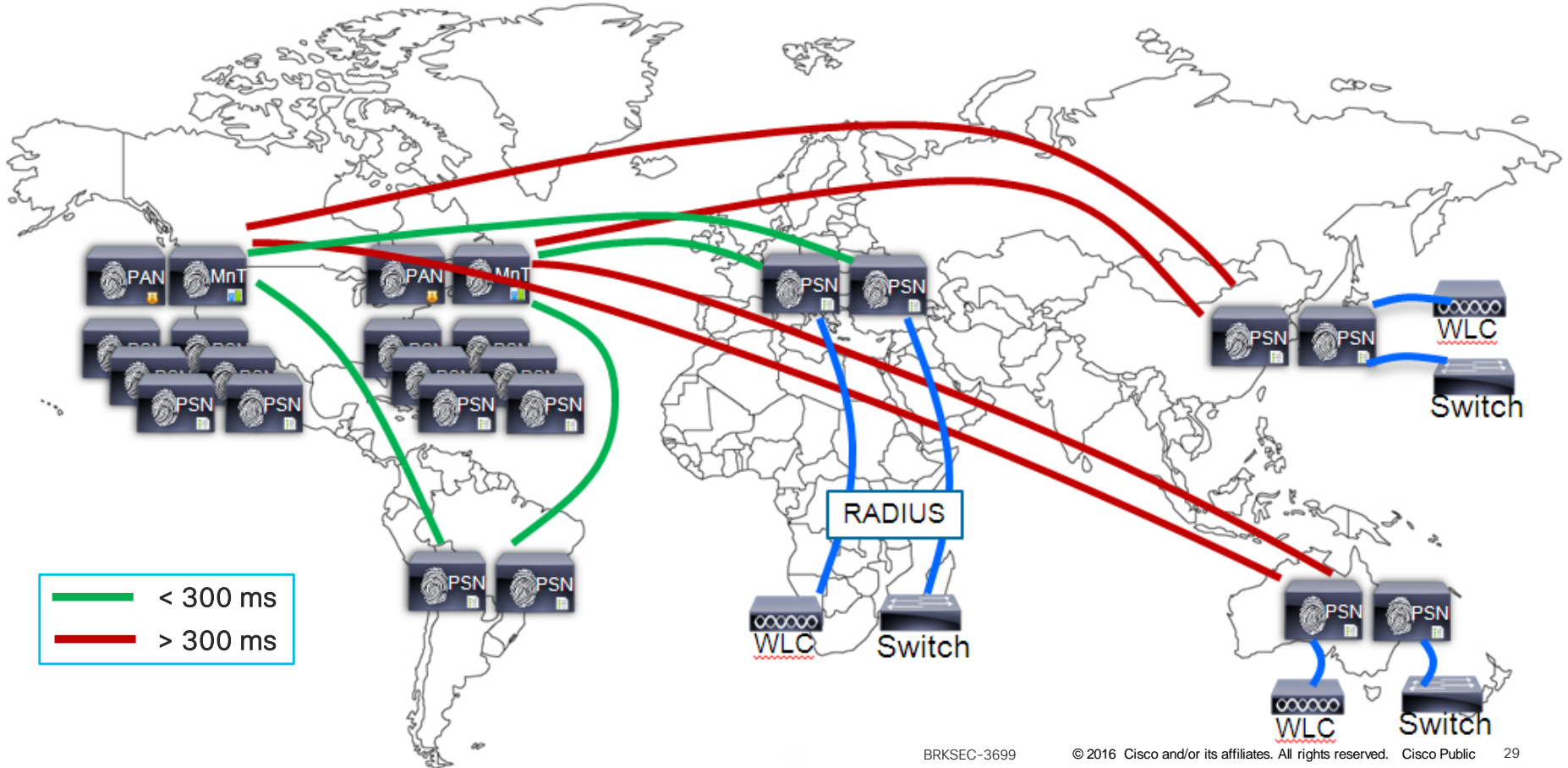


Have I Told You My Story Over Latency Yet?

“Over Latency?” “No. I Don’t Think I’ll Ever Get Over Latency.”

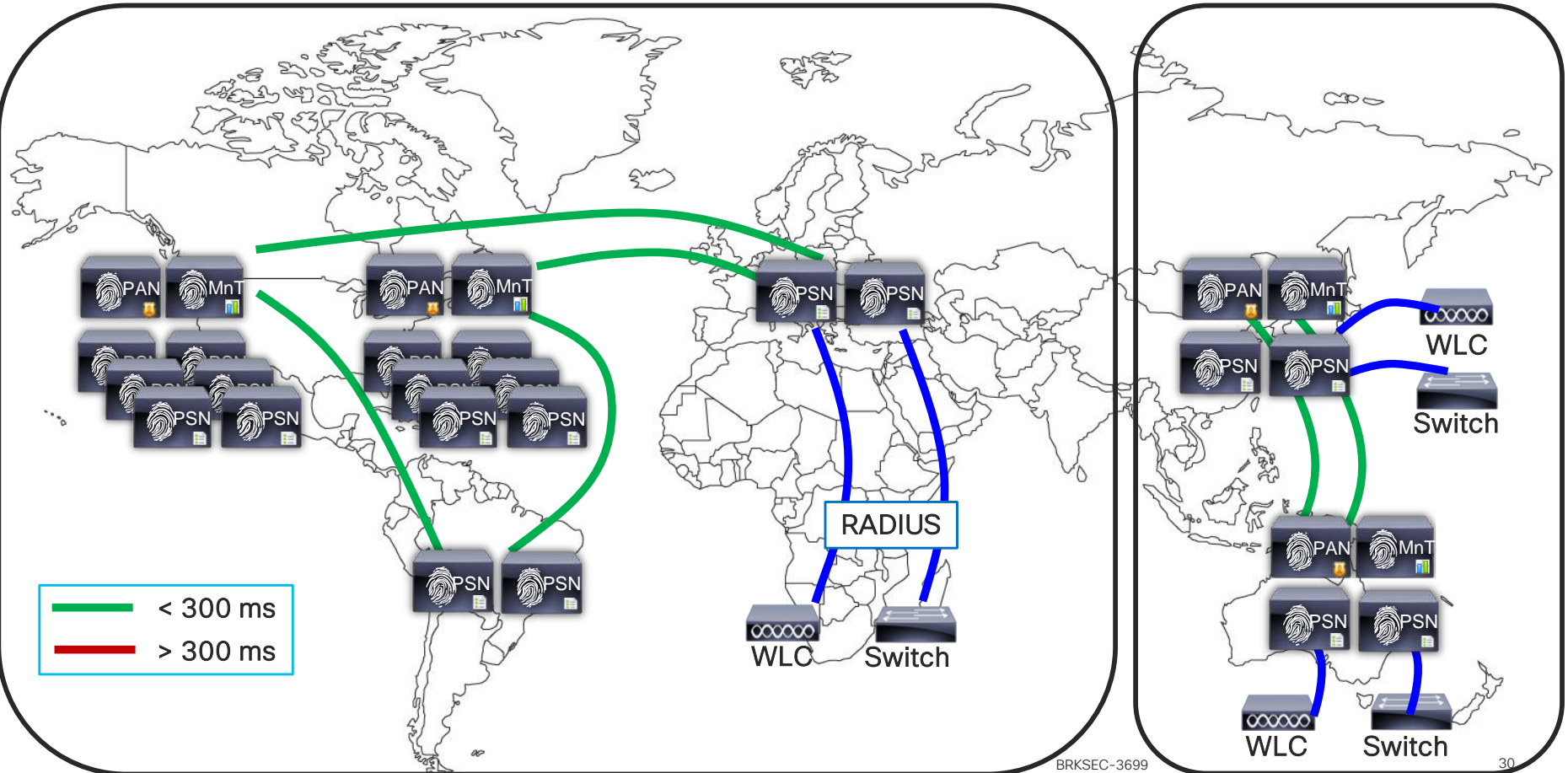
- Latency guidance is not a “fall off the cliff” number, but a guard rail based on what QA has tested.
- Not all customers have issues with > 300ms while others may have issues with < 100ms latency due to overall ISE design and deployment.
- Profiler config is primary determinant in replication requirements between PSNs and PAN which translates to latency.
- When providing guidance, max 300ms roundtrip latency is the correct response from SEs for their customers to design against.

What if Distributed PSNs > 300ms RTT Latency?



Option #1: Deploy Separate ISE Instances

Per-Instance Latency < 300ms



ISE Bandwidth Calculator – Updated for ISE 2.1+

ISE 2.x Network Bandwidth Calculation for Multiple Remote Locations

Total Active Endpoints: 25,000
% Mobile Endpoints: 20
Remote Locations with PSNs (Not including data centers): 2
Sending profile data for same endpoints to multiple locations? YES
Reauth Interval (Default 2 hrs): 2
DHCP Lease Period (Default 4 hrs): 4

INSTRUCTIONS:
 1. Update values in GREEN cells.
 2. Bandwidth results appear in BLUE cells.
 3. Charts summarize results

Reset Remote Location Data

Location	Bandwidth Reqd to DC1 (Mbps)	Bandwidth Reqd to DC2 (Mbps)	Total DC Bandwidth (Mbps)	(P)=Primary (S)=Secondary				# PSNs	# Active Endpoints	Aggregate DC Head-End WAN Bandwidth (Mbps)			
				PAN(P)	PAN(S)	MNT(P)	MNT(S)			MnT Log BW	Replication BW	Ownership Change BW	Total
DC1/Main Campus	N/A	0.432	0.432	○	○	●	○	2	10,000	0.648	2.160	0.864	3.672
DC2/Secondary Campus	1.998	N/A	1.998	○	●	○	○	2	10,000	0.648	1.080	0.486	2.214
Remote Site 1	0.902	0.151	1.053					2	3,500				
Remote Site 2	0.772	0.065	0.837					2	1,500				
Total PSNs and Endpoints								8	25,000				

Remote to DC Bandwidth Requirements (Mbps)

Total DC Head-End Bandwidth Requirement (Mbps)

Note: Bandwidth required for RADIUS traffic is not included. Calculator is focused on inter-ISE node bandwidth requirements.

Available to customers @ <https://communities.cisco.com/docs/DOC-64317>

Scaling ISE Services

Scaling ISE Services Agenda

- Auth Policy and Service Scale
- Guest and Web Authentication and Location Services
- Compliance Services—Posture and MDM
- Scaling TACACS+
- Profiling and Database Replication
- MnT (Optimize Logging and Noise Suppression)

ISE Personas and Services

Enable Only What Is Needed !!

Session Services includes base user services such as RADIUS, Guest, Posture, MDM, BYOD/CA

• ISE Personas:

- PAN
- MNT
- PSN
- pxGrid

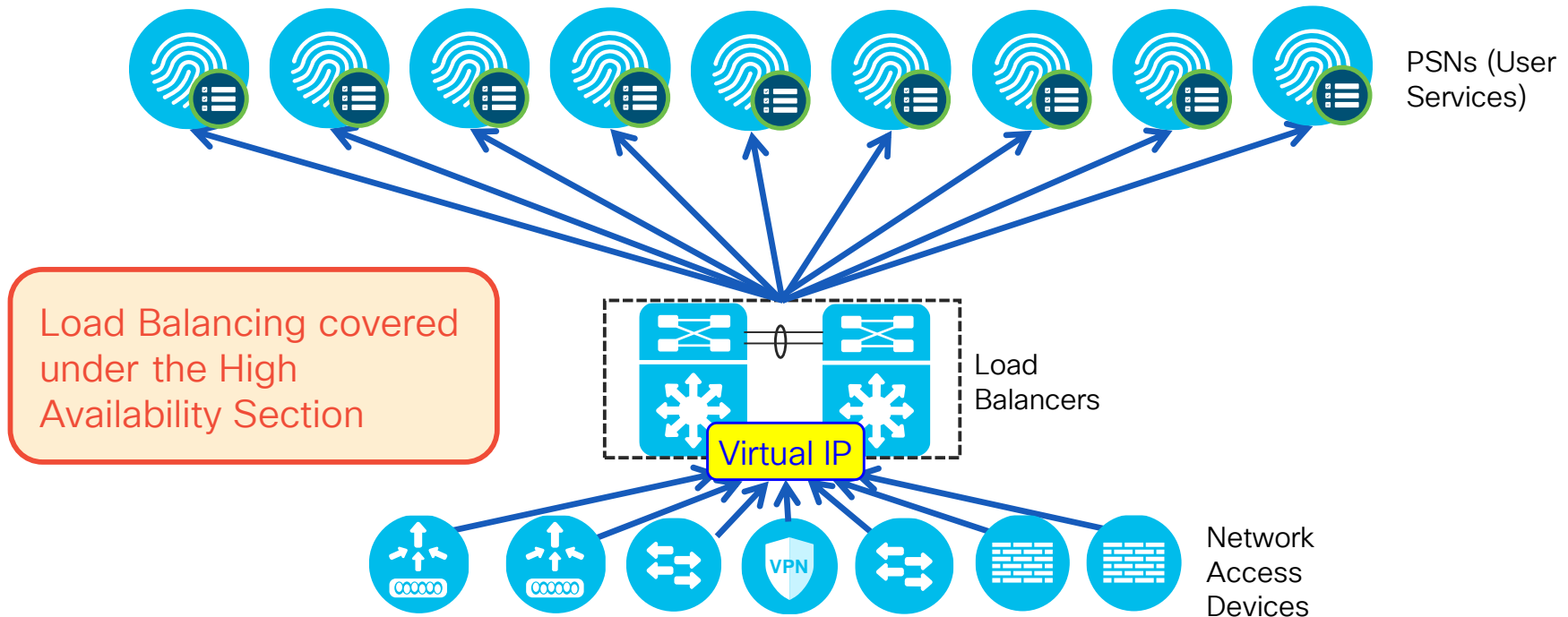
• PSN Services

- Session
- Profiling
- TC-NAC
- ISE SXP
- Device Admin (TACACS+)
- Passive Identity (Easy Connect)

The screenshot shows the 'Personas' configuration page in Cisco ISE. The 'Policy Service' section is highlighted with a red box. The 'Enable SXP Service' checkbox is checked. A blue callout box points to this checkbox with the text: 'Avoid unnecessary overload of PSN services' and 'Some services should be dedicated to one or more PSNs'. Other services listed include 'Enable Session Services', 'Enable Profiling Service', 'Enable Threat Centric NAC Service', 'Enable Device Admin Service', and 'Enable Passive Identity Service'. The 'pxGrid' checkbox is also checked at the bottom.

Scaling RADIUS, Web, Profiling, and TACACS+ w/LB

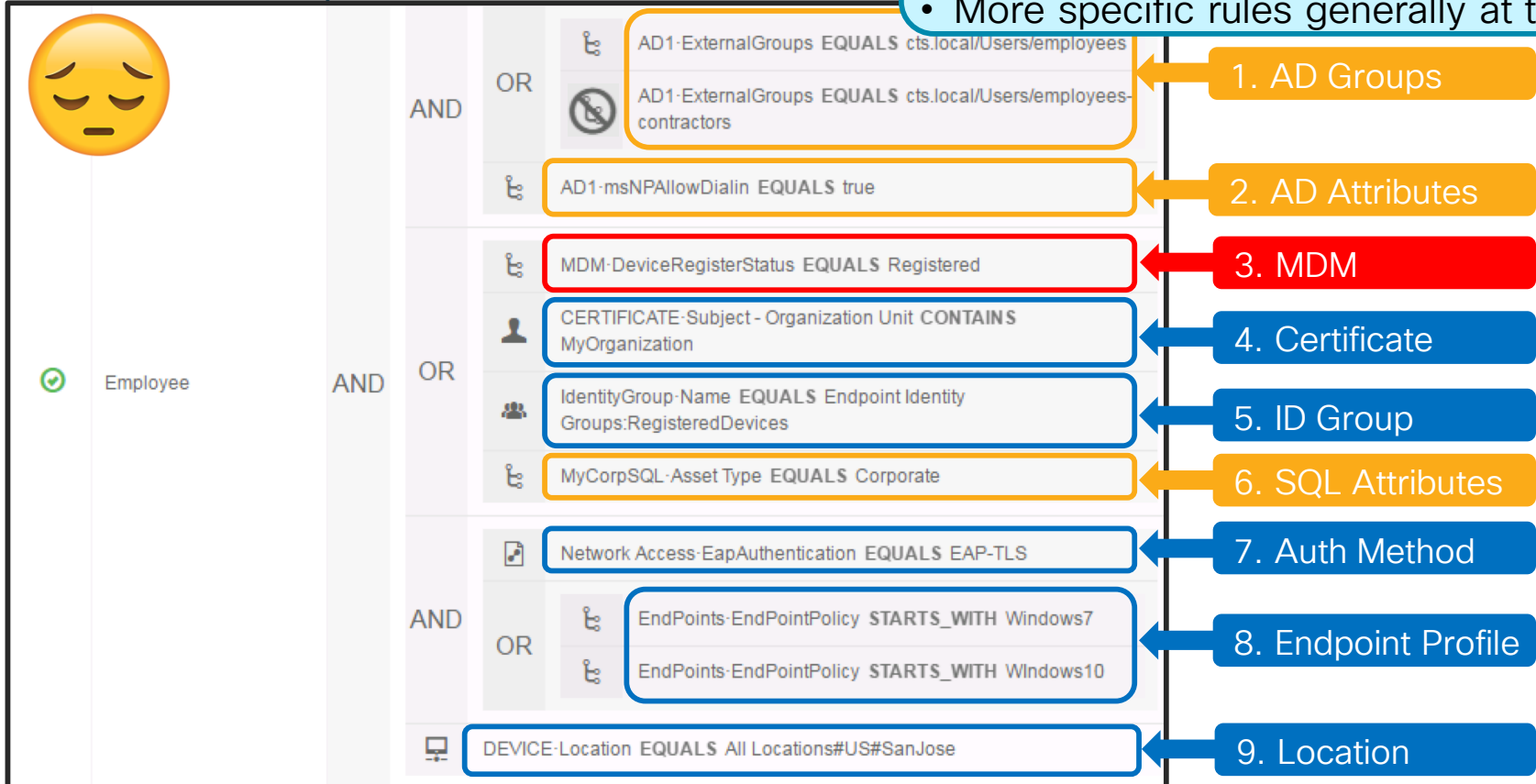
- Policy Service nodes can be configured in a cluster behind a load balancer (LB).
- Access Devices send RADIUS and TACACS+ AAA requests to LB virtual IP.



Auth Policy Optimization

ISE 2.3 Bad Example

- Policy Logic:
 - First Match, Top Down
 - Skip Rule on first negative match
- More specific rules generally at top



1. AD Groups

2. AD Attributes

3. MDM

4. Certificate

5. ID Group

6. SQL Attributes

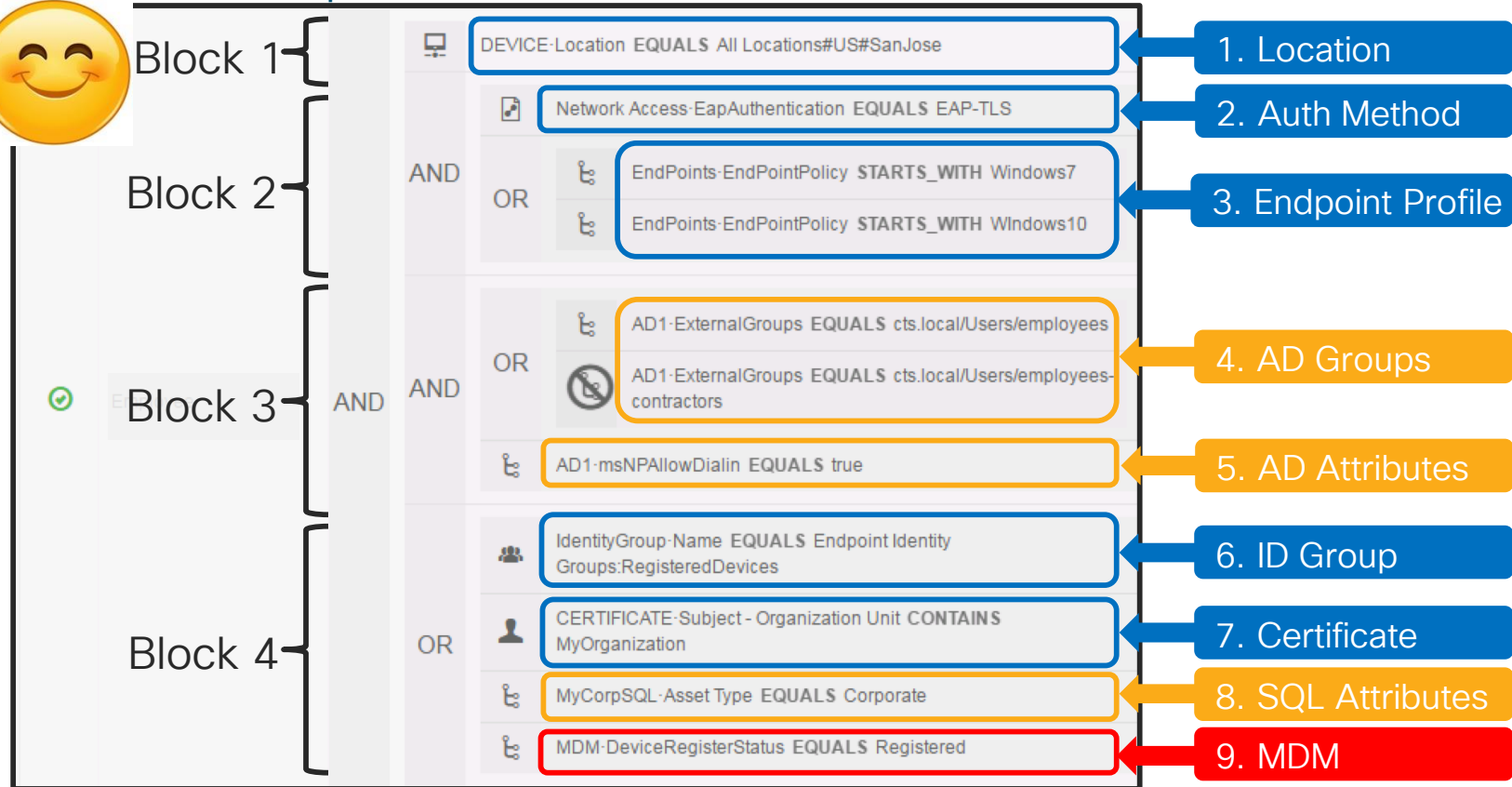
7. Auth Method

8. Endpoint Profile

9. Location

Auth Policy Optimization

ISE 2.3 Better Example!





ISE 2.4 Auth Policy Scale

- Max Policy Sets = **200**
(up from 100 in 2.2; up from 40 in 2.1)
- Max Authentication Rules = **1000**
(up from 200 in 2.2; up from 100 in 2.1)
- Max Authorization Rules = **3000**
(up from 700 in 2.2; up from 600 in 2.1)
- Max Authorization Profiles = **3200**
(up from 1000 in 2.2; up from 600 in 2.1)



Dynamic Variable Substitution

Rule Reduction

- Authorization Policy Conditions

- Match conditions to unique values stored per-User/Endpoint in internal or external ID stores (AD, LDAP, SQL, etc)
- ISE supports custom User and Endpoint attributes

▼ **Authorization Policy**

Standard

Status	Rule Name	Conditions (identity groups and other conditions)	Permissions
✓	Dynamic Match Rule	if Radius:Calling-Station-ID MATCHES LDAP1 Department then	Permit Access

- Authorization Profile Conditions

ID Store Attribute

▼ **Advanced Attributes Settings**

Radius:Class = InternalEndpoint groupPolicy

Enable EAP Session Resume / Fast Reconnect

Major performance boost, but not complete auth so avoid excessive timeout value

The screenshot shows the Cisco Identity Services Engine (ISE) configuration interface. The left sidebar contains a navigation menu with categories like Client Provisioning, Posture, Profiling, Protocols, and RADIUS. Under Protocols, EAP-FAST is expanded, showing EAP FAST Settings and Generate PAC. The main content area is titled 'EAP TLS Settings' and contains two sections: 'EAP TLS Settings' and 'Peap Settings'. In the 'EAP TLS Settings' section, the checkbox 'Enable EAP TLS Session Resume' is checked, and the 'EAP TLS Session Timeout' is set to 7,200 seconds. In the 'Peap Settings' section, both 'Enable PEAP Session Resume' and 'Enable Fast Reconnect' are checked, and the 'PEAP Session Timeout' is set to 7,200 seconds. There are 'Save' and 'Reset' buttons at the bottom of the Peap Settings section. A 'Select Authentication Method' dropdown is set to 'Win 7 Supplicant', and the 'Enable Fast Reconnect' checkbox is also checked. A 'Configure...' button is visible next to the dropdown. The interface is annotated with several callouts: an orange box highlights the 'Enable EAP TLS Session Resume' checkbox and the 'EAP TLS Session Timeout' field; a blue box highlights the 'Cache TLS (TLS Handshake Only/Skip Cert)' text; another blue box highlights the 'Cache TLS session' text; a third blue box highlights the 'Skip inner method' text; and a red box highlights the 'Enable Fast Reconnect' checkbox in the bottom right section. A blue arrow points from the 'EAP-TLS' menu item to the 'EAP TLS Settings' section, and another blue arrow points from the 'PEAP' menu item to the 'Peap Settings' section.



For Your Reference

Cache TLS (TLS Handshake Only/Skip Cert)

Cache TLS session

Skip inner method

Note: Both Server and Client must be configured for Fast Reconnect

ISE Stateless Session Resume

Allows Session Resume Across All PSNs

New in ISE 2.2!

- Session ticket extension per RFC 5077 [Transport Layer Security (TLS) Session Resumption without Server-Side State]
- ISE issues TLS client a session ticket that can be presented to any PSN to shortcut reauth process (Default = Disabled)

▼ Allow EAP-TLS

Allow Authentication of expired certificates to allow certificate renewal in Authorization Policy ⓘ

Enable Stateless Session Resume

Session ticket time to live

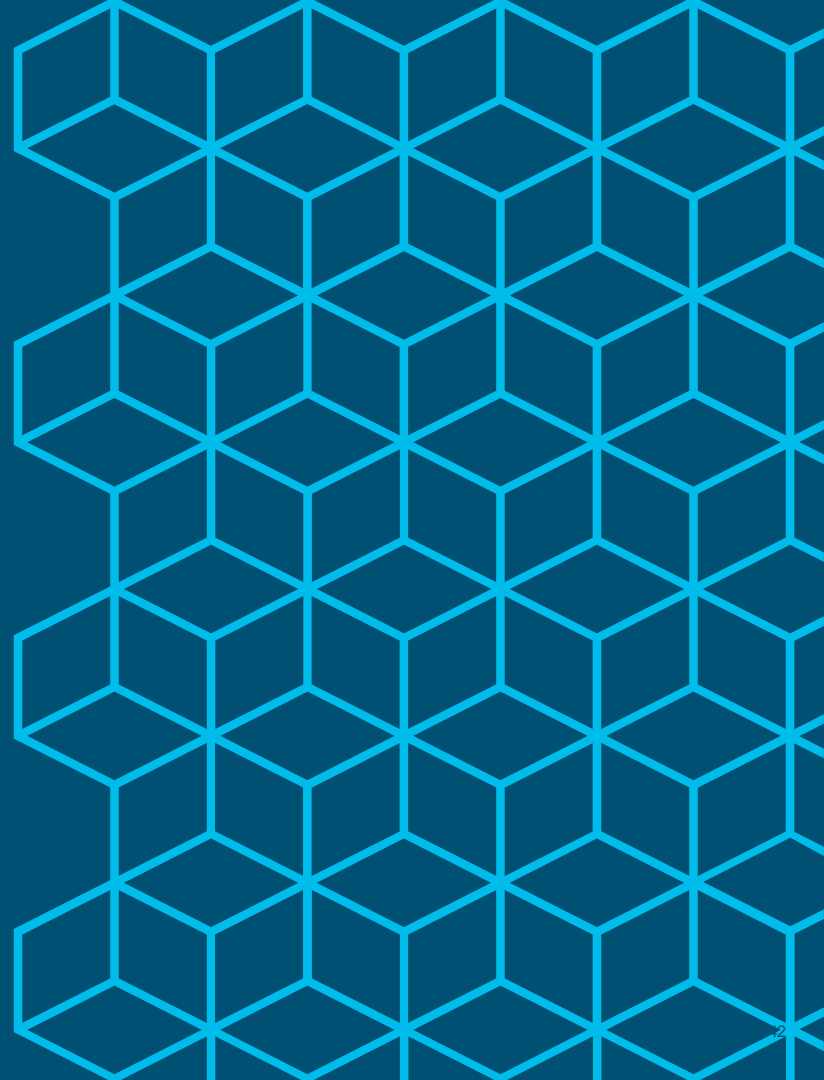
Proactive session ticket update will occur after % of Time To Live has expired

Allows resume with Load Balancers

Time until session ticket expires

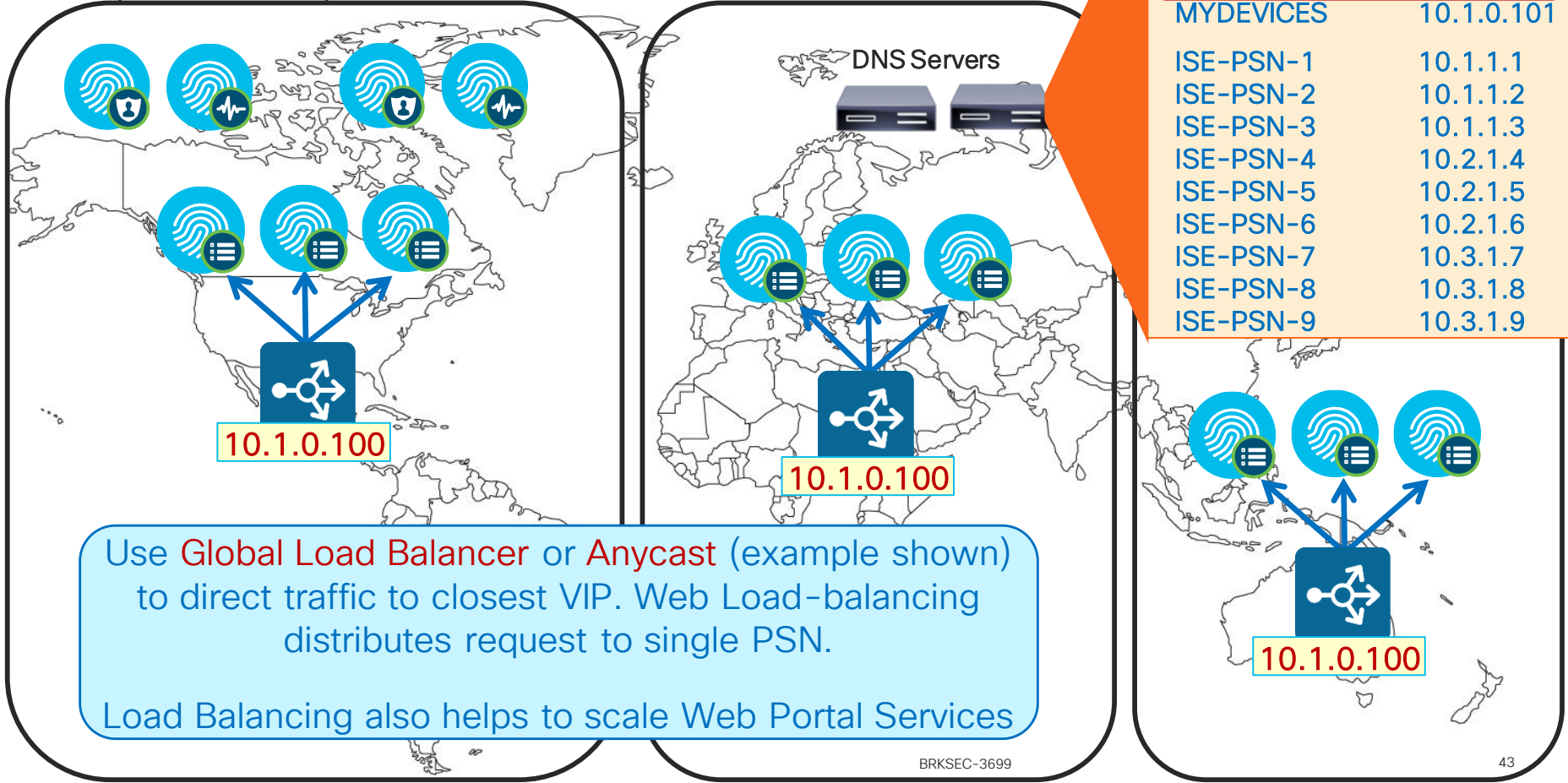
Policy > Policy Elements > Results > Authentication > Allowed Protocols

Scaling Guest and Web Authentication Services



Scaling Global Sponsor / MyDevices

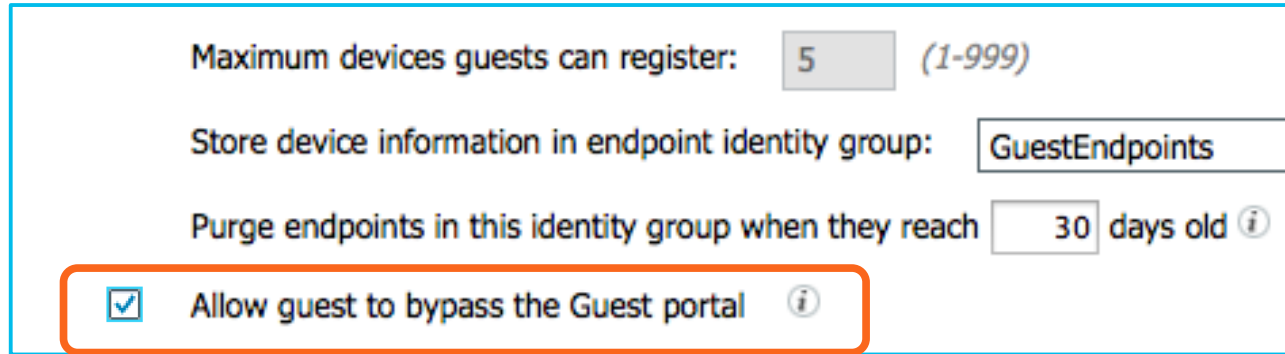
Anycast Example



Scaling Guest Authentications Using 802.1X

“Activated Guest” allows guest accounts to be used without ISE web auth portal

- Guests auth with 802.1X using EAP methods like PEAP-MSCHAPv2 / EAP-GTC
- 802.1X auth performance generally much higher than web auth



Maximum devices guests can register: (1-999)

Store device information in endpoint identity group:

Purge endpoints in this identity group when they reach days old ⓘ

Allow guest to bypass the Guest portal ⓘ

Warning:
Watch for
expired
guest
accounts,
else high #
auth failures !

Note: AUP and Password Change cannot be enforced since guest bypasses portal flow.

Scaling Web Auth

“Remember Me” Guest Flows

- User logs in to Hotspot/CWA portal and MAC address auto-registered into GuestEndpoint group
- AuthZ Policy for GuestEndpoints ID Group grants access until device purged



Endpoint identity group: *

Purge endpoints in this identity group when they reach days

Configure endpoint purge at
[Administration](#) > [Identity Management](#) > [Settings](#) > [Endpoint purge](#)

Work Centers > Guest Access > Settings > Logging

When guest portal is bypassed, authorization is based on endpoint group

Show endpoint's associated portal user ID (vs. MAC address) as the username

Reset

Save

Guest users are tracked by the MAC address of their device. When guest users are displayed in reports, the username is the MAC address. If you select this option, reports will display the portal user ID as the username, instead of the MAC address.

New in
ISE 2.4

Cisco live!

Scaling Posture & MDM

Posture Lease

Once Compliant, user may leave/reconnect multiple times before re-posture

The screenshot shows the Cisco Identity Services Engine (ISE) Administration console. The main navigation bar includes Home, Operations, Policy, Guest Access, and Administration. Below this, there are tabs for System, Identity Management, Identity Mapping, Network Resources, Web Portal Management, and Feed Service. A secondary navigation bar contains Deployment, Licensing, Certificates, Logging, Maintenance, Backup & Restore, Admin Access, and Settings. The left sidebar lists various settings categories, with 'Posture' expanded to show 'General Settings', 'Reassessments', 'Updates', 'Acceptable Use Policy', 'Profiling', and 'Protocols'. The main content area displays 'Posture General Settings' with fields for Remediation Timer (4 Minutes), Network Transition Delay (3 Seconds), Default Posture Status (Compliant), and a checkbox for 'Automatically Close Login Success Screen After' (0 Seconds). Below this, the 'Posture Lease' section is highlighted with a blue box. It contains two radio button options: 'Perform posture assessment every time a user connects to the network' (selected) and 'Perform posture assessment every 1 Days'. A note below states: 'Note : The above configuration applies only to AnyConnect Agent and not to NAC Agent and Web Agent.' There are 'Save' and 'Reset' buttons at the bottom of the section.

This is a close-up view of the 'Posture Lease' configuration section. It shows two radio button options: 'Perform posture assessment every time a user connects to the network' (unselected) and 'Perform posture assessment every 7 Days' (selected). Below the options, a red-bordered box contains the note: 'Note : The above configuration applies only to AnyConnect Agent and not to NAC Agent and Web Agent.'

MDM Scalability and Survivability

What Happens When the MDM Server is Unreachable?

- Scalability \approx 30 Calls per second per PSN.
 - Cloud-Based deployment typically built for scale and redundancy
 - For cloud-based solutions, Internet bandwidth and latency must be considered.
 - Premise-Based deployment may leverage load balancing
 - ISE 1.4+ supports multiple MDM servers – could be same or different vendors.
 - Authorization permissions can be set based on MDM connectivity status:
 - **MDM:MDMServerReachable Equals UnReachable**
MDM:MDMServerReachable Equals Reachable
- MobileDevice_Unreachable if (EndPoints:BYODRegistration EQUALS Yes AND MDM:MDMServerReachable EQUALS UnReachable) then MDM_Fail_Open
- All attributes retrieved & reachability determined by single API call on each new session.

Scaling MDM

Prepopulate MDM Enrollment and/or Compliance via ERS API




```
<groupId>groupId</groupId>
<identityStore>identityStore</identityStore>
<identityStoreId>identityStoreId</identityStoreId>
<mac>00:01:02:03:04:05</mac>
<mdmComplianceStatus>false</mdmComplianceStatus>
<mdmEncrypted>false</mdmEncrypted>
<mdmEnrolled>true</mdmEnrolled>
<mdmIMEI>IMEI</mdmIMEI>
<mdmJailBroken>false</mdmJailBroken>
<mdmManufacturer>Apple Inc.</mdmManufacturer>
<mdmModel>iPad</mdmModel>
<mdmOS>iOS</mdmOS>
<mdmPhoneNumber>Phone Number</mdmPhoneNumber>
<mdmPinlock>true</mdmPinlock>
<mdmReachable>true</mdmReachable>
<mdmSerial>AB23D0E45BC01</mdmSerial>
<mdmServerName>AirWatch</mdmServerName>
<portalUser>portalUser</portalUser>
<profileId>profileId</profileId>
<staticGroupAssignment>true</staticGroupAssignment>
<staticProfileAssignment>false</staticProfileAssignment>
```

```
<customAttributes>
  <customAttributes>
    <entry>
      <key>MDM_Registered</key>
      <value>true</value>
    </entry>
    <entry>
      <key>MDM_Compliance</key>
      <value>false</value>
    </entry>
    <entry>
      <key>Attribute_XYZ</key>
      <value>Value_XYZ</value>
    </entry>
  </customAttributes>
</customAttributes>
```

TACACS+ Scaling

Options for Deploying Device Admin

<https://communities.cisco.com/docs/DOC-63930>

Priorities according to Policy and Business Goals		Separate Deployment  RADIUS TACACS	Separate PSNs  RADIUS TACACS	Mixed PSNs  RADIUS/TACACS
Separation of Configuration/Duty	Yes: Specialization for TACACS+	Green	Red	Red
	No: Shared resources/Reduced \$\$	Red	Yellow	Green
Independent Scaling of Services	Yes: Scale as needed/No impact on Device Admin from RADIUS services	Green	Yellow	Red
	No: Avoid underutilized PSNs	Red	Yellow	Green
Suitable for high-volume Device Admin	Yes: Services dedicated to TACACS+	Green	Green	Red
	No: Focus on “human” device admins	Red	Yellow	Green
Separation of Logging Store	Yes: Optimize log retention VM	Green	Red	Red
	No: Centralized monitoring	Red	Green	Green

ISE 2.4 TACACS+ Multi-Service Scaling (RADIUS and T+)

Max Concurrent RADIUS + TACACS+ TPS by Deployment Model and Platform

- By Deployment

Deployment Model		Platform	Max # Dedicated PSNs	Max RADIUS Sessions per Deployment	Max TACACS+ TPS per Deployment
Standa-alone	All personas on same node	3515	0	7,500	100
		3595	0	20,000	100
Hybrid	PAN+MnT+PXG on same node; Dedicated PSN	3515 as PAN+MNT	* 5 / 3+2	7,500	250 / 2,000
		3595 as PAN+MNT	* 5 / 3+2	20,000	250 / 3,000
Dedicated	Each Persona on Dedicated Node	3595 as PAN and MNT	* 50 / 47+3	500,000	2,500 / 4,000
		3595 as PAN and Large MNT	* 50 / 47+3	500,000	2,500 / 6,000

* Device Admin service enabled on same PSNs also used for RADIUS OR Split RADIUS and T+ PSNs

- By PSN

Each dedicated T+ PSN node reduces dedicated RADIUS PSN count by 1

Scaling per PSN	Platform	Max RADIUS Sessions per PSN	Max TACACS+ TPS per PSN
Dedicated Policy nodes (Max Sessions Gated by Total Deployment Size)	SNS-3515	7,500	2,000
	SNS-3595	40,000	3,000

ISE 2.4 TACACS+ Multi-Service Scaling (TACACS+ Only)

Max Concurrent TACACS+ TPS by Deployment Model and Platform

- By Deployment

Deployment Model		Platform	Max # Dedicated PSNs	Max RADIUS Sessions per Deployment	Max TACACS+ TPS per Deployment
Stand-alone	All personas on same node	3515	0	N/A	1,000
		3595	0	N/A	1,500
Hybrid	PAN+MnT+PXG on same node; Dedicated PSN	3515 as PAN+MNT	* 5 / 2	N/A	**2,000 / 2,000
		3595 as PAN+MNT	* 5 / 2	N/A	**3,000 / 3,000
Dedicated	Each Persona on Dedicated Node	3595 as PAN and MNT	* 50 / 4	N/A	**5,000 / 5,000
		3595 as PAN and Large MnT	* 50 / 5	N/A	**10,000 / 10,000

* Device Admin service can be enabled on each PSN; minimally 2 for redundancy.

