



i i i i i i i i

You make **possible**

A decorative graphic of vertical bars in various colors (blue, green, orange, red) is positioned on both the left and right sides of the text. The text itself consists of the word "You make" followed by the word "possible" in a large, bold, blue font. The letter "i" in "possible" is repeated nine times, each in a different color: blue, green, blue, orange, red, orange, blue, green, blue.



Deploying ISE in a Dynamic Environment

(Best Practice)

Clark Gambrel, CCIE #18179
@clarkgambrel
BRKSEC-2059



June 9-13, 2019 • San Diego, CA

#CLUS



Abstract

Managing a secure, yet flexible network in today's public access environments can be very challenging. Public access networks in areas like universities, hospitals and airports host a broad array of devices, both privately owned and corporately managed. With the increasing importance of the Internet of Things, the variety of devices that need to connect to these public networks is rapidly increasing. Cisco Identity Services Engine (ISE) plays an integral role in controlling the access to these dynamic public networks. This session will share lessons learned (best practice) from an ISE escalation engineer in troubleshooting complex customer environments.

Introduction



You make customer experience **possible**



Bruce Gambrel, CCIE #18179

Technical Leader - Engineering

cgambrel@cisco.com

✉ @ClarkGambrel





Clark

Bruce Gambrel, CCIE #18179

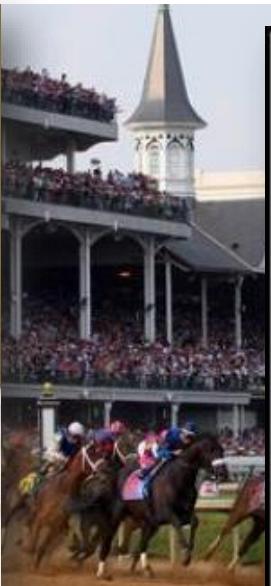
Technical Leader - Engineering

cgambrel@cisco.com



@ClarkGambrel





KENTUCKY

"I might be a redneck"

Housekeeping



You make networking **possible**

Cisco Policy and Access Sessions: Building Blocks

Sunday

08:00

TECSEC-3672

Implementing
Identity Services
Engine 2.6

Monday

16:00

BRKSEC-1003

Cisco Platform
Exchange Grid
(pxGrid) Inside Out

Tuesday

08:00

BRKSEC-2059

Deploying ISE in a
Dynamic
Environment (Best
Practices)

Wednesday

08:00

BRKSEC-3229

ISE under
magnifying glass.
How to troubleshoot
ISE

Thursday

08:00

BRKSEC-3432

Advanced ISE –
Architect, Design and
Scale ISE for your
production network

16:00

BRKCCIE-3222

Identity
Management and
Access Control for
CCIE Candidates

08:00

BRKSEC-3018

IPV6 AAA, Port-
Based auth and
Security
Implementation

13:00

BRKSEC-3690

Advanced Security
Group Tags: The
Detailed Walk
Through

08:00

BRKSEC-3016

Demystifying Zero Trust
– What does it really
mean? How do you
achieve it with Cisco and
DUO Security

16:00

BRKSEC-2430

ISE Deployment
Staging and
Planning

16:00

BRKSEC-2026

Building Network
Security Policy
Trough Data
Intelligence

13:00

BRKSEC-2039

Cisco Medical
Device
Segmentation

Cisco Webex Teams

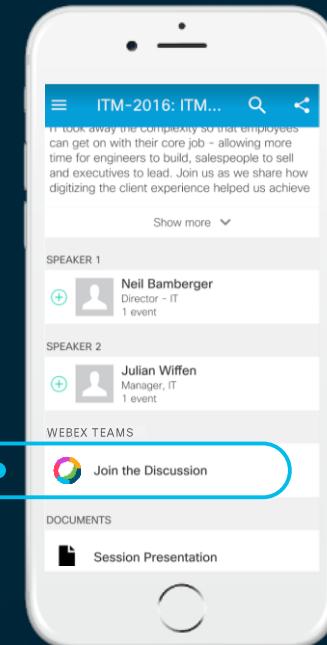
Questions?

Use Cisco Webex Teams to chat with the speaker after the session

How

- 1 Find this session in the Cisco Live Mobile 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

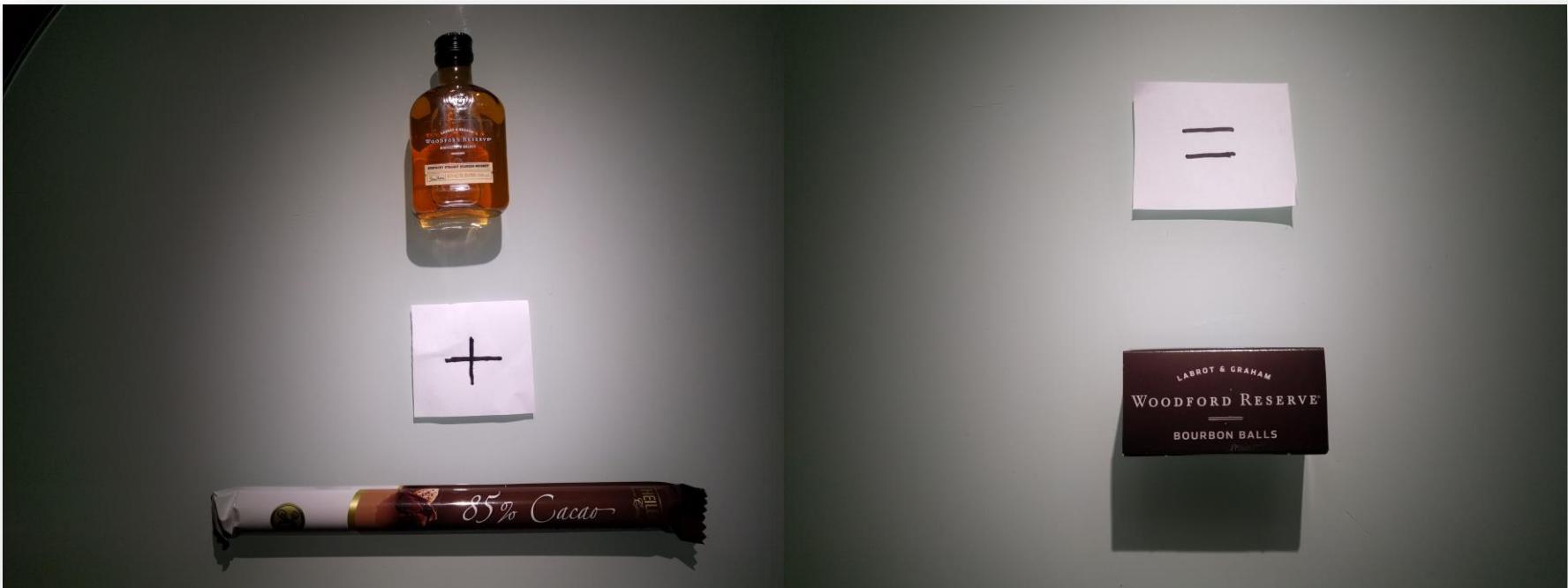
Webex Teams will be moderated by the speaker until June 16, 2019.



cs.co/ciscolivebot#BRKSEC-2059

Please ask questions!!!

“What are bourbon balls?”



Agenda

- Introduction
- Housekeeping
- Public environments, Why are they so challenging?
- Advice – Words to live by in any environment (Best Practice!)
- WLC Best Practice Check List
- VMWare for ISE Best Practice Check List
- Load Balancer for ISE Best Practice Check List
- Conclusion

Public
environments,
Why are they so
challenging?



You make networking **possible**

Public environments, Why are they so challenging?

- On average each person carries 3.8 devices



Public environments, Why are they so challenging?

- On average each person carries 3.8 devices
- Each year new devices are introduced



Public environments, Why are they so challenging?

- On average each person carries 3.8 devices
- Each year new devices are introduced
- Devices add new technology enhancements,
i.e. TLS versions, mini browsers



New and Improved - <http://tv tropes.org>

Public environments, Why are they so challenging?

- On average each person carries 3.8 devices
- Each year new devices are introduced
- Devices add new technology enhancements,
i.e. TLS versions, mini browsers
- Device behavior differs from one OS version
to the next



Public environments, Why are they so challenging?



- Devices are mostly unmanaged

Public environments, Why are they so challenging?



- Devices are mostly unmanaged
- End users have different levels of knowledge when it comes to configuring their own devices

Public environments, Why are they so challenging?



- Devices are mostly unmanaged
- End users have different levels of knowledge when it comes to configuring their own devices
- Users expect a simple experience, similar to home use

Public environments, Why are they so challenging?



- Devices are mostly unmanaged
- End users have different levels of knowledge when it comes to configuring their own devices
- Users expect a simple experience, similar to home use
- Lots of configuration parameters on ISE, Wireless Controller, Load-balancer, etc which are correct?

Advice - Words to live by in any environment (Best Practice)

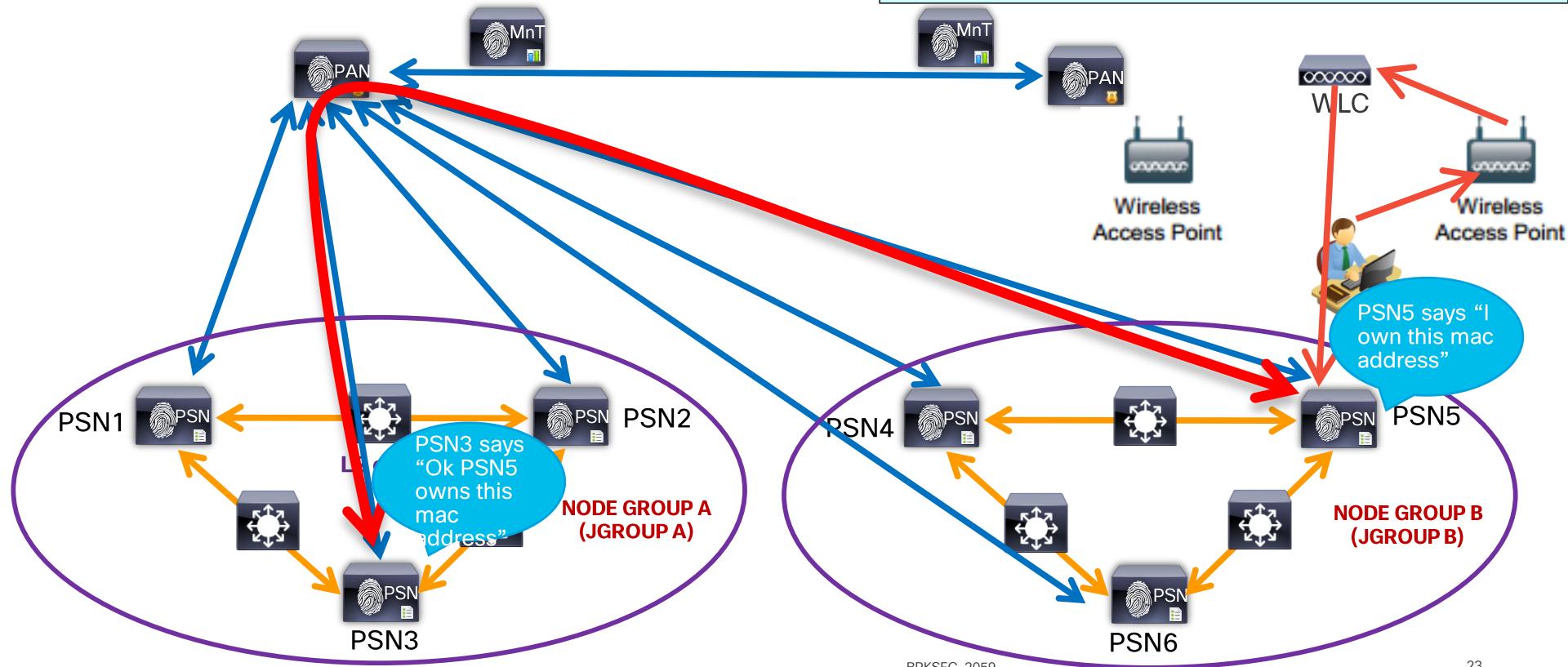


You make networking **possible**

Inter-Node Communications

Radius Flapping can be a real mess!