** Max log capacity for MNT

- By PSN

Scaling per PSN	Platform	Max RADIUS Sessions per PSN	Max TACACS+ TPS per PSN
Dedicated Policy nodes (Max Sessions Gated by Total Deployment Size)	SNS-3515	7,500	2,000
	SNS-3595	40,000	3,000

TACACS+ MnT Scaling

Human Versus Automated Device Administration

- Consider the “average” size syslog from TACACS+ based on following guidance:

Each TACACS+ Session	Each Command Authorization (per session)
Authentication: 2kB	Command authorization: 2kB
Session authorization: 2kB	Command accounting : 1kB
Session accounting: 1kB	



- “Human” Device Admin Example:

- For a normal “human” session we may expect to see 10 commands, so a session would be approximately: $[5\text{kB} + (10 * 3\text{kB})] = 35\text{kB}$. Suppose a maximum of 50 such sessions per admin per day from 50 admins (and few organizations have > 50 admins)
 - 50 human admins would generate < 1 TPS average, ~60k logs/day, or ~90MB/day.**

- Automated/Script Device Admin Example:

- Consider a script that runs 4 times a day against 30,000 devices, (for example, to backup config on all devices). Generally the interaction will be short, say 5 commands:
 - Storage = $30,000 * 4 * [5\text{kB} + (5 * 3\text{kB})] = \sim 2.4 \text{ GB/day}$**
 - Total TPS = $30\text{k} * 4 * [3 + (5 * 2)] = 1.56\text{M logs} = 18 \text{ TPS average; } 1300 \text{ TPS peak.}$**

```
Announce which device we are working on and at what time
send_user "in"
send_user "==== Working on Shostname @ [exec date] <<<<<<<===="
send_user "in"

Don't check keys
open ssh -o StrictHostKeyChecking=no Supername@shostname

Allow this script to handle connection issues
expect {
  timeout { send_user "\nTimeout Exceeded - Check Host!" ;
  eof { send_user "\nSSH Connection to Shostname Failed!\n";
  "" }
  ""password" {
    send "password\n"
  }
}

If we're not already in enable mode, get us there
expect {
  send_user "enable Mode Failed - Check Password"
}
```

TACACS+ Multi-Service Scaling

Required TACACS+ TPS by # Admins and # NADs

		Session Authentication and Accounting Only				Command Accounting Only (10 Commands / Session)				Command Authorization + Acctg (10 Commands / Session)			
		Avg TPS	Peak TPS	Logs/Day	Storage/day	Avg TPS	Peak TPS	Logs/Day	Storage/day	Avg TPS	Peak TPS	Logs/Day	Storage/day
Human Admin	# Admins	Based on 50 Admin Sessions per Day											
	1	< 1	< 1	150	< 1MB	< 1	< 1	650	1MB	< 1	< 1	1.2k	2MB
	5	< 1	< 1	750	1MB	< 1	< 1	3.3k	4MB	< 1	< 1	5.8k	9MB
	10	< 1	< 1	1.5k	3MB	< 1	< 1	6.5k	8MB	< 1	1	11.5k	17MB
	25	< 1	< 1	3.8k	7MB	< 1	1	16.3k	19MB	< 1	2	28.8k	43MB
	50	< 1	1	7.5k	13MB	< 1	2	32.5k	37MB	1	4	57.5k	86MB
	100	< 1	1	15k	25MB	1	4	65k	73MB	2	8	115k	171MB
Script Admin	# NADs	Based on 4 Scripted Sessions per Day											
	500	< 1	5	6k	10MB	< 1	22	26k	30MB	1	38	46k	70MB
	1,000	< 1	10	12k	20MB	1	43	52k	60MB	1	77	92k	140MB
	5,000	< 1	50	60k	100MB	3	217	260k	300MB	5	383	460k	700MB
	10,000	1	100	120k	200MB	6	433	520k	600MB	11	767	920k	1.4GB
	20,000	3	200	240k	400MB	12	867	1.04M	1.2GB	21	1.5k	1.84M	2.7GB
	30,000	5	300	480k	600MB	18	1.3k	1.56M	1.7GB	32	2.3k	2.76M	4.0GB
	50,000	7	500	600k	1GB	30	2.2k	2.6M	2.9GB	53	3.8k	4.6M	6.7GB

Peak values based on 5-minute burst to complete each batch request.

TACACS+ Multi-Service Scaling

Required TACACS+ TPS by # Admins and # NADs

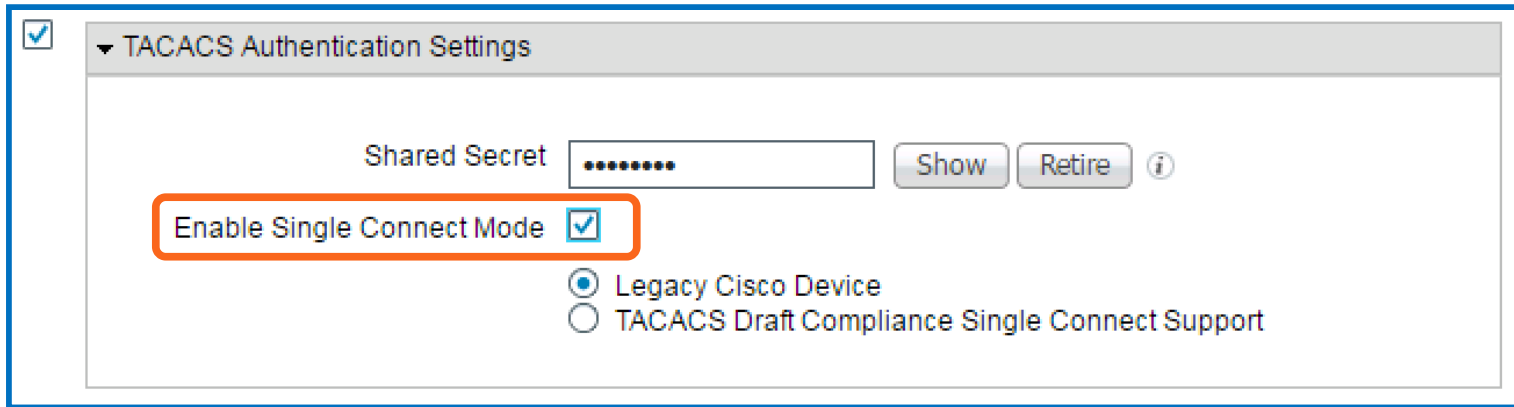
		Session Authentication and Accounting Only				Command Accounting Only (10 Commands / Session)				Command Authorization + Acctg (10 Commands / Session)			
		Avg TPS	Peak TPS	Logs/Day	Storage/day	Avg TPS	Peak TPS	Logs/Day	Storage/day	Avg TPS	Peak TPS	Logs/Day	Storage/day
Human Admin	# Admins	Based on 50 Admin Sessions per Day											
	1	< 1	< 1	150	< 1MB	< 1	< 1	650	1MB	< 1	< 1	1.2k	2MB
	5	< 1	< 1	750	1MB	< 1	< 1	3.3k	4MB	< 1	< 1	5.8k	9MB
	10	< 1	< 1	1.5k	3MB	< 1	< 1	6.5k	8MB	< 1	1	11.5k	17MB
	25	< 1	< 1	3.8k	7MB	< 1	1	16.3k	19MB	< 1	2	28.8k	43MB
	50	< 1	1	7.5k	13MB	< 1	2	32.5k	37MB	1	4	57.5k	86MB
	100	< 1	1	15k	25MB	1	4	65k	73MB	2	8	115k	171MB
Script Admin	# NADs	Based on 4 Scripted Sessions per Day											
	500	< 1	5	6k	10MB	< 1	22	26k	30MB	1	38	46k	70MB
	1,000	< 1	10	12k	20MB	1	43	52k	60MB	1	77	92k	140MB
	5,000	< 1	50	60k	100MB	3	217	260k	300MB	5	383	460k	700MB
	10,000	1	100	120k	200MB	6	433	520k	600MB	11	767	920k	1.4GB
	20,000	3	200	240k	400MB	12	867	1.04M	1.2GB	21	1.5k	1.84M	2.7GB
	30,000	5	300	480k	600MB	18	1.3k	1.56M	1.7GB	32	2.3k	2.76M	4.0GB
	50,000	7	500	600k	1GB	30	2.2k	2.6M	2.9GB	53	3.8k	4.6M	6.7GB

Peak values based on 5-minute burst to complete each batch request.

Single Connect Mode

Scaling TACACS+ for High-Volume NADs

- Multiplexes T+ requests over single TCP connection
 - All T+ requests between NAD and ISE occur over single connection rather than separate connections for each request.
- Recommended for TACACS+ “Top Talkers”
- Note: TCP sockets locked to NADs, so limit use to NADs with highest activity.



TACACS Authentication Settings

Shared Secret ⓘ

Enable Single Connect Mode

Legacy Cisco Device
 TACACS Draft Compliance Single Connect Support

Administration > Network Resources > Network Devices > (NAD)

Internal User Cache for T+ Authorization

New in
ISE 2.3

Scaling TACACS+ for High-Volume Admin Users

Identity Services Engine Home Context Visibility Operations Policy Administration Work Centers

Network Access Guest Access TrustSec BYOD Profiler Posture Device Administration PassiveID

Overview Identities User Identity Groups Ext Id Sources Network Resources Policy Elements Device Admin Policy Sets Reports Settings

Connection Settings Password Change Control Session Key Assignment

Protocol Session Timeout * 5 Minutes (Range 1-9999)

Connection Timeout * 10 Minutes (Range 1-9999)

Maximum Packet Size * 32768 kb (Range 4096-65536)

Single Connect Support

Username Prompt * Username:

Password Prompt * Password:

Default Shared Secret Retirement Period * 7 Days (Range 1-99)

Authorization cache timeout * 0 Minutes (Range 0-5)

Global Setting for Single Connect Mode (enabled by default)

First authorization caches

- 1) User Name
- 2) User Specific Attributes (Ex: Group ID, custom attributes)

Successive requests served from cache
Default = 0 <<Cache Disabled>>

Scaling Profiling and Database Replication

Endpoint Attribute Filter and Whitelist Attributes

Reduces Data Collection and Replication to Subset of Profile-Specific Attributes

- Endpoint Attribute Filter – aka “Whitelist filter”
 - Disabled by default. If enabled, only these attributes are collected or replicated.

The screenshot shows the 'Profiler Configuration' page. At the top right, there is a breadcrumb trail: 'Administration > System Settings > Profiling'. The main configuration area includes a dropdown for '* CoA Type:' set to 'Reauth'. Below this are fields for 'Current custom SNMP community strings' (masked with dots) and 'Change custom SNMP community strings' (empty), both with a 'Show' button to their right. A note below these fields states '(For NMAP, comma separated. Field will be cleared on successful saved change.)'. The 'Confirm changed custom SNMP community strings' field is also empty with the same note. At the bottom, there are 'Save' and 'Reset' buttons. A red box highlights the 'EndPoint Attribute Filter:' setting, which is checked and labeled 'Enabled'.

- Whitelist Filter limits profile attribute collection to those required to support default (Cisco-provided) profiles and critical RADIUS operations.
 - Filter must be disabled to collect and/or replicate other attributes.
 - Attributes used in custom conditions are automatically added to whitelist.

Whitelist Attributes vs Significant Attributes

Sampling of All Endpoint

PolicyVersion
 OUI
 EndPointMACAddress
 MatchedPolicy
 EndPointMatchedProfile
 EndPointPolicy
 Total Certainty Factor
 EndPointProfilerServer
 EndPointSource
 StaticAssignment
 StaticGroupAssignment
 UpdateTime
 Description
 IdentityGroup
 ElapsedDays
 InactiveDays
 NetworkDeviceGroups
 Location
 Device Type
 IdentityAccessRestricted
 IdentityStoreName
 ADDomain
 AuthState
 ISEPolicySetName
 IdentityPolicyMatchedRule
 AllowedProtocolMatchedRule
 SelectedAccessService
 SelectedAuthenticationIdentityStore
 s
 AuthenticationIdentityStore
 AuthenticationMethod
 AuthorizationPolicyMatchedRule
 SelectedAuthorizationProfiles
 CPMSessionID
 AAA-Server
 OriginalUserName
 DetailedInfo
 EapAuthentication
 NasRetransmissionTimeout
 TotalFailedAttempts
 TotalFailedTime

UseCase
 UserType
 GroupsOrAttributesProcess
 ExternalGroups
 Called-Station-ID
 Calling-Station-ID
 DestinationIPAddress
 DestinationPort
 Device IP Address
 MACAddress
 MessageCode
 NADAddress
 NAS-IP-Address
 NAS-Port
 NAS-Port-Id
 NAS-Port-Type
 NetworkDeviceName
 RequestLatency
 Service-Type
 Timestamp
 User-Name
 Egress-VLANID
 Egress-VLAN-Name
 Airespace-Wlan-Id
 Device Port
 EapTunnel
 Framed-IP-Address
 NAS-Identifier
 RadiusPacketType
 Vlan
 VlanName
 cafSessionAuthUserName
 cafSessionAuthVlan
 cafSessionAuthorizedBy
 cafSessionDomain
 cafSessionStatus
 dot1dBasePort
 dot1xAuthAuthControlledPo
 ol
 dot1xAuthAuthControlledPortStatus
 dot1xAuthSessionUserName

Whitelist Attributes

161-udp
 AAA-Server
 AC_User_Agent
 AUPAccepted
 BYODRegistration
 CacheUpdateTime
 Calling-Station-ID
 cdpCacheAddress
 cdpCacheCapabilities
 cdpCacheDevicelid
 cdpCachePlatform
 cdpCacheVersion
 Certificate Expiration Date
 Certificate Issue Date
 Certificate Issuer Name
 Certificate Serial Number
 ciaddr
 CreateTime
 Description
 DestinationIPAddress
 Device Identifier
 Device Name
 DeviceRegistrationStatus
 dhcp-class-identifier
 dhcp-requested-address
 EndPointPolicy
 EndPointPolicyID
 EndPointProfilerServer
 EndPointSource
 FirstCollection
 FQDN
 Framed-IP-Address
 host-name
 hrDeviceDescr
 IdentityGroup
 IdentityGroupID
 IdentityStoreGUID
 IdentityStoreName
 ifIndex
 ip
 L4_DST_PORT
 LastNmapScanTime
 IldpCacheCapabilities
 IldpCapabilitiesMapSupported
 IldpSystemDescription
 MACAddress
 MatchedPolicy
 MatchedPolicyID
 MDMCompliant
 MDMCompliantFailureReason
 MDMDiskEncrypted
 MDMErolled
 MDMimei
 MDMJailBroken
 MDMManufacturer
 MDMModel
 MDMOSVersion
 MDMPhoneNumber

Triggers Node Group Update and Ownership Change

Triggers Global Replication

Significant Attributes

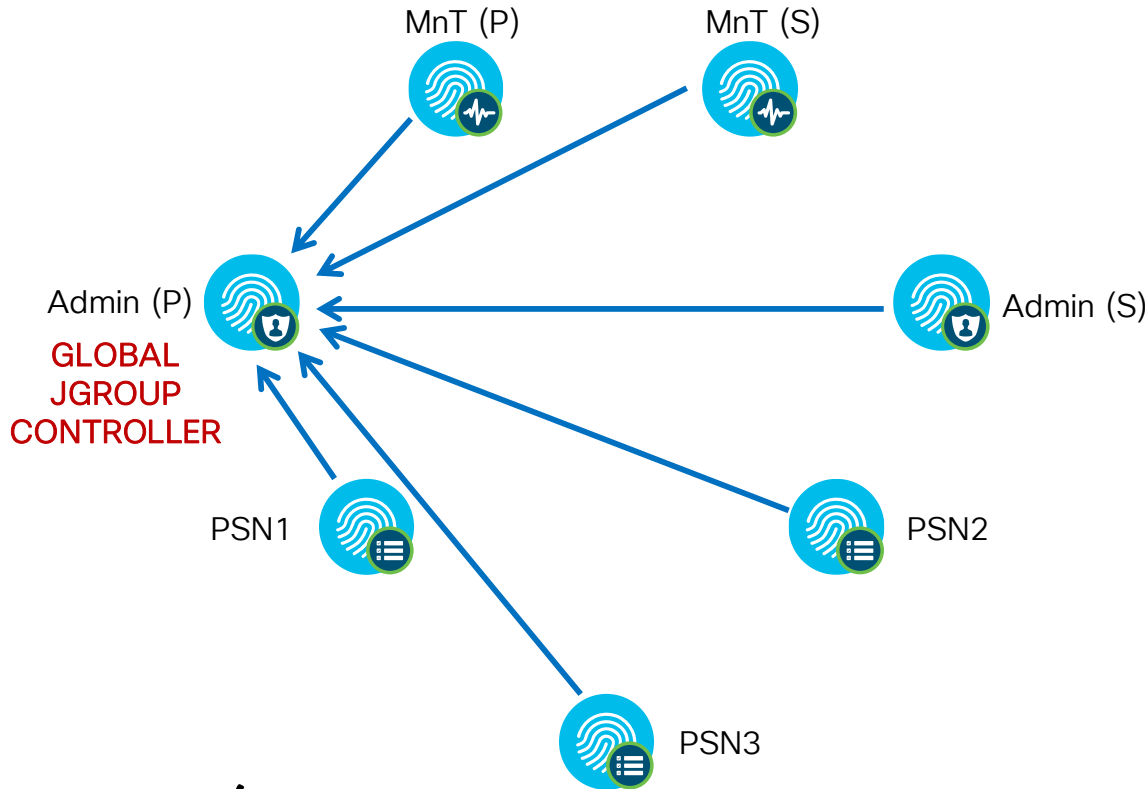
MACADDRESS
 MATCHEDVALUE
 ENDPOINTPOLICY
 ENDPOINTPOLICYVERSION
 STATICASSIGNMENT
 STATICGROUPASSIGNMENT
 NMAPSUBNETSCANID
 PORTALUSER
 DEVICEREGISTRATIONSTATUS

138-udp
 139-udp

Inter-Node Communications

JGroup Connections - Global Cluster

— TCP/12001 JGroups Tunneled

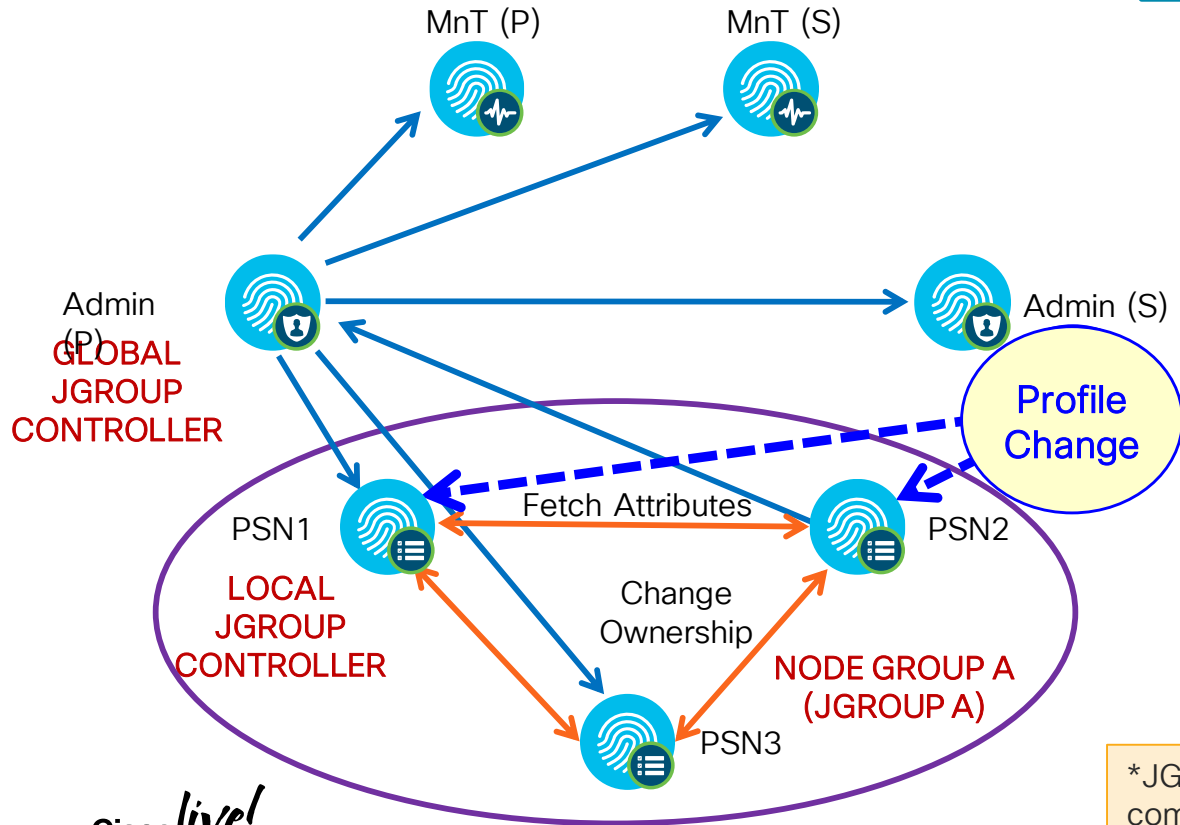


- All Secondary nodes* establish connection to Primary PAN (JGroup Controller) over tunneled connection (TCP/12001) for config/database sync.
- Secondary Admin also listens on TCP/12001 but no connection established unless primary fails/secondary promoted
- All Secondary nodes participate in the Global JGroup cluster.

***Secondary node** = All nodes except Primary Admin node; includes PSNs, MnT, pxGrid, and Secondary Admin nodes

Inter-Node Communications

Local JGroups and Node Groups



- TCP/7800 JGroup Peer Communication
JGroup Failure Detection
- TCP/12001 JGroups Tunneled

- Node Groups can be used to define local JGroup* clusters where members exchange heartbeat and sync profile data over SSL (TLS v1.2).
- PSN claims endpoint ownership only if change in whitelist attribute; triggers ownership update to local PSNs. Whitelist check always occurs regardless of global whitelist filter.
- Replication to PAN occurs if significant attribute changes, then sync all attributes via PAN; if whitelist filter enabled, only whitelist attributes synced to all nodes.

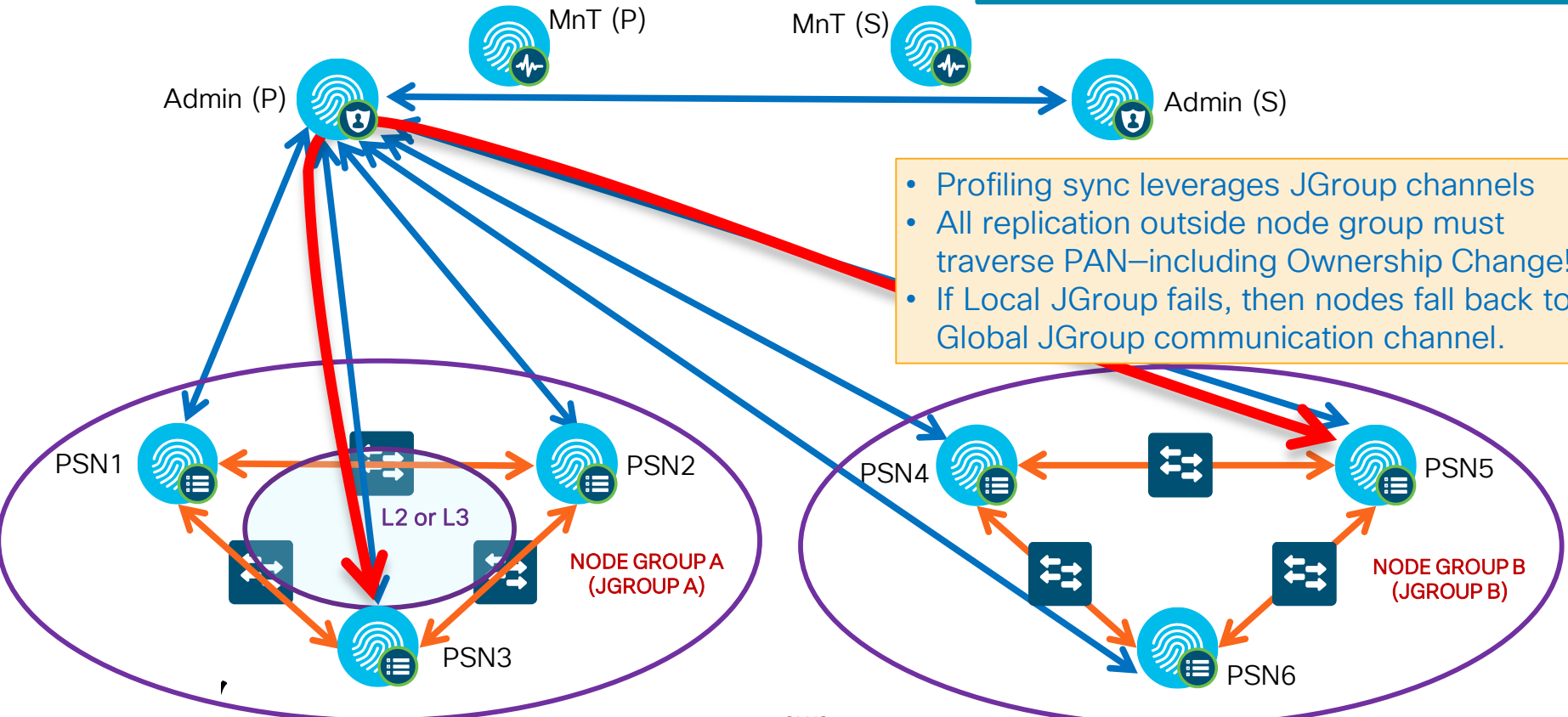
*JGroups: Java toolkit for reliable multicast communications between group/cluster members.

Inter-Node Communications

Local JGroups and Node Groups

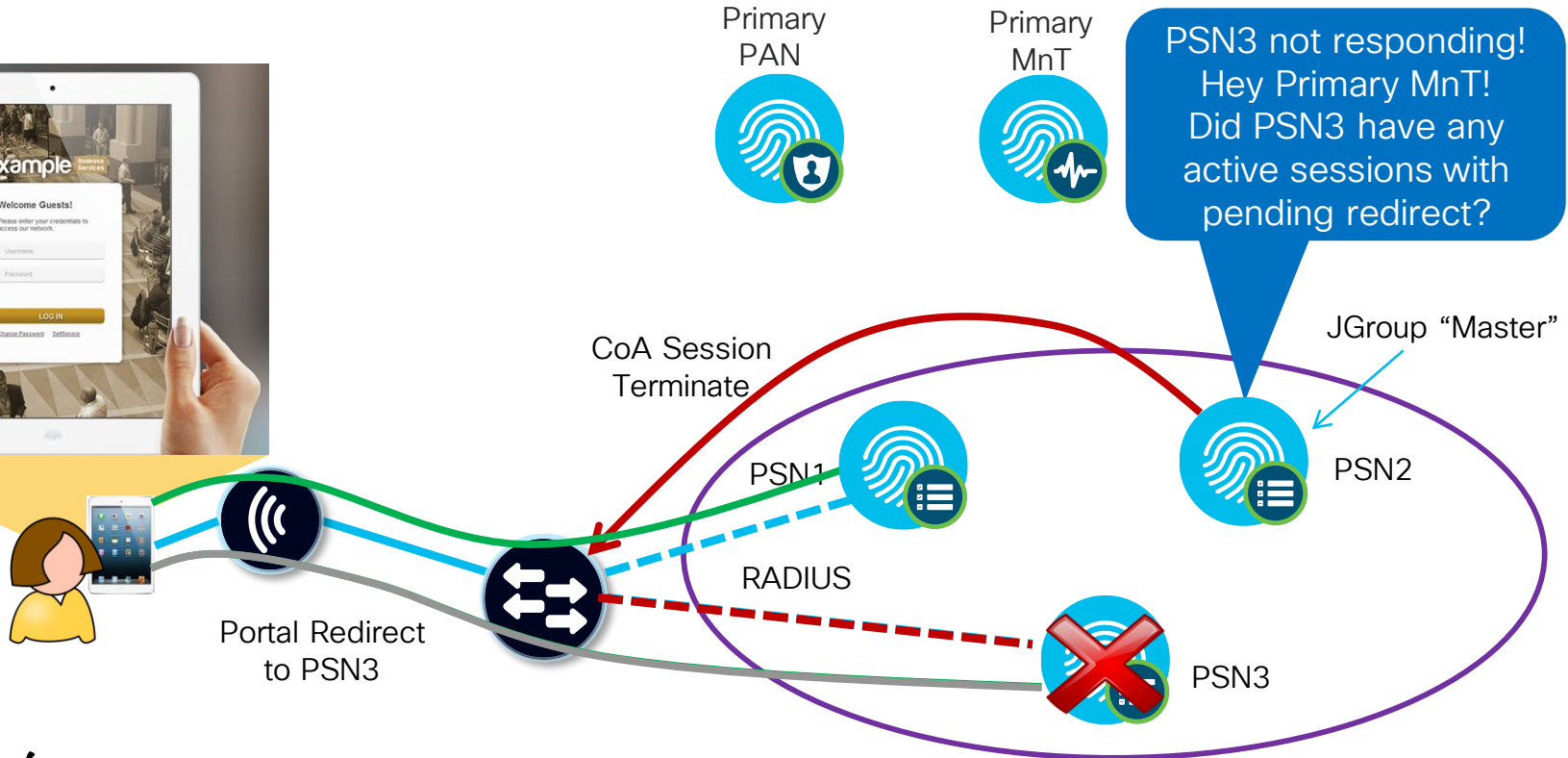
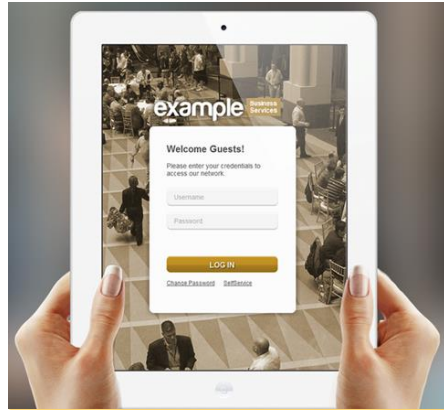
— TCP/7800 JGroup Peer Communication
JGroup Failure Detection