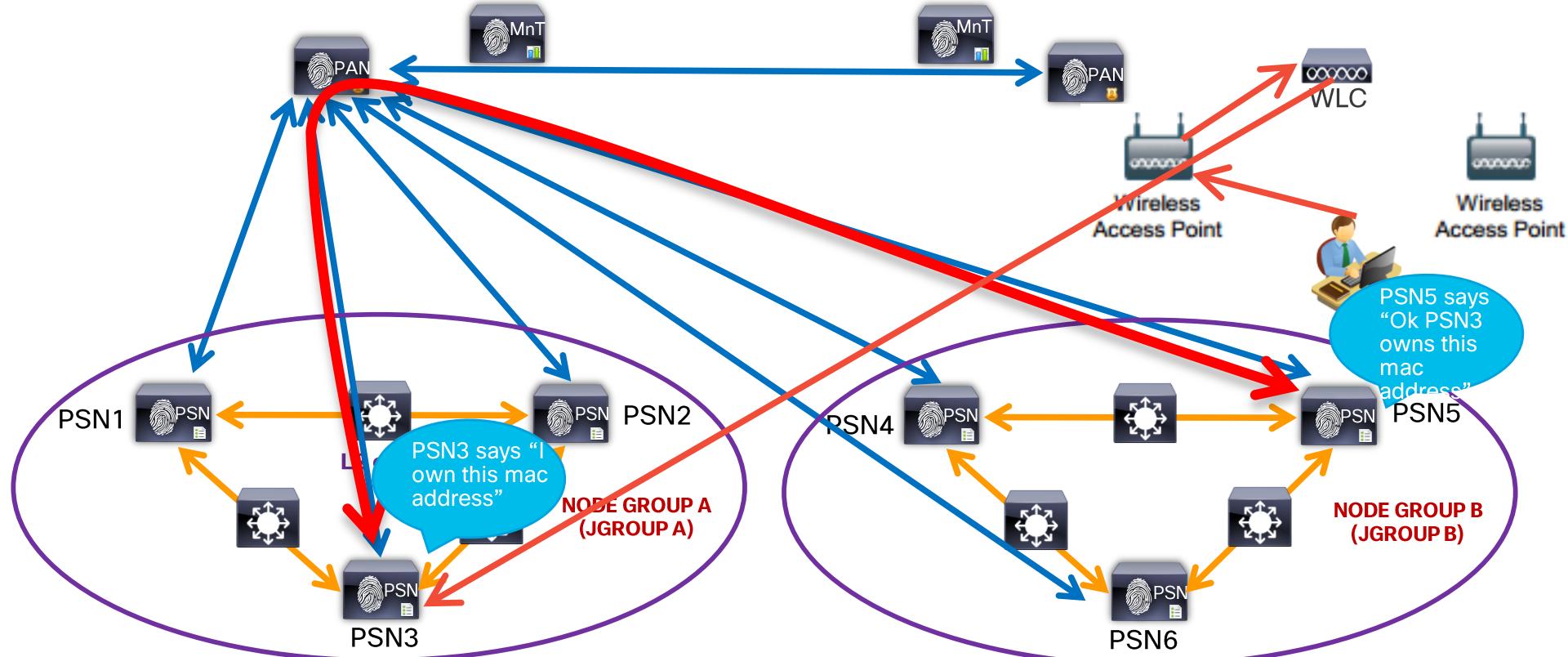
- Profiling sync leverages JGroup channels
- All replication outside node group must traverse PAN—including Ownership Change!
- If Local JGroup fails, then nodes fall back to Global JGroup communication channel.



Inter-Node Communications

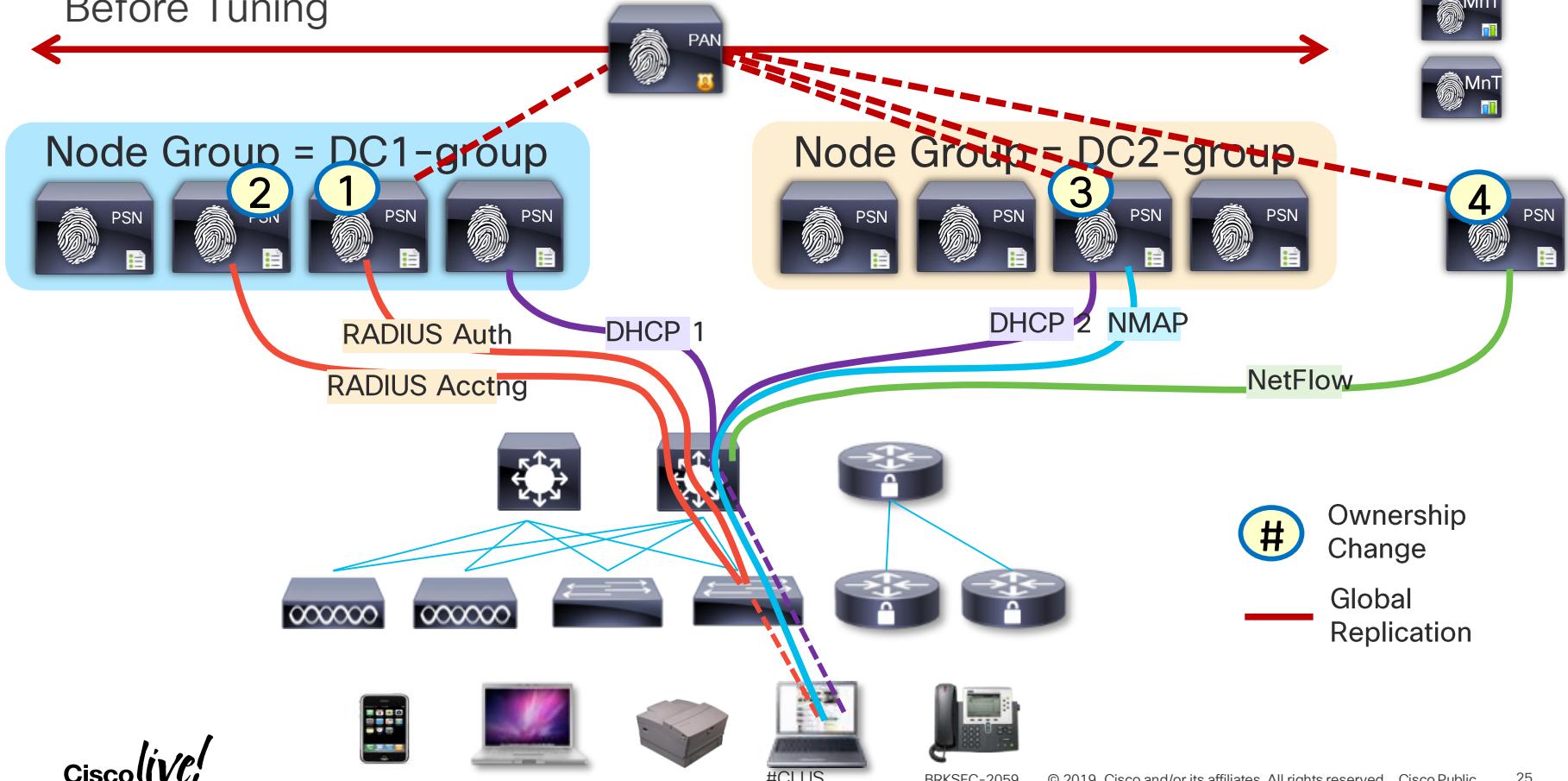
Radius Flapping can be a real mess!

- Ok, now Radius flapping occurs.
- This could be due to timeouts received to WLC or due to the “Radius NAC” accounting bug
- This will also happen if a PSN receives profiling information for an endpoint that it doesn’t own



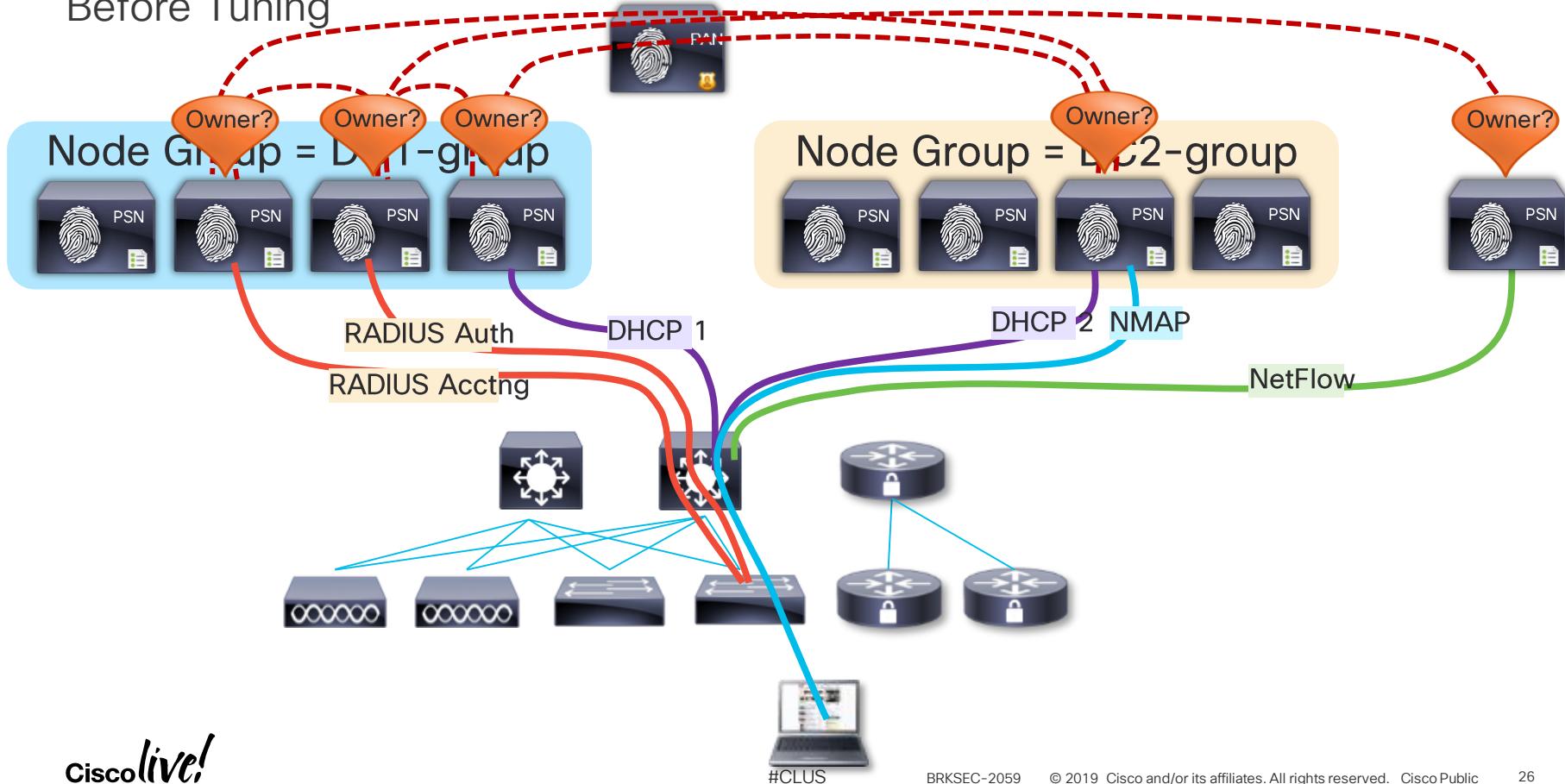
Profiling and Data Replication

Before Tuning



Impact of Ownership Changes

Before Tuning



WLC Best Practice Check List



You make networking **possible**

WLC Best Practice Check List

- Radius Authentication and Accounting timeout 5-10 seconds
- Enable Radius Fallback (Either Active or Passive)
- DISABLE Aggressive Failover in the CLI
- Don't send unintended traffic to ISE
- Set Interim update to 0 and enable
- Session Timeout 7200+ sec
- Enable Client Exclusion and set to 180 seconds and enable policies
- Client idle timeout 3600+ secs for 802.1x Keep at 300 secs for Open-SSID/Guest
- Avoid forcing roaming events with DCA policies that are too aggressive

Advice: Timers

A collection of antique pocket watches and alarm clocks, all showing different times, symbolizing the concept of time and timing.