— TCP/12001 JGroups Tunneled

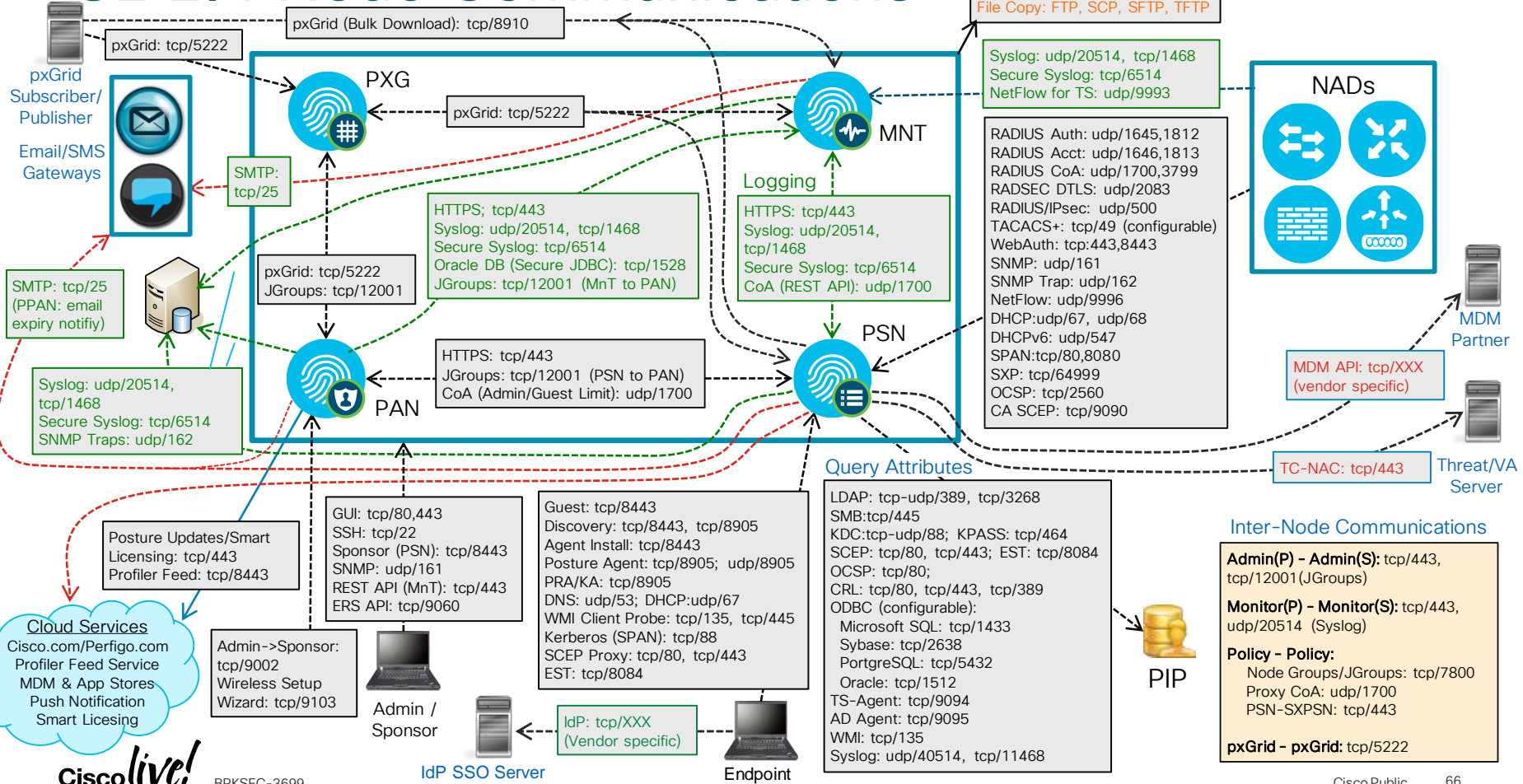


Node Groups and Session Recovery

Dynamic Clean Up for Orphaned URL-Redirected Sessions

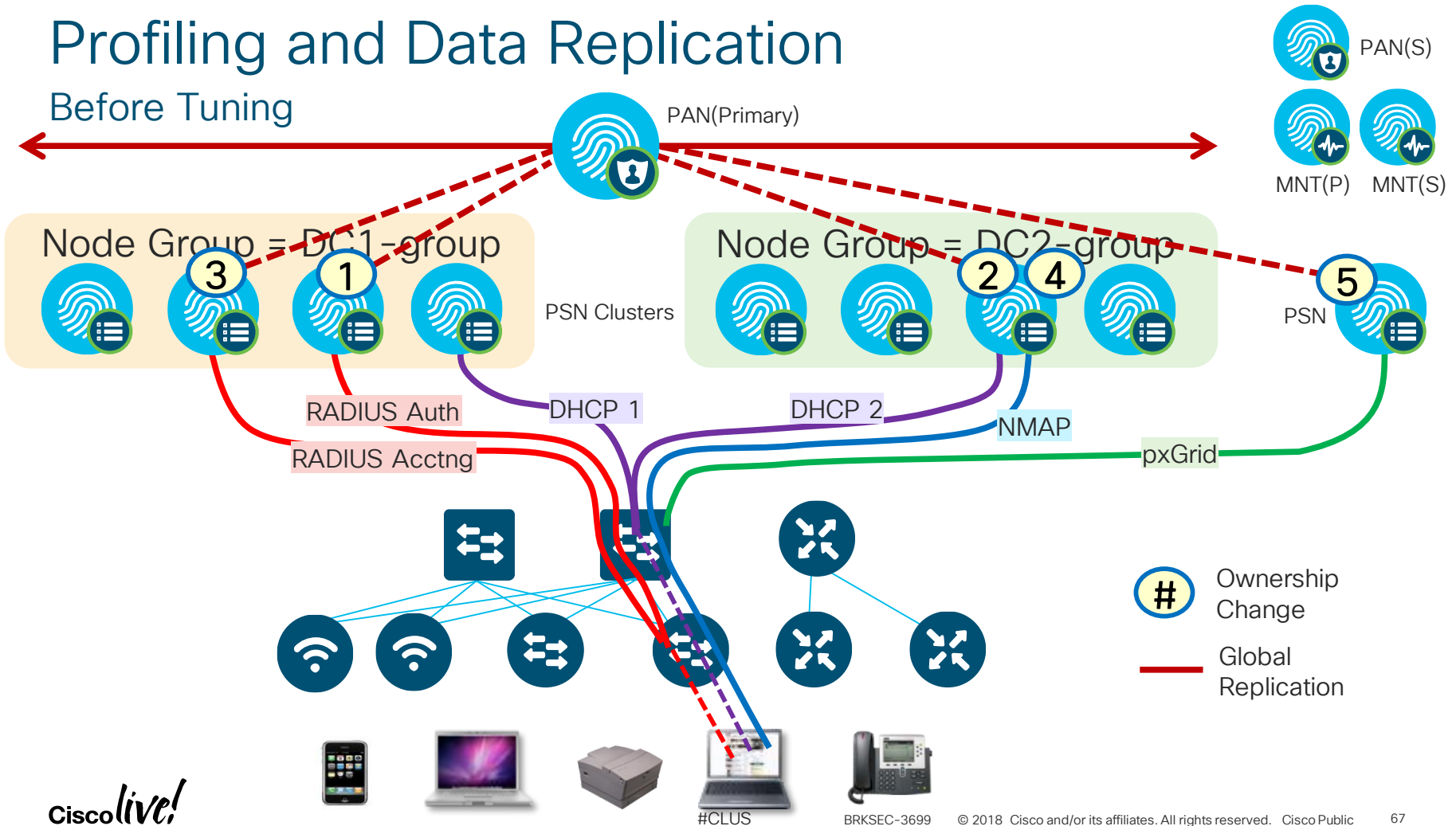


ISE 2.4 Node Communications



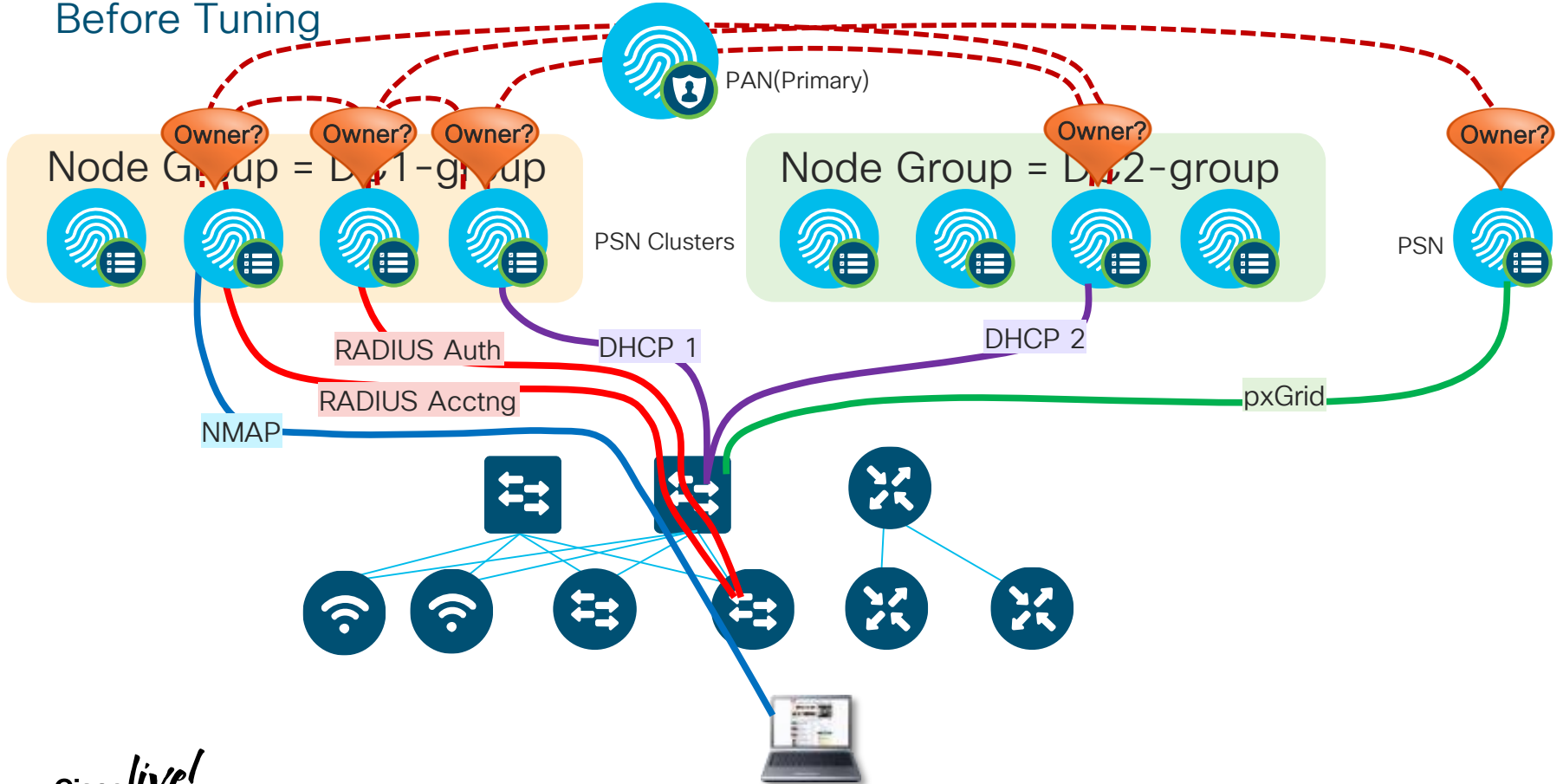
Profiling and Data Replication

Before Tuning



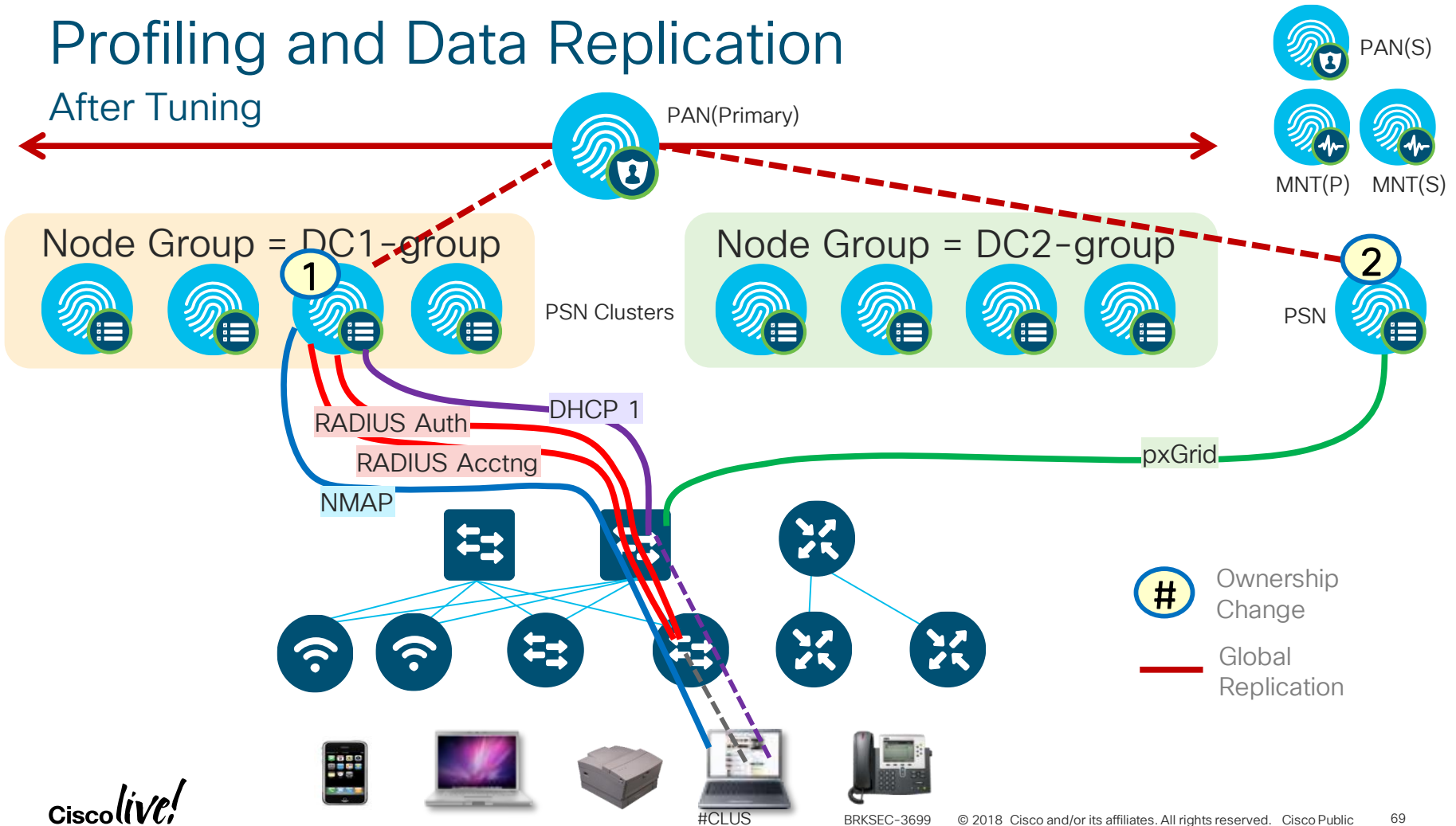
Impact of Ownership Changes

Before Tuning



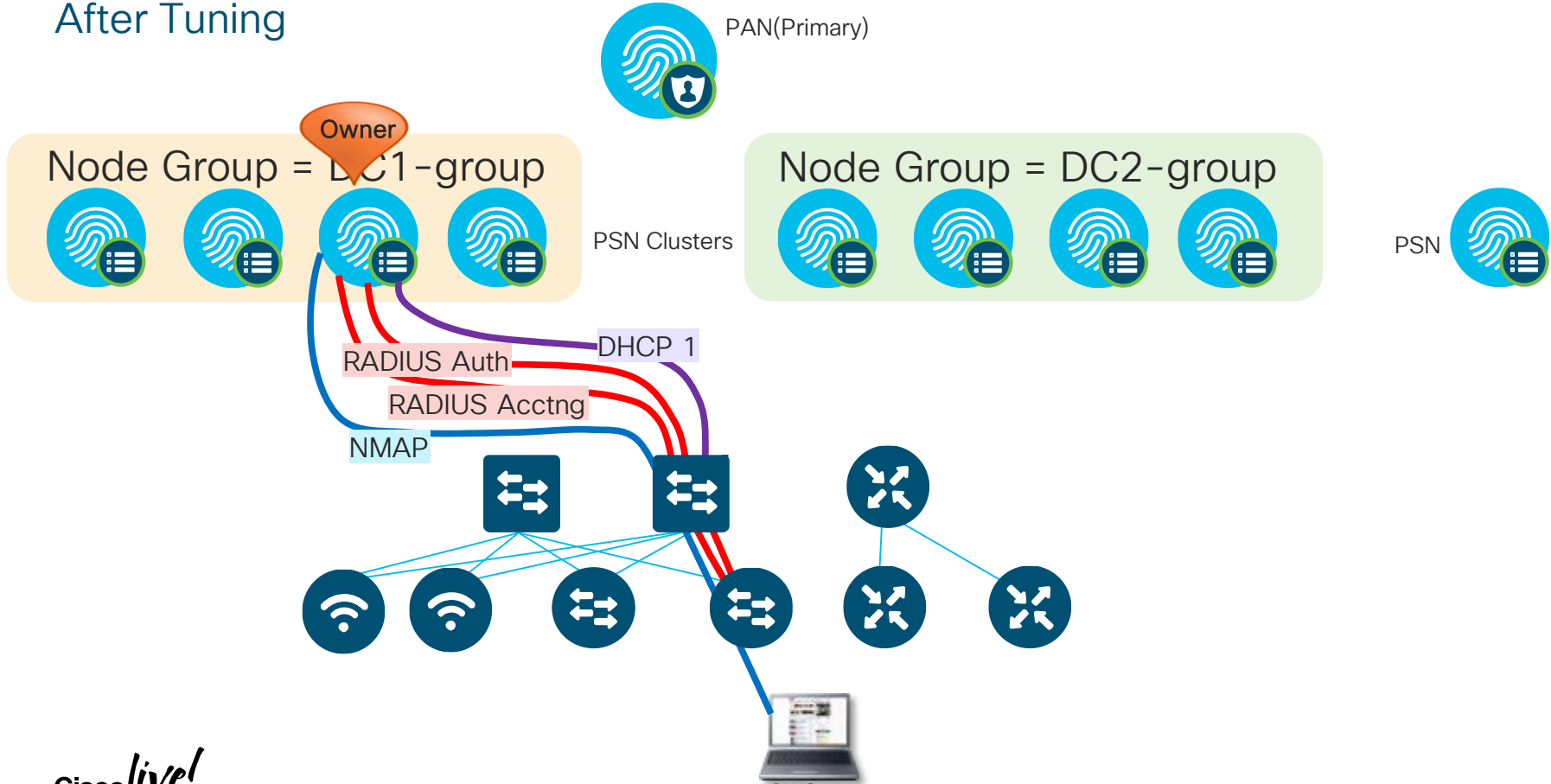
Profiling and Data Replication

After Tuning



Impact of Ownership Changes

After Tuning



ISE Profiling Best Practices

Whenever Possible...

- Use Device Sensor on Cisco switches & Wireless Controllers to optimize data collection.
- **Do NOT send profile data to multiple PSNs!**
 - Ensure profile data for a given endpoint is sent to a single PSN (or maximum of 2)
 - Sending same profile data to multiple PSNs increases inter-PSN traffic and contention for endpoint ownership.
 - For redundancy, consider Load Balancing and Anycast to support a single IP target for RADIUS or profiling using...
 - DHCP IP Helpers
 - SNMP Traps
 - DHCP/HTTP with ERSPAN (Requires validation)
- **DO send profile data to single and same PSN or Node Group!**
 - Ensure profile data for a given endpoint is sent to the *same* PSN
 - Same issue as above, but not always possible across different probes
- **DO use Device Sensor!**
 - Use node groups and ensure profile data for a given endpoint is sent to *same* node group.
 - Node Groups receive the PSN information and change to ensure endpoint changes outside of node group.
- **DO enable the Profiler Attribute Filter!**
- Avoid probes that collect the same endpoint attributes
 - Example: Device Sensor + SNMP Query/IP Helper
- Enable Profiler Attribute Filter

ISE Profiling Best Practices

General Guidelines for Probes

- **HTTP Probe:**

- Use URL Redirects instead of SPAN to centralize collection and reduce traffic load related to SPAN/RSPAN.
- **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:**

- **Do NOT enable all probes by default !**
- **Avoid DHCP SPAN.** If used, make sure probe captures traffic to central DHCP Server. HA challenges.

- **Avoid SNMP, SNMP Traps, and NetFlow probes !**

- For polled SNMP queries, avoid short polling intervals. Be sure to set optimal PSN for polling in ISE NAD config.

Limit pxGrid probe to two PSNs max for HA - possibly dedicated !

- **NetFlow Probe:**

- Use only for specific use cases in centralized deployments—Potential for high load on network devices and ISE.

- **pxGrid Probe:**

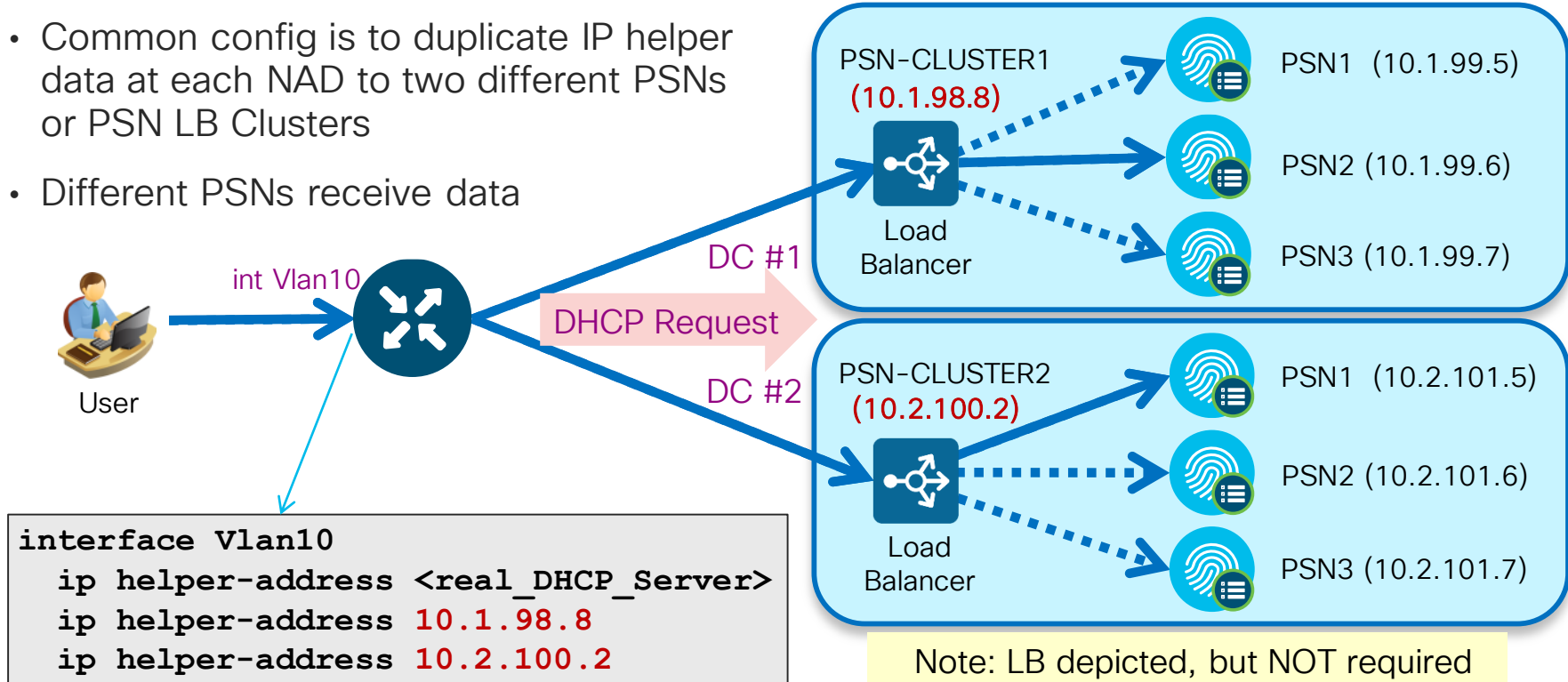
- Limit # PSNs enabled for pxGrid as each becomes a Subscriber to same data. 2 needed for redundancy.
- Dedicate PSNs for pxGrid Probe if high-volume data from Publishers.

Profiling Redundancy – Duplicating Profile Data

Different DHCP Addresses

- Provides Redundancy but Leads to Contention for Ownership = Replication

- Common config is to duplicate IP helper data at each NAD to two different PSNs or PSN LB Clusters
- Different PSNs receive data



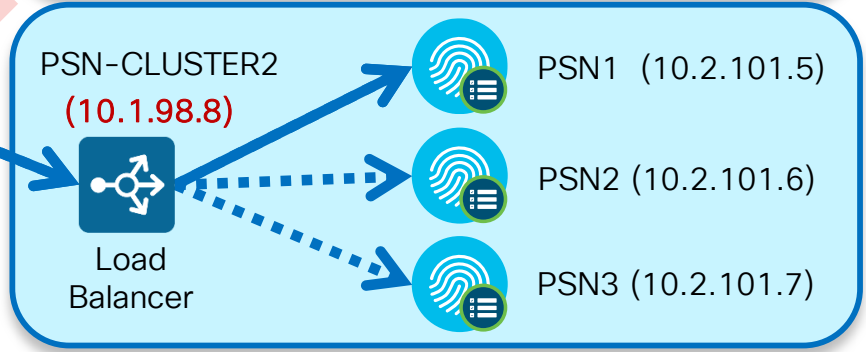
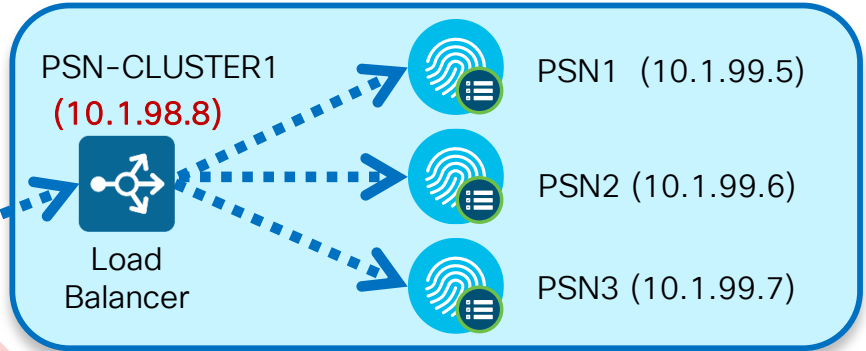
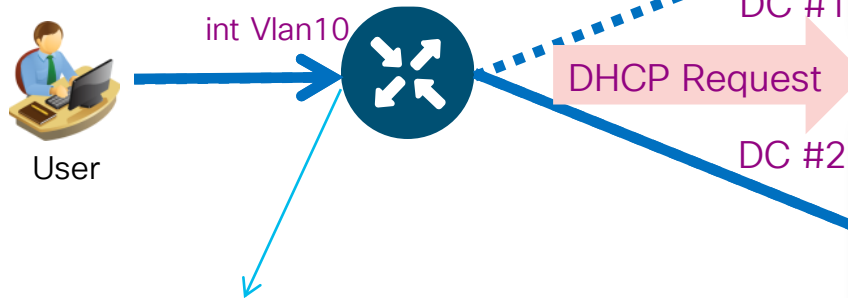
Note: LB depicted, but NOT required

Scaling Profiling and Replication

Single DHCP VIP Address using Anycast

- Limit Profile Data to a Single PSN and Node Group

- Different PSNs or Load Balancer VIPs host same target IP for DHCP profile data
- Routing metrics determine which PSN or LB VIP receives DHCP from NAD

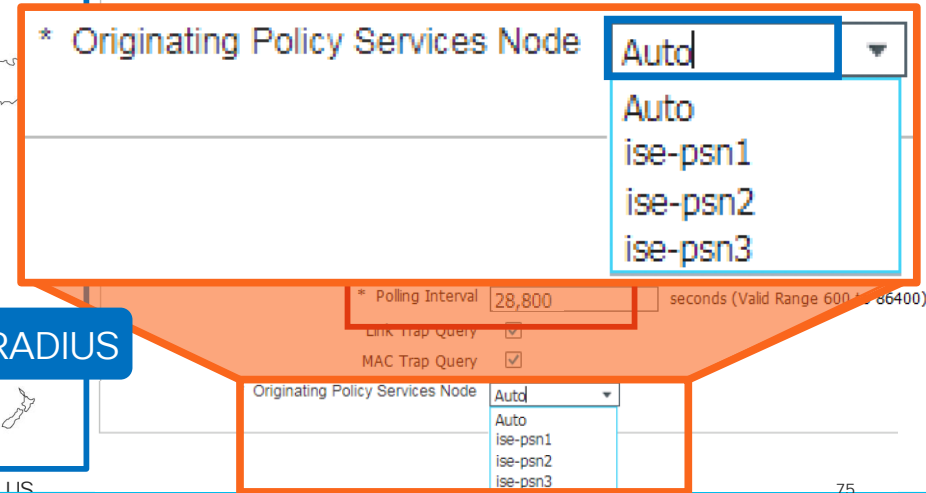
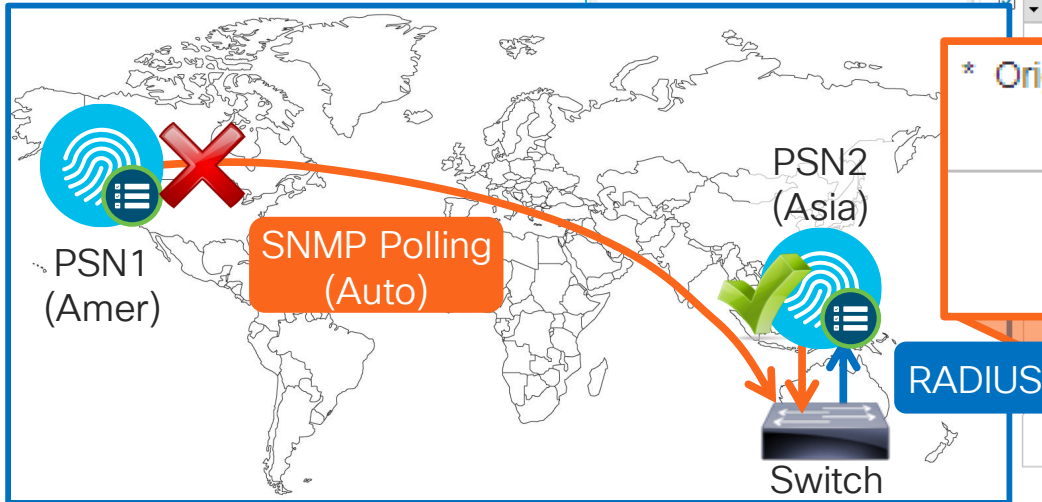
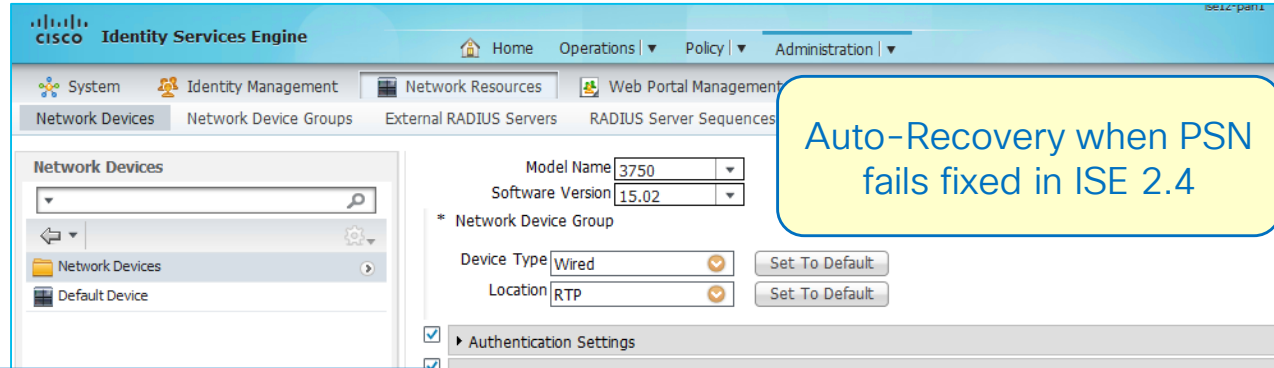


```
interface Vlan10
ip helper-address <real_DHCP_Server>
ip helper-address 10.1.98.8
```

Note: LB depicted, but NOT required

Profiler Tuning for Polled SNMP Query Probe

- Set specific PSNs to periodically poll access devices for SNMP data.
- Choose PSN closest to access device.

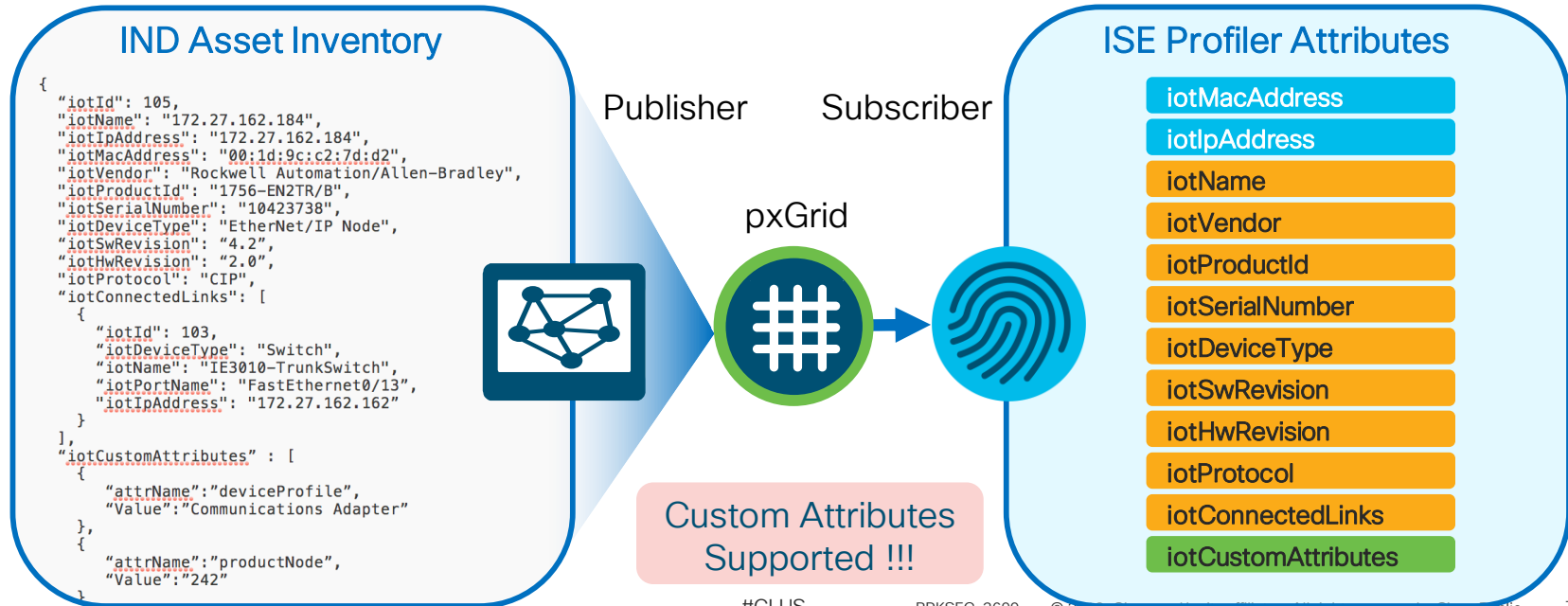


pxGrid Profiler Probe (Context In)

New in
ISE 2.4

First Integration with Cisco Industrial Network Director (IND)

- IND communicates with Industrial Switches and Security Devices and collects detailed information about the connected manufacturing devices.
- IND v1.3 adds pxGrid Publisher interface to communicate IoT attributes to ISE.



pxGrid Profiler Probe

Deployment

- Deployment
- PAN Failover

Deployment Nodes List > pmbudev-vm80

Edit Node

General Settings | **Profiling Configuration**

▶ NETFLOW

▼ DHCP

Interface GigabitEthernet 0

Port 67

Description The DHCP probe listens for DHCP packets from IP helper.

Recommend limit probe to two PSNs (2 for HA). Each PSN becomes a pxGrid Subscriber to IND Asset topic

Profiler Conditions Based on Custom Attribute

New in
ISE 2.4

The screenshot displays the Cisco Identity Services Engine (ISE) interface for configuring a new profiler condition. The breadcrumb trail is: Home > Context Visibility > Operations > Policy > Administration > Work Centers > Policy Sets > Profiling > Posture > Client Provisioning > Policy Elements > Dictionaries > Conditions > Results. The current page is titled 'Profiler Condition List > New Profiler Condition'.

The 'Profiler Condition' form includes the following fields:

- * Name: Custom_Attribute_Check5
- * Type: CUSTOMATTRIBUTE (selected from a dropdown menu)
- * Attribute Name: AssetDB_Device_Type
- * Operator: STARTSWITH
- * Attribute Value: CIP_PLC-5

Below the form, it indicates 'System Type Administrator Created'. At the bottom, there are 'Submit' and 'Cancel' buttons.

The dropdown menu for 'Type' is open, showing the following options:

- DHCP
- MAC
- SNMP
- IP
- RADIUS
- NetFlow
- CDP
- LLDP
- NMAP
- NMAPExtension
- Multimedia
- ACIDEX
- IoTAsset
- ACTIVEDIRECTORY_PROBE
- CUSTOMATTRIBUTE** (highlighted with a red box)

Profiling Based on Custom Attributes

Performance Hit so Disabled By Default

New in ISE 2.4

- Global Setting **MUST** be **enabled**
- If disabled:
 - Custom Attributes are NOT updated over pxGrid
 - Profiler ignores any conditions based on Customer Attributes, even if Custom Attribute is populated.

The screenshot shows the Cisco Identity Services Engine (ISE) Profiler Configuration page. The left sidebar contains a navigation menu with categories like Client Provisioning, FIPS Mode, Security Settings, Alarm Settings, Posture, Profiling, and Protocols. The main content area is titled 'Profiler Configuration' and includes several settings:

- * CoA Type: Port Bounce
- Current custom SNMP community strings: ●●●●●● (Show)
- Change custom SNMP community strings: (For NMAP)
- Confirm changed custom SNMP community strings: (For NMAP)
- EndPoint Attribute Filter: Enabled
- Enable Anomalous Behaviour Detection: Enabled
- Enable Anomalous Behaviour Enforcement: Enabled
- Enable Custom Attribute for Profiling: Enabled

A blue callout box highlights the 'Enable Custom Attribute for Profiling' checkbox and another one below it, both showing the checkbox is checked and labeled 'Enabled'.

New and Updated IoT Profile Libraries

Delivered via ISE Community: <https://communities.cisco.com/docs/DOC-66340>

- 700+ Automation and Control
 - Industrial / Manufacturing
 - Building Automation
 - Power / Lighting
 - Transportation / Logistics
 - Financial (ATM, Vending, PoS, eCommerce)
 - IP Camera / Audio-Video / Surveillance and Access Control
 - Other (Defense, HVAC, Elevators, etc)
- Windows Embedded
- 300+ Profiles in Medical NAC Profile Library



Why Do I Care about # Profiles?



- ISE 2.1+ supports a MAX of **2000** profiles
- Let's Do the Math...
 - ~600 Base Profiles
 - 600+ New Feed Profiles (2.4)
 - 300+ Medical NAC Profiles
 - 700+ Automation & Control Profiles

2300+ Profiles

- No restrictions on profile import, so must check # profiles in library before import large batch of new profiles.

Scaling MnT (Optimize Logging and Noise Suppression)

The Fall Out From the Mobile Explosion and IoT

- Explosion in number and type of endpoints on the network.
- High auth rates from mobile devices—many personal (unmanaged).
 - Short-lived connections: Continuous sleep/hibernation to conserve battery power, roaming, ...
- Misbehaving supplicants: Unmanaged endpoints from numerous mobile vendors may be misconfigured, missing root CA certificates, or running less-than-optimal OS versions
- Misconfigured NADs. Often timeouts too low & misbehaving clients go unchecked/not throttled.
- Misconfigured Load Balancers—Suboptimal persistence and excessive RADIUS health probes.
- Increased logging from Authentication, Profiling, NADs, Guest Activity, ...
- System not originally built to scale to new loads.
- End user behavior when above issues occur.
- Bugs in client, NAD, or ISE.



Clients Misbehave!

- Example education customer:
 - **ONLY 6,000 Endpoints** (all BYOD style)
 - **10M Auths / 9M Failures in a 24 hours!**
 - 42 Different Failure Scenarios – all related to clients dropping TLS (both PEAP & EAP-TLS).
- Supplicant List:
 - Kyocera, Asustek, Murata, Huawei, Motorola, HTC, Samsung, ZTE, RIM, SonyEric, ChiMeiCo, Apple, Intel, Cybertan, Liteon, Nokia, HonHaiPr, Palm, Pantech, LgElectr, TaiyoYud, Barnes&N
- **5411 No response received during 120 seconds on last EAP message sent to the client**
 - This error has been seen at a number of Escalation customers
 - Typically the result of a misconfigured or misbehaving supplicant not completing the EAP process.



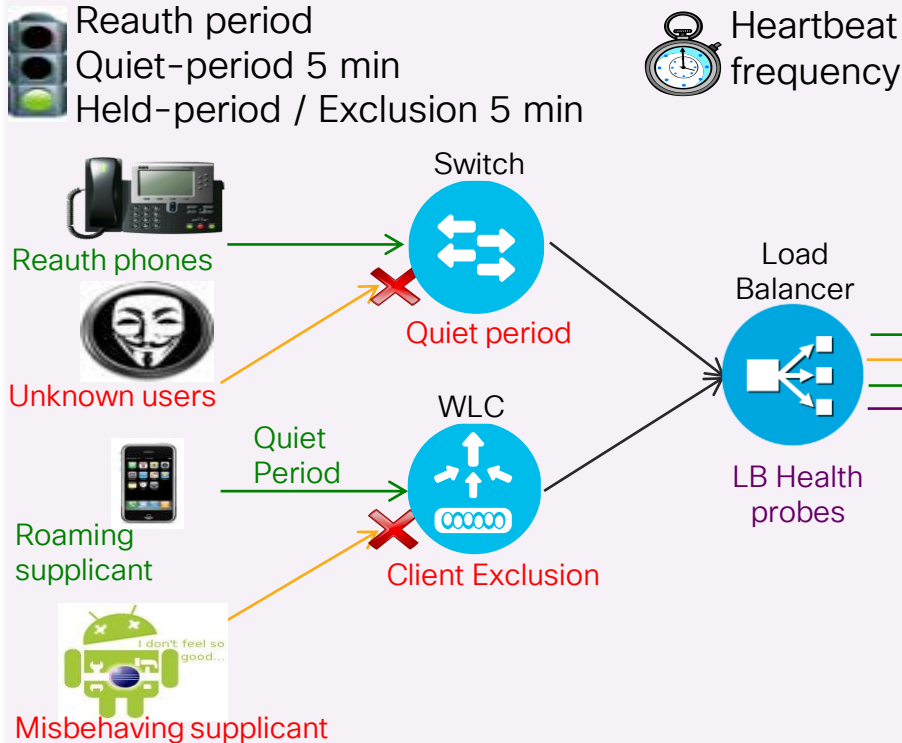
Challenge: How to reduce the flood of log messages while increasing PSN and MNT capacity and tolerance



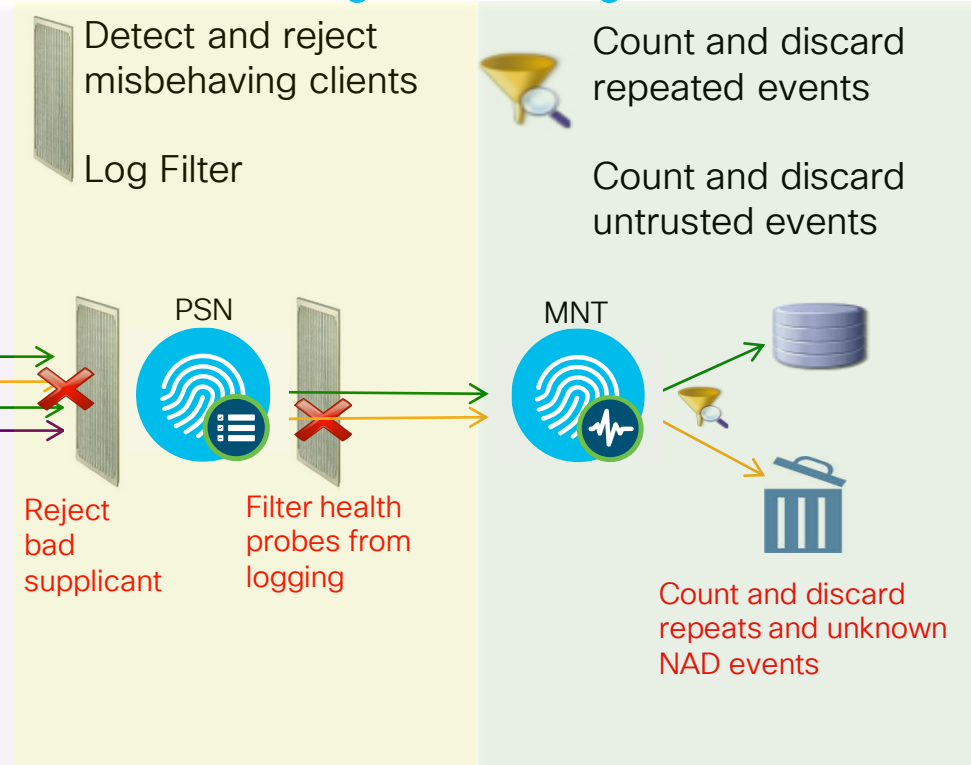
Getting More Information With Less Data

Scaling to Meet Current and Next Generation Logging Demands

Rate Limiting at Source



Filtering at Receiving Chain



Tune NAD Configuration

Rate Limiting at **Wireless** Source

BRKSEC-2059 Deploying ISE in a Dynamic Environment - Clark Gambrel
Monday, June 11 @ 1:30pm



Reauth period
Quiet-period 5 min
Held-period / Exclusion 5 min



Reauth phones



Unknown users



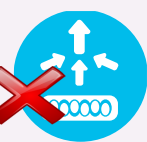
Roaming supplicant



Misbehaving supplicant

Quiet
Period

WLC



Client Exclusion

Wireless (WLC)

- **RADIUS Server Timeout:** Increase from default of 2 to 5 sec
- **RADIUS Aggressive-Failover:** Disable aggressive failover
- **RADIUS Interim Accounting:** v7.6: Disable; v8.0+: Enable with interval of 0. (Update auto-sent on DHCP lease or Device Sensor)
- **Idle Timer:** Increase to 1 hour (3600 sec) for secure SSIDs
- **Session Timeout:** Increase to 2+ hours (7200+ sec)
- **Client Exclusion:** Enable and set exclusion timeout to 180+ sec
- **Roaming:** Enable CCKM / SKC / 802.11r (when feasible)
- **Bugfixes:** Upgrade WLC software to address critical defects

Prevent Large-Scale Wireless RADIUS Network Melt Downs

<http://www.cisco.com/c/en/us/support/docs/wireless-mobility/wireless-lan-wlan/118703-technote-wlc-00.html>

Added in WLC 8.4

One-Click Setup for ISE Best Practice Config

MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT

RADIUS Authentication Servers > New

Server Index (Priority) 2

Server IP Address(Ipv4/Ipv6) 10.1.101.17

Shared Secret Format ASCII

Shared Secret

Confirm Shared Secret

Apply Cisco ISE Default settings

Key Wrap (Designed for FIPS customers and requires...)

Port Number 1812

Server Status Enabled

Support for CoA Disabled

Server Timeout 2 seconds

Network User

Management

Management Retransmit Time

Tunnel Proxy Enable

IPSec Enable

CISCO MONITOR WLANs CONTROLLER WIRELESS SECUR

WLANs > Edit 'v-employee'

WLANs

Advanced

Layer 2 Layer 3 AAA Servers

Select AAA servers below to override use of default servers on th

RADIUS Servers

RADIUS Server Overwrite interface Enabled

Apply Cisco ISE Default Settings Enabled

Authentication Servers	Accounting Servers
<input checked="" type="checkbox"/> Enabled	<input checked="" type="checkbox"/> Enabled
Server 1 IP:10.1.98.8, Port:1812	IP:10.1.98.8, Port:1813
Server 2 None	None
	None
	None
	None
Server 6 None	None

RADIUS Server Accounting

Apply Cisco ISE Default Settings Enabled



Which WLC Software Should I Deploy?

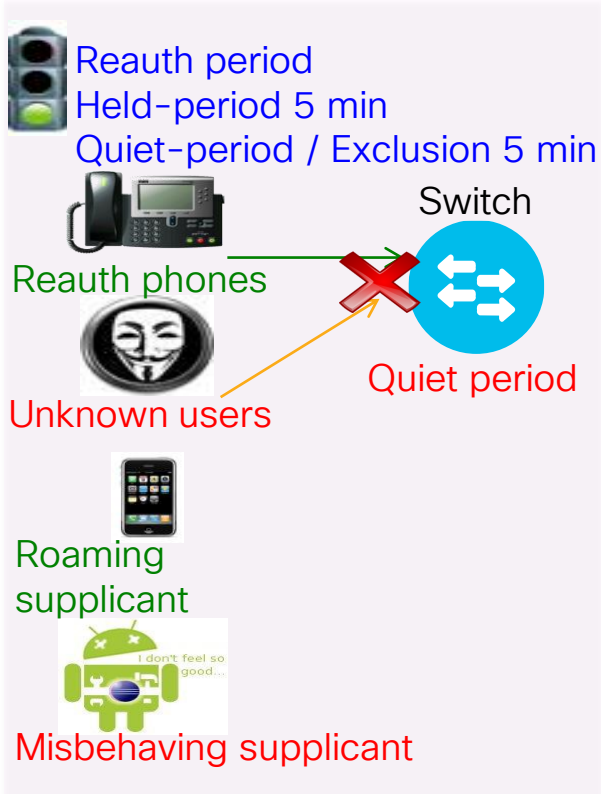
- **8.0.152.0** – Currently the most mature and reliable release.
- **8.2.167.6** – Mature – Recommended when need new feature/hardware support.
- **8.3.141.0** – Less Mature – Recommend if require new features in 8.3.x
- **8.5.124.55** – Cutting edge – Recommend if require new features in 8.5.x
- **8.6.101.0** – Bleeding edge – Only if absolutely require new features in 8.6.x
- **8.7.102.0** – Only if absolutely require new features in 8.7.x
- Example critical defects resolved in maintenance and new releases:

CDETS	Title
CSCul83594	Session-id is not synchronized across mobility, if the network is open (fixed in 8.6)
CSCuu82607	Evaluation of all for OpenSSL June 2015
CSCuu68490	duplicate radius-acct update message sent while roaming
CSCus61445	DNS ACL on wlc is not working - AP not Send DTLS to WLC
CSCuq48218	Cisco WLC cannot process multiple sub-attributes in single RADIUS VSA
CSCuo09947	RADIUS AVP #44 (Acct-Session-ID) to be sent in RADIUS authentication messages

<https://www.cisco.com/c/en/us/support/docs/wireless/wireless-lan-controller-software/200046-TAC-Recommended-AireOS.html>

Tune NAD Configuration

Rate Limiting at **Wired** Source

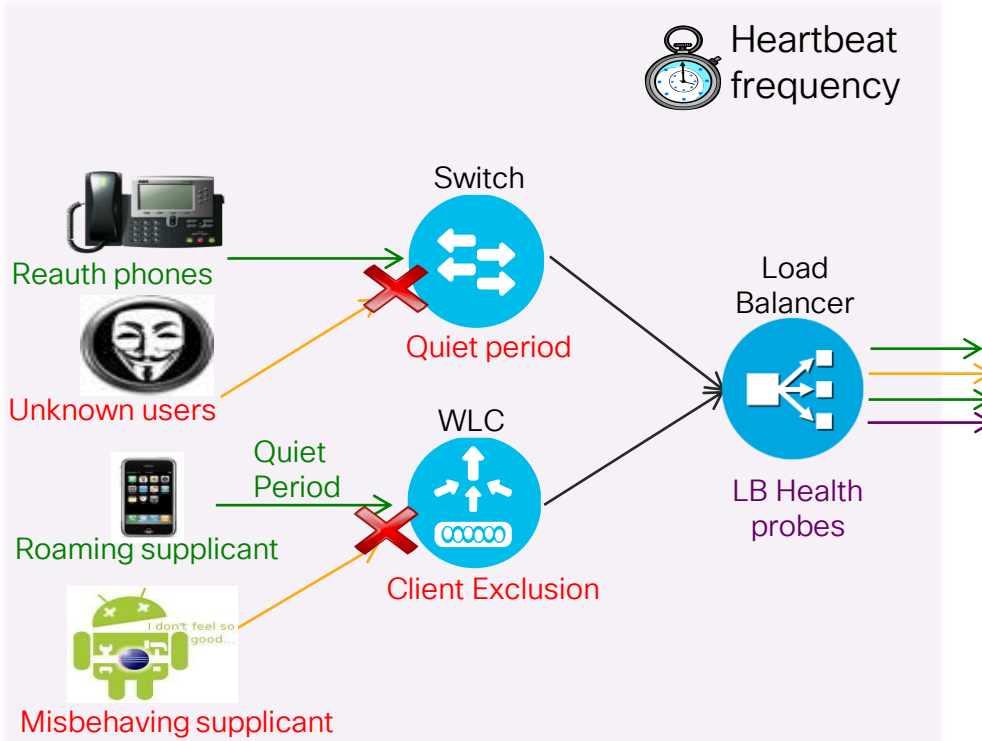


Wired (IOS / IOS-XE)

- **RADIUS Interim Accounting:** Use *newinfo* parameter with long interval (for example, 24-48 hrs), if available. Otherwise, set 15 mins. **If LB present, set shorter than RADIUS persist time.**
- **802.1X Timeouts**
 - held-period: Increase to 300+ sec
 - quiet-period: Increase to 300+ sec
 - ratelimit-period: Increase to 300+ sec
- **Inactivity Timer:** Disable or increase to 1+ hours (3600+ sec)
- **Session Timeout:** Disable or increase to 2+ hours (7200+ sec)
- **Reauth Timer:** Disable or increase to 2+ hours (7200+ sec)
- **Bugfixes:** Upgrade software to address critical defects.

RADIUS Test Probes

Reduce Frequency of RADIUS Server Health Checks



- **Wired NAD:** RADIUS test probe interval set with **idle-time** parameter in radius-server config; Default is 60 minutes
 - No action required
- **Wireless NAD:** If configured, WLC only sends “active” probe when server marked as dead.
 - No action required
- **Load Balancers:** Set health probe intervals and retry values short enough to ensure prompt failover to another server in cluster occurs prior to NAD RADIUS timeout (typically 20-60 sec.) but long enough to avoid excessive test probes.

Load Balancer RADIUS Test Probes



Citrix Example

- Probe frequency and retry settings:
 - Time interval between probes:
`interval seconds` # Default: 5
 - Number of retries
`retries number` # Default: 3
- Sample Citrix probe configuration:

```
add lb monitor PSN-Probe RADIUS -respCode 2
-userName citrix_probe -password citrix123
-radKey cisco123 -LRTM ENABLED -interval 10
-retries 3 -destPort 1812
```

- Recommended setting:** Failover must occur before RADIUS timeout (typically 15-35 sec) while avoiding excessive probing

F5 Example

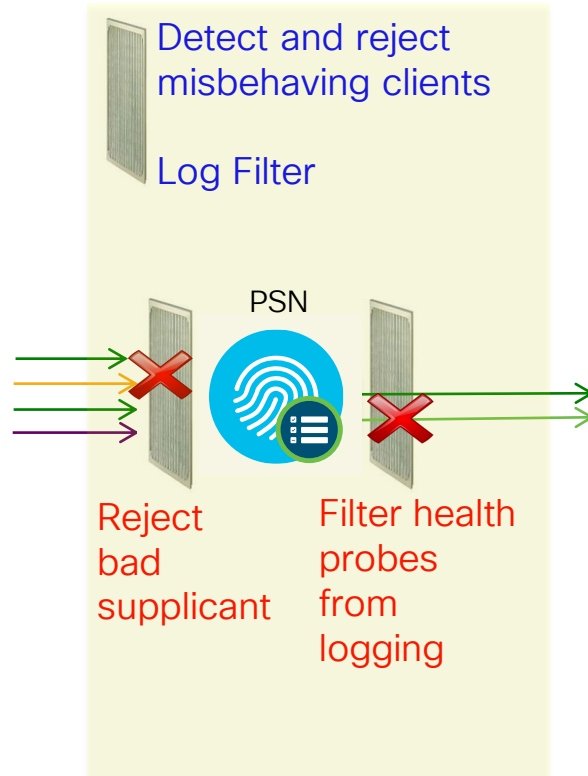
- Probe frequency and retry settings:
 - Time interval between probes:
`Interval seconds` # Default: 10
 - Timeout before failure = $3 * (\text{interval}) + 1$:
`Timeout seconds` # Default: 31
- Sample F5 RADIUS probe configuration:

```
Name PSN-Probe
Type RADIUS
Interval 10
Timeout 31
Manual Resume No
Check Util Up Yes
User Name f5-probe
Password f5-ltm123
Secret cisco123
Alias Address * All Addresses
Alias Service Port 1812
Debug No
```

PSN Noise Suppression and Smarter Logging

Filter Noise and Provide Better Feedback on Authentication Issues

- PSN Collection Filters
- PSN Misconfigured Client Dynamic Detection and Suppression
- PSN Accounting Flood Suppression
- Detect Slow Authentications
- Enhanced Handling for EAP sessions dropped by supplicant or Network Access Server (NAS)
- Failure Reason Message and Classification
- Identify RADIUS Request From Session Started on Another PSN
- Improved Treatment for Empty NAK List



PSN - Collection Filters

Static Client Suppression

- PSN static filter based on single attribute:
 - User Name
 - Policy Set Name
 - NAS-IP-Address
 - Device-IP-Address
 - MAC (Calling-Station-ID)

Administration > System > Logging > Collection Filters

Logging

- Local Log Settings
- Remote Logging Targets
- Logging Categories
- Message Catalog
- Debug Log Configuration
- Collection Filters

Collection Filter List > **New Collection Filter**

Collection Filters

* Attribute

* Value

* Filter Type

Submit

Filter All
Filter Passed
Filter Failed
Disable Suppression

User Name
Policy Set Name
NAS IP Address
Device IP Address
MAC Address

- Filter Messages Based on Auth Result:
 - All (Passed/Fail)
 - All Failed
 - All Passed
- Select Messages to **Disable Suppression** for failed auth @PSN and successful auth @Mn

Collection Filters

Edit Add Duplicate Delete

<input type="checkbox"/>	Attribute	Value	Filter Type
<input type="checkbox"/>	MAC Address	11:22:44:AA:BB:CC	Disable Suppression
<input type="checkbox"/>	NAS IP Address	10.6.6.6	Filter Failed
<input type="checkbox"/>	Policy Set Name	RADIUS_Probes	Filter Passed
<input type="checkbox"/>	User Name	chyps	Filter All

PSN Filtering and Noise Suppression

Dynamic Client Suppression

Updated
in ISE 2.2!

Flag misconfigured supplicants for same auth failure within specified interval and stop logging to MnT

Send alarm with failure statistics

RADIUS Settings Administration > System > Settings > Protocols > RADIUS

Suppression & Reports UDP Ports DTLS

Suppress Repeated Failed Clients

- Suppress repeated failed clients ⓘ
- Detect two failures within ⓘ minutes(1 - 30)
- Report failures once every ⓘ minutes (15 - 60)

Reject repeated failed RADIUS requests ⓘ

Failures prior to automatic rejection ⓘ (2-100)

Continue rejecting ⓘ seconds (1-10)

Ignore repeated accounting updates within ⓘ seconds (1 - 86,400)

Suppress Successful Clients

- Suppress repeated successful clients ⓘ

Authentication Details

Highlight steps longer than ⓘ seconds (500 - 10,000)

Valid Time ranges displayed by default

Each endpoint tracked by:

- Calling-Station-ID (MAC Address)
- NAS-IP-Address (NAD address)
- Failure reason

PSN Filtering and Noise Suppression

Dynamic Client Suppression

Flag misconfigured supplicants for same auth failure within specified interval and stop logging to MnT

Send alarm with failure statistics

Send immediate Access-Reject (do not even process request) IF:
1) Flagged for suppression
2) Fail auth total X times for same failure reason (inc 2 prev)

Fully process next request after rejection period expires.

RADIUS Settings Administration > System > Settings > Protocols > RADIUS

Suppression & Reports | UDP Ports | DTLS

Suppress Repeated Failed Clients

- Suppress repeated failed clients ⓘ
- Detect two failures within: ⓘ minutes (1 - 30)
- Report failures once every: ⓘ minutes (15 - 60)
- Reject repeated failed RADIUS requests ⓘ
- Failures prior to automatic rejection: ⓘ
- Continue rejecting requests for: ⓘ minutes (5 - 180)
- Ignore repeated accounting updates within: ⓘ seconds (1 - 86,400)

Suppress Successful Reports

- Suppress repeated successful authentications ⓘ

Authentication Details

- Highlight steps longer than: ⓘ milliseconds (500 - 10,000)

Hard-coded @ 5 in ISE 2.0

PSN Noise Suppression

Drop Excessive RADIUS Accounting Updates from “Misconfigured NADs”

RADIUS Settings Administration > System > Settings > Protocols > RADIUS

Suppression & Reports UDP Ports DTLS

Suppress Repeated Failed Clients

Suppress repeated failed clients ⓘ

Detect two failures within ⓘ minutes (1 - 30)

Report failures once every ⓘ minutes (15 - 60)

Reject repeated failed RADIUS requests ⓘ

Failures prior to automatic rejection ⓘ (2-100)

Continue rejecting requests for ⓘ minutes (5 - 180)

Ignore repeated accounting updates within ⓘ seconds (1 - 86,400)

Suppress Successful Reports

Suppress repeated successful authentications ⓘ

Authentication Details

Highlight steps longer than ⓘ milliseconds (500 - 10,000)

Allow 2 RADIUS Accounting Updates for same session in specified interval, then drop.

MnT Log Suppression and Smarter Logging

Drop and Count Duplicates / Provide Better Monitoring Tools

- Drop duplicates and increment counter in Live Log for “matching” passed authentications
- Display repeat counter to Live Sessions entries.
- Update session, but do not log RADIUS Accounting Interim Updates
- Log RADIUS Drops and EAP timeouts to separate table for reporting purposes and display as counters on Live Log Dashboard along with Misconfigured Supplicants and NADs
- Alarm enhancements
- Revised guidance to limit syslog at the source.
- MnT storage allocation and data retention limits
- More aggressive purging
- Allocate larger VM disks to increase logging capacity and retention.



MnT Noise Suppression

Suppress Storage of Repeated Successful Auth Events

Suppress Successful Reports
= Do not save **repeated** successful
auth events for the **same session**
to MnT DB

These events will not display in
Live Authentications Log but do
increment Repeat Counter.

RADIUS Settings Administration > System > Settings > Protocols > RADIUS

Suppression & Reports UDP Ports DTLS

Suppress Repeated Failed Clients

Suppress repeated failed clients ⓘ

Detect two failures within ⓘ minutes (1 - 30)

Report failures once every ⓘ minutes (15 - 60)

Reject repeated failed RADIUS requests ⓘ

Failures prior to automatic rejection ⓘ (2-100)

Continue rejecting requests for ⓘ minutes (5 - 180)

Ignore repeated accounting updates within ⓘ seconds (1 - 86,400)

Suppress Successful Reports

Suppress repeated successful authentications ⓘ

Authentication Details

Highlight steps longer than ⓘ milliseconds (500 - 10,000)

MnT Noise Suppression

Suppress Storage of Repeated Successful Auth Events

Step latency is visible in Live Logs details

Suppress Successful Reports
= Do not save **repeated** successful auth events for the **same session** to MnT DB

These events will not display in Live Authentications Log but do increment Repeat Counter.

Detect NAD retransmission timeouts and Log auth steps > threshold.

```
12304 Extracted EAP-Response containing PEAP challenge-response
11808 Extracted EAP-Response containing EAP-MSCHAP challenge-response for inner method
15041 Evaluating Identity Policy (Step latency=1048 ms)
15006 Matched Default Rule
15013 Selected Identity Source - Internal Users
24430 Authenticating user against Active Directory
24454 User authentication against Active Directory failed because of a timeout error (Step latency=30031 ms)
24210 Looking up User in Internal Users IDStore - test1
24212 Found User in Internal Users IDStore
22037 Authentication Passed
11824 EAP-MSCHAP authentication attempt passed
12305 Prepared EAP-Request with another PEAP challenge
11006 Returned RADIUS Access-Challenge
5411 Supplicant stopped responding to ISE (Step latency=120001 ms)
```

Suppress Successful Reports

Suppress repeated successful authentications ⓘ

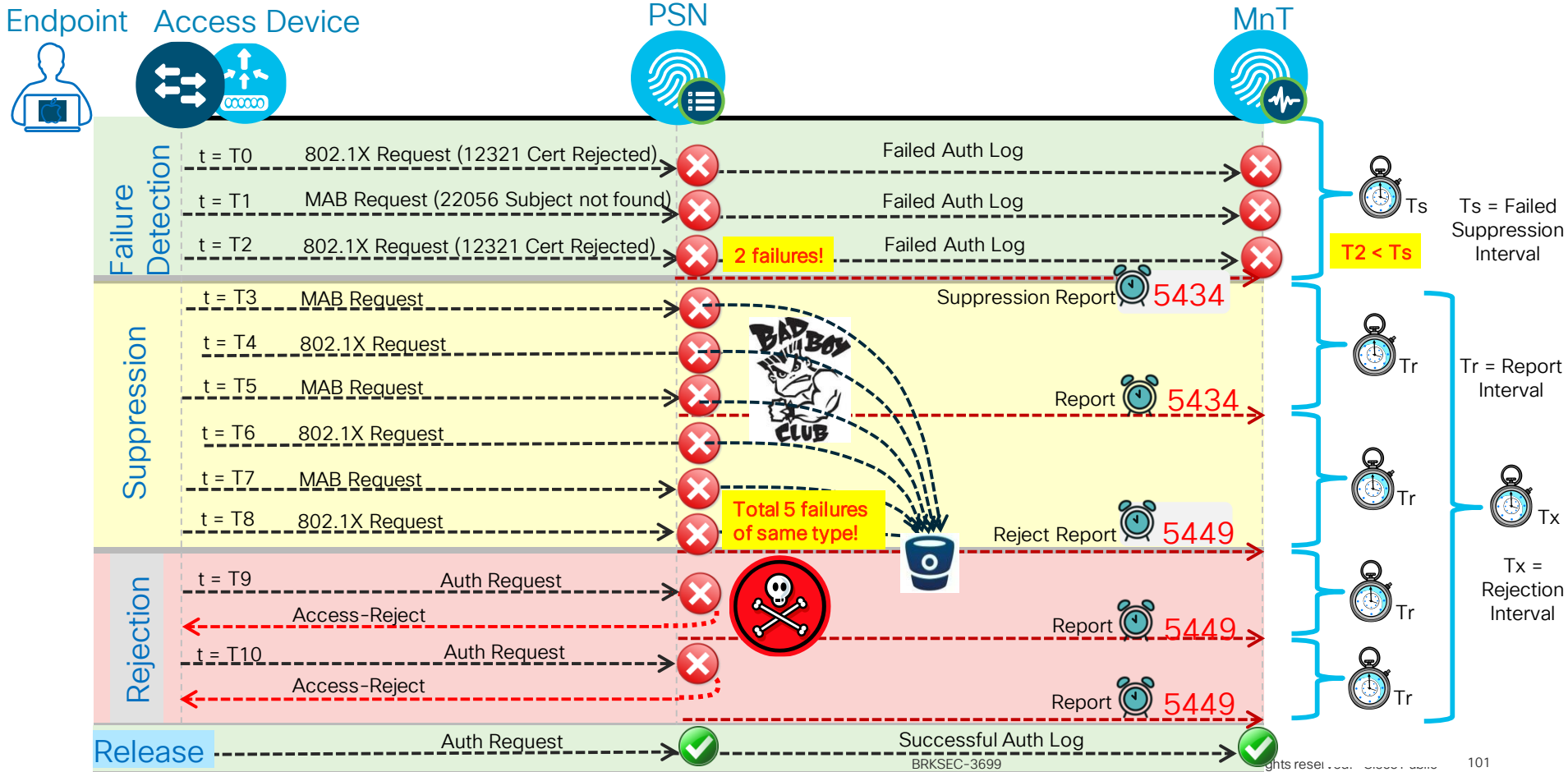
Authentication Details

Highlight steps longer than

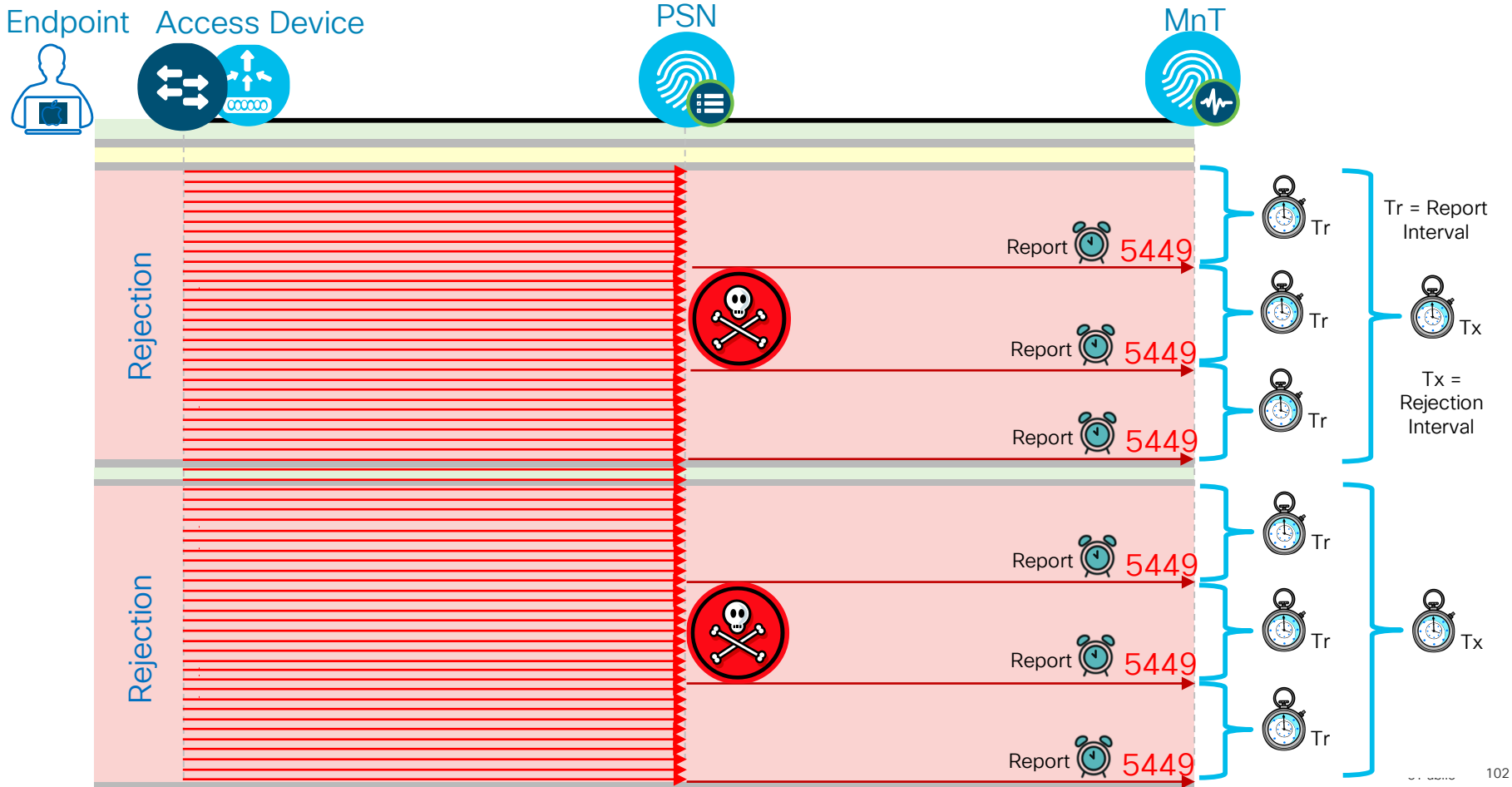


milliseconds (500 - 10,000)

Client Suppression and Reject Timers

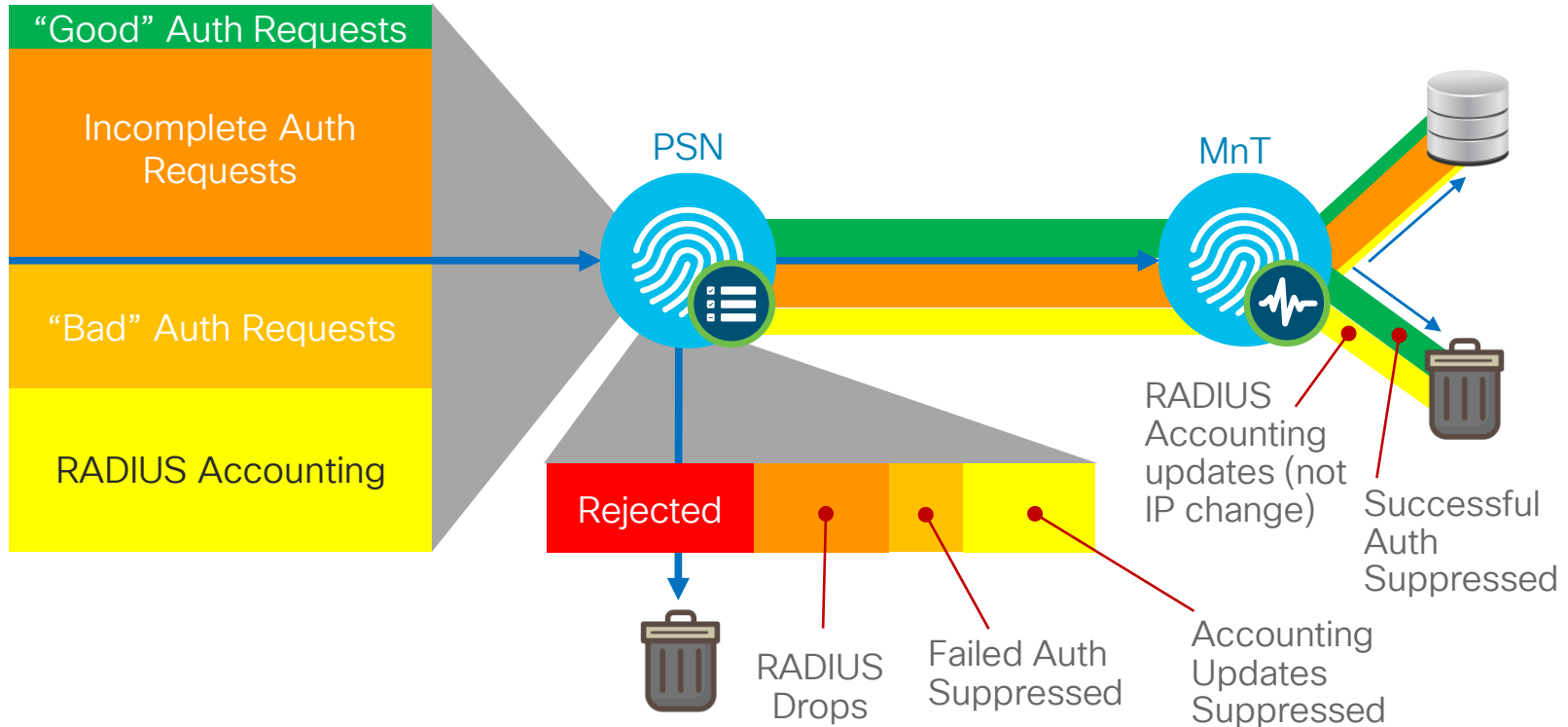


Client Suppression and Reject Timers

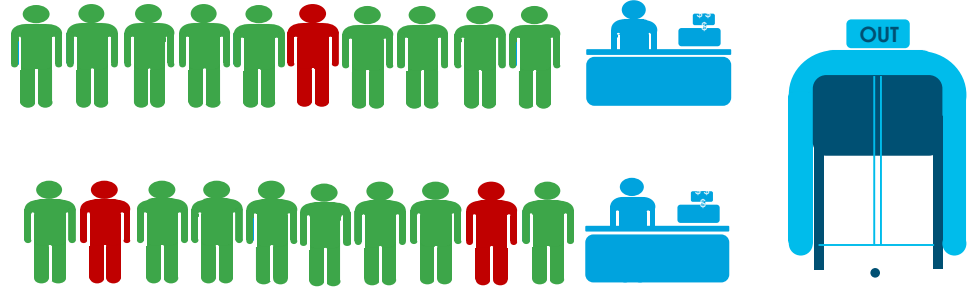
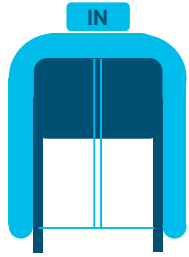


ISE Log Suppression

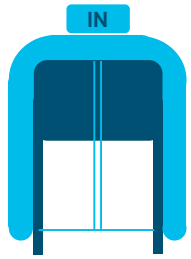
“Good”-put Versus “Bad”-put



Typical Load Example



Extreme Noise Load Example

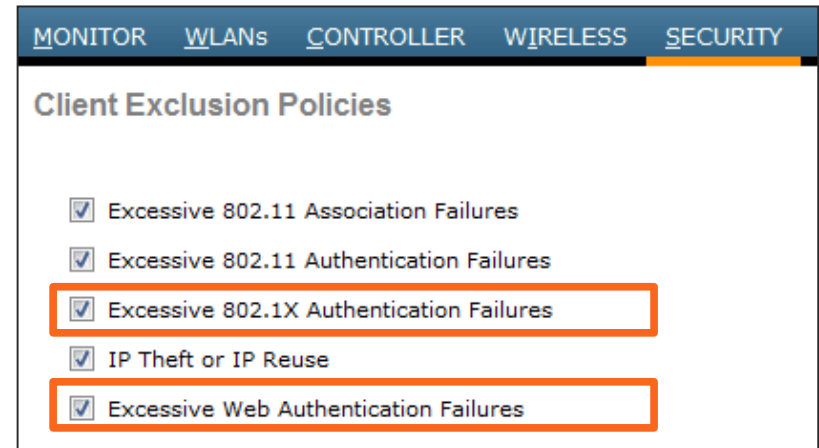
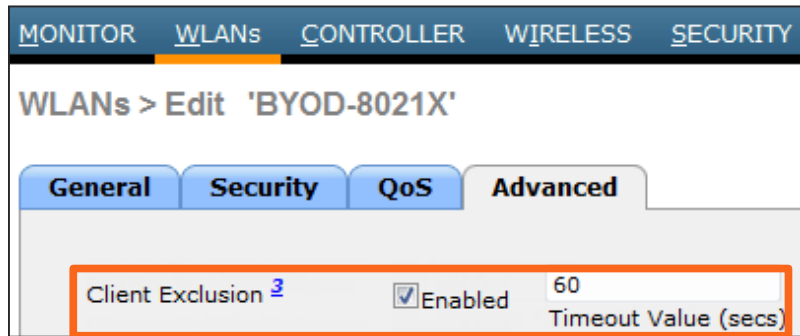


WLC - Client Exclusion

Blacklist Misconfigured or Malicious Clients



- **Excessive Authentication Failures**—Clients are excluded on the fourth authentication attempt, after three consecutive failures.
- Client excluded for Time Value specified in WLAN settings. Recommend increase to 1-5 min (60-300 sec). **3 min** is a good start.



Note: Diagrams show default values

Live Authentications and Sessions

21 10 521 6716 19052

Time	Status	Details	Repeat Count	Identity	Endpoint ID	Endpoint Profile	Network Device
2013-09-27 14:46:33.005	🟢	🔗	0	vipinj	CC:3A:61:12:ED:D5	Android-Samsung	
2013-09-27 14:46:30.890	🟢	🔗	11	aarondek	64:A3:CB:52:74:B1	Apple-iDevice	
2013-09-27 14:46:29.658	🟢	🔗	99	wekang	B8:78:2E:60:7F:14	Apple-iDevice	
2013-09-27 14:46:29.252	🟢	🔗	1	mutama	CC:78:5F:43:97:71	Apple-iDevice	
2013-09-27 14:46:25.595	🟢	🔗	0	jeffreed	F0:CB:A1:75:31:4D	Apple-iPhone	
2013-09-27 14:46:25.595	🟢	🔗	0	jeffreed	F0:CB:A1:75:31:4D	Apple-iPhone	WNBU_NGWC...
2013-09-27 14:46:22.636	🟢	🔗	0	jeffreed	F0:CB:A1:75:31:4D	Apple-iPhone	WNBU-WLC1
2013-09-27 14:46:21.486	🔴	🔗	0	anonymous	00:1E:65:D6:93:E2		WNBU-WLC1
2013-09-27 14:46:18.884	🟢	🔗	7	dsladden	0C:77:1A:9A:F6:73	Apple-iPhone	

Blue entry = Most current Live Sessions entry with repeated successful auth counter

Authentication Suppression

Enable/Disable

- **Global Suppression Settings:** Administration > System > Settings > Protocols > RADIUS

Failed Auth Suppression

Suppress Anomalous Clients ⓘ

Successful Auth Suppression

Suppress Repeated Successful Authentications ⓘ

Caution: Do not disable suppression in deployments with very high auth rates.

It is highly recommended to keep Auth Suppression enabled to reduce MnT logging

- **Selective Suppression using Collection Filters:** Administration > System > Logging > Collection Filters

Configure specific traffic to bypass Successful Auth Suppression

Useful for troubleshooting authentication for a specific endpoint or group of endpoints, especially in high auth environments where global suppression is always required.

Collection Filter List > Calling-Station-ID

Collection Filters

* Attribute

* Value

* Filter Type

Save

Filter All
Filter Passed
Filter Failed
Disable Suppression

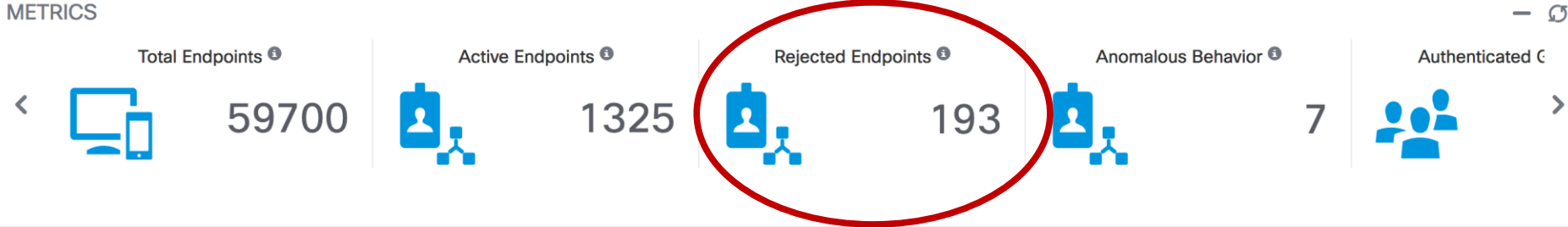
Per-Endpoint Time-Constrained Suppression

The screenshot displays the Cisco Identity Services Engine (ISE) interface. At the top, there are navigation tabs for 'Authentication', 'Reports', 'Endpoint Protection Service', and 'Troubleshoot'. Below these, there are summary statistics: 'Misconfigured Supplicants: 21', 'Misconfigured Network Devices: 10', 'ANCS Drop: 521', 'Client Stopped Responding: 6716', and 'Repeat Counts: 19052'. The main area shows a table of endpoint sessions with columns: Time, Status, Details, Repeat Count, Identity, Endpoint ID, Endpoint Profile, and Network Device. A context menu is open over a row, with the following options: 'Endpoint Debug...', 'Modify Collection Filters...', 'Bypass Suppression Filtering for 1 hour' (highlighted with an orange border), 'Settings...', 'Global Settings...', and 'About Adobe Flash Player 11.7.700.224...'. A mouse cursor is pointing at the 'Endpoint ID' cell of the selected row, and a blue callout box with the text 'Right Click' is positioned next to it.

Time	Status	Details	Repeat Count	Identity	Endpoint ID	Endpoint Profile	Network Device
2013-09-27 14:46:33.005			0	vipinj	CC:3A:61:12:ED:D5	Android-Samsung	
2013-09-27 14:46:30.890			11	aarondek	64:A3:CB:52:74:B1	Apple-iDevice	
2013-09-27 14:46:21					B8:78:2E:60:7F:14	Apple-iDevice	
2013-09-27 14:46:21					CC:78:5F:43:97:71	Apple-iDevice	
2013-09-27 14:46:21					F0:CB:A1:75:31:4D	Apple-iPhone	WNBU_NGWC...
2013-09-27 14:46:21					F0:CB:A1:75:31:4D	Apple-iPhone	WNBU-WLC1
2013-09-27 14:46:21					F0:CB:A1:75:31:4D	Apple-iPhone	WNBU-WLC1
2013-09-27 14:46:21					00:1E:65:D6:93:E2		WNBU-WLC1
2013-09-27 14:46:21					0C:77:1A:9A:F6:73	Apple-iPhone	

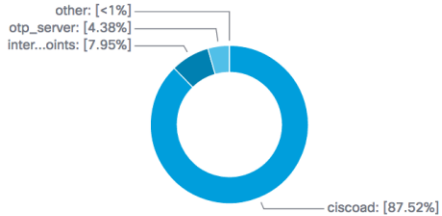
Visibility into Reject Endpoints!

New in ISE 2.2!



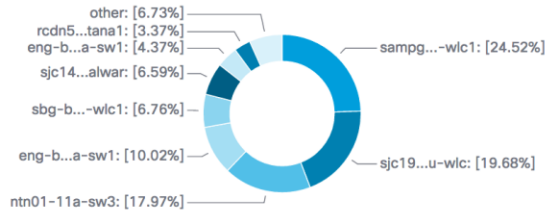
AUTHENTICATIONS ³

Identity Store | Identity Group | Network Device | Failure Reason



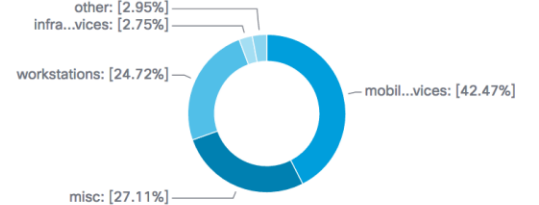
NETWORK DEVICES ³

Device Name | Type | Location



ENDPOINTS ³

Type | Profile



Releasing Rejected Endpoints

New in ISE 2.2!

The screenshot displays the Cisco Identity Services Engine (ISE) interface. The top navigation bar includes 'Home', 'Context Visibility', 'Operations', 'Policy', 'Administration', and 'Work Centers'. The main content area is divided into several sections:

- INACTIVE ENDPOINTS**: Shows a list of endpoints with columns for 'MAC Address' and 'Status'. A modal window is open for 'Change Authorization' with a dropdown menu showing 'Rejected' selected. The modal also includes a search bar for 'MAC Address' and 'Status'.
- AUTHENTICATION STATUS**: Shows a list of endpoints with columns for 'Endpoint Profile' and 'Authentication Failure Reason'. A table below shows details for various endpoints.
- AUTHENTICATIONS**: Shows a donut chart representing authentication failure reasons. The chart data is as follows:

Failure Reason	Percentage
other	5.29%
22056...re(s)	3.86%
5440 ...d new	4.73%
12937...ssage	7%
12930...ssage	17.02%
24408...sword	22.9%

Releasing Rejected Endpoints

The screenshot displays the Cisco Identity Services Engine (ISE) interface. The top navigation bar includes 'Home', 'Context Visibility', 'Operations', 'Policy', 'Administration', and 'Work Centers'. The main content area is divided into 'Endpoints' (Users, Network Devices) and 'Authentication' (BYOD, Compliance, Compromised Endpoints, Endpoint Classification, Guest, Vulnerable Endpoints). The 'Inactive Endpoints' section shows 3500 endpoints. The 'Authentication Status' section shows a table of endpoints with their status. A modal window titled 'Change Authorization' is open, displaying a table with columns for 'MAC Address' and 'Status'. The table lists four MAC addresses: 1C:99:4C:2A:95:C2, 10:2A:B3:A0:AF:07, E4:98:D6:1C:7C:6C, and 24:A0:74:F2:DE:DC. The status for the first three is 'Rejected' (indicated by a red minus sign), and for the last one is 'Success' (indicated by a green plus sign). A callout box highlights the 'Release Rejected' button. A yellow box at the bottom states 'Query/Release Rejected also available via ERS API!'.

MAC Address	Status
1C:99:4C:2A:95:C2	Rejected
10:2A:B3:A0:AF:07	Rejected
E4:98:D6:1C:7C:6C	Rejected
24:A0:74:F2:DE:DC	Success

Release Rejected

Query/Release Rejected also available via ERS API!