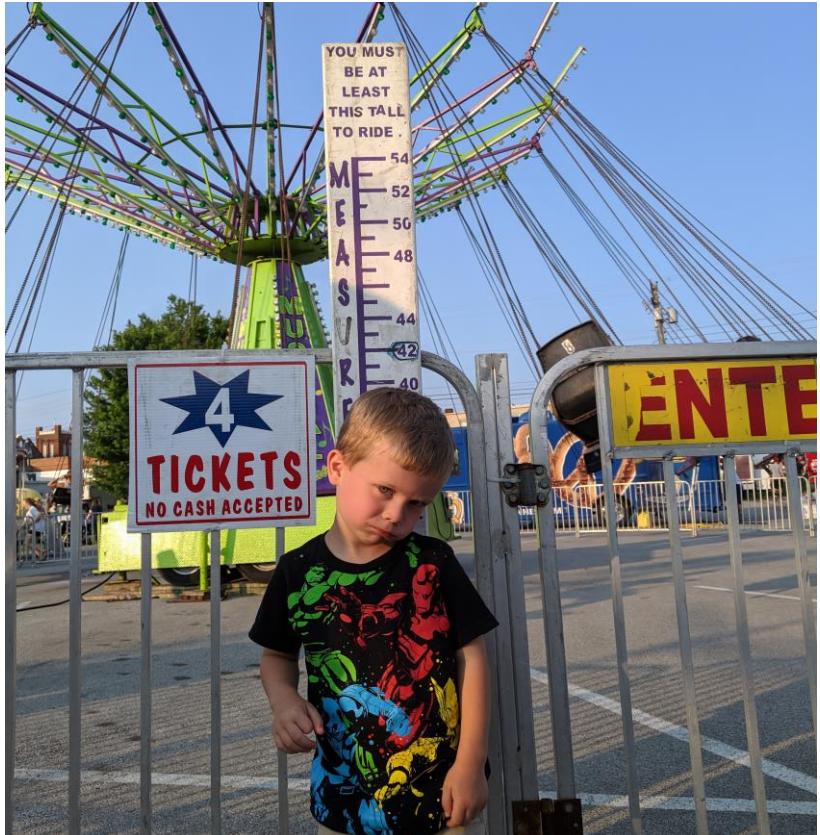
"I once told a NTP joke, the timing was perfect!"

Displaying a Clock Collection - www.doityourself.com

Advice: Timers

WLC: Radius

- Default timer value of 2 seconds is too short



Advice: Timers

WLC: Radius

- Default timer value of 2 seconds is too short
- During busy times, Authentication latency may increase and exceed the default value



Advice: Timers

WLC: Radius

- Default timer value of 2 seconds is too short
- During busy times, Authentication latency may increase and exceed the default value
- Use best practice value between 5-10 seconds, typically



Advice: Timers

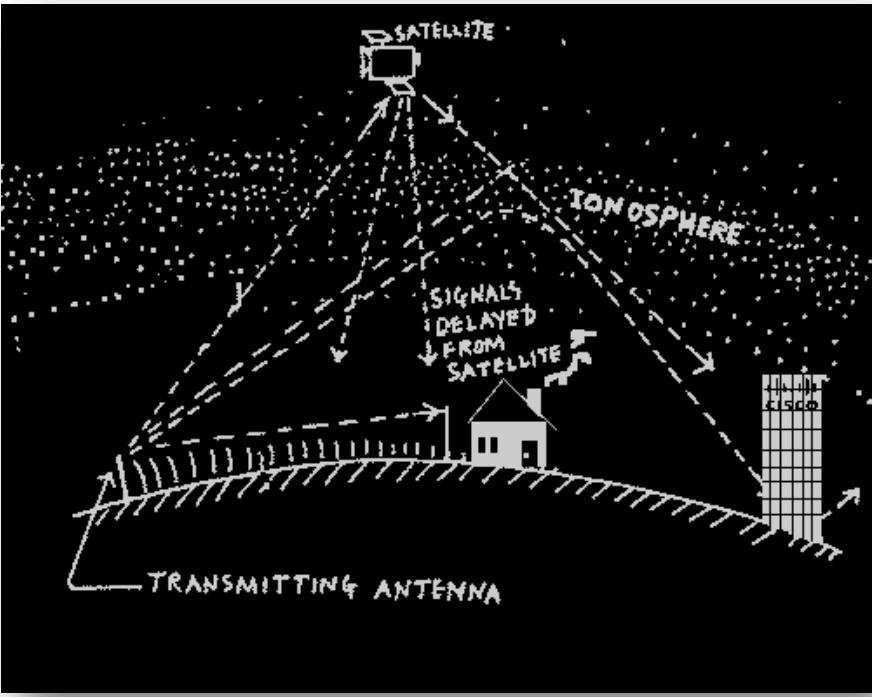
WLC: Radius



- Use timers appropriate to the environment (tune for your environment)

Advice: Timers

WLC: Radius



- Use timers appropriate to the environment (tune for your environment)
- Some remote/cloud based radius servers may have higher authentication latency and require some tweaking.

Advice: Timers

WLC: Radius - Continued

- Setting timers too long and the client might restart its session, retries from radius server will be dropped



PSN1

- Avoid unnecessary radius server flaps with timers that are too short



PSN2

- Radius **flapping** can have some major impacts on an ISE deployment

Advice: Timers - Radius

The screenshot shows the Cisco Controller web interface under the 'Security' tab. In the 'AAA' section, 'RADIUS' is selected, leading to the 'Authentication' sub-section. The 'RADIUS Authentication Servers > Edit' page is displayed. A red box highlights the 'Edit' button at the top right of the configuration area. The configuration fields include:

- Server Index: 1
- Server Address(Ipv4/Ipv6): 172.16.200.22
- Shared Secret Format: ASCII (dropdown)
- Shared Secret: (redacted)
- Confirm Shared Secret: (redacted)
- Key Wrap: (checkbox) (Designed for FIPS customers and requires a key wrap compliant RADIUS server)
- Port Number: 1812
- Server Status: Enabled (dropdown)
- Support for RFC 3576: Enabled (dropdown)
- Server Timeout: 5 seconds (highlighted with a red box)
- Network User: Enable (checkbox)
- Management: Enable (checkbox)
- Realm List: (link)
- IPSec: Enable (checkbox)

A large blue banner with white text 'Typically 5-10 seconds' is overlaid on the right side of the configuration area.

Advice: Timers - Radius

The screenshot shows the Cisco WebUI interface for managing RADIUS Accounting Servers. The top navigation bar includes links for MONITOR, WLANs, CONTROLLER, WIRELESS, SECURITY (which is highlighted), MANAGEMENT, COMMANDS, HELP, and FEEDBACK. On the left, a sidebar under the Security heading shows the AAA configuration, including General, RADIUS (selected), Authentication, Accounting (highlighted), Fallback, DNS, Downloaded AVP, TACACS+, LDAP, Local Net Users, MAC Filtering, Disabled Clients, User Login Policies, AP Policies, and Password Policies. Below that are sections for Local EAP, Advanced EAP, Priority Order, Certificate, and Access Control Lists. The main content area is titled "RADIUS Accounting Servers > Edit". It displays the following configuration parameters:

Server Index	1
Server Address(Ipv4/Ipv6)	172.16.200.22
Shared Secret Format	ASCII
Shared Secret	***
Confirm Shared Secret	***
Port Number	1813
Server Status	Enabled
Server Timeout	5 seconds
Network User	<input checked="" type="checkbox"/> Enable
Realm List	
IPSec	<input type="checkbox"/> Enable

A red box highlights the "Server Timeout" field, which is set to "5 seconds". A blue box contains the following text:

Typically 5-10 seconds
Usually matches Auth server timeout value

Advice: Timers - Radius

The screenshot shows the Cisco WebUI interface. The top navigation bar includes links for MONITOR, WLANs, CONTROLLER, WIRELESS, SECURITY, MANAGEMENT, COMMANDS, HELP, and FEEDBACK. The SECURITY tab is selected. On the left, a sidebar under the Security heading lists AAA (General, RADIUS), TACACS+, Local EAP, Advanced EAP, Priority Order, Certificate, Access Control Lists, and Wireless Protection. The RADIUS section is expanded, showing Authentication, Accounting, Fallback, DNS, and Downloaded AVP. The Fallback Parameters page is displayed, with a red box highlighting the title 'RADIUS > Fallback Parameters'. It contains three fields: 'Fallback Mode' set to 'active', 'Username' set to 'cisco-probe', and 'Interval in sec.' set to '300'.

RADIUS > Fallback Parameters

Fallback Mode: active

Username: cisco-probe

Interval in sec.: 300

Enable either passive or active. 300 seconds is a good starting point

Advice: Timers

WLC: Radius - Continued

- Make sure that **Aggressive Failover is disabled** in the command line of the WLC

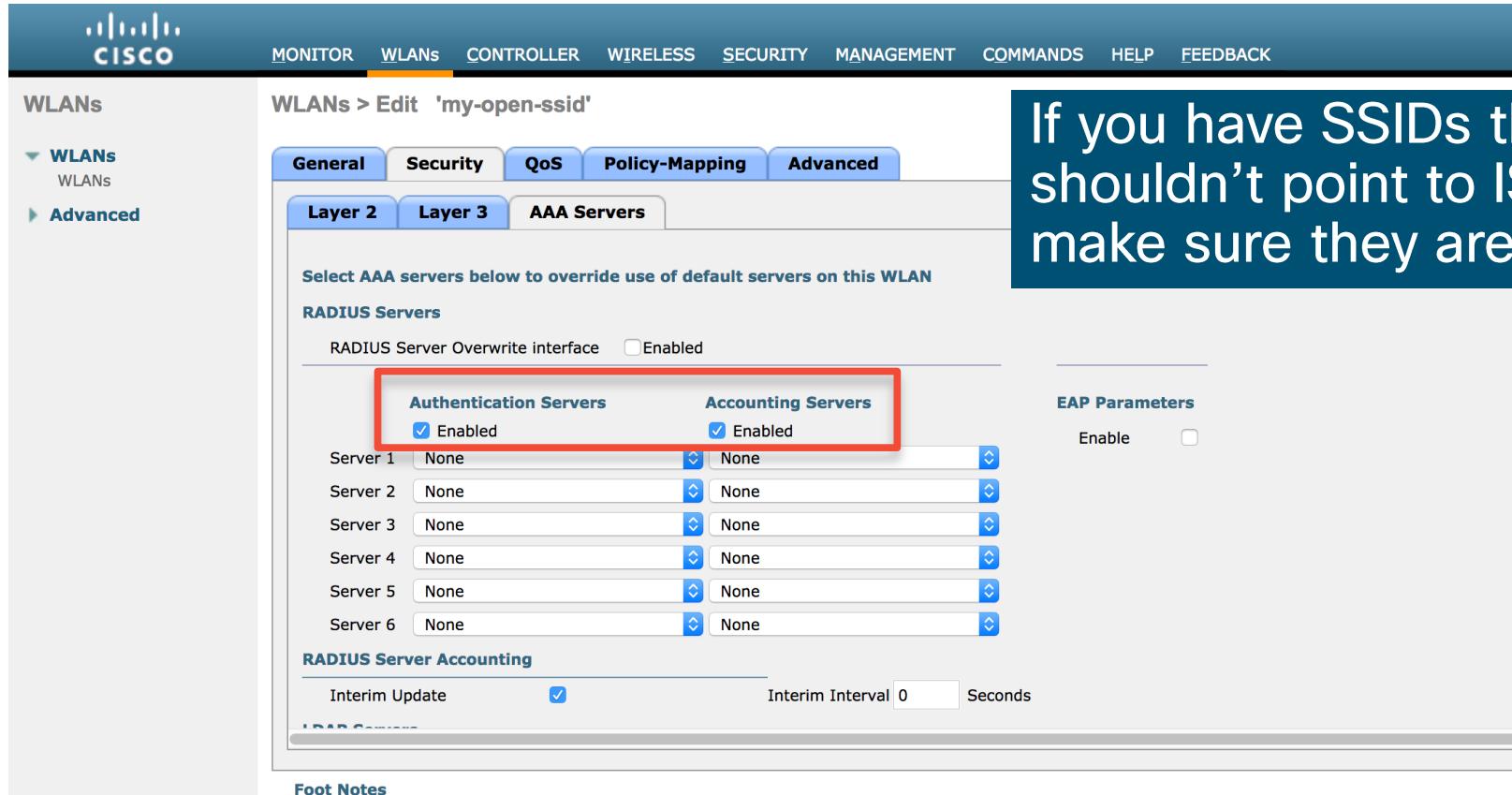
```
(Cisco Controller) >show radius summary
```

```
Vendor Id Backward Compatibility..... Disabled
Call Station Id Case..... lower
Acct Call Station Id Type..... AP's Radio MAC Address:SSID
Auth Call Station Id Type..... AP's Radio MAC Address:SSID
Aggressive Failover..... Disabled
Keywrap..... Disabled
Fallback Test:
  Test Mode..... Active
  Probe User Name..... cisco-probe
  Interval (in seconds)..... 300
MAC Delimiter for Authentication Messages..... hyphen
MAC Delimiter for Accounting Messages..... hyphen
```

This can have a big impact
on ISE and Wireless Auths
in general

```
(Cisco Controller) >config radius aggressive-failover disable
```

Advice: Timers - WLANs



The screenshot shows the Cisco Identity Services Engine (ISE) web interface for managing WLANs. The top navigation bar includes links for MONITOR, WLANs, CONTROLLER, WIRELESS, SECURITY, MANAGEMENT, COMMANDS, HELP, and FEEDBACK. The left sidebar shows a tree structure with WLANS selected, and sub-options for WLANs and Advanced. The main content area is titled "WLANs > Edit 'my-open-ssid'". It features tabs for General, Security, QoS, Policy-Mapping, Advanced, Layer 2, Layer 3, and AAA Servers. The AAA Servers tab is active. A note at the top says "Select AAA servers below to override use of default servers on this WLAN". Under "RADIUS Servers", there is a section for "Authentication Servers" and "Accounting Servers", both of which have checkboxes labeled "Enabled" checked and highlighted with a red box. Below this is a table for "RADIUS Server Accounting" with fields for "Interim Update" (checkbox checked) and "Interim Interval" (set to 0 seconds). The bottom of the page has a "Foot Notes" section.