No Log Suppression



With Log Suppression



Distributed Logging

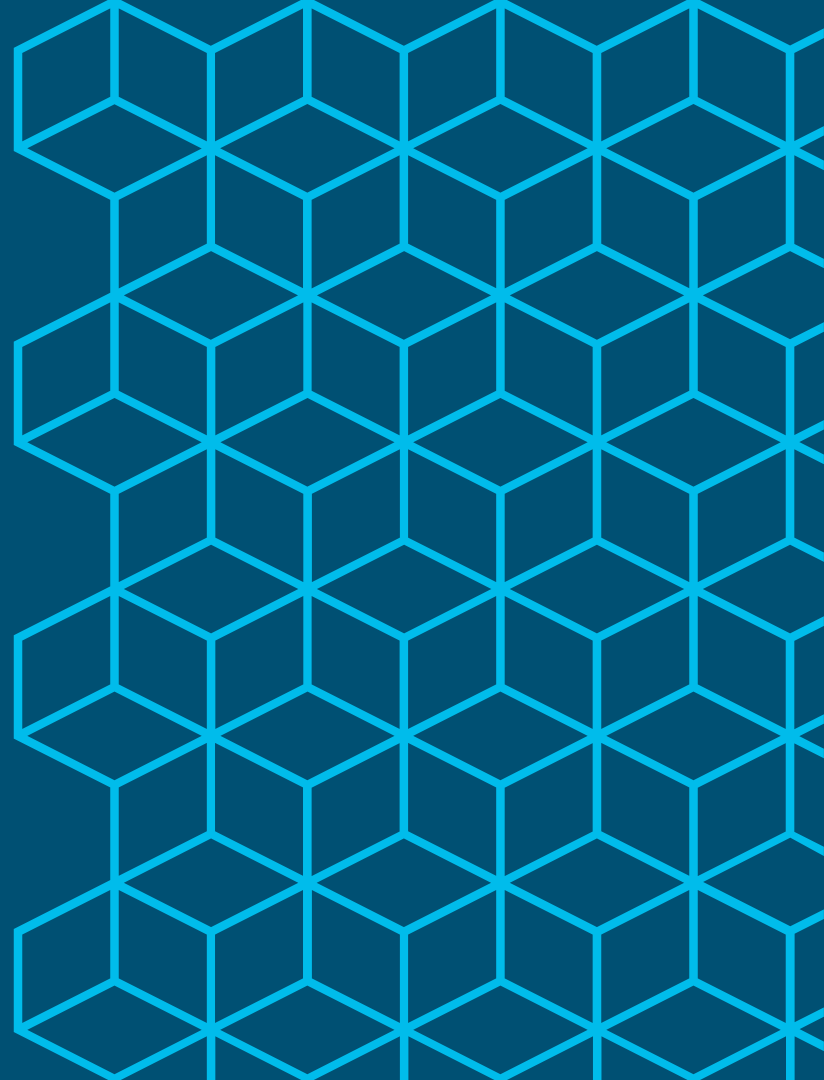


High Availability

High Availability Agenda

- ISE Appliance Redundancy
- ISE Node Redundancy
 - Administration Nodes
 - Monitoring Nodes
 - pxGrid Nodes
- HA for Certificate Services
- Policy Service Node Redundancy
 - Load Balancing
 - Non-LB Options
- NAD Fallback and Recovery

ISE Appliance Redundancy



Appliance Redundancy

In-Box High Availability

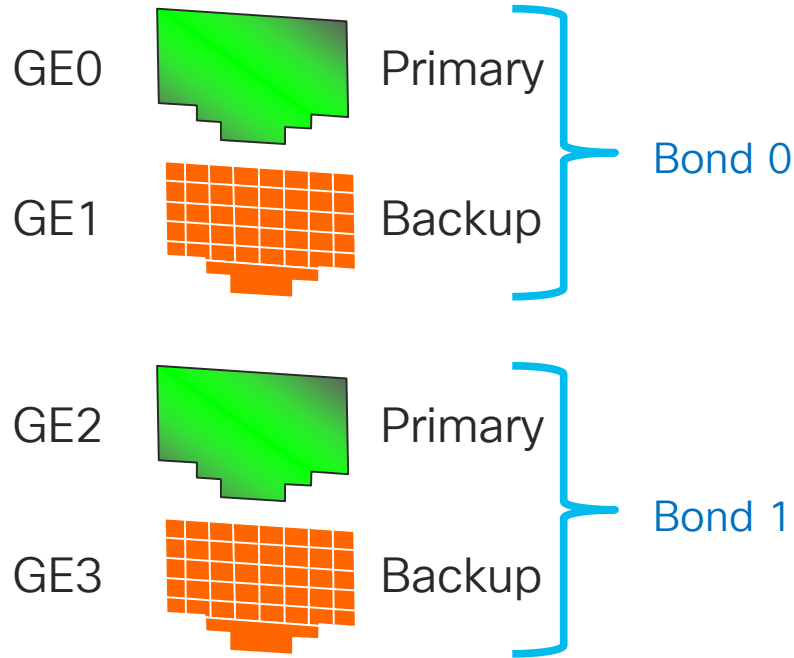
SNS-3500 Series

Platform	SNS-3415 (34x5 Small)	SNS-3495 (34x5 Large)	SNS-3515 (35x5 Small)	SNS-3595 (35x5 Large)
Drive Redundancy	No (1) 600GB disk	Yes (2) 600-GB	No (1) 600GB disk	Yes (4) 600GB disk
Controller Redundancy	No	Yes (RAID 1)	No (1GB FBWC Controller Cache)	Yes (RAID 10) (1GB FBWC Cache)
Ethernet Redundancy	Yes* 4 GE NICs = Up to 2 bonded NICs	Yes* 4 GE NICs = Up to 2 bonded NICs	Yes* 6 GE NICs = Up to 3 bonded NICs	Yes* 6 GE NICs = Up to 3 bonded NICs
Redundant Power	No (2 nd PSU optional) UCSC-PSU-650W	Yes	No (2 nd PSU optional) UCSC-PSU1-770W	Yes

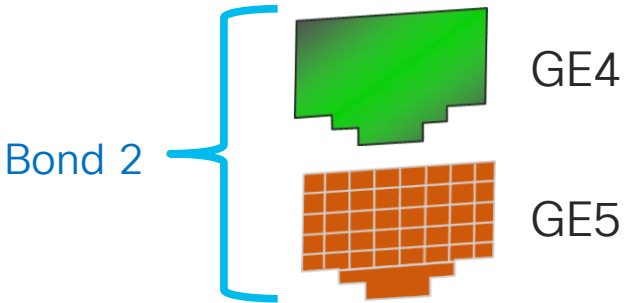
* ISE 2.1 introduced NIC Teaming support for High Availability only (not active/active)

NIC Bonding

Network Card Redundancy

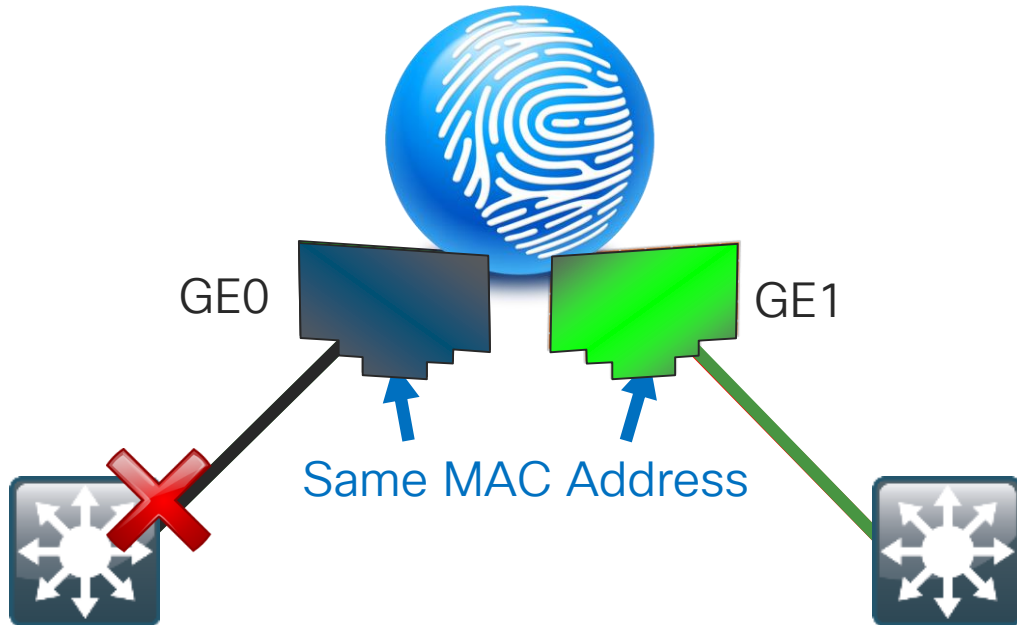


- For Redundancy only–NOT for increasing bandwidth.
- Up to (3) bonds in ISE 2.1
- Bonded Interfaces Preset–Non-Configurable



Bonded Interfaces for Redundancy

When GE0 is Down, GE1 Takes Over



- Both interfaces assume the same L2 address.
- When GE0 fails, GE1 assumes the IP address and keeps the communications alive.
- Based on Link State of the Primary Interface
- Every 100 milliseconds the link state of the Primary is inspected.

NIC Teaming

NIC Teaming / Interface Bonding

- Configured using CLI only!
- GE0 + GE1 Bonding Example:
admin(config-GigabitEthernet0) # **backup interface GigabitEthernet 1**
- Requires service restart. After restart, ISE recognizes bonded interfaces for Deployment and Profiling; Guest requires manual config of eligible interfaces.

```
interface GigabitEthernet 0
  ipv6 address autoconfig
  ipv6 enable
  backup interface GigabitEthernet 1
  ip address 10.1.100.18 255.255.255.0
?
interface GigabitEthernet 1
  ipv6 address autoconfig
```

Edit Node

General Settings **Profiling Configuration**

DHCP

Interface

Port GigabitEthernet 2

Description GigabitEthernet 3

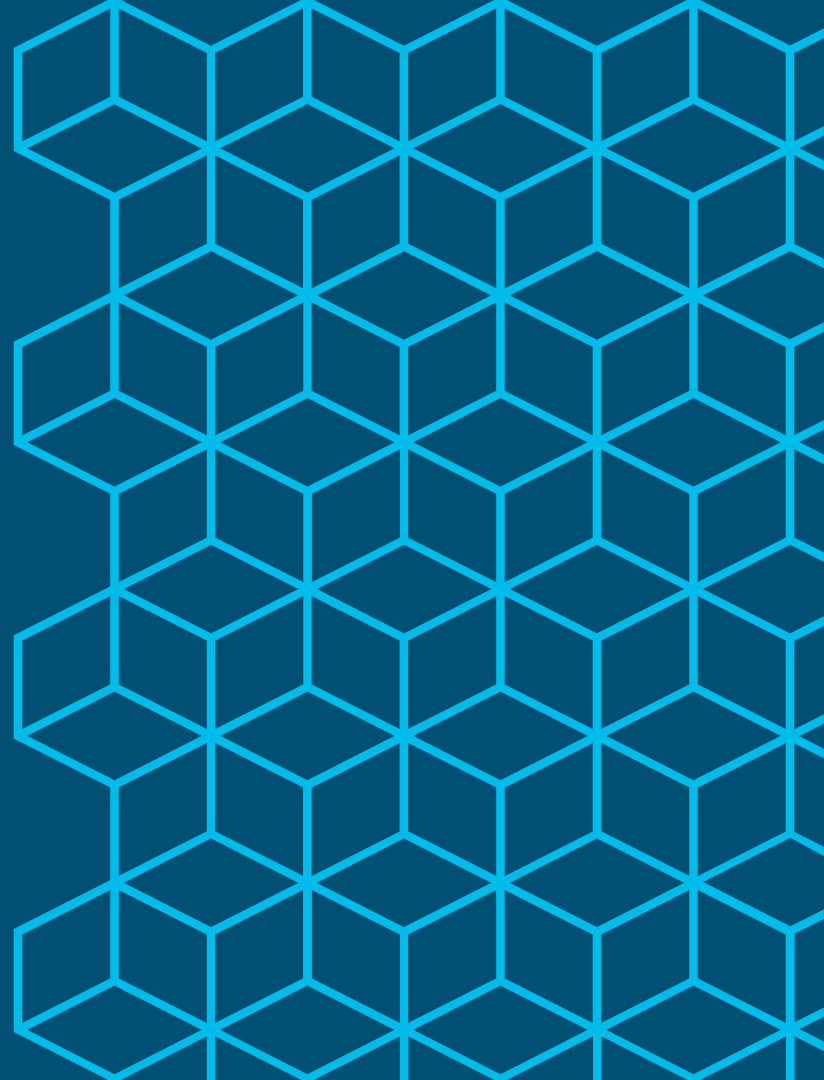
All

Allowed Make selections in one or both columns based on your PSN configurations.

interfaces: If bonding is **not** configured ⓘ
* on a PSN, use:

<input checked="" type="checkbox"/> Gigabit Ethernet 0	<input type="checkbox"/> Bond 0 <i>Uses Gigabit Ethernet 0 as primary, 1 as backup.</i>
<input checked="" type="checkbox"/> Gigabit Ethernet 1	<input checked="" type="checkbox"/> Bond 1 <i>Uses Gigabit Ethernet 2 as primary, 3 as backup.</i>
<input type="checkbox"/> Gigabit Ethernet 2	<input type="checkbox"/> Bond 2 <i>Uses Gigabit Ethernet 4 as primary, 5 as backup.</i>
<input type="checkbox"/> Gigabit Ethernet 3	
<input checked="" type="checkbox"/> Gigabit Ethernet 4	
<input type="checkbox"/> Gigabit Ethernet 5	

ISE Node/Persona Redundancy

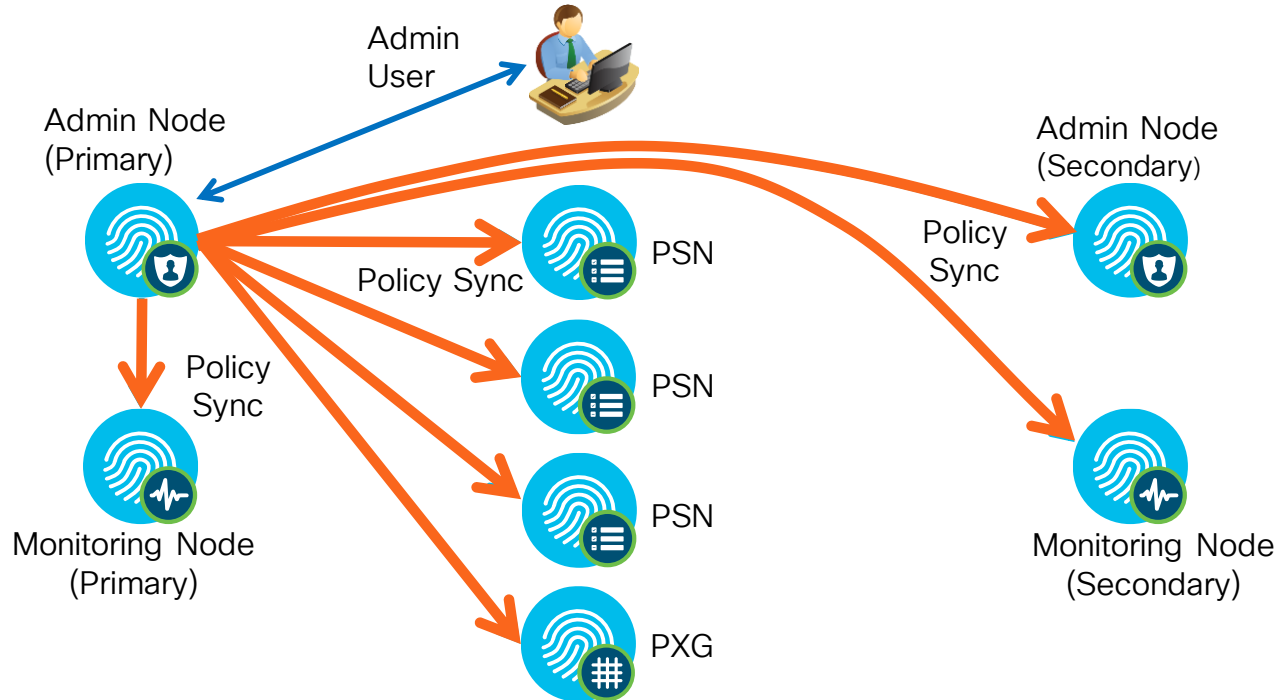


Admin Node HA and Synchronization

PAN Steady State Operation

- Changes made to Primary Administration DB are automatically synced to all nodes.

- Maximum two PAN nodes per deployment
- Active / Standby



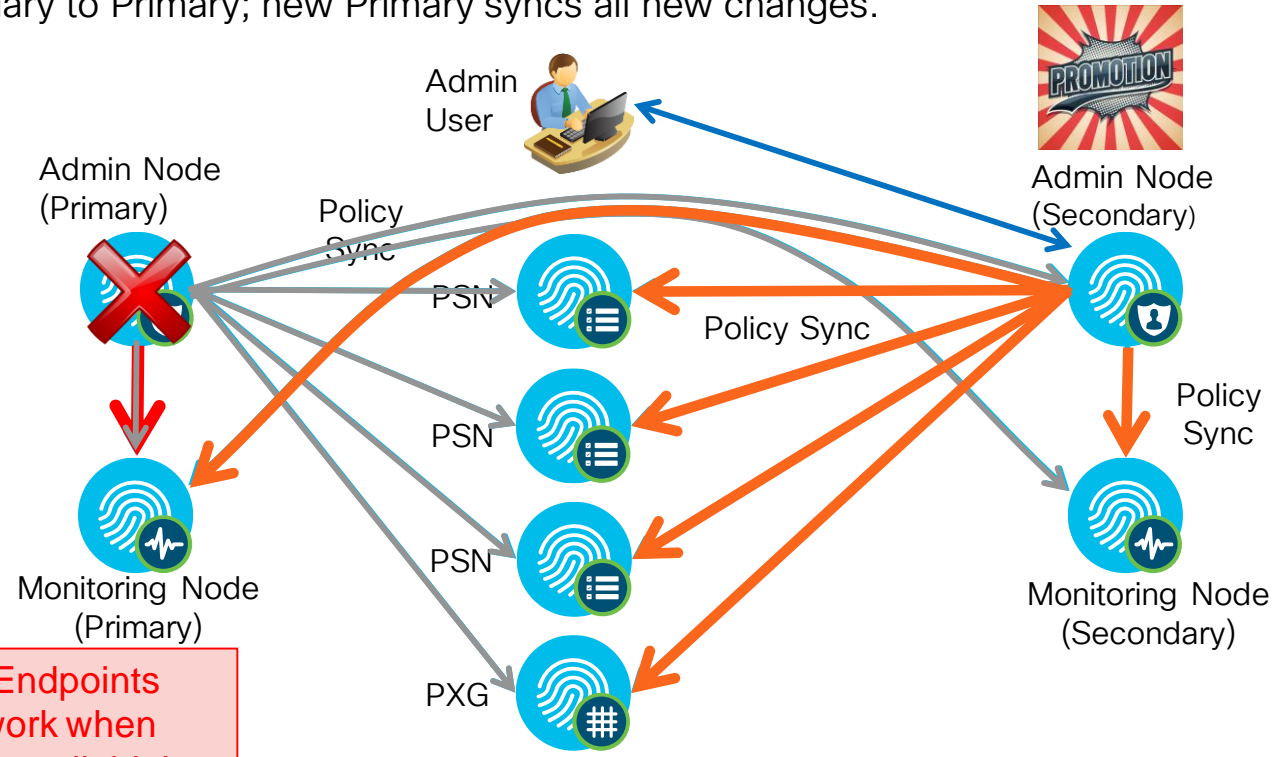
Admin Node HA and Synchronization

Primary PAN Outage and Recovery

- Prior to ISE 1.4, upon Primary PAN failure, admin user must connect to Secondary PAN and **manually promote** Secondary to Primary; new Primary syncs all new changes.
- PSNs buffer endpoint updates if Primary PAN unavailable; buffered updates sent once PAN available.

Promoting Secondary Admin may take 10-15 minutes before process is complete.

New Guest Users or Registered Endpoints cannot be added/connect to network when Primary Administration node is unavailable!



Policy Service Survivability When Admin Down/Unreachable

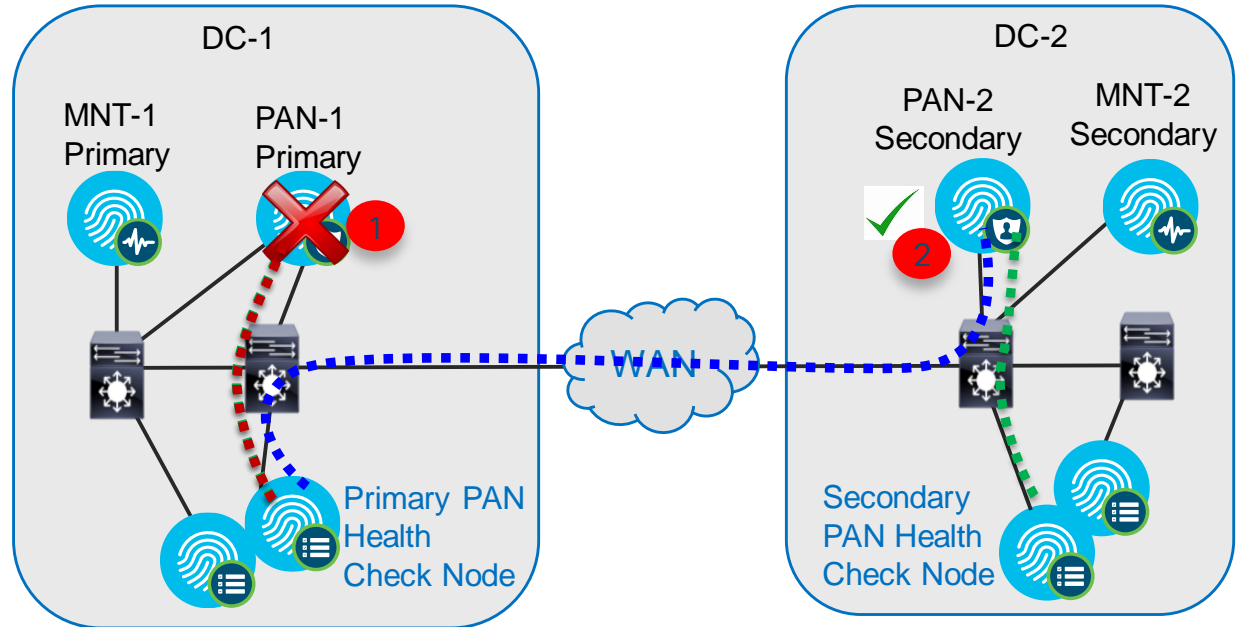
Which User Services Are Available if Primary Admin Node Is Unavailable?

Service	Use case	Works (Y / N)
RADIUS Auth	Generally all RADIUS auth should continue provided access to ID stores	Y
Guest	All existing guests can be authenticated, but new guests, self-registered guests, or guest flows relying on device registration will fail.	N
Profiler	Previously profiled endpoints can be authenticated with existing profile. New endpoints or updates to existing profile attributes received by owner should apply, but not profile data received by PSN in foreign node group.	Y
Posture	Provisioning/Assessment work, but Posture Lease unable to fetch timer.	Y
Device Reg	Device Registration fails if unable to update endpoint record in central db.	N
BYOD/NSP	BYOD/NSP relies on device registration. Additionally, any provisioned certificate cannot be saved to database.	N
MDM	MDM fails on update of endpoint record	N
CA/Cert Services	See BYOD/NSP use case; certificates can be issued but will not be saved and thus fail. OCSP functions using last replicated version of database	N
pxGrid	Clients that are already authorized for a topic and connected to controller will continue to operate, but new registrations and connections will fail.	N
TACACS+	TACACS+ requests can be locally processed per ID store availability.	Y

Automatic PAN Switchover

Introduced ISE 1.4

- Primary PAN (PAN-1) down or network link down.
- If Health Check Node unable to reach PAN-1 but can reach PAN-2 → trigger failover
- Secondary PAN (PAN-2) is promoted by Health Check Node
- PAN-2 becomes Primary and takes over PSN replication.



Don't forget, after switchover admin must connect to PAN-2 for ISE management!

Note: Switchover is NOT immediate. Total time based on polling intervals and promotion time. Expect ~15 - 30 minutes.

PAN Failover

Health Check Node Configuration

- Configuration using GUI only under [Administration > System > Deployment > PAN Failover](#)

Health Check Node CANNOT be a PAN !!

Requires Minimum of 3 nodes – 3rd node is independent observer

Primary Administration Node: npf-sjca-pap01.cisco.com

Secondary Administration Node: npf-sjca-pap02.cisco.com

Configuration Details:

- * Enable PAN Auto Failover:
- * Primary Health Check Node: npf-sjca-mnt01.cisco.com
- * Secondary Health Check Node: npf-sjca-mnt02.cisco.com
- * Polling Interval: 120 (Seconds (Range 30 - 300))
- * Number Of Failure Polls Before Failover: 5 (Count (Range 2 - 60))

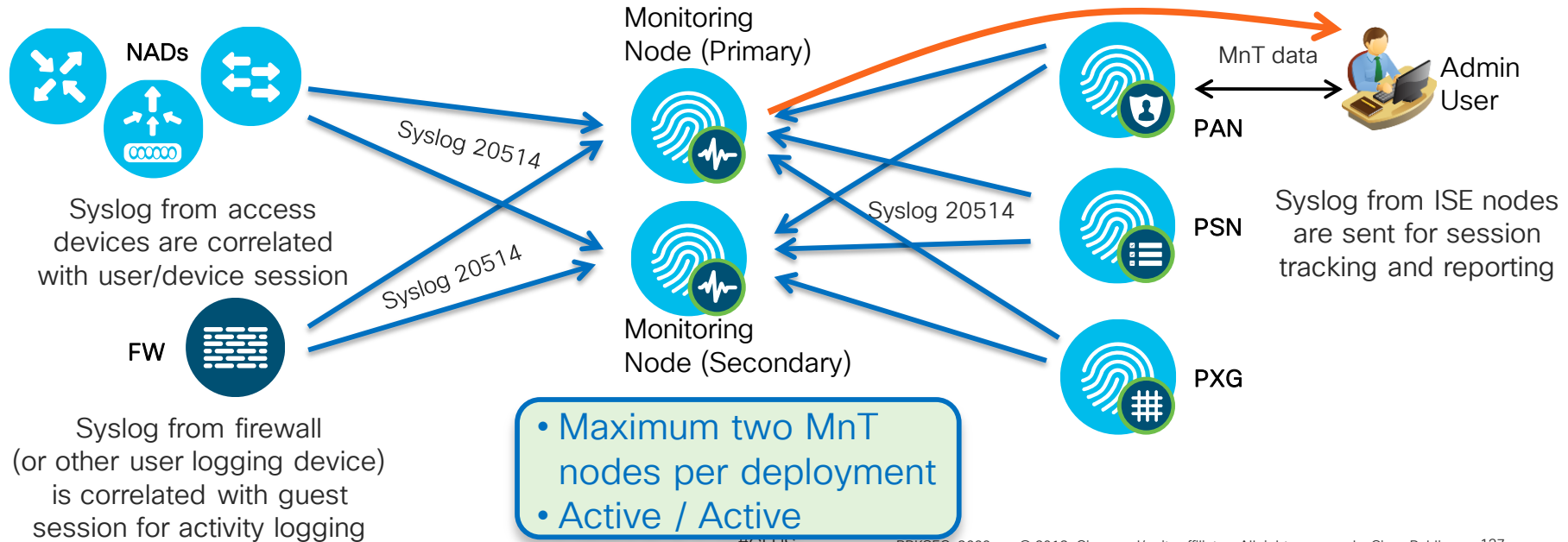
Deployment Tree:

- Deployment
 - bxb22-11a-pdp1
 - npf-sjca-ipep01
 - npf-sjca-ipep02
 - npf-sjca-mnt01
 - npf-sjca-mnt02
 - npf-sjca-pap01
 - npf-sjca-pap02
 - sbg-bgla-pdp01
 - AlphaNodeGroup
 - PAN Failover**

HA for Monitoring and Troubleshooting

Steady State Operation

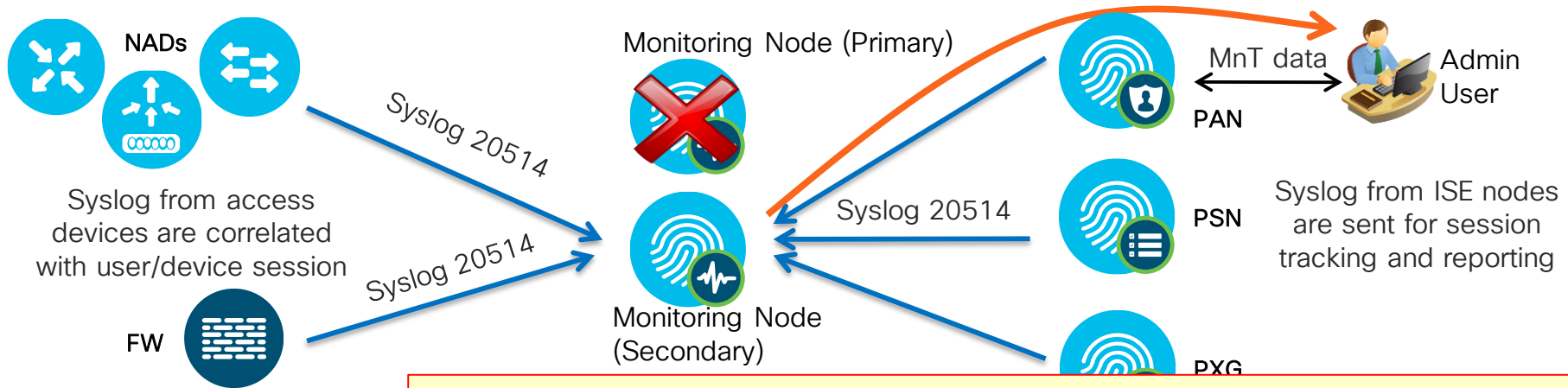
- MnT nodes concurrently receive logging from PAN, PSN, IPN*, NAD, and ASA
- PAN retrieves log/report data from Primary MnT node when available



HA for Monitoring and Troubleshooting

Primary MnT Outage and Recovery

- Upon MnT node failure, PAN, PSN, NAD, and ASA continue to send logs to remaining MnT node
- PAN auto-detects Active MnT failure and retrieves log/report data from Secondary MnT node.
- Full failover to Secondary MnT may take from 5-15 min depending on type of failure.



Syslog from access devices are correlated with user/device session

Syslog from firewall (or other user logging device) is correlated with guest session for activity logging

- PSN logs are not locally buffered when MnT down unless use TCP/Secure syslog.
- Log DB is not synced between MnT nodes.
- Upon return to service, recovered MnT node will not include data logged during outage
- Backup/Restore required to re-sync MnT database

Log Buffering

TCP and Secure Syslog Targets

- Default UDP-based audit logging does not buffer data when MnT is unavailable.
- TCP and Secure Syslog options can be used to buffer logs locally
- Note: Overall log performance will decrease if use these acknowledged options.

The screenshot displays the Cisco Identity Services Engine (ISE) Administration interface. The breadcrumb navigation shows 'Remote Logging Targets List > TCPLogCollector'. The 'Logging Target' configuration page for 'TCPLogCollector' is shown with the following details:

- Name:** TCPLogCollector
- Description:** TCP SysLog collector
- Target Type:** TCP SysLog
- Status:** Enabled
- IP Address:** 10.1.100.13
- Port:** 1468
- Facility Code:** LOCAL6
- Maximum Length:** 1024 (Valid Range 200 to 1024)
- Buffer Messages When Server Down:**
- Buffer Size (MB):** 100 (Valid Range 10 to 100)
- Reconnect Timeout (Sec):** 30 (Valid Range 30 to 120)

Buttons for 'Save' and 'Reset' are visible at the bottom of the configuration area.

HA for pxGrid v1

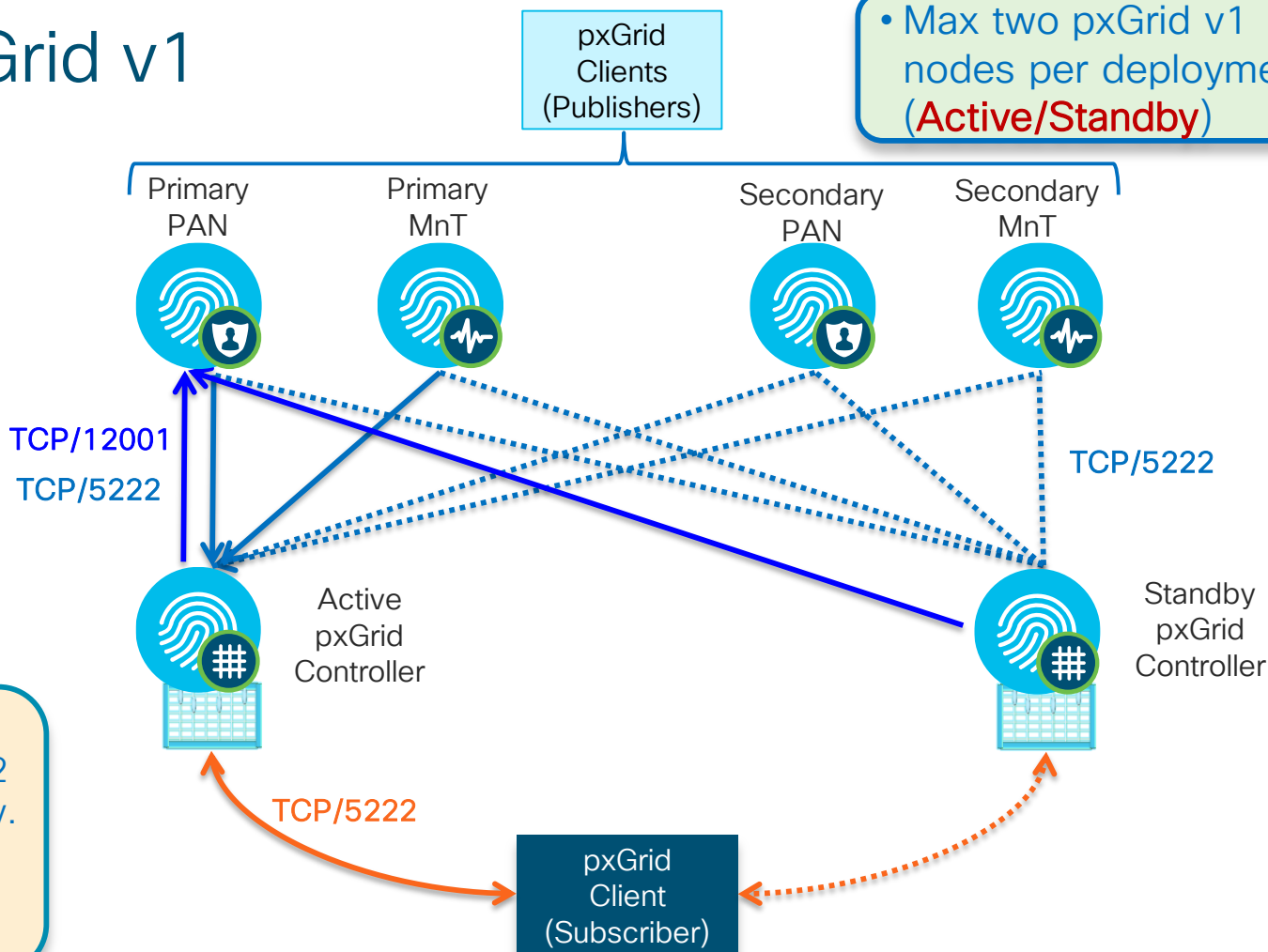
Steady State

• Max two pxGrid v1 nodes per deployment (**Active/Standby**)

- PAN Publisher Topics:
- Controller Admin
 - TrustSec/SGA
 - Endpoint Profile

- MnT Publisher Topics:
- Session Directory
 - Identity Group
 - ANC (EPS)

- pxGrid clients can be configured with up to 2 servers for redundancy.
- Clients connect to single active controller for given domain



HA for pxGrid v1

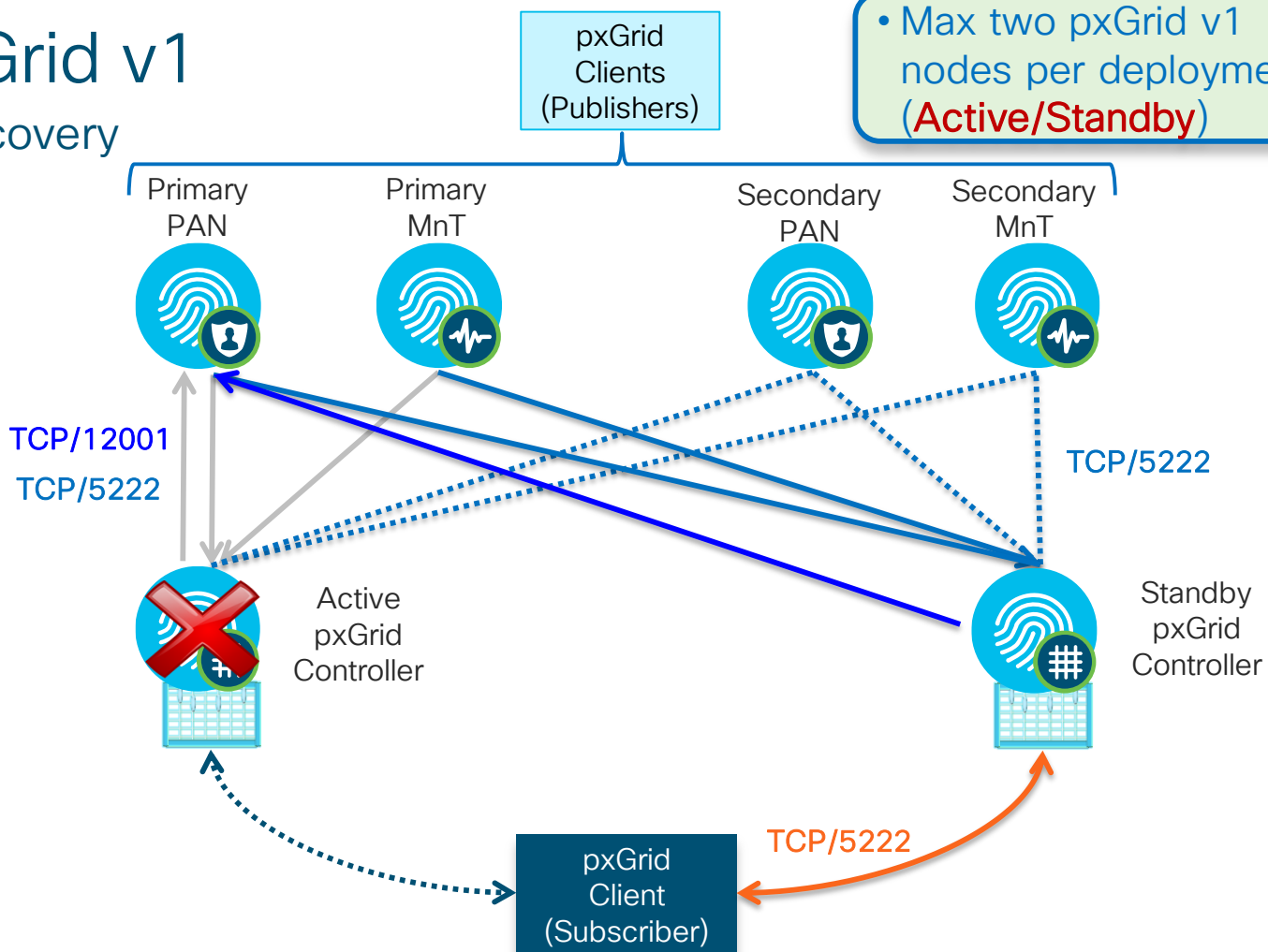
Failover and Recovery

• Max two pxGrid v1 nodes per deployment (**Active/Standby**)

- PAN Publisher Topics:
- Controller Admin
 - TrustSec/SGA
 - Endpoint Profile

- MnT Publisher Topics:
- Session Directory
 - Identity Group
 - ANC (EPS)

If active pxGrid Controller fails, clients automatically attempt connection to standby controller.



HA for pxGrid v2 (ISE 2.3+)

Steady State

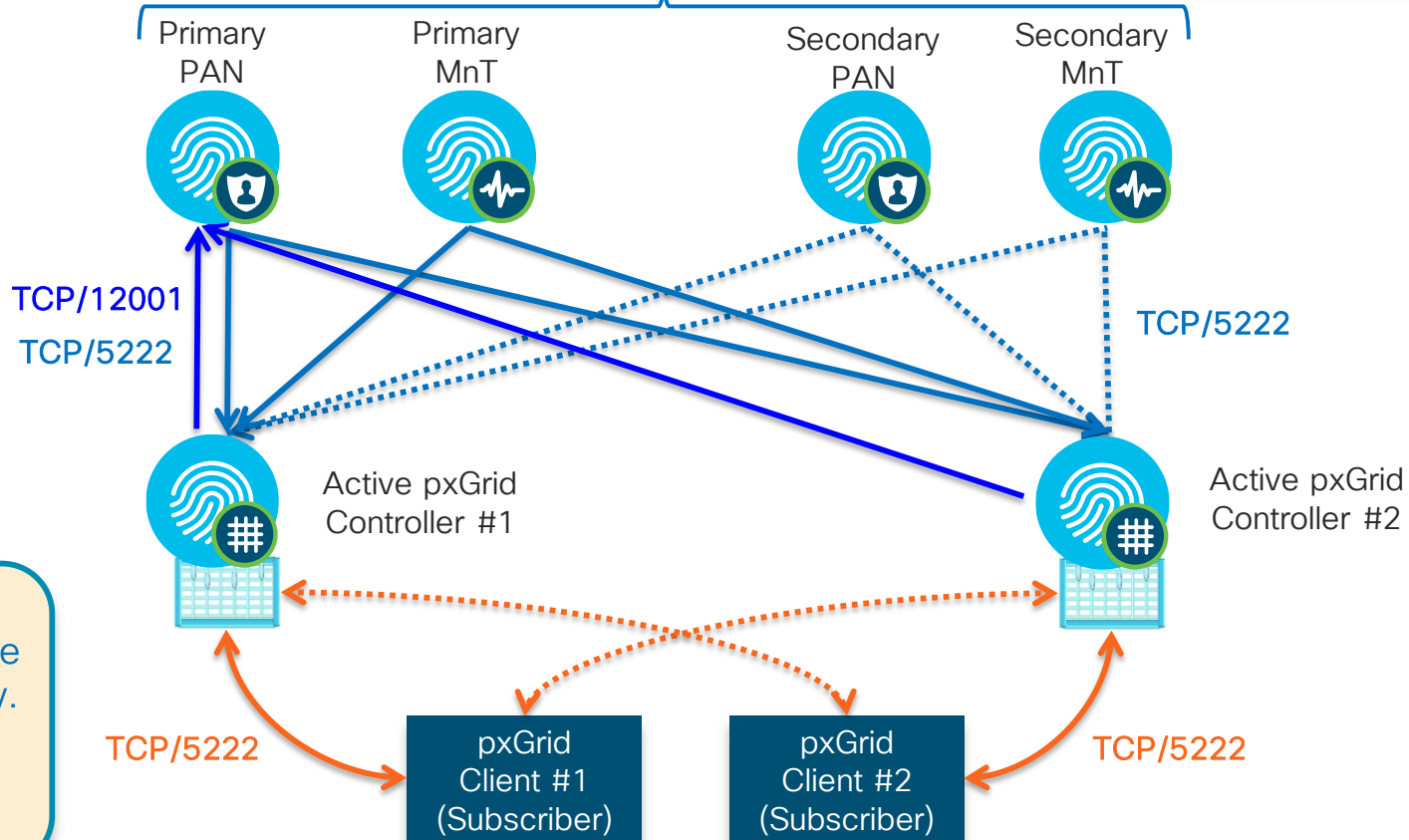
pxGrid Clients
(Publishers)

- 2.3: Max two pxGrid v2 nodes/ deployment (**Active/Active**)
- 2.4: Max 4 nodes (**All Active**)

- PAN Publisher Topics:
- Controller Admin
 - TrustSec/SGA
 - Endpoint Profile

- MnT Publisher Topics:
- Session Directory
 - Identity Group
 - ANC (EPS)

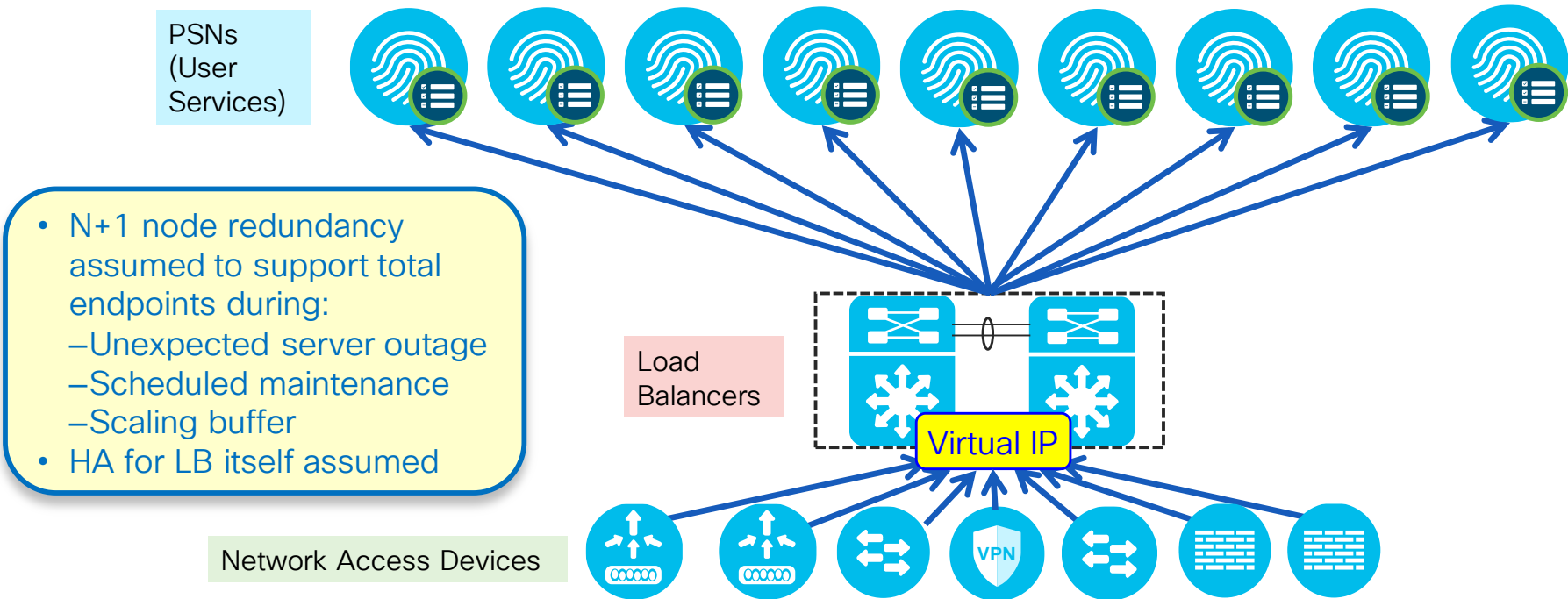
- pxGrid clients can be configured with multiple servers for redundancy.
- Clients connect to single active controller for given domain



PSN Load Balancing

Load Balancing RADIUS, Web, and Profiling Services

- Policy Service nodes can be configured in a cluster behind a load balancer (LB).
- Access Devices send RADIUS and TACACS+ AAA requests to LB virtual IP.

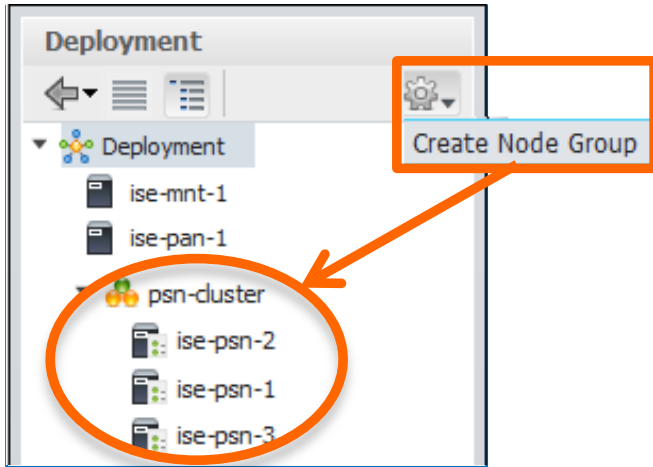


Configure Node Groups for LB Cluster

Place all PSNs in LB Cluster in Same Node Group

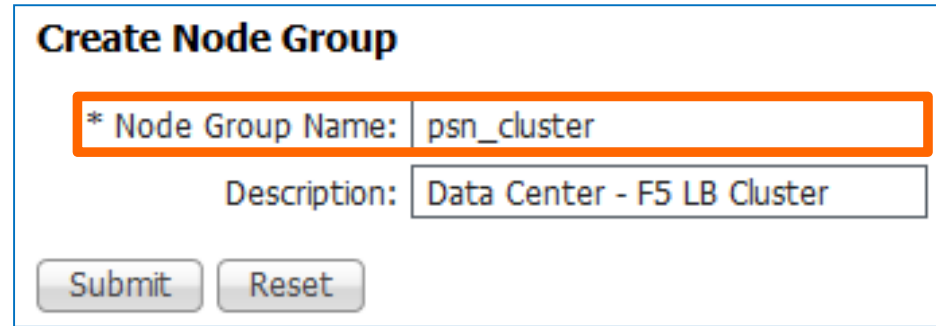
- Administration > System > Deployment

1) Create node group



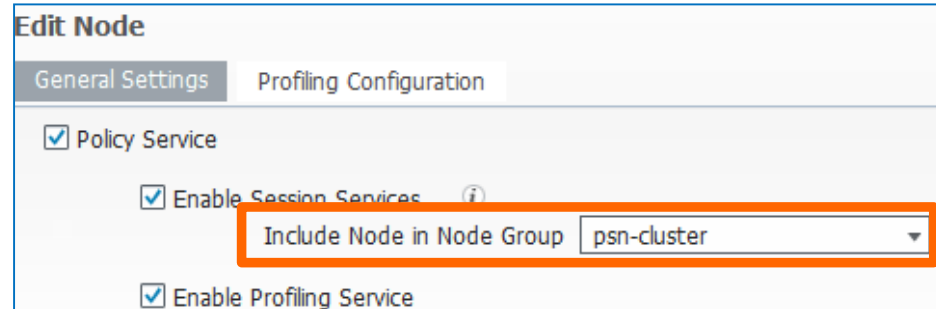
- Node group members can be L2 or L3
- Multicast not required

2) Assign name



The 'Create Node Group' form is shown. The '* Node Group Name' field is highlighted in orange and contains the text 'psn_cluster'. The 'Description' field contains the text 'Data Center - F5 LB Cluster'. There are 'Submit' and 'Reset' buttons at the bottom.

3) Add individual PSNs to node group

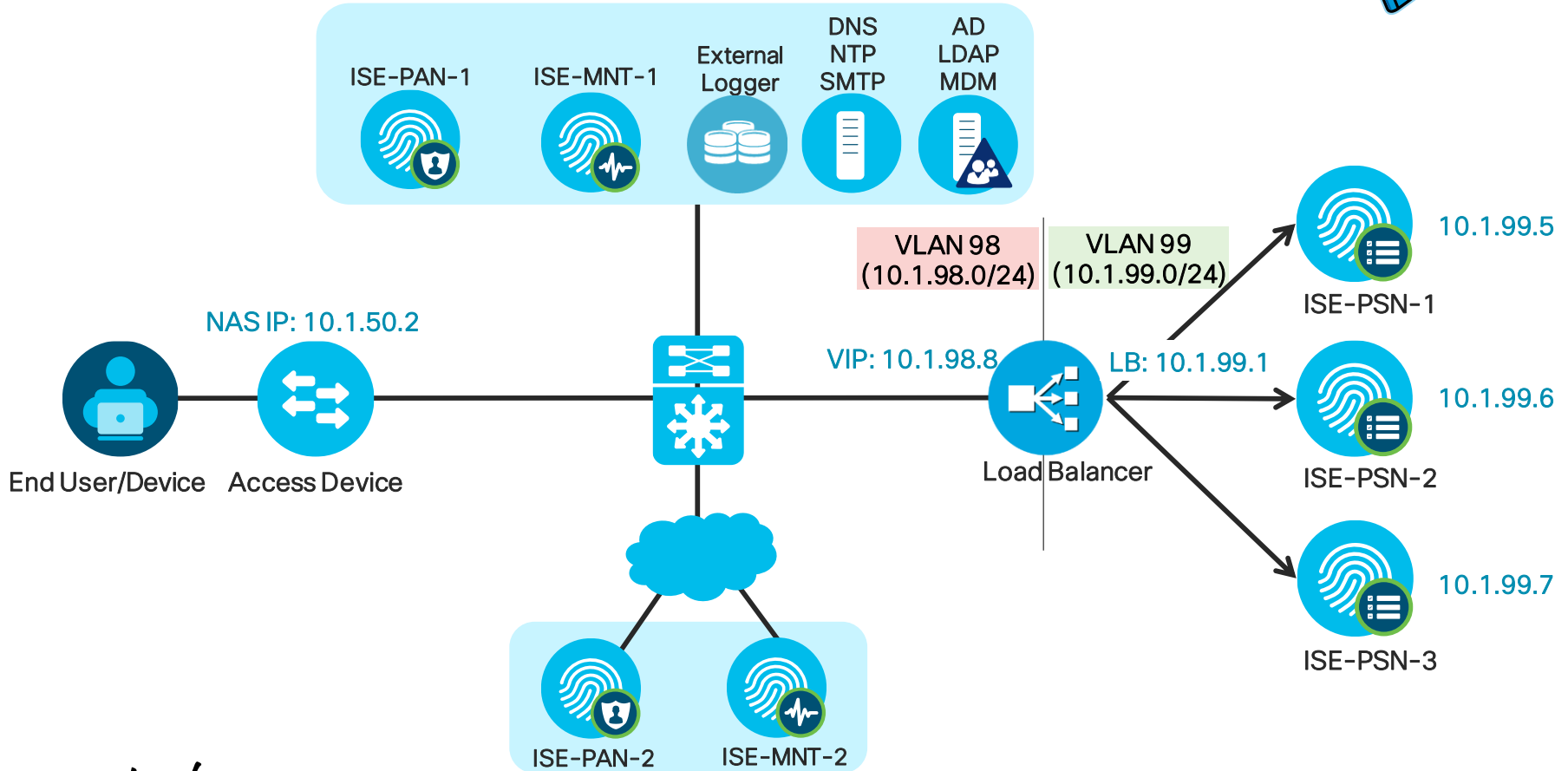


The 'Edit Node' page is shown. The 'General Settings' tab is active. The 'Policy Service' checkbox is checked. The 'Include Node in Node Group' dropdown menu is highlighted in orange and set to 'psn-cluster'. The 'Enable Profiling Service' checkbox is also checked.

High-Level Load Balancing Diagram



For Your Reference

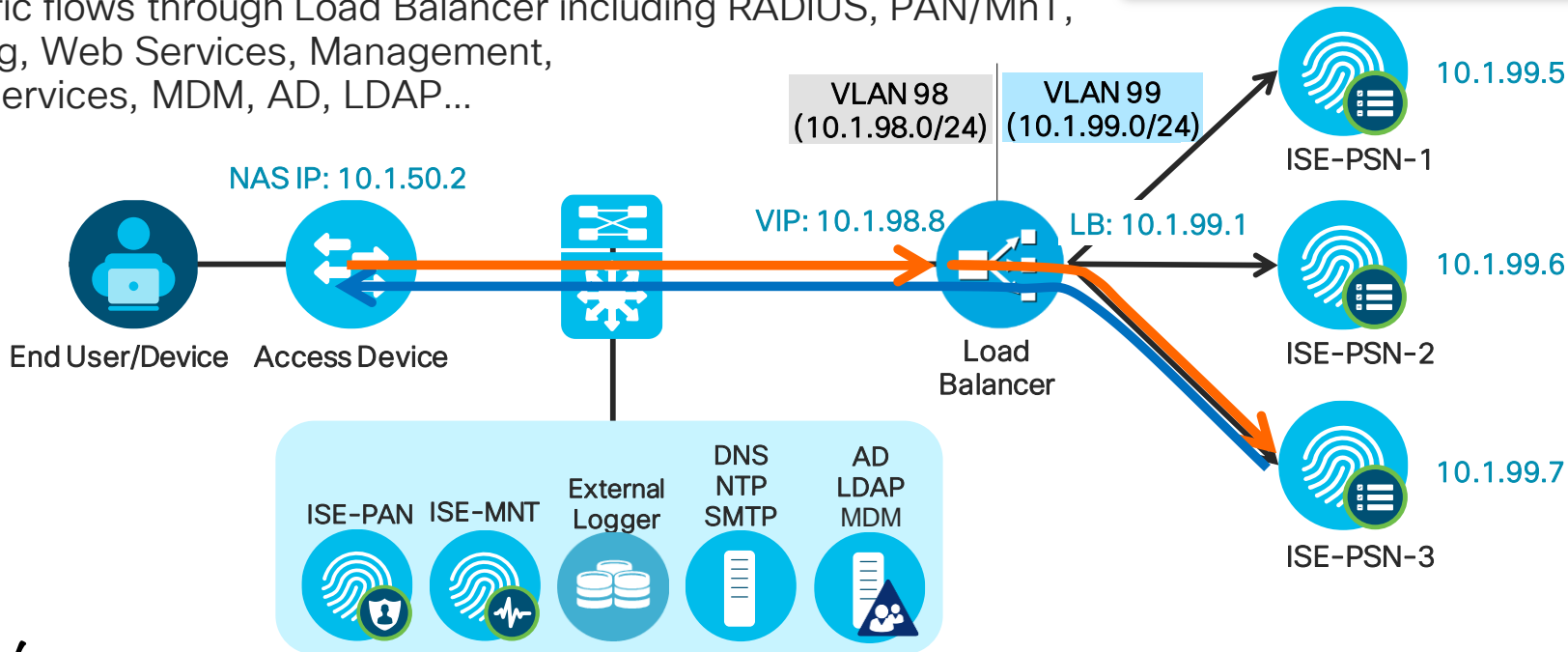


Traffic Flow—Fully Inline: Physical Separation

Physical Network Separation Using Separate LB Interfaces

Fully Inline Traffic Flow recommended—physical or logical

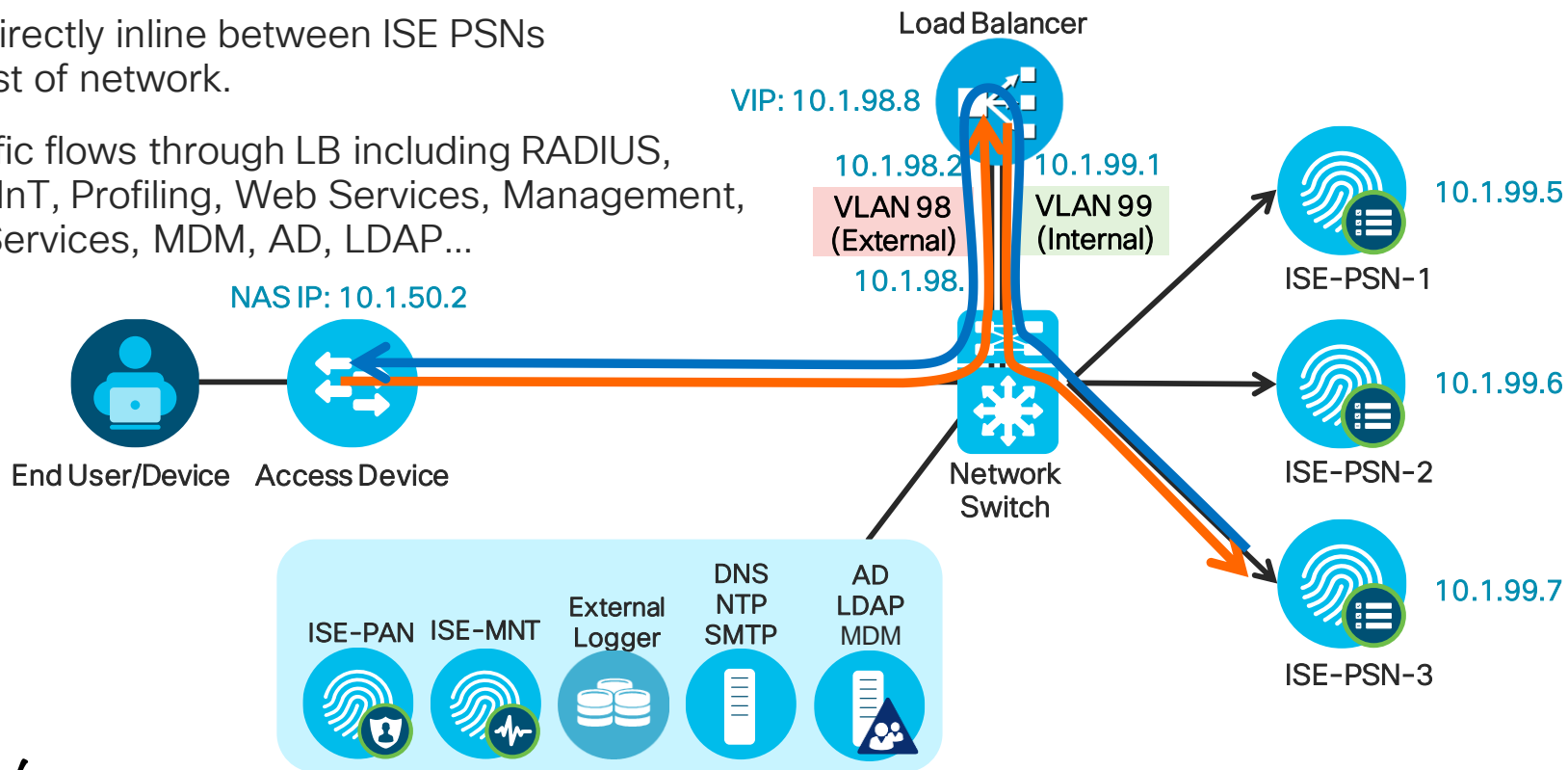
- Load Balancer is directly inline between PSNs and rest of network.
- All traffic flows through Load Balancer including RADIUS, PAN/MnT, Profiling, Web Services, Management, Feed Services, MDM, AD, LDAP...



Traffic Flow—Fully Inline: VLAN Separation

Logical Network Separation Using Single LB Interface and VLAN Trunking

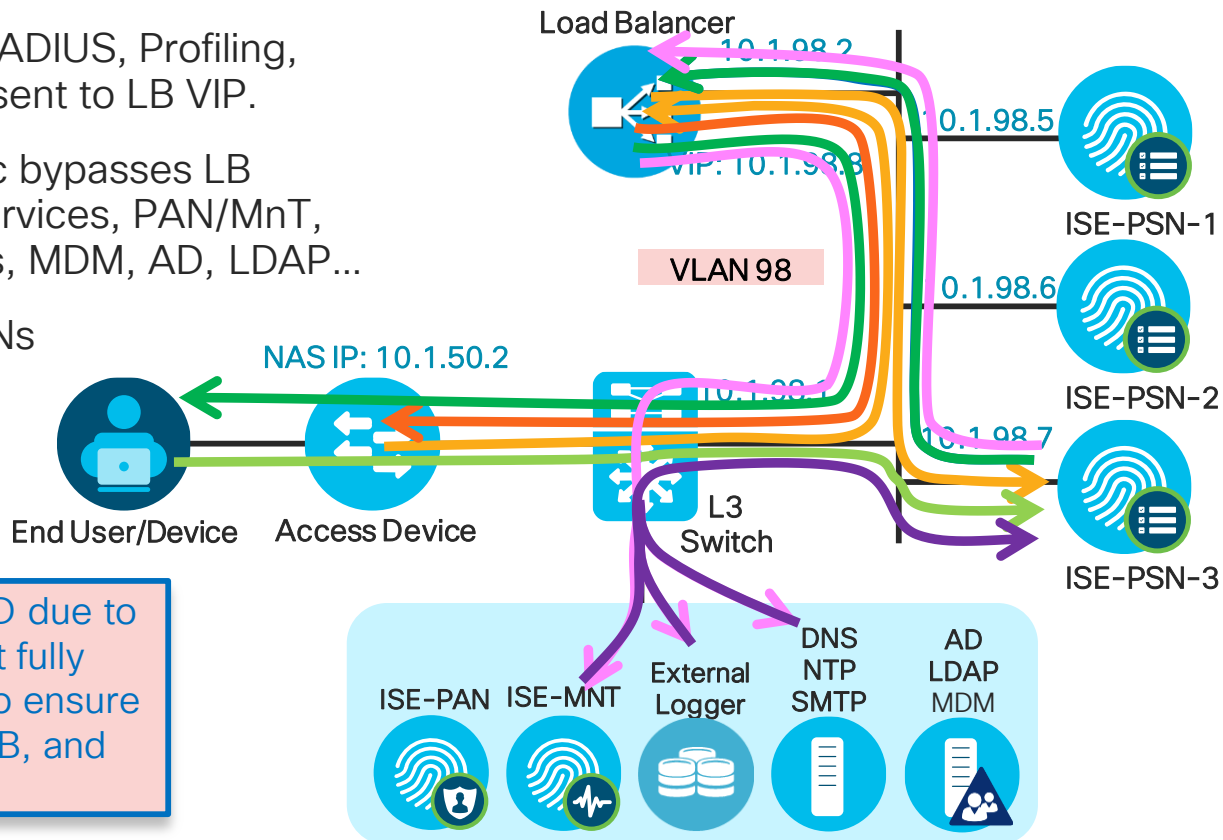
- LB is directly inline between ISE PSNs and rest of network.
- All traffic flows through LB including RADIUS, PAN/MnT, Profiling, Web Services, Management, Feed Services, MDM, AD, LDAP...



Partially Inline: Layer 2/Same VLAN (One PSN Interface)

Direct PSN Connections to LB and Rest of Network

- All inbound LB traffic such as RADIUS, Profiling, and directed Web Services sent to LB VIP.
- Other inbound non-LB traffic bypasses LB including redirected Web Services, PAN/MnT, Management, Feed Services, MDM, AD, LDAP...
- All outbound traffic from PSNs sent to LB as DFGW.
- LB must be configured to allow Asymmetric traffic



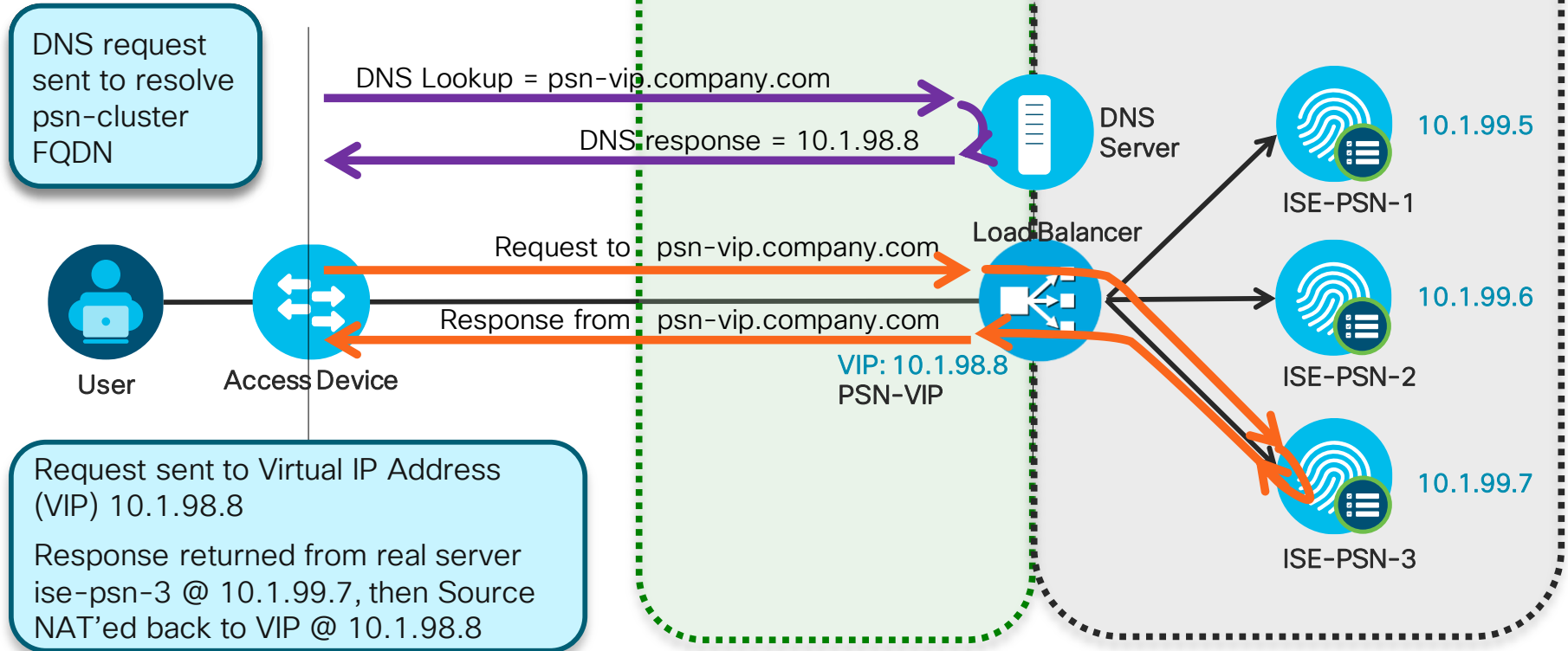
Generally NOT RECOMMENDED due to traffic flow complexity—must fully understand path of each flow to ensure proper handling by routing, LB, and end stations.

PSN Load Balancing

Sample Topology and Flow



For Your Reference



Load Balancing Policy Services

- **RADIUS AAA Services**

Packets sent to LB virtual IP are load-balanced to real PSN based on configured algorithm. Sticky algorithm determines method to ensure same Policy Service node services same endpoint.

- **Web Services:**

- **URL-Redirected:** Posture (CPP) / Central WebAuth (CWA) / Native Supplicant Provisioning (NSP) / Hotspot / Device Registration WebAuth (DRW), Partner MDM.

No LB Required! PSN that terminates RADIUS returns URL Redirect with its own certificate CN name substituted for 'ip' variable in URL.

Direct HTTP/S: Local WebAuth (LWA) / Sponsor / MyDevices Portal, OCSP

Single web portal domain name should resolve to LB virtual IP for http/s load balancing.

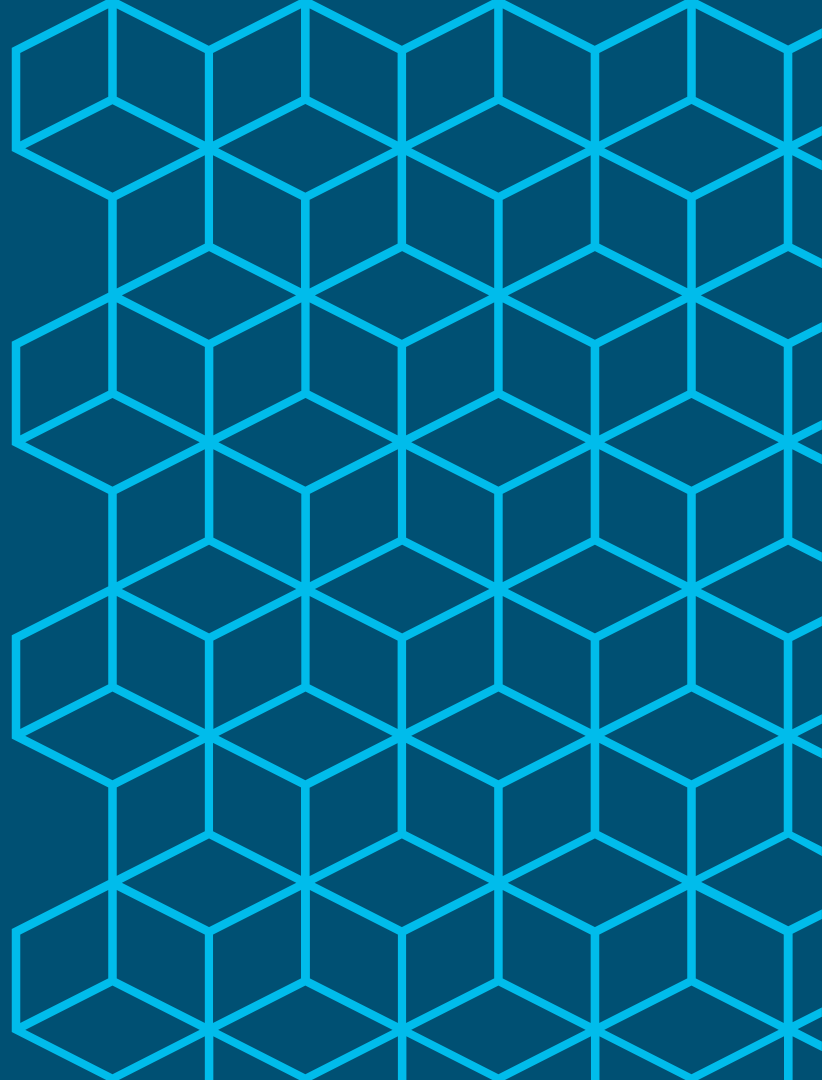
- **Profiling Services:** DHCP Helper / SNMP Traps / Netflow / RADIUS

LB VIP is the target for one-way Profile Data (no response required). VIP can be same or different than one used by RADIUS LB; Real server interface can be same or different than one used by RADIUS

- **TACACS+ AAA Services: (Session and Command Auth and Accounting)**

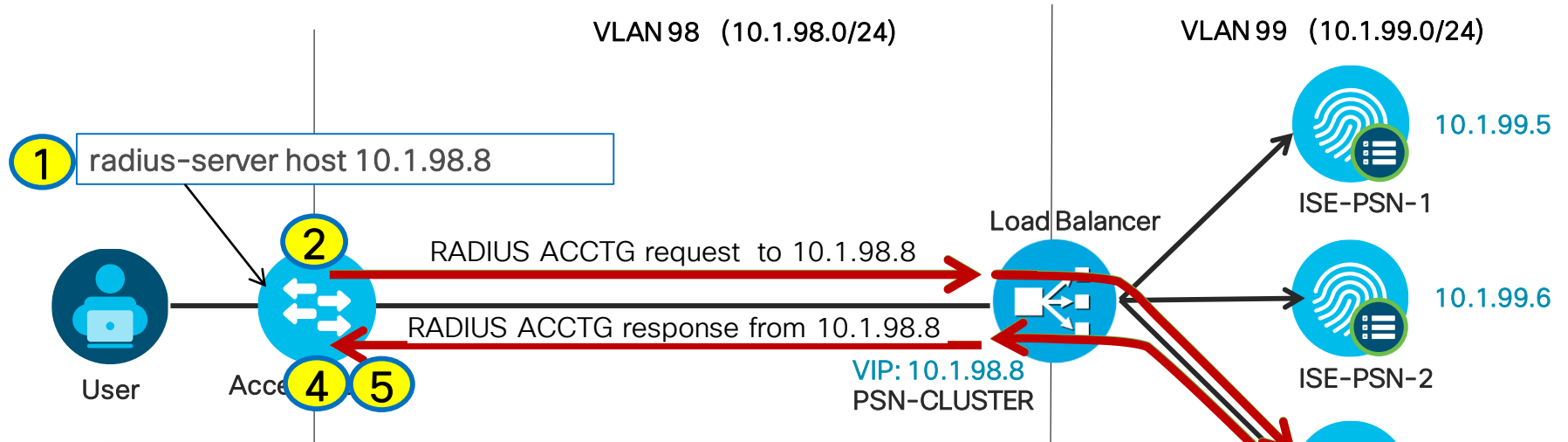
LB VIP is target for TACACS+ requests. T+ not session based like RADIUS, so not required that requests go to same PSN

Load Balancing RADIUS



Load Balancing RADIUS

Sample Flow



1. NAD has single RADIUS Server defined (10.1.98.8)
2. RADIUS Auth requests sent to VIP @ 10.1.98.8
3. Requests for same endpoint load balanced to same PSN via sticky based on RADIUS Calling-Station-ID and Framed-IP-Address
4. RADIUS response received from VIP @ 10.1.98.8
(originated by real server ise-psn-3 @ 10.1.99.7 and source translated by LB)
5. RADIUS Accounting sent to/from same PSN based on sticky

Load Balancer Persistence (Stickiness) Guidelines

Persistence Attributes

- Common RADIUS Sticky Attributes

- **Client Address**

- Calling-Station-ID → MAC Address=00:C0:FF:1A:2B:3C
- Framed-IP-Address → IP Address=10.1.10.101

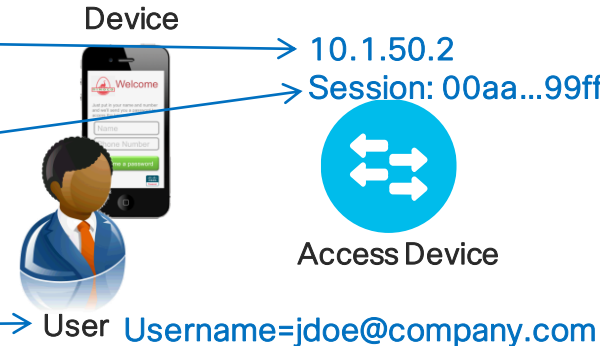
- **NAD Address**

- NAS-IP-Address
- Source IP Address

- **Session ID**

- RADIUS Session ID
- Cisco Audit Session ID

- **Username**



- Best Practice Recommendations (depends on LB support and design)

1. Calling-Station-ID for persistence across NADs and sessions
2. Source IP or NAS-IP-Address for persistence for all endpoints connected to same NAD
3. Audit Session ID for persistence across re-authentications

Load Balancer Stickiness Guidelines

Config Examples Based on Calling-Station-ID (MAC Address)

- Cisco ACE Example:

```
sticky radius framed-ip calling-station-id RADIUS-STICKY  
serverfarm ise-psn
```

- F5 LTM iRule Example:

```
ltm rule RADIUS_iRule {  
  when CLIENT_ACCEPTED {  
    persist uie [RADIUS::avp 31]  
  }  
}
```

Be sure to monitor load balancer resources when performing advanced parsing.

- Citrix NetScaler Example:

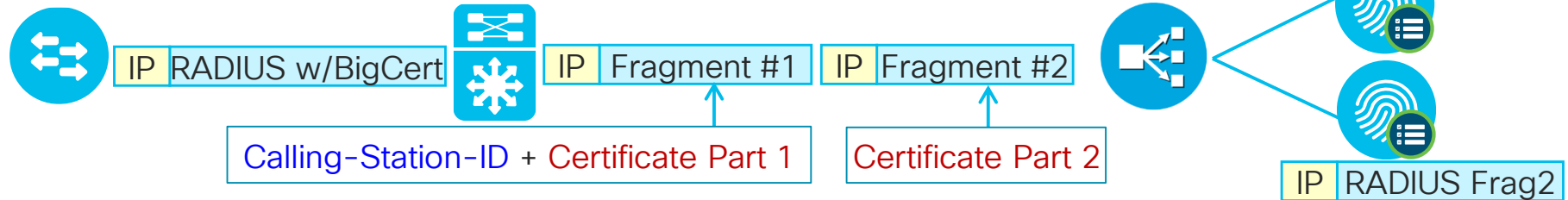
```
add lb vserver radius-auth RADIUS 172.16.0.16 1812 -rule "CLIENT.UDP.RADIUS.ATTR_TYPE(31)" -cltTimeout 120  
add lb vserver radius-acct RADIUS 172.16.0.16 1813 -rule "CLIENT.UDP.RADIUS.ATTR_TYPE(31)" -cltTimeout 120  
set lb group RADIUS-Calling-Station-ID -persistenceType RULE -rule "CLIENT.UDP.RADIUS.ATTR_TYPE(31)"
```

LB Fragmentation and Reassembly

Be aware of load balancers that do not reassemble RADIUS fragments!

Also watch for fragmented packets that are too small. LBs have min allowed frag size and will drop !!!