If you have SSIDs that shouldn't point to ISE, make sure they are not!

Advice: Timers - WLANs

Interim Update

- WLC 7.6:
 - Recommended setting: **Disabled**
- WLC 8.0+:
 - Recommended setting: **Enabled with Interval set to 0**
 - Behavior: Only send update on IP address change
 - Device Sensor updates not impacted
- Settings mapped correctly on upgrades

The screenshot shows the 'AAA Servers' tab in the 'Layer 3' section of the WLC configuration. It displays settings for Radius Servers, Authentication Servers, and Accounting Servers. A red arrow points from the 'Enabled with Interval set to 0' note in the list above to the 'Radius Server Accounting' section at the bottom of the configuration screen.

Radius Servers

Radius Server Overwrite interface 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
Server 3 None	None
Server 4 None	None
Server 5 None	None
Server 6 None	None

Radius Server Accounting

Interim Update Interim Interval 0

Advice: Timers - WLANs

The screenshot shows the Cisco Wireless LAN Controller (WLC) interface. The top navigation bar includes links for MONITOR, WLANs (which is highlighted), CONTROLLER, WIRELESS, SECURITY, MANAGEMENT, COMMANDS, HELP, and FEEDBACK. On the left, a sidebar under the WLANs heading shows WLANS and Advanced options. The main content area is titled "WLANs > Edit 'GDCSecure'". Below this, there are tabs for General, Security, QoS, Policy-Mapping, and Advanced (which is selected). In the General tab, several settings are listed: Allow AAA Override (Enabled), Coverage Hole Detection (Enabled), Enable Session Timeout (checkbox checked, value 28800, labeled "Session Timeout (secs)", highlighted with a red box), AIRMONET IE (Enabled), Diagnostic Channel 18 (Disabled), and Override Interface ACL (IPv4 set to None, IPv6 set to None). To the right, sections for DHCP and OEAP are visible, each with their own configuration options.

Increase Session Timeout
to 2+ hours (7200+ sec), if
Enabled (recommended)

Advice: Timers - WLANs

The screenshot shows the Cisco Identity Services Engine (ISE) interface. The top navigation bar includes links for Home, Operations, Policy, Guest Access, and Administration. The main content area is titled "Authorization Profiles > Wireless_Guest" and displays the "Authorization Profile" configuration. The profile has the following settings:

- Name: Wireless_Guest
- Description: Authz for Wireless Guest
- Access Type: ACCESS_ACCEPT
- Network Device Profile: Cisco
- Service Template: (unchecked)
- Track Movement: (unchecked)

In the "Common Tasks" section, there are two options:

- Auto Smart Port (unchecked)
- Reauthentication (checked)

The "Reauthentication" section is highlighted with a red box and contains the following fields:

- Timer: 7200 (Enter value in seconds)
- Maintain Connectivity During Reauthentication: RADIUS-Request

This can also be sent as a Radius attribute in ISE under the AuthZ Profile

Advice: Timers - WLANs

The screenshot shows the Cisco Wireless LAN Controller (WLC) interface under the 'WLANS' tab. The 'Edit 'GDCSecure'' screen is displayed. A red box highlights the 'Client Exclusion' section, which includes a checked checkbox for 'Enabled' and a value of '180' in the 'Timeout Value (secs)' field. Other visible settings include 'Maximum Allowed Clients' set to '0', 'Static IP Tunneling' disabled, 'Wi-Fi Direct Clients Policy' set to 'Allow', 'Maximum Allowed Clients Per AP Radio' set to '200', 'Clear HotSpot Configuration' disabled, and 'Client user idle timeout(15-100000)' set to '3600'.

Increase Client Exclusion
to 180+ seconds (3+ mins)

Advice: Timers - WLANs

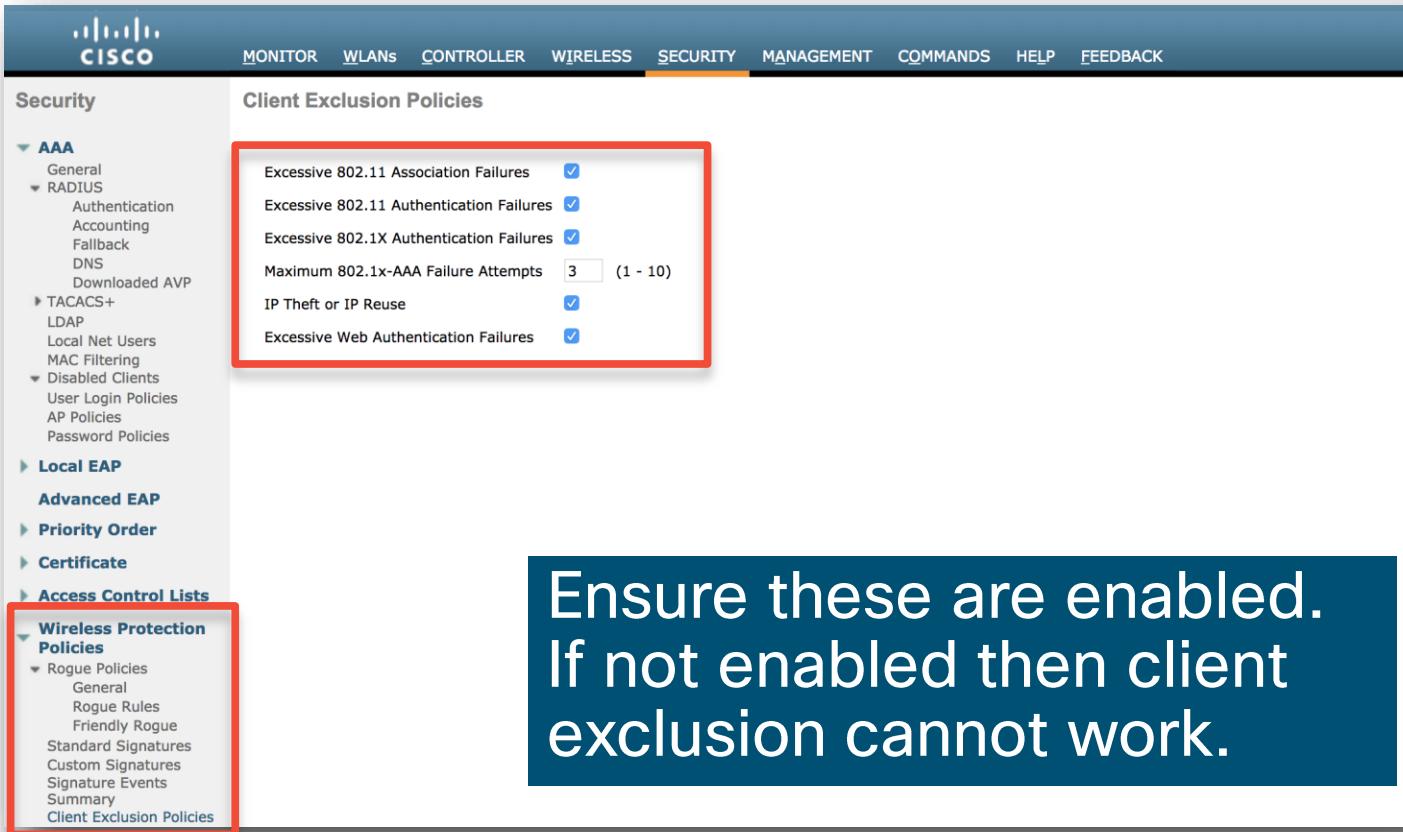
The screenshot shows the Cisco Security interface with the following navigation bar:

- MONITOR
- WLANs
- CONTROLLER
- WIRELESS
- SECURITY**
- MANAGEMENT
- COMMANDS
- HELP
- FEEDBACK

The main content area displays two sections, both highlighted with red boxes:

- Client Exclusion Policies**: This section contains several policy options:
 - Excessive 802.11 Association Failures
 - Excessive 802.11 Authentication Failures
 - Excessive 802.1X Authentication Failures
 - Maximum 802.1x-AAA Failure Attempts: (1 - 10)
 - IP Theft or IP Reuse
 - Excessive Web Authentication Failures
- Wireless Protection Policies**: This section contains the following sub-options:
 - Rogue Policies
 - General
 - Rogue Rules
 - Friendly Rogue
 - Standard Signatures
 - Custom Signatures
 - Signature Events
 - Summary
 - [Client Exclusion Policies](#)

Advice: Timers - WLANs



The screenshot shows the Cisco Wireless LAN Controller (WLC) interface under the 'SECURITY' tab. On the left, a navigation tree includes 'AAA', 'Local EAP', 'Advanced EAP', 'Priority Order', 'Certificate', 'Access Control Lists', and 'Wireless Protection Policies'. The 'Client Exclusion Policies' section is highlighted with a red box. It lists several policy items with checkboxes:

- Excessive 802.11 Association Failures (checked)
- Excessive 802.11 Authentication Failures (checked)
- Excessive 802.1X Authentication Failures (checked)
- Maximum 802.1x-AAA Failure Attempts: 3 (1 - 10)
- IP Theft or IP Reuse (checked)
- Excessive Web Authentication Failures (checked)

A large blue callout box on the right side of the page contains the text:

Ensure these are enabled.
If not enabled then client exclusion cannot work.