- Example: EAP-TLS with large certificates
- Need to address path fragmentation or persist on source IP

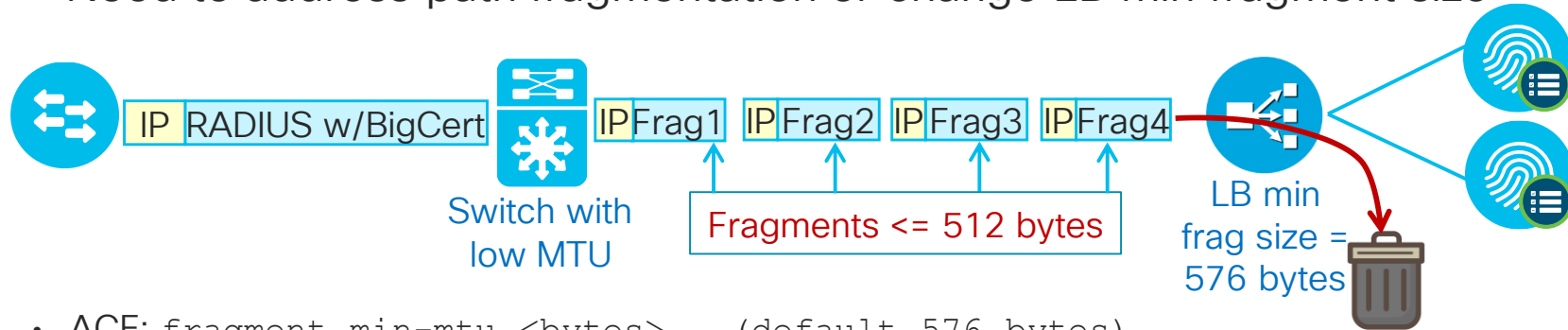


- ACE reassembles RADIUS packet.
- F5 LTM reassembles packets by default except for FastL4 Protocol
 - Must be manually enabled under the FastL4 Protocol Profile
- Citrix NetScaler fragmentation defect—Resolved in NetScaler 10.5 Build 50.10
 - Issue ID 429415 addresses fragmentation and the reassembly of large/jumbo frames

LB Fragmentation and Reassembly

Watch for packet fragments smaller than LB will accept!

- Example: Intermediate switch/gateway fragments packets below LB minimum
- Need to address path fragmentation or change LB min fragment size



- ACE: `fragment min-mtu <bytes>` (default 576 bytes)
- F5 LTM: `# tmsh modify sys db tm.minipfragsize value 1`
 - Pre-11.6: Default = 576 bytes
 - 11.6.0+: Default = 566 bytes

NAT Restrictions for RADIUS Load Balancing

Why Source NAT (SNAT) Fails for NADs

SNAT results in less visibility as all requests appear sourced from LB - makes troubleshooting more difficult.

- With SNAT, LB appears as the Network Access Device (NAD) to PSN.
- CoA sent to wrong IP address

Authentication Details	
Logged At:	October 10, 2012 10:15:59.418 AM
Occurred At:	October 10, 2012 10:15:59.416 AM
Server:	ise-psn-2
Authentication Method:	dot1x
EAP Authentication Method :	EAP-MSCHAPv2
EAP Tunnel Method :	PEAP
Username:	CTS\employee1
RADIUS Username :	CTS\employee1
Calling Station ID:	00:50:56:A0:0B:3A
Framed IP Address:	10.1.10.101
Use Case:	
Network Device:	ace4710
Network Device Groups:	Device Type#All Device Types#Wire
NAS IP Address:	10.1.50.2

Network Device	Server	Authorization Pr...	Identity Group
ace4710	ise-psn-2		
ace4710	ise-psn-3	Central_Web_Auth	Profiled:Workst
ace4710	ise-psn-1	Central_Web_Auth	Profiled
ace4710	ise-psn-3	Central_Web_Auth	Profiled:Workst
ace4710	ise-psn-1	Cisco_IP_Phones	Profiled:Cisco-IP
ace4710	ise-psn-2	Cisco_IP_Phones	Profiled:Cisco-IP
ace4710	ise-psn-2	Employee,SGT_Emp..	RegisteredDevi
ace4710	ise-psn-3	Posture_Remediation	Profiled:Workst
ace4710	ise-psn-3	RADIUS_Probes	

NAS IP Address is correct, but not currently used for CoA

User Story 8601 : CoA support for NAT'ed load balanced environments

SNAT of NAD Traffic: Live Log Example

Auth Succeeds/CoA Fails: CoA Sent to Load Balancer and Dropped

Status	Identity	Endpoint ID	IP Address	Network Device	Session ID	Event
❌		7C:6D:62:E3:D5:05		f5-bigip	0a012c5a000000f154199b09	RADIUS Request dropped
❌		7C:6D:62:E3:D5:05		f5-bigip	0a012c5a000000f154199b09	Dynamic Authorization failed
ℹ️	employee1	7C:6D:62:E3:D5:05	10.1.40.101		0a012c5a000000f154199b09	Session State is Started
✅	employee1	7C:6D:62:E3:D5:05		f5-bigip	0a012c5a000000f154199b09	Authentication succeeded

Event	Failure Reason
RADIUS Request dropped	11213 No response received from Network Access Device after sending a Dynamic Authorization request
Dynamic Authorization failed	11215 No response has been received from Dynamic Authorization Client in ISE
Session State is Started	
Authentication succeeded	

Allow Source NAT for PSN CoA Requests

Simplifying Switch CoA Configuration

- Match traffic from PSNs to UDP/1700 or UDP/3799 (RADIUS CoA) and translate to PSN cluster VIP.

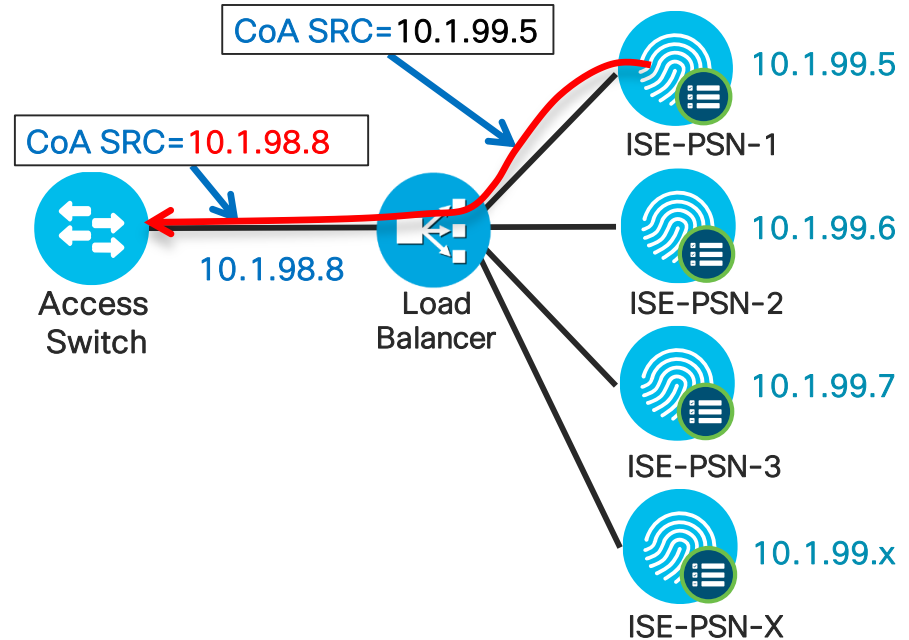
- Access switch config:

- Before:

```
aaa server radius dynamic-author
client 10.1.99.5 server-key cisco123
client 10.1.99.6 server-key cisco123
client 10.1.99.7 server-key cisco123
client 10.1.99.8 server-key cisco123
client 10.1.99.9 server-key cisco123
client 10.1.99.10 server-key cisco123
<...one entry per PSN...>
```

- After:

```
aaa server radius dynamic-author
client 10.1.98.8 server-key cisco123
```



Allow Source NAT for PSN CoA Requests

Simplifying WLC CoA Configuration

- Before:

MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK

RADIUS Authentication Servers

Acct Call Station ID Type System MAC Address

Auth Call Station ID Type AP MAC Address:SSID

Use AES Key Wrap (Designed for FIPS customers and requires a key wrap compliant RADIUS server)

MAC Delimiter Hyphen

Network User	Management	Server Index	Server Address	Port	IPSec	Admin Status
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	1	10.1.101.3			
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	2	10.1.99.15			
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	3	10.1.99.16			
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	4	10.1.99.17			
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	5	10.1.99.5			
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	6	10.1.99.6			
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	7	10.1.99.7	1812	Disabled	Enabled
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	8	10.1.98.10	1812	Disabled	Enabled
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	9				Enabled
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	10				Enabled
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	11				Disabled
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	12				Disabled
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	13				Enabled
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	14	10.1.120.56	1812	Disabled	Enabled
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	15	10.1.120.57	1812	Disabled	Enabled
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	16	10.1.120.58	1812	Disabled	Enabled
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	17	10.1.120.59	1812	Disabled	Enabled

Can't create more than 17 entries

OK

One RADIUS Server entry required per PSN that may send CoA from behind load balancer

- After

MONITOR WLANs CONTROLLER WIRELESS

RADIUS Authentication Servers

Acct Call Station ID Type System MAC Address

Auth Call Station ID Type AP MAC Address:SSID

Use AES Key Wrap (Designed for FIPS customers and requires a key wrap compliant RADIUS server)

MAC Delimiter Hyphen

Network User	Management	Server Index	Server Address	Port	IPSec	Admin Status
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	1	10.1.101.3	1812	Disabled	Enabled

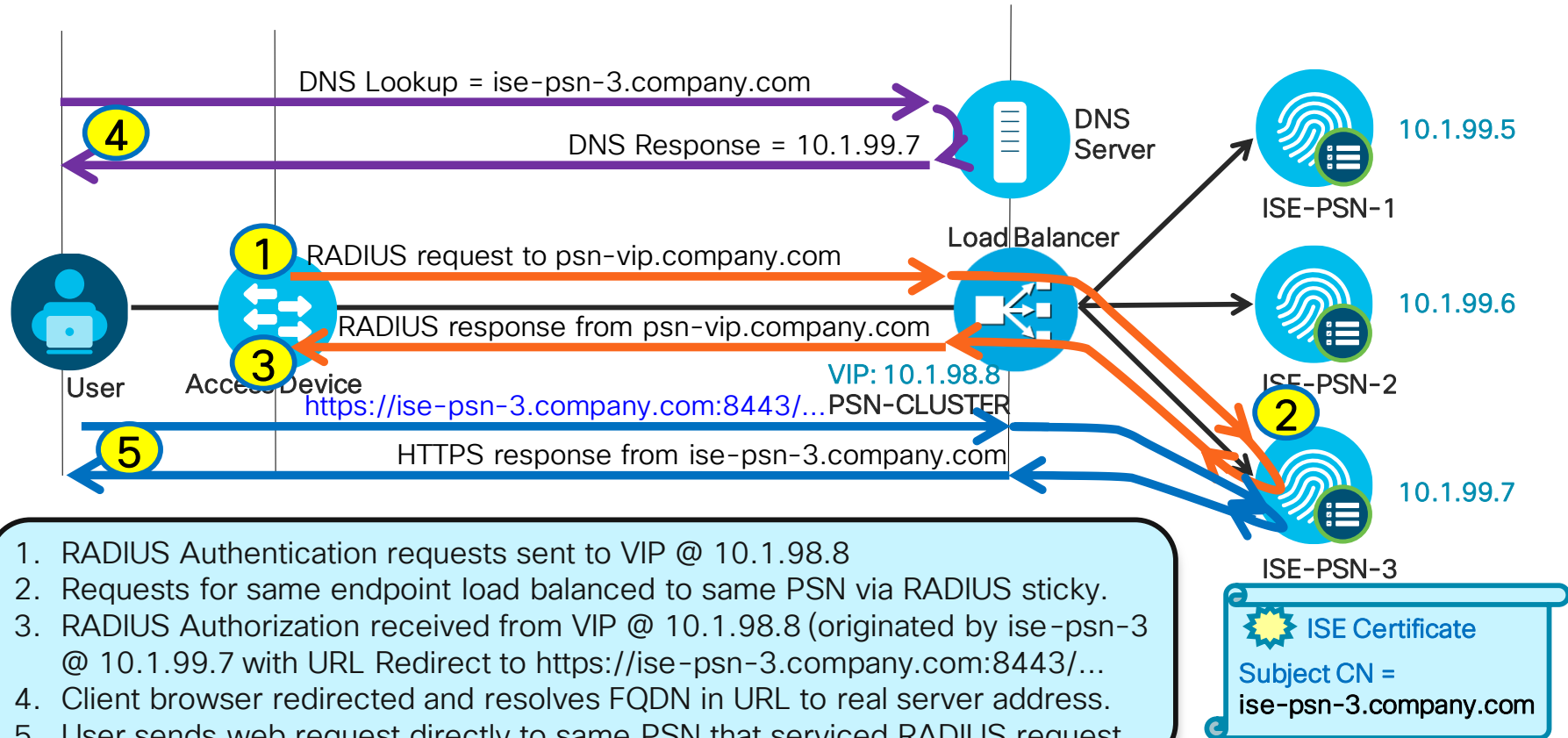
One RADIUS Server entry required per load balancer VIP.

Simplifies config and reduces # ACL entries required to permit access to each PSN

Load Balancing ISE Web Services

Load Balancing with URL-Redirection

URL Redirect Web Services: Hotspot/DRW, CWA, BYOD, Posture, MDM



Load Balancing URL-Redirected Services

When and How to Override Default URL Redirection from Client to PSN

- Use Cases for LB to Terminate redirected HTTPS Requests
 - Obfuscate PSN node names/IP addresses. (Do not want PSN name exposed to browser)
 - Ability to use a different certificate for user facing connection
 - Apply security inspections on web-based requires
 - As a way to secure PSN interfaces in DMZ.
- Requires Authorization Profile be configured with Static Hostname option.
- Load Balancer must be able to persist web request to same PSN that serviced RADIUS session Common methods (else rely on ISE policy logic):
 - LB includes Framed-IP-Address with RADIUS sticky; correlates Framed-IP to HTTPS source IP
 - LB includes Session Id with RADIUS sticky; correlates Session Id in web request

```
url-redirect=https://<PSN_CN>:8443/guestportal/gateway?sessionId=SessionIdValue&action=cwa
```

F5 LTM loadbalancing Radius and HTTP traffic for ISE

<http://www.cisco.com/c/en/us/support/docs/security/identity-services-engine/200317-F5-LTM-loadbalancing-Radius-and-HTTP-tra.html>

Note: Since ISE assumes HTTPS for web access, offload cannot be used to increase SSL performance. Load Balancer must reestablish SSL connection to real PSN servers.

URL Redirection Using Static IP/Hostname

Overriding Automatic Redirection to PSN IP Address/FQDN

- Allows static IP or FQDN value to be returned for CWA or other URL-Redirected Flows
- Common use case: Public DNS or IP address (no DNS available) must be used while preserving variable substitution for *port* and *sessionId* variables.

▼ Common Tasks Policy > Policy Elements > Results > Authorization > Authorization Profiles

Web Redirection (CWA, DRW, MDM, NSP, CPP)

Centralized Web Auth ACL

Static IP/Host name

DMZ PSN Certificate must match IP/Static FQDN

Specified IP Address/Hostname MUST point to the same PSN that terminates the RADIUS session.

If multiple PSNs, requires LB persistence or AuthZ Policy logic to ensure redirect occurs to correct PSN.

Status	Rule Name	Conditions (identity groups and other conditions)	Permissions
<input checked="" type="checkbox"/>	DMZ_Guest	Select an item AND Network Access:ISE Host Name EQUALS ise-dmz.cts.local	Central_Web_Auth_IP
<input checked="" type="checkbox"/>	Default	if no matches, then	Central_Web_Auth

“Universal Certs”

UCC or Wildcard SAN Certificates

Subject Alternative Name (SAN) - +
 - +

Check box to use wildcards

Allow Wildcard Certificates ⓘ

Node(s)

Generate CSR's for these Nodes:

Node	CSR Friendly Name
<input checked="" type="checkbox"/> ise-psn	ise-psn/Admin

Subject

Common Name (CN) ⓘ

Organizational Unit (OU)

Organization (O)

City (L)

State (ST)

Country (C)

CN must also exist in SAN

Universal Cert options:

- UCC / Multi-SAN
- Wildcard SAN

Subject Alternative Name (SAN) - +

- +

- +

Other FQDNs or wildcard as “DNS Names”

- +

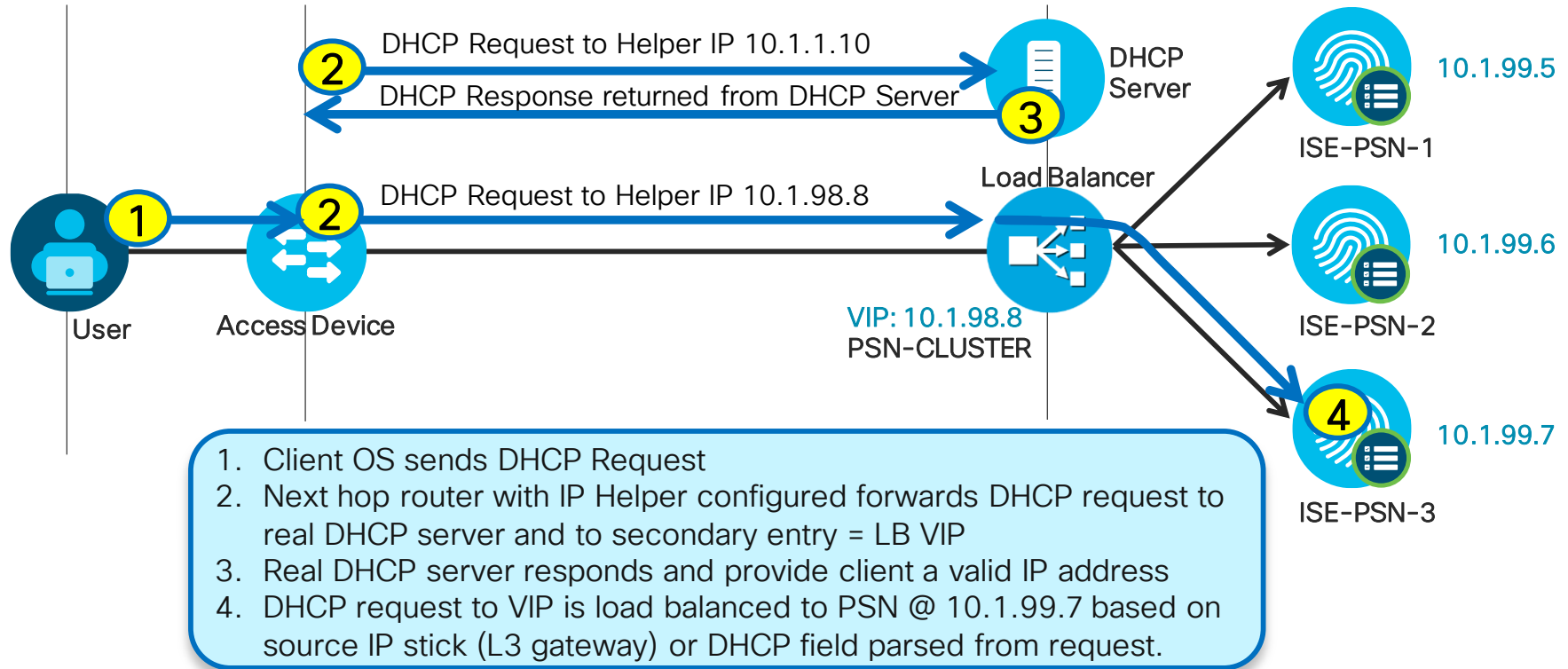
IP Address is also option

Load Balancing ISE Profiling Services



Load Balancing Profiling Services

Sample Flow



Load Balancing Simplifies Device Configuration

L3 Switch Example for DHCP Relay

- Before

```
!  
interface Vlan10  
  description EMPLOYEE  
  ip address 10.1.10.1 255.255.255.0  
  ip helper-address 10.1.100.100 <--- Real DHCP Server  
  ip helper-address 10.1.99.5 <--- ISE-PSN-1  
  ip helper-address 10.1.99.6 <--- ISE-PSN-2  
!
```

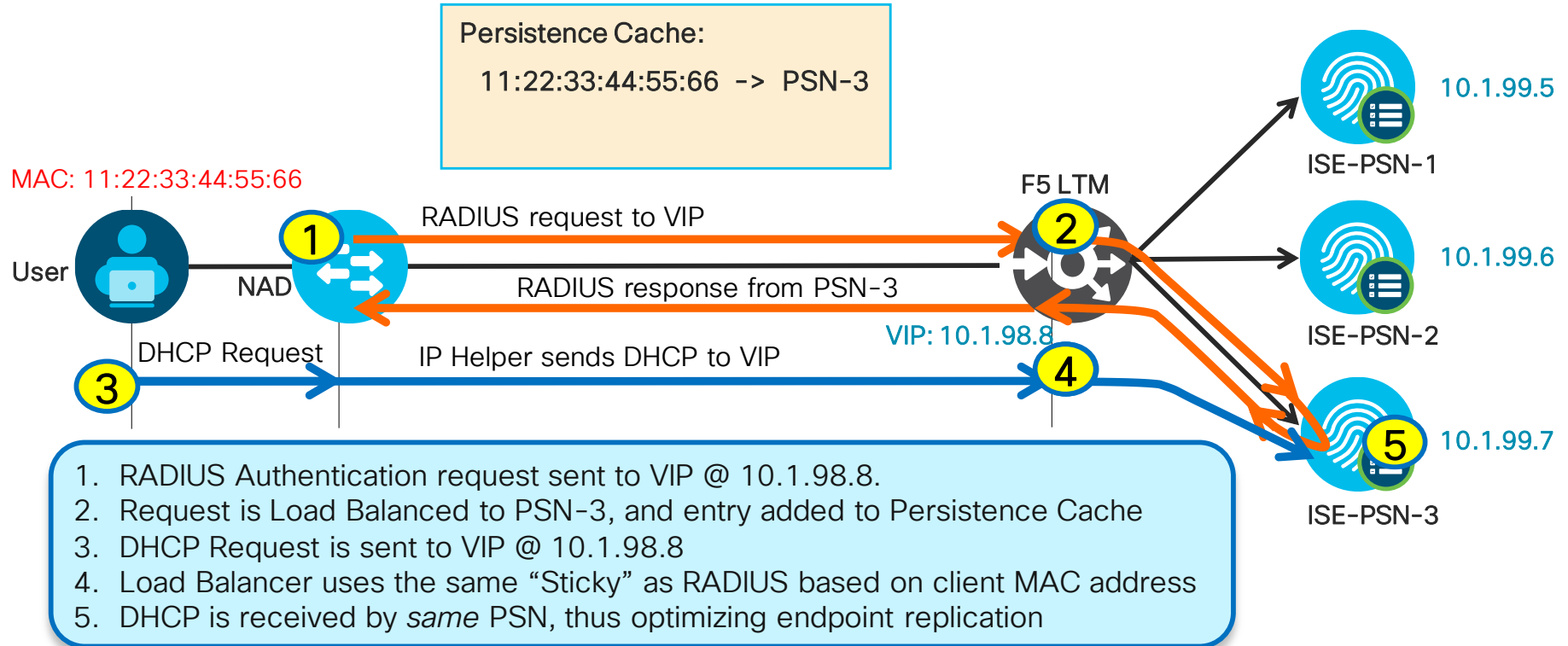
Settings apply to each
L3 interface servicing
DHCP endpoints

- After

```
!  
interface Vlan10  
  description EMPLOYEE  
  ip address 10.1.10.1 255.255.255.0  
  ip helper-address 10.1.100.100 <--- Real DHCP Server  
  ip helper-address 10.1.98.8 <--- LB VIP  
!
```

Load Balancing Sticky Guidelines

Ensure DHCP and RADIUS for a Given Endpoint Use Same PSN



F5 iRule to Drop DHCP Informs

courtesy of



```
when RULE_INIT {
  set static::DDIP_debug 1
}
when CLIENT_ACCEPTED {
  if { [UDP::payload length] > 200 } {
    binary scan [UDP::payload] x240H* dhcp_option_payload

    set option_hex 0
    set options_length [expr {[UDP::payload length] - 240} * 2]
    for {set i 0} {$i < $options_length} {incr i [expr {$length * 2 + 2}]} {
```

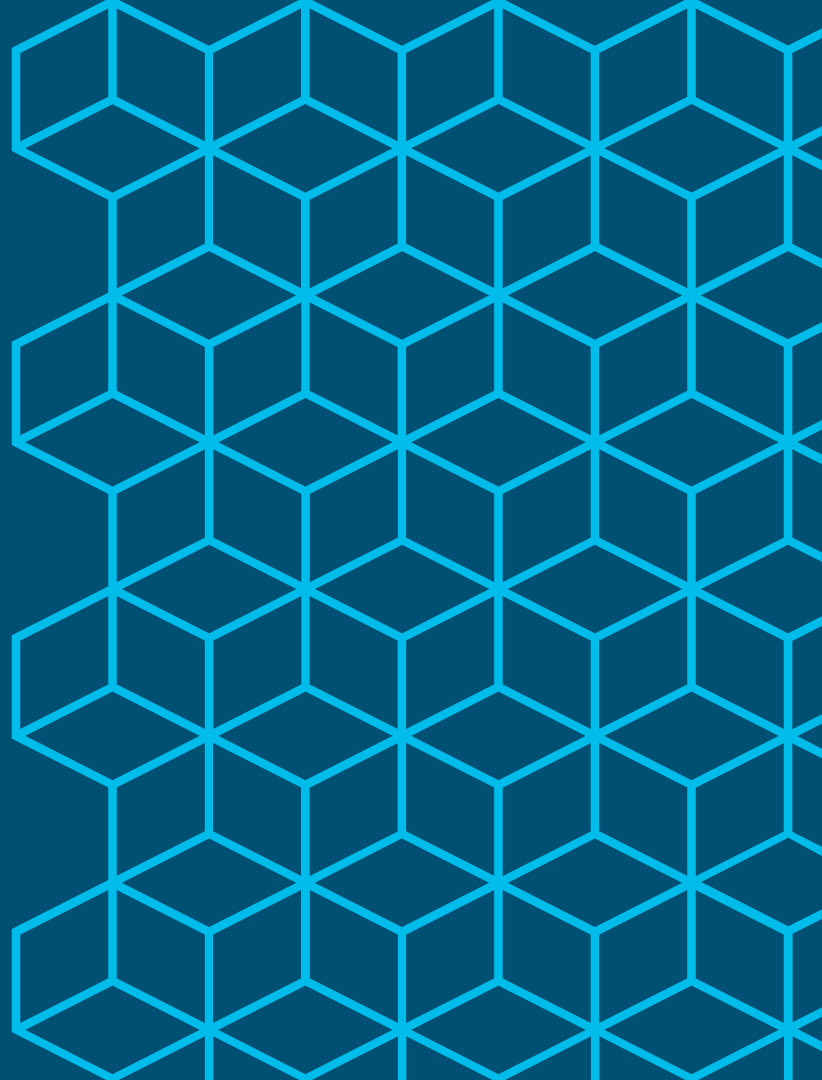
```
      # extract option value and convert into decimal
      # for human readability
      binary scan $dhcp_option_payload x[expr {$i}] a2 option_hex
      set tmpvalue1 0x$option_hex
      set option [expr {$tmpvalue1}]
      # move index to get length field
      incr i 2
```

```
      # extract length value and convert length from Hex string to decimal
      binary scan $dhcp_option_payload x[expr {$i}] a2 length_hex
      set tmpvalue2 0x$length_hex
      set length [expr {$tmpvalue2}]
      # extract value filed in hexadecimal format
      binary scan $dhcp_option_payload x[expr {$i + 2}] a[expr {$length * 2}] value_hex
```

iRule Continued

```
      if { $static::DDIP_debug } { log local0.
        "DHCP option is $option, value is $value_hex" }
      switch $option {
        53 {
          # DHCP Message Type
          switch $value_hex {
            08 {
              if { $static::DDIP_debug } {
                log local0.
                "Dropping DHCP Inform packet: $value_hex"
              }
              drop
              return
            }
            default { }
          }
        }
      }
    }
  }
}
```

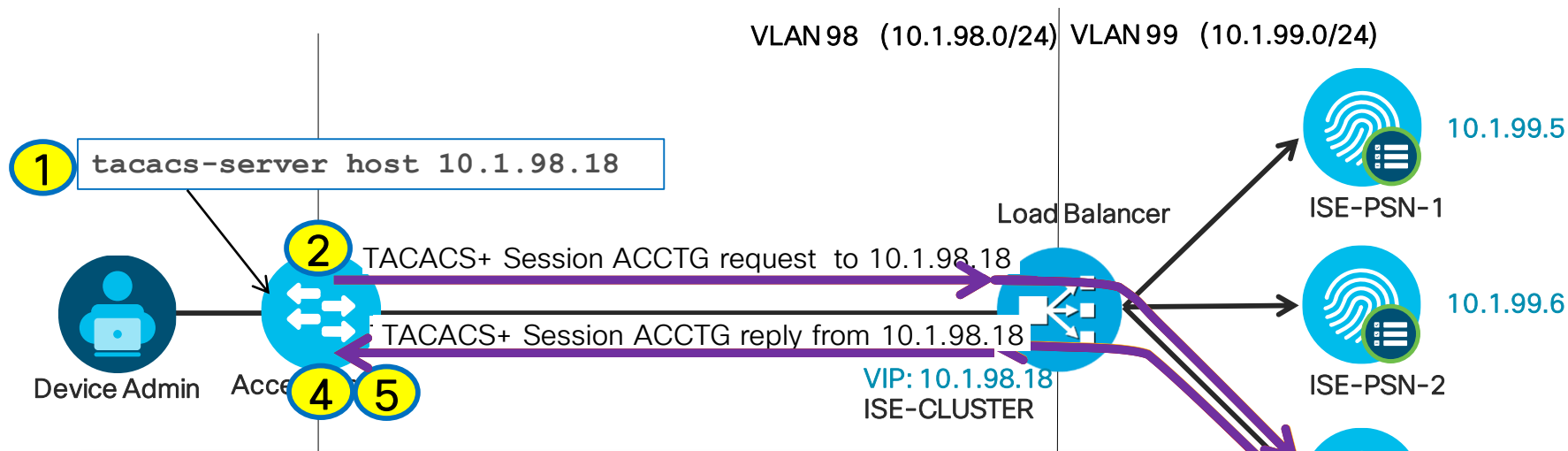
Load Balancing TACACS+



Load Balancing TACACS+

Session Authentication, Authorization, and Accounting

- Virtual IP = TACACS+ Server
- VIP listens on TCP/49
- Sticky based on source IP



1. NAD has single TACACS+ Server defined (10.1.98.18)
2. TACACS+ Session Authentication requests sent to VIP @ 10.1.98.18
3. Requests from same Admin user load balanced to same PSN via sticky based on Source IP (NAD IP Address)
4. TACACS+ response received from VIP @ 10.1.98.18 (originated by real server ise-psn-3 @ 10.1.99.7 and source translated by LB)
5. TACACS+ Session Authorization & Accounting sent to/from same PSN per sticky

Load Balancing TACACS+

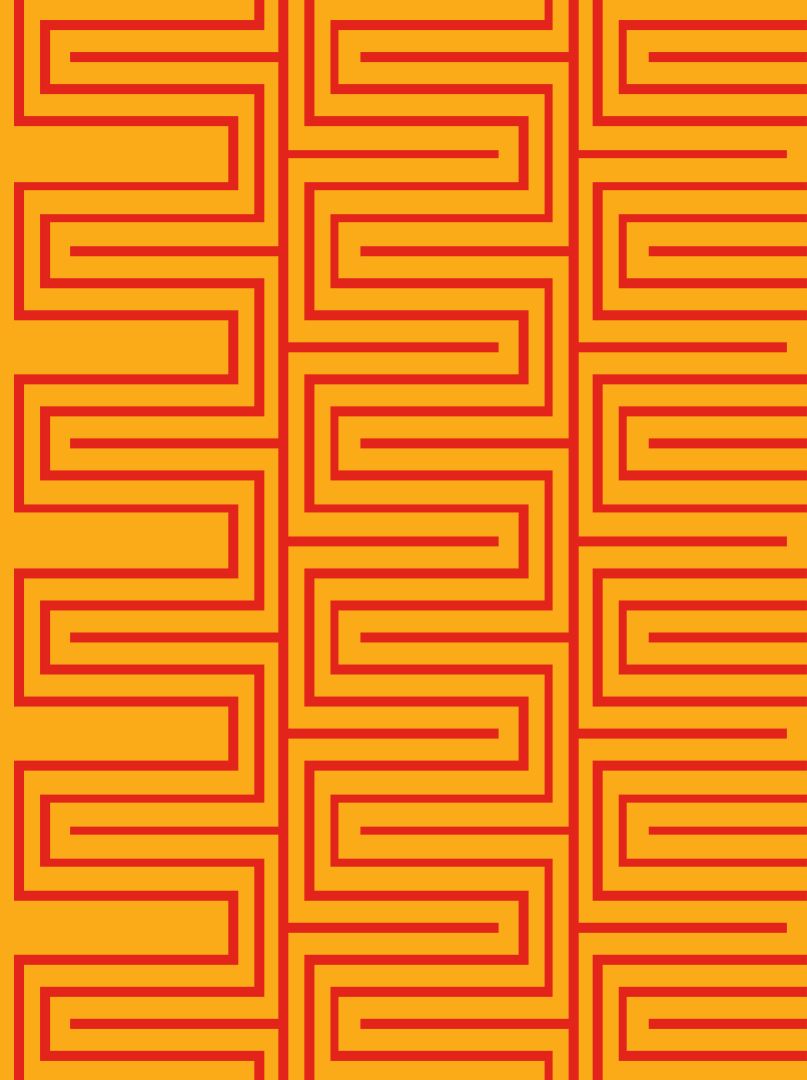
General Recommendations

- Load Balance based on TCP/49.
- Source NAT (SNAT) can be used – No CoA like RADIUS
 - Recommend LB inline with TACACS traffic, else need to address TCP asymmetry.
 - Without SNAT, make sure PSNs set default gateway to LB internal interface IP.
- Persistence – Recommend source IP address
 - Based on assumption that number of T+ clients high and requests per client is low.
- Health Monitoring options:
 - Simple response to TCP/49
 - 3-way handshake expected response
 - Scripts can be used to validate full auth flow.

Packet format: <http://www.cisco.com/warp/public/459/tac-rfc.1.76.txt>

Packet capture(encrypted): <https://www.cloudshark.org/captures/1a9c284c49b0>

LDAP Server Redundancy and Load Balancing



Per-PSN LDAP Servers

Added in
ISE 2.2!

- Assign unique Primary and Secondary to each PSN
- Allows each PSN to use local or regional LDAP Servers

LDAP Identity Sources List > LDAP1

LDAP Identity Source

General **Connection** Directory Organization Groups Attributes Advanced Settings

Primary Server

Hostname/IP: ad.cts.local
Port: 389

Secondary Server

Enable Secondary Server

Hostname/IP: ad2.cts.local
Port: 389

Specify server for each ISE node

Name	Primary Hostname/IP	Port	Secondary Hostname/IP	Port
ise22-psn1.company.com	ldap1-us-west.company.com	389	ldap2-us-west.company.com	389
ise22-psn2.company.com	ldap1-us-east.company.com	389	ldap2-us-east.company.com	389
ise22-psn3.company.com	ldap1-europe.company.com	389	ldap2-europe.company.com	389
ise22-psn4.company.com	ldap1-asia-west.company.com	389	ldap2-asia-west.company.com	389
ise22-psn5.company.com	ldap1-africa.company.com	389	ldap2-aftica.company.com	389
ise22-psn6.company.com	ldap1-india.company.com	389	ldap2-india.company.com	389

Load Balancing LDAP Servers

Lookup2 = ldap.company.com

Response = 10.1.95.7



15 minute reconnect timer



PSN

LDAP Query to 10.1.95.7

LDAP Response from 10.1.95.7

External Identity Sources

- Certificate Authentication Profile
- Active Directory
- LDAP
 - LDAP1
- ODBC
- RADIUS Token
- RSA SecurID
- SAML Id Providers



LDAP Identity Sources List > LDAP1

LDAP Identity Source

General | **Connection** | Directory Organization

Primary Server

* Hostname/IP: ldap.company.com

* Port: 389

Access: Anonymous Access Authenticated Access

Admin DN: * CN=admin,DC=company,DC=con

Password: *

Secure Authentication: Enable Secure Authentication Enable Server Identity Check

LDAP Server Root CA: Cisco Root CA 2048

Issuer CA of ISE Certificates: Select if required (optional)

* Server Timeout: 10 Seconds

* Max. Admin Connections: 20

Force reconnect every 15 Minutes

Test Bind to Server

Vendor-Specific LB Configurations

- F5 LTM
- Citrix NetScaler
- Cisco ACE
- Cisco ITD (Note)

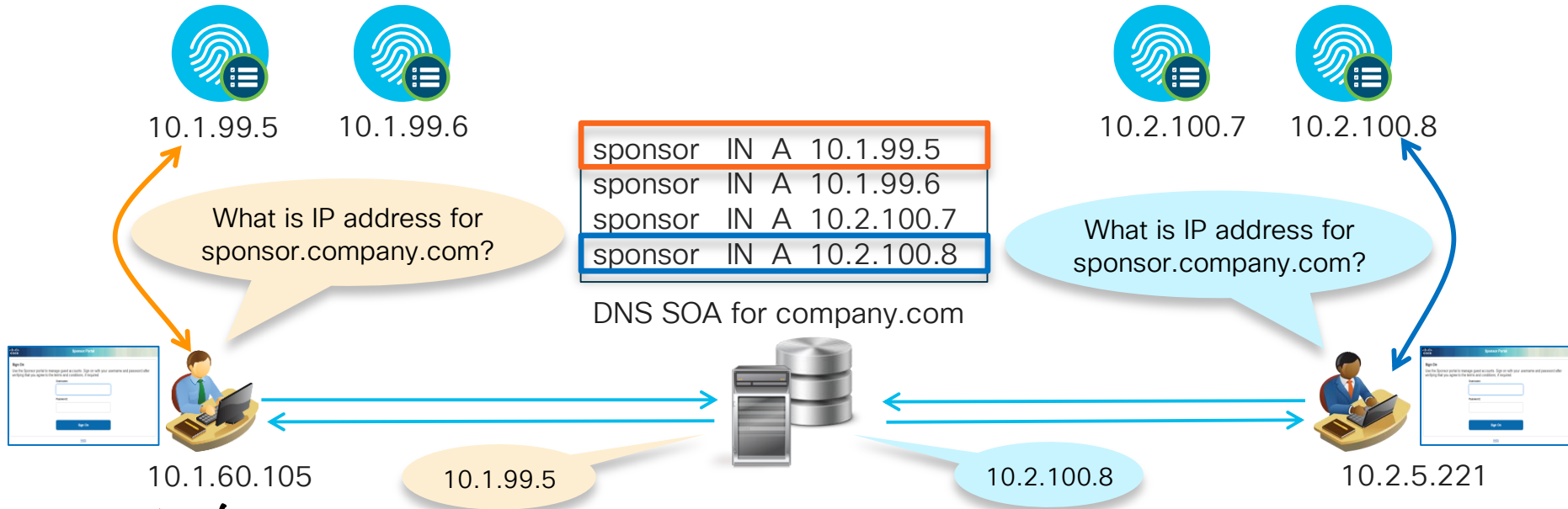
<https://communities.cisco.com/docs/DOC-64434>

PSN HA Without Load Balancers

Load Balancing Web Requests Using DNS

Client-Based Load Balancing/Distribution Based on DNS Response

- Examples:
 - Cisco Global Site Selector (GSS) / F5 BIG-IP GTM / Microsoft's DNS Round-Robin feature
 - Useful for web services that use static URLs including LWA, Sponsor, My Devices, OCSP.



ISE Configuration for Anycast

Anycast address should only be applied to ISE secondary interfaces, or LB VIP, but never to ISE GE0 management interface.

On each PSN that will participate in Anycast..

1. Configure PSN probes to profile DHCP (IP Helper), SNMP Traps, or NetFlow **on dedicated interface**
2. From CLI, configure dedicated interface with same IP address on each PSN node.

ISE-PSN-1 Example:

```
#ise-psn-1/admin# config t  
#ise-psn-1/admin (config)# int GigabitEthernet1  
#ise-psn-1/admin (config-GigabitEthernet)# ip address 10.10.10.10 255.255.255.0
```

ISE-PSN-2 Example:

```
#ise-psn-1/admin# config t  
#ise-psn-1/admin (config)# int GigabitEthernet1  
#ise-psn-1/admin (config-GigabitEthernet)# ip address 10.10.10.10 255.255.255.0
```

The screenshot shows the 'Edit Node' configuration page for 'ise-psn-2'. The 'Profiling Configuration' tab is active. Under the 'DHCP' section, the 'Interface' dropdown is set to 'GigabitEthernet 1', the 'Port' is '67', and the 'Description' is 'DHCP'. A red box highlights the 'Interface' dropdown menu.

Sample Routing Configuration for Anycast

• Access Switch 1

```
interface gigabitEthernet 1/0/23
no switchport
ip address 10.10.10.50 255.255.255.0
!
router eigrp 100
no auto-summary
redistribute connected route-map CONNECTED-2-EIGRP
!
route-map CONNECTED-2-EIGRP permit 10
match ip address prefix-list 5
set metric 1000 100 255 1 1500
set metric-type internal
!
route-map CONNECTED-2-EIGRP permit 20
ip prefix-list 5 seq 5 permit 10.10.10.0/24
```

Both switches
advertise same
network used
for profiling but
different metrics

• Access Switch 2

```
interface gigabitEthernet 1/0/23
no switchport
ip address 10.10.10.51 255.255.255.0
!
router eigrp 100
no auto-summary
redistribute connected route-map CONNECTED-2-EIGRP
!
route-map CONNECTED-2-EIGRP permit 10
match ip address prefix-list 5
set metric 500 50 255 1 1500 # less preferred
set metric-type external
!
route-map CONNECTED-2-EIGRP permit 20
ip prefix-list 5 seq 5 permit 10.10.10.0/24
```

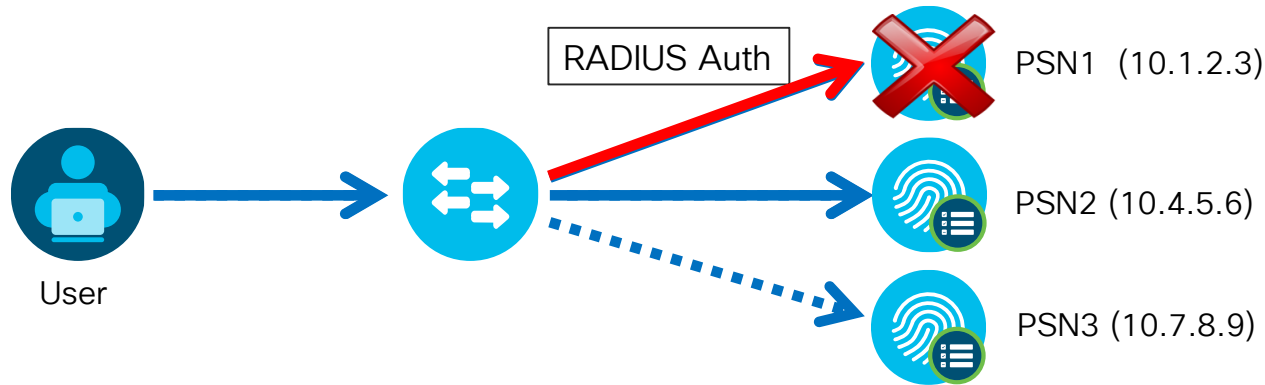
Real-World Customer Example using Anycast with RADIUS:

<http://www.networkworld.com/article/3074954/security/how-to-use-anycast-to-provide-high-availability-to-a-radius-server.html>

NAD-Based RADIUS Server Redundancy (IOS)

Multiple RADIUS Servers Defined in Access Device

- Configure Access Devices with multiple RADIUS Servers.
- Fallback to secondary servers if primary fails

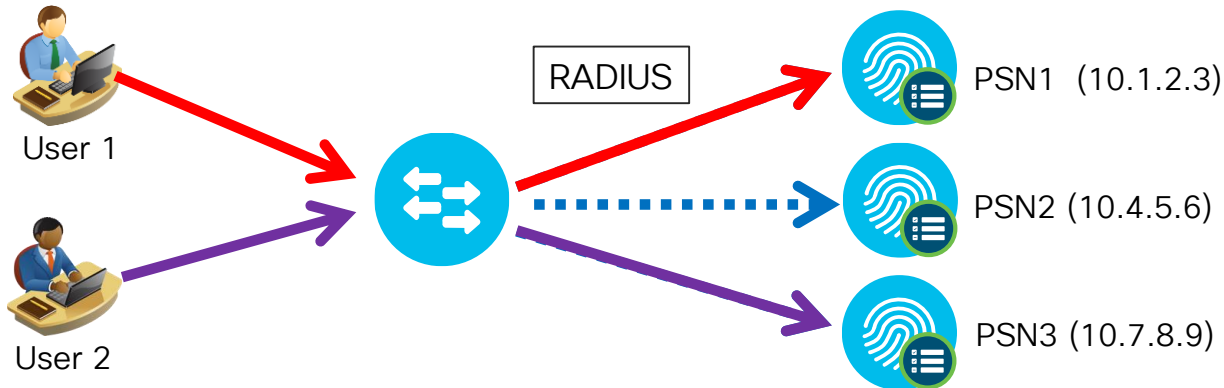


```
radius-server host 10.1.2.3 auth-port 1812 acct-port 1813
radius-server host 10.4.5.6 auth-port 1812 acct-port 1813
radius-server host 10.7.8.9 auth-port 1812 acct-port 1813
```

IOS-Based RADIUS Server Load Balancing

Switch Dynamically Distributes Requests to Multiple RADIUS Servers

- RADIUS LB feature distributes batches of AAA transactions to servers within a group.
- Each batch assigned to server with least number of outstanding transactions.



NAD controls the load distribution of AAA requests to all PSNs in RADIUS group without dedicated LB.

```
radius-server host 10.1.2.3 auth-port 1812 acct-port 1813
radius-server host 10.4.5.6 auth-port 1812 acct-port 1813
radius-server host 10.7.8.9 auth-port 1812 acct-port 1813
radius-server load-balance method least-outstanding batch-size 5
```

NAD-Based RADIUS Redundancy (WLC)

Wireless LAN Controller

- Multiple RADIUS Auth & Accounting Server Definitions
- RADIUS Fallback options: **none**, **passive**, or **active**

RADIUS > Fallback Parameters

Fallback Mode:

 Username:
 Password=
 Username
 Interval in sec.:

Security

AAA

General

RADIUS

Authentication
Accounting
Fallback

RADIUS Authentication Servers

Call Station ID Type ¹

Use AES Key Wrap (Designed for FIPS customers and requires...)

MAC Delimiter

Network User	Management	Server Index	Server Address	Port
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<u>1</u>	10.1.99.5	1812
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<u>6</u>	10.1.99.6	1812
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<u>7</u>	10.1.99.7	1812
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<u>8</u>	10.1.98.10	1812

Off = Continue exhaustively through list; never preempt to preferred server (entry with lowest index)

Passive = Quarantine failed RADIUS server for interval then return to active list w/o validation; always preempt.

Active = Mark failed server dead then actively probe status per interval w/username until succeed before return to list; always preempt.

NAD Fallback and Recovery

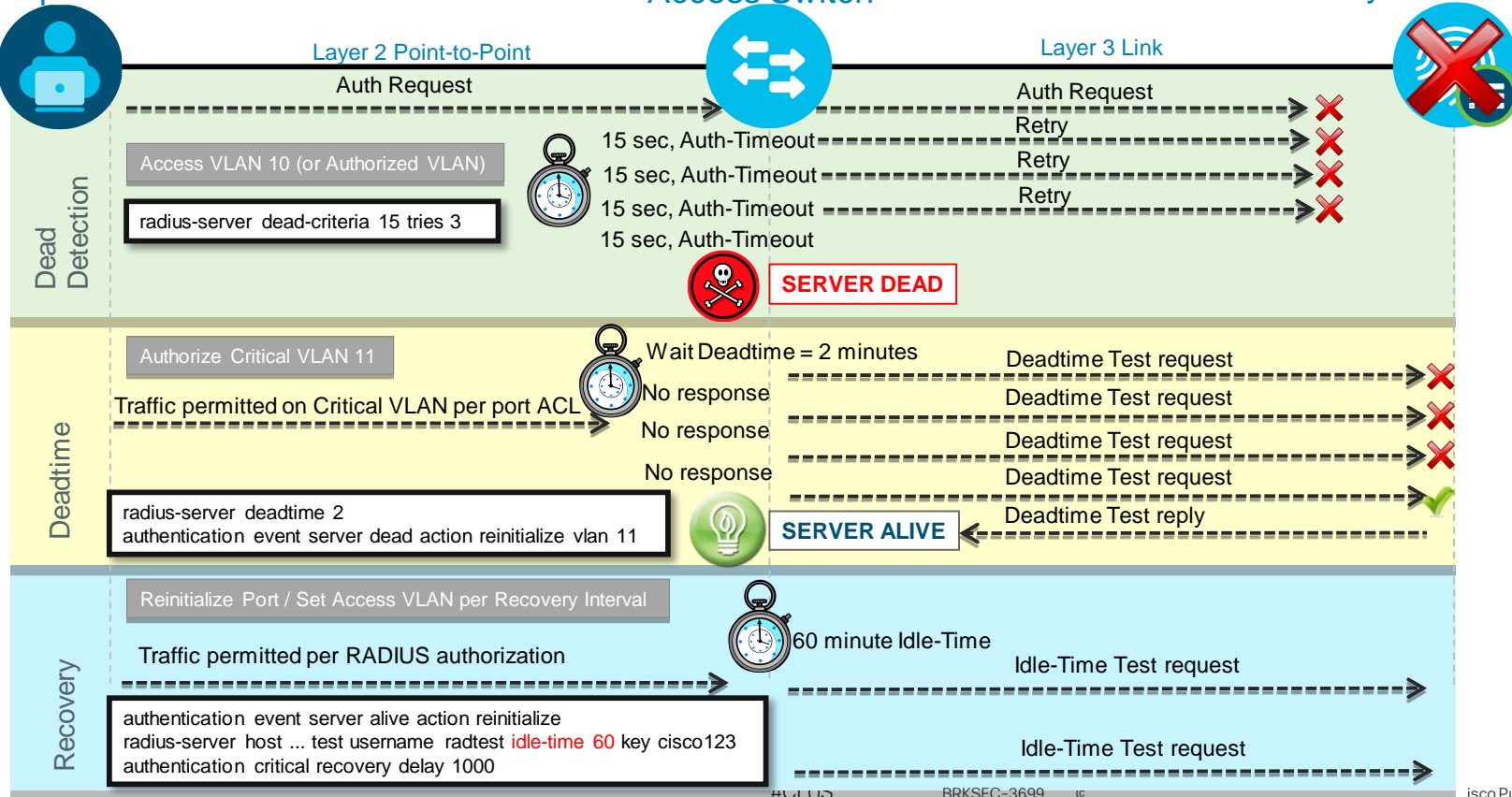


NAD Fallback and Recovery Sequence

Endpoint

Access Switch

Policy Service Node



RADIUS Test User Account

Which User Account Should Be Used?

- Does NAD uniformly treat Auth Fail and Success the same for detecting server health?
IOS treats them the same; F5 RADIUS probe treats Auth Fail= “server down”. Check your LB behavior.
- Do I use an Internal or External ID store account?
If goal is to validate backend ID store, then Auth Fail may not detect external ID store failure.
- **IOS Example:** Failover on AD failure. **Solution:** Drop auth requests when external ID store is down.

• Identity Server Sequence > Advanced Settings:

▼ **Advanced Search List Settings**

Select the action to be performed if a selected identity store cannot be accessed for authentication

Do not access other stores in the sequence and set the "AuthenticationStatus" attribute to "ProcessError"

Treat as if the user was not found and proceed to the next store in the sequence

Authentication Policy >
ID Source custom
processing based on
authentication results

- **ACE Example:** If auth fails, then PSN declared down.
Solution: Create valid user account so ACE test probes return Access-Accept.

AD_Internal_Users

Identity Source AD_Internal_Users

Options

If authentication failed Reject

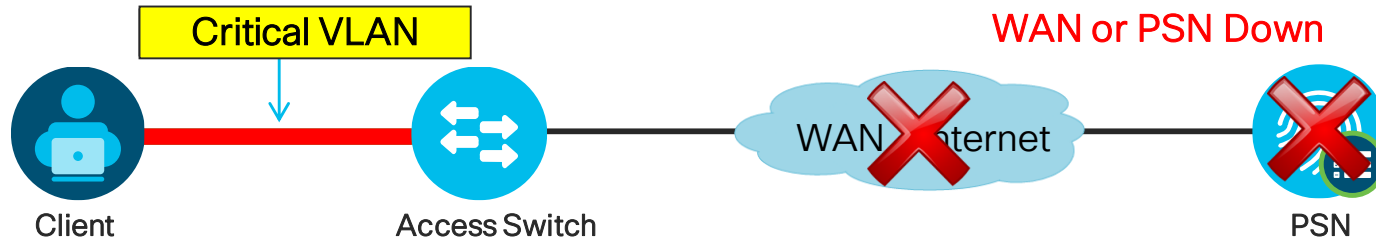
If user not found Reject

If process failed Drop

• Could this present a potential security risk?

Inaccessible Authentication Bypass (IAB)

Also Known As “Critical Auth VLAN” for Data



- Switch detects PSN unavailable by one of two methods
 - Periodic probe
 - Failure to respond to AAA request
- Enables port in critical VLAN
- Existing sessions retain authorization status
- Recovery action can re-initialize port when AAA returns

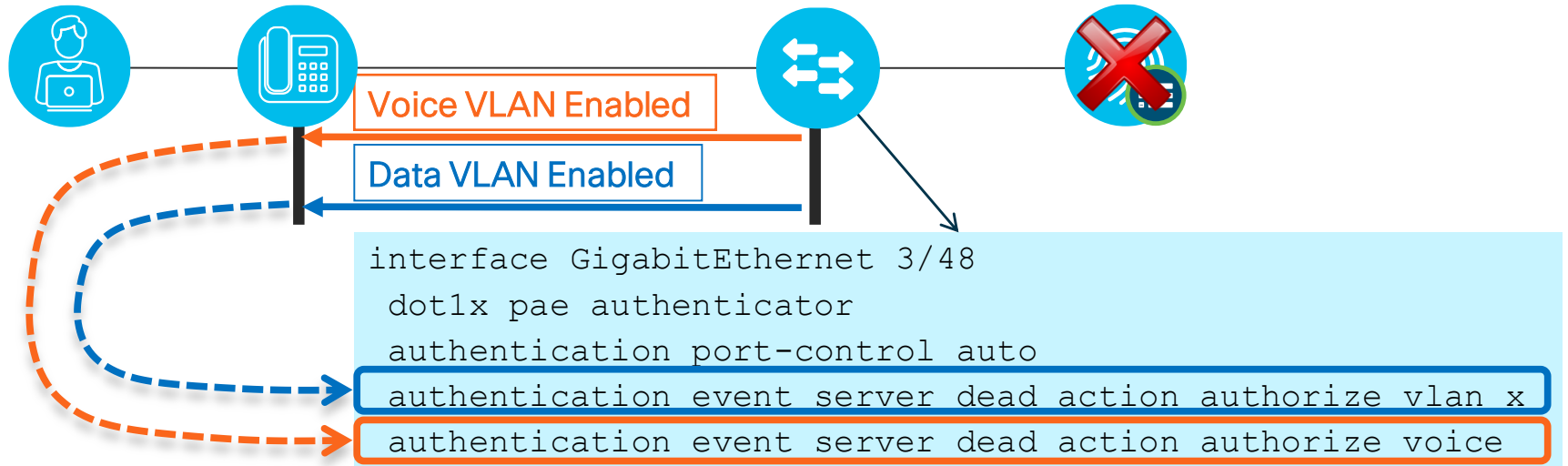
Critical Data VLAN can be anything:

- Same as default access VLAN
- Same as guest/auth-fail VLAN
- New VLAN

```
authentication event server dead action authorize vlan 100
authentication event server alive action reinitialize
authentication event server dead action authorize voice
```

Critical Voice VLAN

Critical Auth for Data and Voice

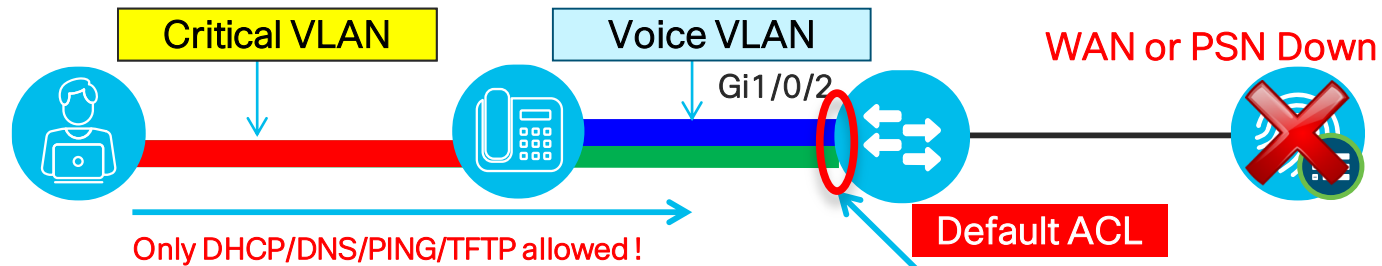


```
# show authentication sessions interface fa3/48
...
Critical Authorization is in effect for domain(s) DATA and VOICE
```

Default Port ACL Issues with Critical VLAN

Limited Access Even After Authorization to New VLAN!

- Data VLAN reassigned to critical auth VLAN, but new (or reinitialized) connections are still restricted by existing port ACL!



```
interface GigabitEthernet1/0/2
switchport access vlan 10
switchport voice vlan 13
ip access-group ACL-DEFAULT in
authentication event server dead action reinitialize vlan 11
authentication event server dead action authorize voice
authentication event server alive action reinitialize
```

```
ip access-list extended ACL-DEFAULT
permit udp any eq bootpc any eq bootps
permit udp any any eq domain
permit icmp any any
permit udp any any eq tftp
```

Using Embedded Event Manager with Critical VLAN

Modify or Remove/Add Static Port ACLs Based on PSN Availability

- Allows scripted actions to occur based on various conditions and triggers

```
track 1 ip route 10.1.98.0 255.255.255.0 reachability
event manager applet default-acl-fallback
  event track 1 state down maxrun 5
  action 1.0 cli command "enable"
  action 1.1 cli command "conf t" pattern "CNTL/Z."
  action 2.0 cli command "ip access-list extended ACL-DEFAULT"
  action 3.0 cli command "1 permit ip any any"
  action 4.0 cli command "end"
event manager applet default-acl-recovery
  event track 1 state up maxrun 5
  action 1.0 cli command "enable"
  action 1.1 cli command "conf t" pattern "CNTL/Z."
  action 2.0 cli command "ip access-list extended ACL-DEFAULT"
  action 3.0 cli command "no 1 permit ip any any"
  action 4.0 cli command "end"
```

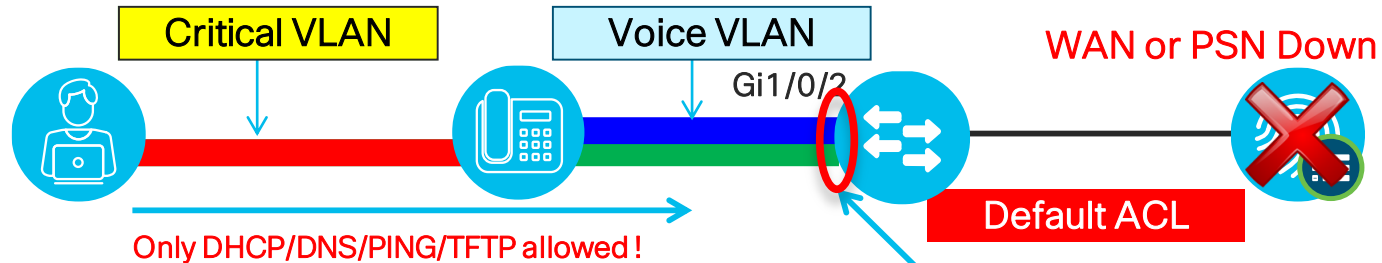
EEM available
on Catalyst
3k/4k/6k
switches

<https://supportforums.cisco.com/document/117596/cisco-eem-basic-overview-and-sample-configurations>
<https://supportforums.cisco.com/document/48891/cisco-eem-best-practices>

Critical ACL using Service Policy Templates

Apply ACL, VLAN, or SGT on RADIUS Server Failure!

- Critical Auth ACL applied on Server Down



```
interface GigabitEthernet1/0/2
switchport access vlan 10
switchport voice vlan 13
ip access-group ACL-DEFAULT in
access-session port-control auto
mab
dot1x pae authenticator
service-policy type control subscriber ACCESS-POLICY
```

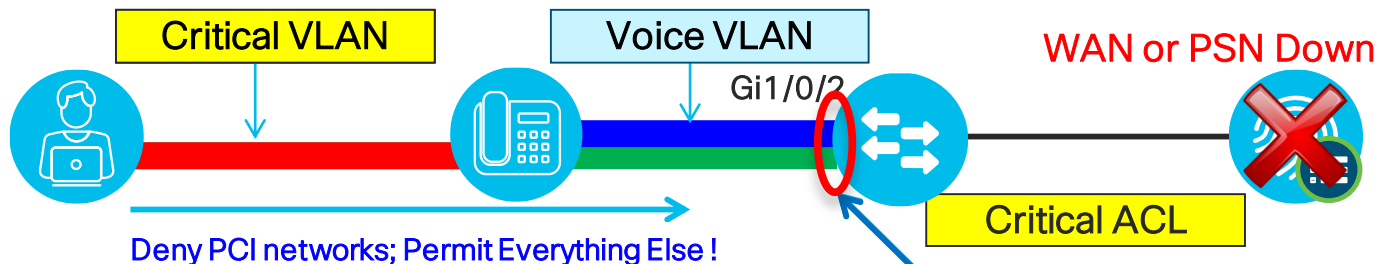
```
ip access-list extended ACL-DEFAULT
permit udp any eq bootpc any eq bootps
permit udp any any eq domain
permit icmp any any
permit udp any any eq tftp
```

Critical ACL using Service Policy Template

Apply ACL, VLAN, or SGT on RADIUS Server Failure!

2k/3k/4k: 15.2(1)E
3k IOS-XE: 3.3.0SE
4k: IOS-XE 3.5.0E
6k: 15.2(1)SY

- Critical Auth ACL applied on Server Down

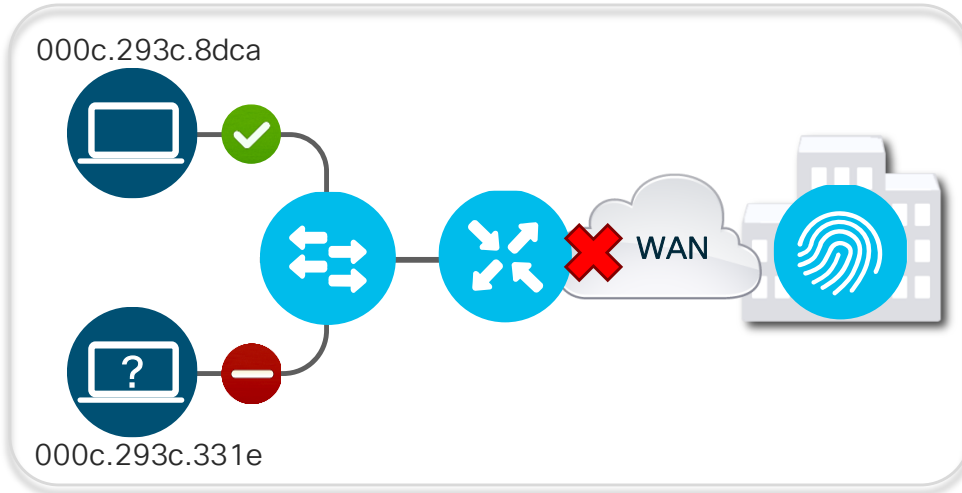


```
policy-map type control subscriber ACCESS-POLICY
 event authentication-failure match-first
  10 class AAA_SVR_DOWN_UNAUTHD do-until-failure
  10 activate service-template CRITICAL_AUTH_VLAN
  20 activate service-template DEFAULT_CRITICAL_VOICE_TEMPLATE
  30 activate service-template CRITICAL-ACCESS
service-template CRITICAL-ACCESS
 access-group ACL-CRITICAL
!
service-template CRITICAL_AUTH_VLAN
 vlan 10
service-template DEFAULT_CRITICAL_VOICE_TEMPLATE
 voice vlan
class-map type control subscriber match-all AAA_SVR_DOWN_UNAUTHD
 match result-type aaa-timeout
 match authorization-status unauthorized
```

```
ip access-list extended ACL-CRITICAL
 remark Deny access to PCI zone scopes
 deny tcp any 172.16.8.0 255.255.240.0
 deny udp any 172.16.8.0 255.255.240.0
 deny ip any 192.168.0.0 255.255.0.0
 permit ip any any
```


Critical MAB

Local Authentication During Server Failure



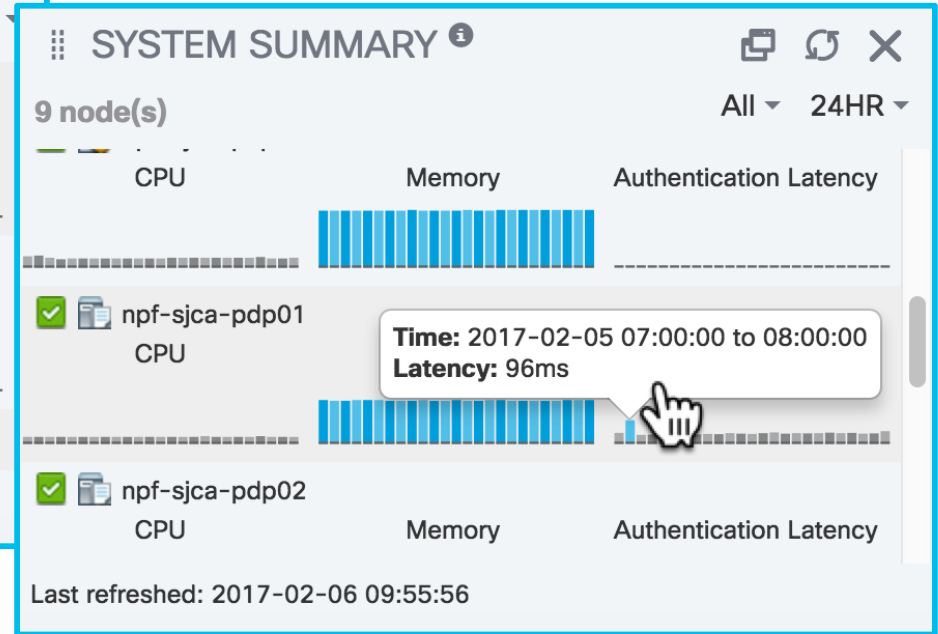
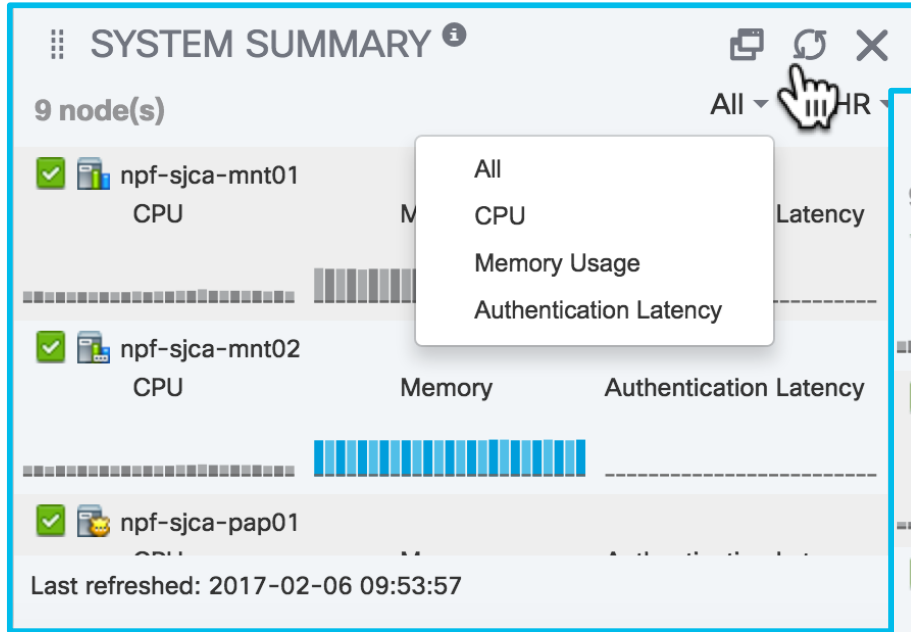
```
username 000c293c8dca password 0 000c293c8dca
username 000c293c8dca aaa attribute list mab-local
!
aaa local authentication default authorization mab-local
aaa authorization credential-download mab-local local
!
aaa attribute list mab-local
  attribute type tunnel-medium-type all-802
  attribute type tunnel-private-group-id "150"
  attribute type tunnel-type vlan
  attribute type inacl "CRITICAL-V4"
!
policy-map type control subscriber ACCESS-POL
...
event authentication-failure match-first
  10 class AAA_SVR_DOWN_UNAUTHD_HOST do-
    until-failure
  10 terminate mab
  20 terminate dot1x
  30 authenticate using mab aaa authc-
    list mab-local authz-list mab-local
...

```

- Additional level of check to authorize hosts during a critical condition.
- EEM Scripts could be used for dynamic update of whitelist MAC addresses
- Sessions re-initialize once the server connectivity resumes.

Monitoring Load and System Health

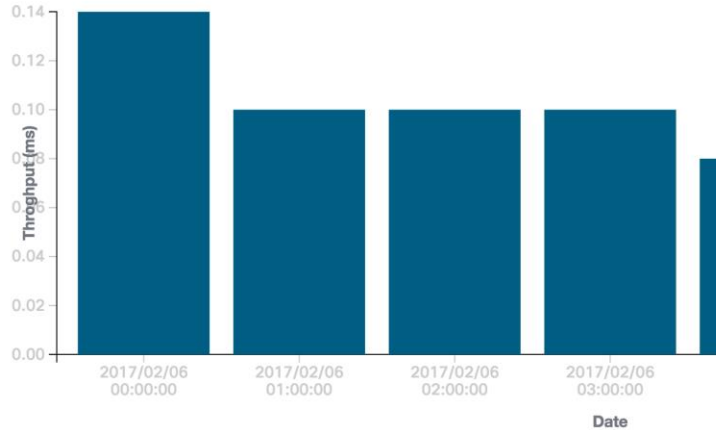
Home Dashboard - High-Level Server Health



Server Health/Utilization Reports

Operations > Reports > Diagnostics > Health Summary

Chart: Time Vs Throughput



Health Summary

Logged At	CPU Utilization	Memory Utilization	RADIUS Respo
2017/02/06 00:00:00	2.42	40.23	222.22
2017/02/06 01:00:00	2.37	40.07	158.12
2017/02/06 02:00:00	2.42	40.17	186.1
2017/02/06 03:00:00	2.35	40.02	232.25
2017/02/06 04:00:00	2.33	40.22	69.77

Recent Disk Space Utilization (%)

Logged At	/root	/boot	/localdisk	/storedconfig	/tmp
2017-02-06 06:40:38.907	14	23	1	2	1

CPU Usage (Updated every 15 min)

ISE Function	% CPU Usage	CPU Time	Number of Threads
Database Server	0.24	285:51.58	79 processes
Admin Process JVM Thr...	0.13	156:17.80	15
Admin Webapp	0.12	139:27.18	169
Profiler	0.06	69:48.71	52
NSF Persistence Layer	0.04	42:09.45	46
Quartz Scheduler	0.02	29:39.21	29
Profiler Database	0.02	18:00.93	3

Key Performance Metrics (KPM)

- KPM Reports added in ISE 2.2: [Operations](#) > [Reports](#) > [Diagnostics](#) > [KPM](#)
- Also available from CLI (# application configure ise) since ISE 1.4
- Provide RADIUS Load, Latency, and Suppression Stats

Key Performance Metrics ⓘ

From 2017-01-06 00:00:00.0 to 2017-02-05 22:32:38.128

Logged Time	ⓘ Server	Radius Requests/Hr	Logged To M...	Noise/Hr	Suppression/Hr	Avg Load	Max Load	Avg Latency...	Avg TPS
2017-02-05 18:01:22.0	npf-sjca-pdp01	343	598	-255	-74.34	4.77	10.83	0.67	0.1
2017-02-05 18:01:22.0	sbg-bgla-pdp01	262	174	88	33.59	2.27	3.75	2.57	0.07
2017-02-05 18:01:22.0	npf-sjca-pdp02	169	271	-102	-60.36	2.16	3.75	0.63	0.05
2017-02-05 17:01:40.0	sbg-bgla-pdp01	227	147	80	35.24	2.39	3.75	0.35	0.06
2017-02-05 17:01:40.0	npf-sjca-pdp02	187	275	-88	-47.06	3.33	8.75	0.64	0.05
2017-02-05 17:01:40.0	npf-sjca-pdp01	343	596	-253	-73.76	3.03	4.17	0.69	0.1
2017-02-05 16:01:23.0	npf-sjca-pdp02	188	297	-109	-57.98	2.39	3.75	0.64	0.05
2017-02-05 16:01:23.0	npf-sjca-pdp01	356	625	-269	-75.56	4.39	9.17	0.74	0.1
2017-02-05 16:01:23.0	sbg-bgla-pdp01	253	131	122	48.22	1.67	2.5	0.72	0.07

Serviceability Counter Framework (CF)



The Easy Way: MNT auto-collects key metrics from each node!

- Enable/disable from 'app configure ise'
- Enabled by default
- Threshold are hard set by platform size
- Alarm sent when exceed threshold
- Running count displayed per collection interval

The screenshot shows the Cisco Identity Services Engine (ISE) interface. The main content area displays the 'ISE Counters' report for the period from 2017-04-30 00:00:00.0 to 2017-04-30 15:15:47.612. The report is filtered by 'Server' (npf-sjca-pdp02) and 'Time Range' (Today). A table titled 'Counter Attribute Threshold' lists various counter attributes and their corresponding thresholds. The 'Endpoint Ownership Change' row is highlighted with a red box, and a blue callout box labeled 'Detected platform size' points to the 'IBM_LARGE' value in this row. Another blue callout box labeled 'Thresholds' points to the '5000' value in the same row. A third blue callout box labeled 'Node specific report' points to the 'npf-sjca-pdp02' filter value.

Counter Attribute	Platform Size	Threshold
Endpoint Oracle Persist Received	IBM_LARGE	9000
Endpoint Ownership Change	IBM_LARGE	5000
Endpoint Profiling Events	IBM_LARGE	80000
Endpoint Reprofitting Events	IBM_LARGE	8000
Endpoint Cache Insert Update Received	IBM_LARGE	95000
Hostname Event Fetch from AD	IBM_LARGE	100000
HTTP Endpoint Detected	IBM_LARGE	800
NMAP Scan Event Query	IBM_LARGE	8000

Key Takeaway Points

- CHECK ISE Virtual Appliances for proper resources and platform detection!
- Avoid excessive auth activity through proper NAD / supplicant tuning and Log Suppression
- Minimize data replication by implementing node groups and profiling best practices
- Leverage load balancers for scale, high availability, and simplifying network config changes
- Be sure to have a local fallback plan on you network access devices

Cisco Community Page on Sizing and Scalability

<https://communities.cisco.com/docs/DOC-68347>



Communities

Cisco Communities > Technology > Security > Policy and Access > Identity Services Engine (ISE) > Documents



ISE Performance & Scale

- ISE 2.4 Deployment Scale and Limits
- ISE 2.2+ Deployment Scale and Limits
- ISE Hardware Platforms
- ISE PSN Performance
 - ISE TACACS+ Performance
 - ISE 2.4 RADIUS Performance
 - ISE 2.3 RADIUS Performance
 - ISE 2.2 RADIUS Performances
 - ISE 2.3 Scenario-Based Performance
- ISE 2.4 Passive Identity (Passive ID) and Easy Connect Scaling
 - Passive ID / EZC Scaling Per Deployment
 - Passive ID / Easy Connect Scaling per PSN dedicated to Passive ID Service
- ISE 2.2 and 2.3 Passive Identity (Passive ID) and Easy Connect Scaling
 - Passive ID / EZC Scaling Per Deployment
 - Passive ID / Easy Connect Scaling per PSN dedicated to Passive ID Service
 - Passive ID - Provider and Consumer Scaling
- ISE 2.4 Platform eXchange Grid (pxGrid v2) Scaling
 - pxGrid v2 Scaling per Deployment
 - pxGrid v2 Scaling per Dedicated pxGrid Node

- ISE 2.2 Platform eXchange Grid (pxGrid v1) Scaling
 - pxGrid v1 Scaling per Deployment
 - pxGrid v1 Scaling per Dedicated pxGrid Node
- ISE 2.4 SXP Scaling
 - ISE SXP Scaling per Deployment
 - ISE SXP Scaling per SXPSN
- ISE 2.2 and 2.3 SXP Scaling
 - ISE SXP Scaling per Deployment
 - ISE SXP Scaling per SXPSN
- ISE 2.2/2.3/2.4 Threat-Centric NAC (TC-NAC) Scaling
 - TC-NAC Scaling per Deployment
 - TC-NAC Scaling per PSN
- ISE Storage Requirements
 - VM Disk Size Minimum Requirement
 - MnT Persona Log Storage Requirements
 - RADIUS Log Retention (Days):
 - TACACS+ log retention(Days)
 - Scripted device admin model:
 - Human admin - Device admin model
- ISE Latency & Bandwidth
 - ISE 2.0 Latency
 - ISE 2.1 Latency
 - WAN Bandwidth Calculator
- Sources

ISE Performance & Scale Resources

<https://communities.cisco.com/docs/DOC-65625>

- Community Page
- Cisco Live:
BRKSEC-3699
Reference version
- ISE Load Balancing Design Guide (be sure to read customer notes at bottom of download page—guide errata!)
- Calculators for Bandwidth and Logging

Cisco *live!*



ISE Deployment Sizing and Scalability

created by [Craig Hyps](#) on Feb 14, 2016 1:18 AM, last modified by [Craig Hyps](#) on Mar 10, 2016 12:36 PM

ISE Install Guide on Deployment Sizing

Cisco Live Breakout Session BRKSEC-3699 on ISE Large Scale Design including Sizing, High Availability, Load Balancing, and Best Practices:

Includes Working Configs for ACE and F5

[BRKSEC-3699 Designing ISE for Scale & High Availability](#) presented by [Craig Hyps](#) : [Presentation](#) (PDF) | [Reference](#) (PDF)




ISE Load Balancing



ISE Latency and Bandwidth Calculators



ISE MnT Log sizing calculator for TACACS+ and RADIUS

ISE Performance Metrics are contained in the  [High-Level Design Document](#)

Complete your online session evaluation

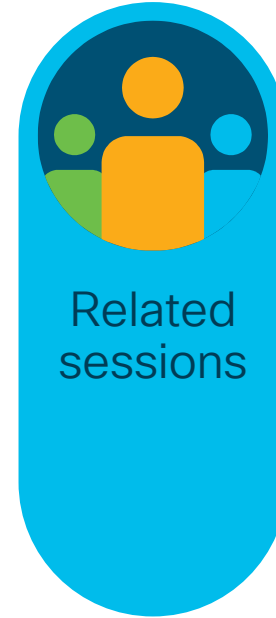
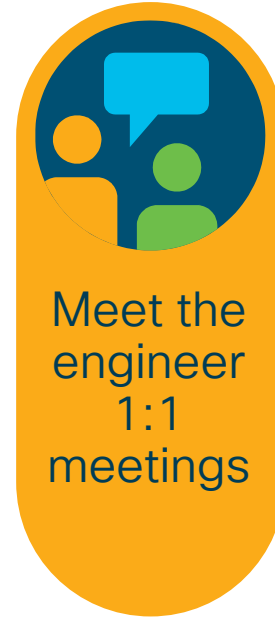
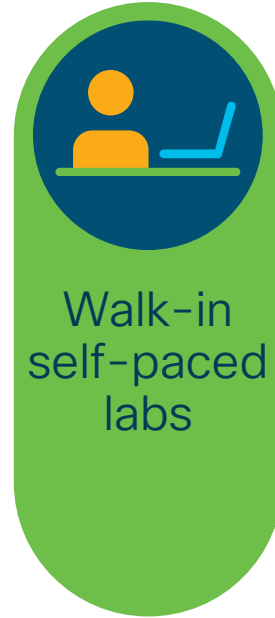
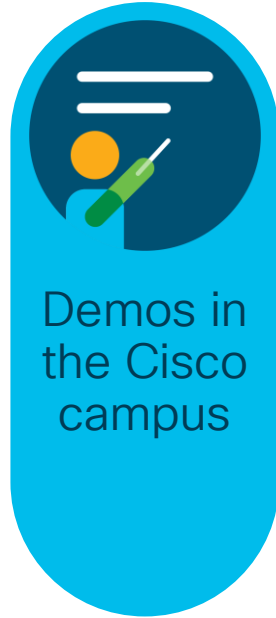
Give us your feedback to be entered into a Daily Survey Drawing.

Complete your session surveys through the Cisco Live mobile app or on www.CiscoLive.com/us.

Don't forget: Cisco Live sessions will be available for viewing on demand after the event at www.CiscoLive.com/Online.



Continue your education





Thank you



INTUITIVE



INTUITIVE