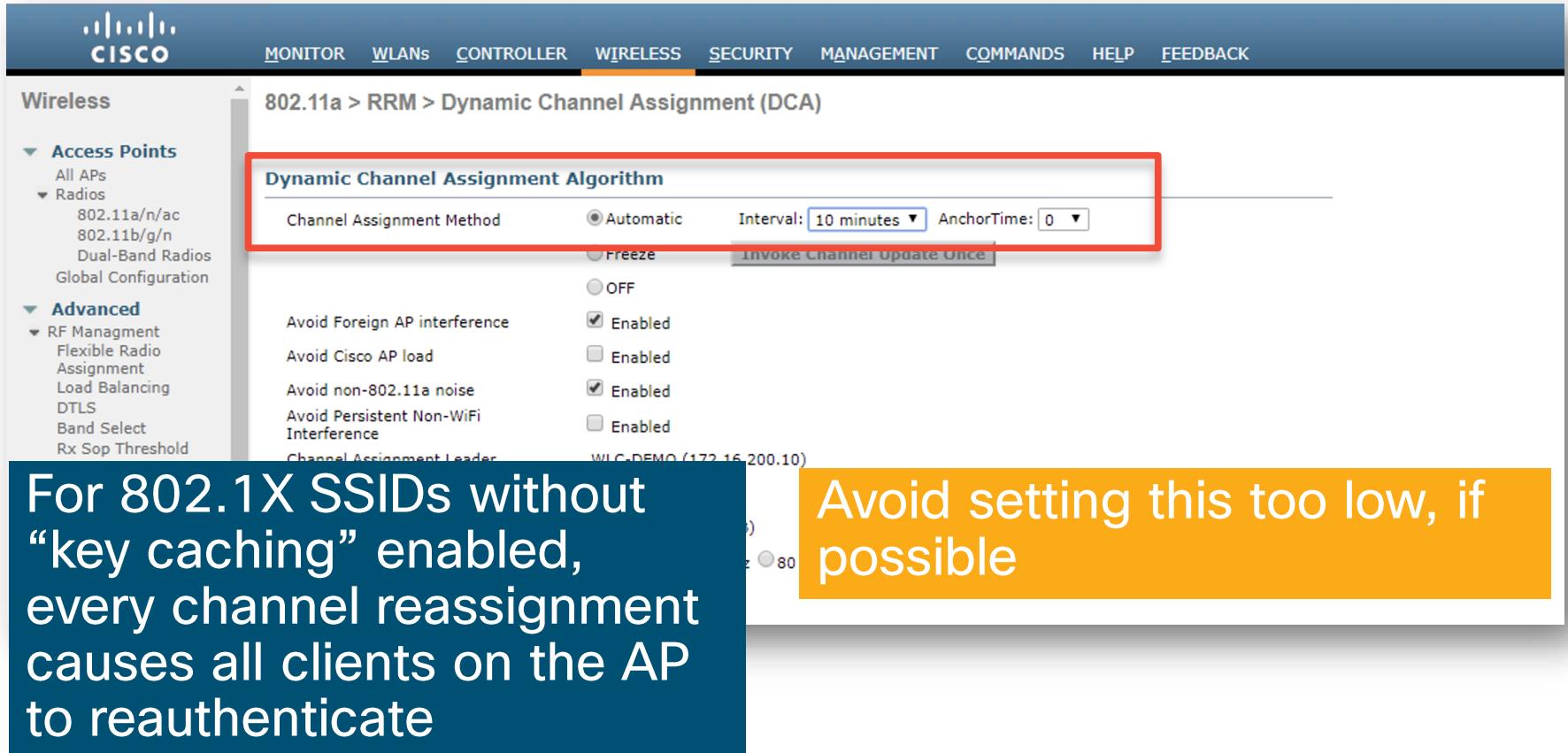
Advice: Timers - WLANs

The screenshot shows the Cisco Wireless LAN Controller (WLC) interface. In the top navigation bar, 'WLANS' is selected. On the left sidebar, 'WLANS' is expanded, and 'Advanced' is selected. The main content area shows the 'Edit 'GDCSecure'' configuration page. The 'Policy-Mapping' tab is active. A red box highlights the 'Client user idle timeout(15-100000)' field, which is set to 3600 seconds. Other visible settings include Client Exclusion (Enabled, 180s), Maximum Allowed Clients (0), Static IP Tunneling (Disabled), Wi-Fi Direct Clients Policy (Allow), Maximum Allowed Clients Per AP Radio (200), and Clear HotSpot Configuration (Disabled).

For 802.1X SSIDs, Increase Client Idle Timeout to 1 hour (3600 sec)

For Guest/Hotspot SSIDs, leave this low (300 sec) to free up resources (http redirect sessions) for clients that have disconnected

Advice: Timers - WLANs



The screenshot shows the Cisco Wireless LAN Controller (WLC) interface. The top navigation bar includes MONITOR, WLANs, CONTROLLER, WIRELESS (which is highlighted), SECURITY, MANAGEMENT, COMMANDS, HELP, and FEEDBACK. The left sidebar under the 'Wireless' heading has sections for Access Points (All APs, Radios: 802.11a/n/ac, 802.11b/g/n, Dual-Band Radios, Global Configuration), Advanced (RF Management: Flexible Radio Assignment, Load Balancing, DTLS, Band Select, Rx Sop Threshold), and a Channel Assignment Leader section showing 'WLC-DEMO (172.16.200.10)'.

The main content area displays the '802.11a > RRM > Dynamic Channel Assignment (DCA)' configuration. A red box highlights the 'Dynamic Channel Assignment Algorithm' section. It contains a table with two columns:

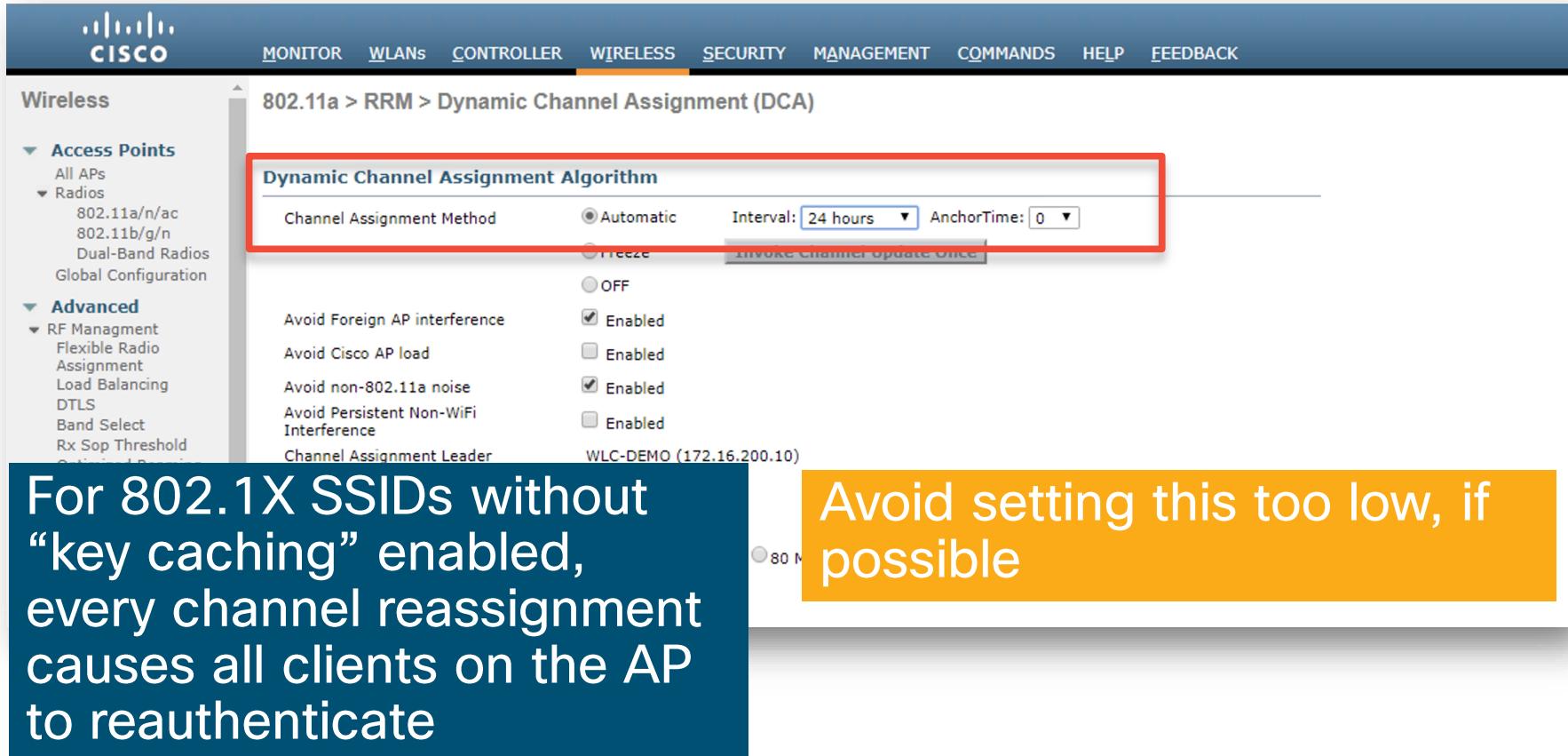
Channel Assignment Method	Setting
Automatic	Selected (radio button)
Freeze	Not selected (radio button)
OFF	Not selected (radio button)

Below the table, there are four checkboxes labeled 'Enabled':

- Avoid Foreign AP interference: Enabled (checkbox checked)
- Avoid Cisco AP load: Enabled (checkbox checked)
- Avoid non-802.11a noise: Enabled (checkbox checked)
- Avoid Persistent Non-WiFi Interference: Enabled (checkbox checked)

A yellow callout box on the right side of the slide contains the text: "For 802.1X SSIDs without ‘key caching’ enabled, every channel reassignment causes all clients on the AP to reauthenticate". Another yellow callout box on the right side of the configuration screen contains the text: "Avoid setting this too low, if possible".

Advice: Timers - WLANs



The screenshot shows the Cisco Wireless Controller (WLC) interface under the 'WIRELESS' tab. On the left, a sidebar lists 'Access Points' (All APs, Radios, 802.11a/n/ac, 802.11b/g/n, Dual-Band Radios, Global Configuration) and 'Advanced' settings (RF Management, Flexible Radio Assignment, Load Balancing, DTLS, Band Select, Rx Sop Threshold). The main pane displays '802.11a > RRM > Dynamic Channel Assignment (DCA)'. A red box highlights the 'Dynamic Channel Assignment Algorithm' section, which includes 'Channel Assignment Method' (set to 'Automatic'), 'Interval' (set to '24 hours'), and 'AnchorTime' (set to '0'). Below this, several checkboxes are listed: 'Avoid Foreign AP interference' (Enabled), 'Avoid Cisco AP load' (Enabled), 'Avoid non-802.11a noise' (Enabled), and 'Avoid Persistent Non-WiFi Interference' (Enabled). The 'Channel Assignment Leader' field shows 'WLC-DEMO (172.16.200.10)'. A yellow callout box on the right contains the text: 'For 802.1X SSIDs without “key caching” enabled, every channel reassignment causes all clients on the AP to reauthenticate'.

For 802.1X SSIDs without “key caching” enabled, every channel reassignment causes all clients on the AP to reauthenticate

Avoid setting this too low, if possible

VMWare for ISE Best Practice Check List



You make networking **possible**

VMWare for ISE Best Practice Check List

- Enable Reservations!!!!
- Enable Reservations!!!!
- Enable Reservations!!!!
- Mimic current shipping hardware
- Use Fast Storage
- SNAPSHOTS are NOT supported
- Use Vmotion at your own risk!

Advice: VM Resources

Reservations

- To be successful (and supported) ISE VMs must be built with **Dedicated Resources** that are equivalent to the hardware appliance.

Specifications listed in ISE 1.3+ Installation Guide

Table 2 Minimum VM Appliance Specifications for a Production Environment

Platform	Small VM Appliance (based on SNS-3415)
Processor	4 total cores (at 2.0 GHz or above) or a total minimum CPU allocation of 8000 MHz.
Memory	16 GB
Total Disk Space	200 GB to 2 TB. See Disk Space Requirements for more information.
Ethernet NICs	Up to 4 Gigabit Ethernet NICs

Large VM Appliance (based on SNS-3495)
8 total cores (at 2.0 GHz or above) or a total minimum CPU allocation of 16000 MHz.
32 GB
200 GB to 2 TB. See Disk Space Requirements for more information.
Up to 4 Gigabit Ethernet NICs

Advice: VM Resources

Reservations

- To be successful (and supported) ISE VMs must be built with **Dedicated Resources** that are equivalent to the hardware appliance.

Specifications listed in ISE 2.0.1+ Installation Guide

Platform	Small Appliance (based on SNS-395)	Large Appliance (based on SNS-395)
Processor	6 total cores (at 2.0 GHz or above) or a total minimum CPU allocation of 12000 MHz.	total cores (at 2.0 GHz or above) or a total minimum CPU allocation of 16000 MHz.
Memory	16 GB	64 GB
Total Disk Space	200 GB to 2 TB. See Disk Space Requirements, on page 5 for more information.	200 GB to 2 TB. See Disk Space Requirements, on page 5 for more information.
Ethernet NICs	Up to 6 Gigabit Ethernet NICs	Up to 6 Gigabit Ethernet NICs

Advice: Bugs

[CSCvd24296](#) – Revise platform selection rules for ISE installed on VMs

Description

Symptom:

ISE 3315,3355 and 3395 are only supported until ISE 1.4.

However, even in ISE 2.2, is still trying to classify VMs as these hardware.

Ideally there should be a check to ensure there are enough resources as per the supported hardware for that version

Conditions:

Profiles

ISE 3315 - 4 GB RAM; 4 cores CPU

ISE 3355 - 4 GB RAM; 4 cores CPU

ISE 3395 - 4 GB RAM; 8 cores CPU

ISE 3415 - 16 GB RAM; 4 cores CPU

ISE 3495 - 32 GB RAM; 8 cores CPU

ISE 3515 - 16 GB RAM; 12 cores CPU

ISE 3595 - 64 GB RAM; 16 cores CPU

When VM with 16 GB RAM and 8 cores is created; which doesn't match any hardware on top, ISE will end up matching 3395, when in fact the VM is better than a 3415.

Resolved: 2.3

Advice: Bugs

[CSCvh71644](#) – VMware OVA templates for SNS-35xx are not detected correctly in platform.properties-active

Description

Symptom:

Installed OVA templates for SNS-3595 or SNS-3515 don't match the correct platform.properties. This can be seen in a "show tech" or via the /opt/CSCOcpm/config/platform.properties-active file. It will show either ucsLarge or ucsSmall instead of sns3595 or sns3515.

Conditions:

Install OVA for SNS-35xx

Workaround:

None

Further Problem Description:

Resolved: New Templates Posted

Advice: VM Resources

Reservations

- To be successful (and supported) ISE VMs must be built with **Dedicated Resources** that are equivalent to the hardware appliance.

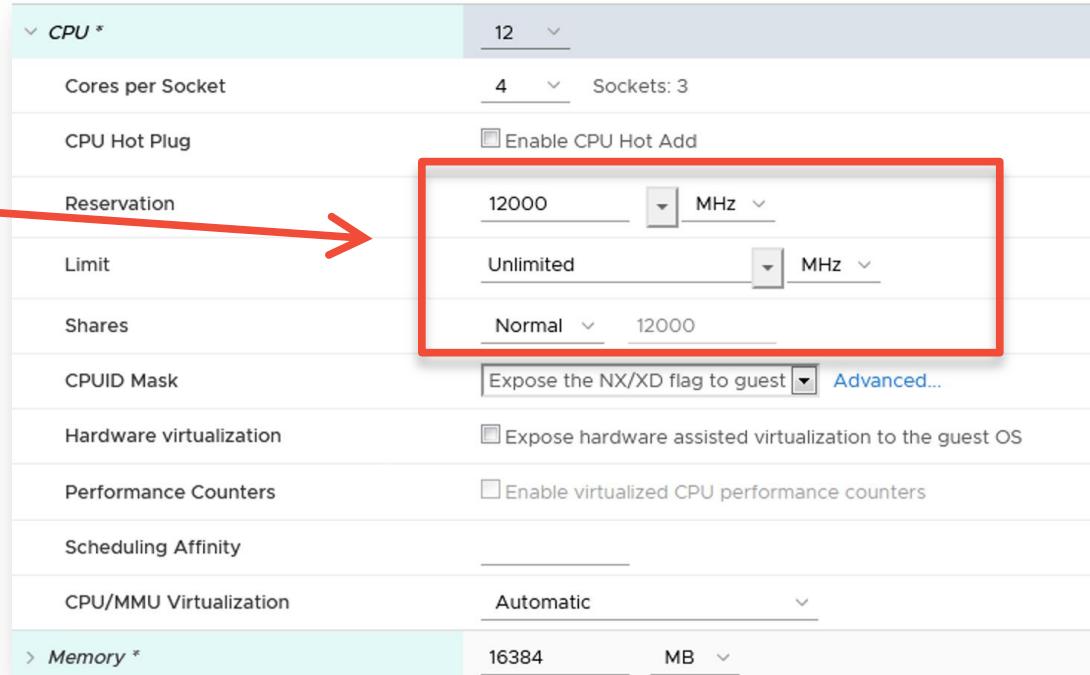
Specifications listed in ISE 2.0.1+ Installation Guide

Platform	Small VM Appliance (based on SNS-3515)	Medium VM Appliance (based on SNS-3595)	Large VM Appliance (Super MnT)
Processor	12 total cores GHz or above) with a minimum CPU allocation of 12000MHz.	16 total cores GHz or above) with a minimum CPU allocation of 16000MHz.	16 total cores 2.0 GHz or above) with a minimum CPU allocation of 16000MHz.
Memory	16 GB	64 GB	256 GB
Disk Space	200 GB-1.999 TB (depending on persona)	200 GB-1.999 TB (depending on persona)	200 GB-1.999 TB (depending on persona)
Ethernet NICs	2-6 (recommended)	2-6 (recommended)	2-6 (recommended)

Advice: VM Resources

Reservations

- To be successful (and supported) ISE VMs must be built with **Dedicated Resources** that are equivalent to the hardware appliance.



Advice: VM Resources

Reservations

- Avoid setting limits. Please note that some OVA templates on CCO contain this issue.



Caution

The screenshot shows the CPU configuration section of a virtual machine setup. It includes fields for Cores per Socket (12), Sockets (3), CPU Hot Plug, Enable CPU Hot Add, Reservation (with a 'Limits' section highlighted by a red box), and various performance and virtualization options like Expose NX/XD flag to guest. A large yellow 'Caution' watermark is overlaid diagonally across the interface.

Setting	Value	Unit
Cores per Socket	12	
Sockets	3	
Reservation	12000	MHz
Limit	12000	MHz
Normal	12000	
Expose the NX/XD flag to guest	<input checked="" type="checkbox"/>	
Expose hardware assisted virtualization to the guest OS	<input type="checkbox"/>	
Enable virtualized CPU performance counters	<input type="checkbox"/>	
CPU/MMU Virtualization	Automatic	
Memory	16	GB

Advice: Bugs

CSCvq00896 - ISE OVA templates are setting CPU limits

Description

Symptom:

Installed OVA templates might be setting limits on CPU usage. This has been seen in images posted on CCO.

Conditions:

Install OVA templates for 2.4 or 2.2 and you will see that limit is set for CPU usage. I have confirmed with ISE-2.4.0.357-6.5OVA-SNS3595-Medium-1200GBHD-64GBRAM-16CPU.ova and also on ISE-2.2.0.470-virtual-SNS3515-200.ova. I suspect all from 2.2 to 2.4 will have this issue.

Workaround:

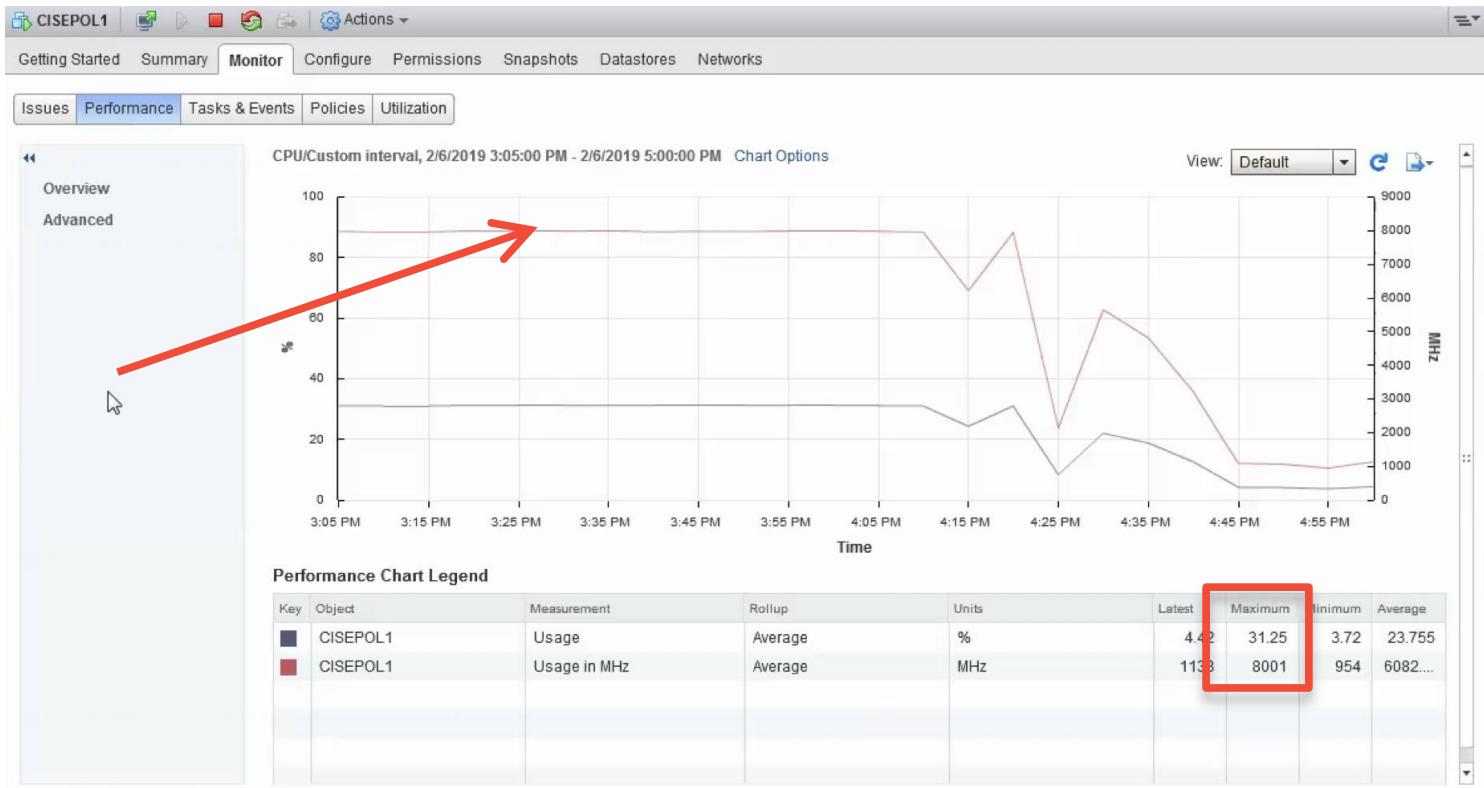
Customer can shutdown the ISE VM client, remove the limit and restart the ISE VM.

Further Problem Description:

Not Resolved: New Templates are needed. Workaround available.

Advice: VM Resources

Reservations



Advice: VM Resources

Reservations

- Avoid setting limits. Please note that some OVA templates on CCO contain this issue.



The screenshot shows a configuration interface for a virtual machine's CPU settings. A red box highlights the "Reservation" and "Limit" fields under the "CPU Hot Plug" section. Both fields are set to 8000 MHz. Other visible settings include:

Setting	Value	Unit
CPU *	12	
Cores per Socket	4	Sockets: 3
Reservation	8000	MHz
Limit	8000	MHz
Shares	Normal	12000
CPUID Mask	Expose the NX/XD flag to guest <input checked="" type="checkbox"/> Advanced...	
Hardware virtualization	<input type="checkbox"/> Expose hardware assisted virtualization to the guest OS	
Performance Counters	<input type="checkbox"/> Enable virtualized CPU performance counters	
Scheduling Affinity		
CPU/MMU Virtualization	Automatic	
Memory	16	GB

Advice: VM Resources

Reservations

- To be successful (and supported) ISE VMs must be built with **Dedicated Resources** that are equivalent to the hardware appliance.

The screenshot shows a configuration interface for a virtual machine. A red arrow points from the text in the slide to the 'Memory' section of the configuration. The 'Memory' section includes fields for 'Reservation' (set to 16384 MB), 'Limit' (set to Unlimited), and 'Shares' (set to Normal). A checkbox labeled 'Reserve all guest memory (All locked)' is checked. Below the memory section, other resource settings are listed: 'Hard disk 1' (200 GB), 'SCSI controller 0' (VMware Paravirtual), 'Network adapter 1' (VLAN_200), and 'Network adapter 2' (VLAN_200). The 'Reservation' field is highlighted with a red box.

Advice: VM Resources

Reservations

- To be successful (and supported) ISE VMs must be built with **Dedicated Resources** that are equivalent to the hardware appliance.
- In 1.3 we added OVA Templates for deploying SNS-3415 and SNS-3495 equivalent hardware. That has been expanded to include the SNS-3515 and SNS-3595 platforms as well.
- It is **highly recommended** that you use these templates!

Release 2.1.0	
File Information	Release Date
OVA file - Virtual SNS-3415 ISE-2.1.0.474-virtual-SNS3415.ova	31-MAY-2016
OVA file - Virtual SNS-3495 ISE-2.1.0.474-virtual-SNS3495.ova	31-MAY-2016
OVA file - Virtual SNS-3515 ISE-2.1.0.474-virtual-SNS3515.ova	31-MAY-2016
OVA file - Virtual SNS-3595 ISE-2.1.0.474-virtual-SNS3595.ova	31-MAY-2016

Advice: VM Resources

Reservations

- To be successful (and supported) ISE VMs must be built with **Dedicated Resources** that are equivalent to the hardware appliance.
- In 1.3 we added OVA Templates for deploying SNS-3415 and SNS-3495 equivalent hardware. That has been expanded to include the SNS-3515 and SNS-3595 platforms as well.
- It is highly recommended that you use these templates!

Caution

Release 2.2.0

File Information

Release Date ▾

ISE 2.2 OVA file - Virtual SNS-3495 (recommend for PAN or MnT)
ISE-2.2.0.470-virtual-1.2TB-SNS3495.ova

31-JAN-2017

ISE 2.2 OVA file - Virtual SNS-3595 (recommend for PAN or MnT)
ISE-2.2.0.470-virtual-1.2TB-SNS3595.ova

31-JAN-2017

ISE 2.2 OVA file - Virtual SNS-3415 200GB (recommend for PSN or PxGrid)
ISE-2.2.0.470-virtual-200GB-SNS3415.ova

31-JAN-2017

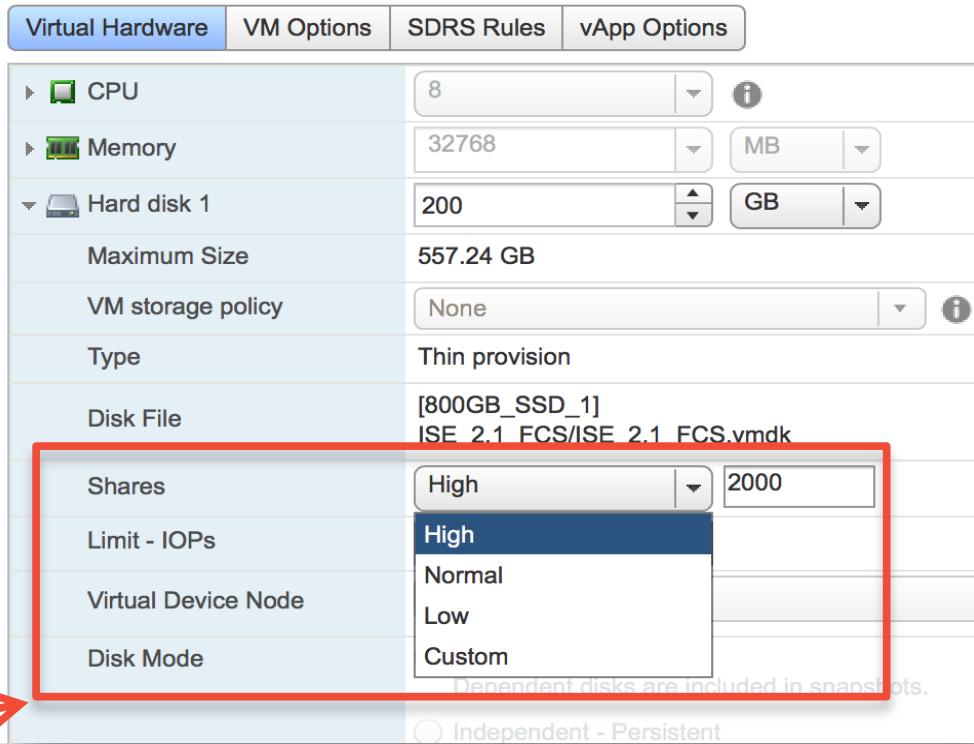
ISE 2.2 OVA file - Virtual SNS-3495 200GB (recommend for PSN or PxGrid)
ISE-2.2.0.470-virtual-200GB-SNS3495.ova

31-JAN-2017

Advice: VM Resources

Reservations

- Admin and MnT nodes rely heavily on disk usage (read/writes).
- Deploying ISE in VMware environments where shared disk storage is utilized may not give a like disk performance when compared to physical appliances
- **Increasing the number of disk shares** that a node is allocated can in most cases increase performance of the node.



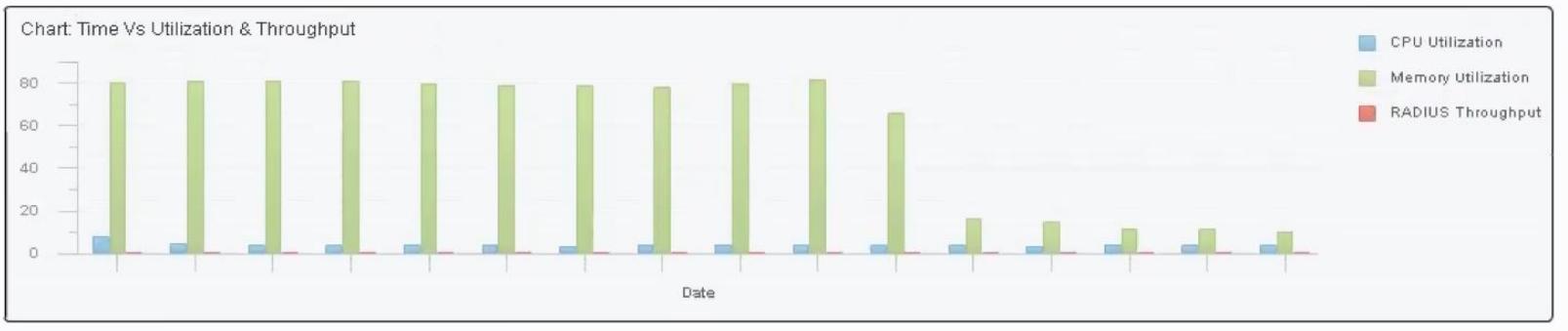
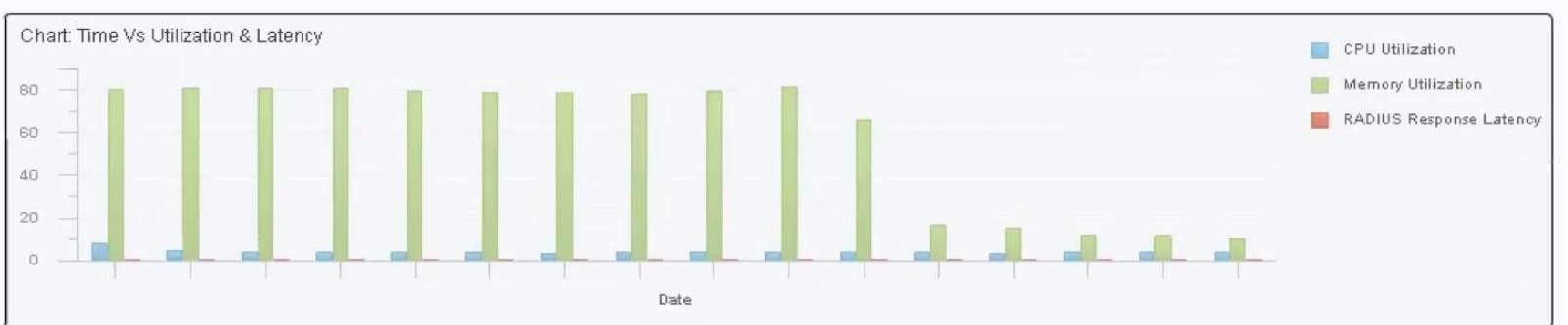
Advice: VM Resources

Reservations - Before & After Chart

From 05/26/2016 12:00:00 AM to 05/26/2016 03:58:56 PM					Generated at 2016-05-26 15:58:56.55
Health Summary					
Logged At	CPU Utilization (%)	Memory Utilization (%)	RADIUS Response Latency (ms)	RADIUS Throughput (mps)	
2016/05/26 00:00:00	8.14	80.18	0.00	0.00	
2016/05/26 01:00:00	4.88	81.28	0.00	0.00	
2016/05/26 02:00:00	4.08	81.41	0.00	0.00	
2016/05/26 03:00:00	3.89	81.22	0.00	0.00	
2016/05/26 04:00:00	4.08	79.99	0.00	0.00	
2016/05/26 05:00:00	3.90	79.36	0.00	0.00	
2016/05/26 06:00:00	3.73	78.96	0.00	0.00	
2016/05/26 07:00:00	4.06	78.34	0.00	0.00	
2016/05/26 08:00:00	4.47	78.81	0.00	0.00	
2016/05/26 09:00:00	3.96	82.16	0.00	0.00	
2016/05/26 10:00:00	4.00	66.06	0.00	0.00	
2016/05/26 11:00:00	4.01	16.61	0.00	0.00	
2016/05/26 12:00:00	3.73	17.91	0.00	0.00	
2016/05/26 13:00:00	4.48	11.82	0.00	0.00	
2016/05/26 14:00:00	4.10	11.55	0.00	0.00	
2016/05/26 15:00:00	3.86	10.69	0.00	0.00	

Advice: VM Resources

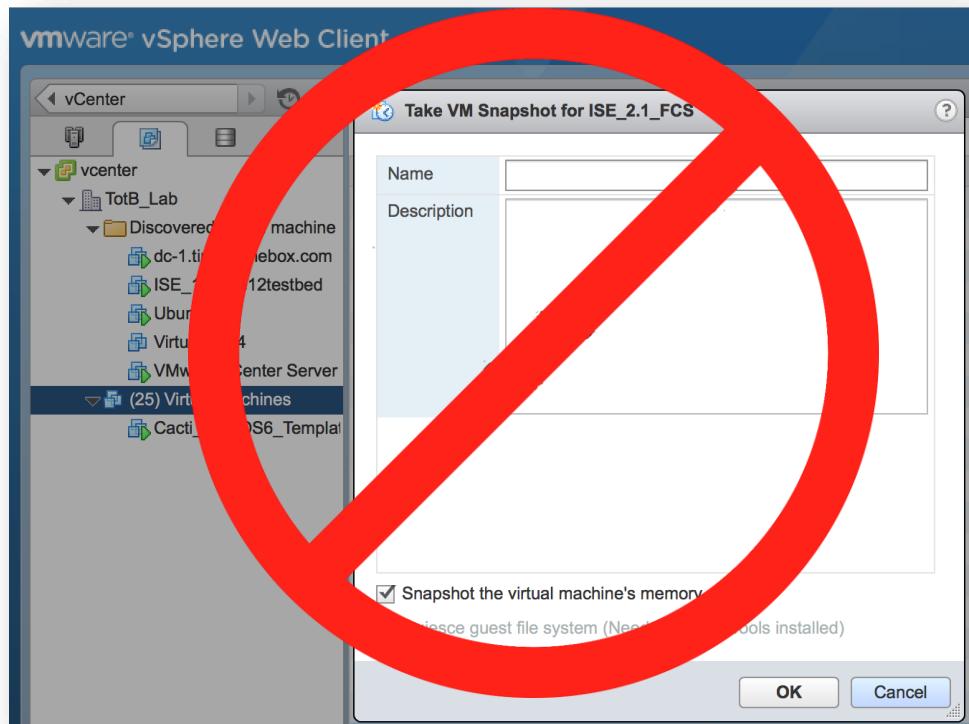
Reservations – Before & After Graph



Advice: VM Settings

Settings

- Snapshots are not supported!



Advice: VM Settings

Settings

- Snapshots are not supported!
- Use vMotion at your own risk!
- vMotion is only supported if the services are stopped or the guest is shutdown.



ISE Best Practice Check List



You make networking **possible**

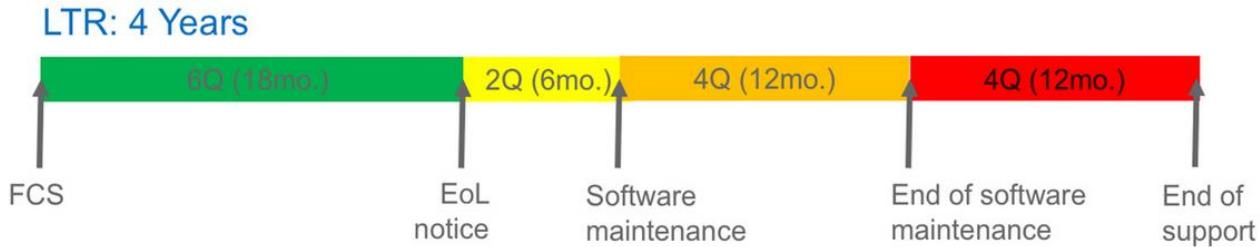
ISE Best Practice Check List

- Long vs Short lived releases
- Size correctly
- Know your clients
- Ensure suppression with rejection is enabled
- Enable Endpoint Attribute Filter
- Avoid ordering policy in a way that does unnecessary lookups (AD)
- Reduce the number of Endpoint Map Ownership Changes
- Watch out for misbehaving clients!

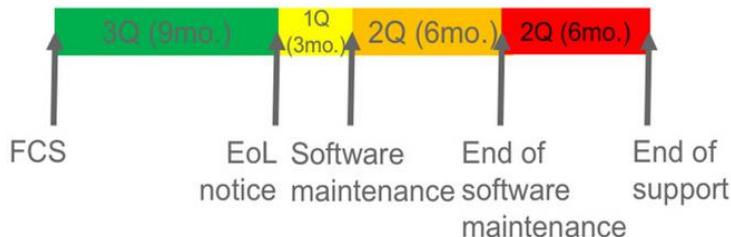
Advice: Versions

Information

- ISE releases have a "Long lived"-“Short lived” cadence



STR: 2 Years



Advice: Versions

Information

- ISE releases have a “Long lived”–“Short lived” cadence
- Releases follow currently an even/odd or every other pattern

ISE Version	Release Duration
2.01	Long Lived
2.1	Short Lived
2.2	Long Lived
2.3	Short Lived
2.4	Long Lived
???	???

Advice: Versions

Information

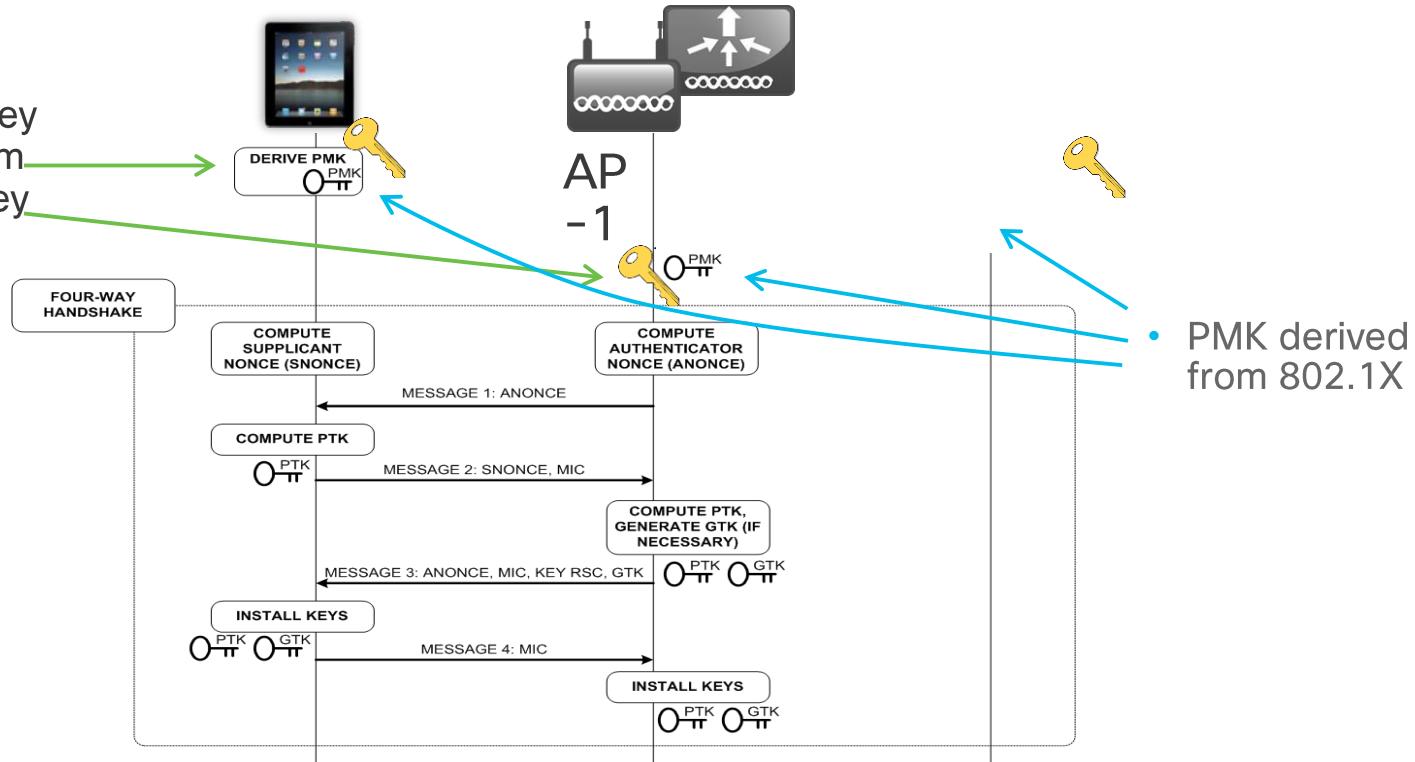
- ISE releases have a “Long lived”–“Short lived” cadence
- Releases follow currently an even/odd or every other pattern

ISE Version	Release Duration
2.01	Long Lived
2.1	Short Lived
2.2	Long Lived
2.3	Short Lived
2.4	Long Lived
2.6	Long Lived

Advice: Sizing

802.1x requires authentication for encryption

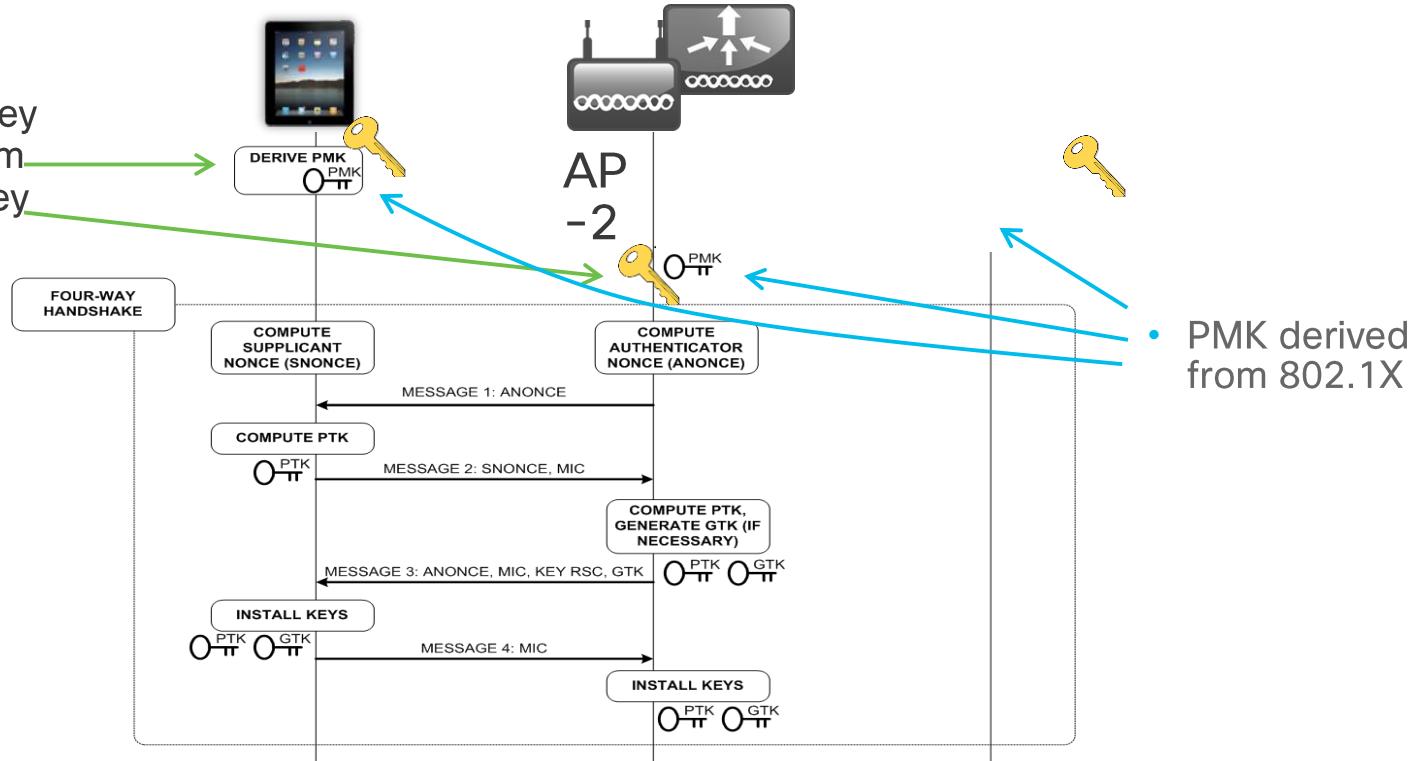
- Pairwise Master Key (PMK) derived from the Pre-Shared Key (PSK)



Advice: Sizing

Without key caching, this happens on every 802.1x roam

- Pairwise Master Key (PMK) derived from the Pre-Shared Key (PSK)



Advice: Sizing

Endpoint Behavior

- Different Endpoints behave differently on a network
- Because of this we need to consider the types of endpoints when sizing deployments
- Mobile (handheld) devices are the most demanding due to wireless/power restrictions
- Based on observations from many deployments, a 1x/2x/5x ratio is a good rule of thumb



=1X



=2X



=5X

Advice: Sizing

Mobile devices typically have...

- Less RF Output power
- Fewer/Smaller Antennas
- Lack support for multiple bands
2.4/5 GHz (some models)



Advice: Sizing

As a Result...

- Roam more often (up to 5x)
- Roam more aggressively
- Repeated Sleep/Wake Cycles to conserve battery.



Advice: Sizing

Maximum Concurrent Sessions

- Typically, deployment sizing has been performed using “Maximum Concurrent Sessions” as the baseline.

Table 1. Maximum Supported Sessions per Deployment Model

Deployment Model	Platform	Maximum Sessions
Standalone (All personas on a single node)	3615	10,000
	3655	25,000
	3695	50,000
	3515	7,500
	3595	20,000
Basic 2-node deployment (redundant)	3615	10,000
	3655	25,000
	3695	50,000
	3515	7,500
	3595	20,000
Hybrid-Distributed deployment (Admin and MnT on same appliance; Policy Service on dedicated appliance)	3615 as PAN and MnT	10,000
	3655 as PAN and MnT	25,000
	3695 as PAN and MnT	50,000
	3515 as PAN and MnT	7,500
	3595 as PAN and MnT	20,000
Dedicated (PAN, MnT, PXG, and PSN Nodes)	3595 as PAN and MnT	500,000
	3655 as PAN and MnT	500,000
	3695 as PAN/MnT	2,000,000

Maximum Supported Sessions for Each Deployment Model 2.6

Advice: Sizing

Maximum Concurrent Sessions

- Typically, deployment sizing has been performed using “Maximum Concurrent Sessions” as the baseline.

Table 2. Maximum Active Sessions per PSN

Scaling per PSN ¹	Max Active Sessions
SNS 3615	10,000
SNS 3655	50,000
SNS 3695	100,000
SNS 3515	7,500
SNS 3595	40,000

Maximum Supported Sessions per PSN model 2.6

Advice: Sizing

Maximum Concurrent Sessions

- Typically, deployment sizing has been performed using “Maximum Concurrent Sessions” as the baseline.
- This is not the complete picture



Advice: Sizing

Maximum Concurrent Sessions

- This scaling is based upon normal load.
- Sessions would flow in gradually overtime and become active.



Advice: Sizing

Maximum Concurrent Sessions

- But happens during peak times or Network Device reboots?
- Traffic can be too much and exceed the "Maximum TPS" for a node or deployment.



Advice: Sizing

Consider Authentications/Second or TPS

- You should also consider the auths/sec
- TPS rates for both RADIUS and TACACS+ should be factored

Authentication values are approximate values. When determining how many PSN is needed for the deployment please use Maximum Concurrent Sessions, RADIUS and TACACS+ authentication rates as your guidelines. Authentication performance for specific use cases is also provided in case it is required to size out the deployment.

ISE Performance and Scale - <https://cs.co/ise-perf-scale>

Advice: Sizing

Consider Authentications/Second or TPS

- You should also consider the auths/sec
- TPS rates for both RADIUS and TACACS+ should be factored

ISE 2.6 RADIUS Performance

Performance per platform.

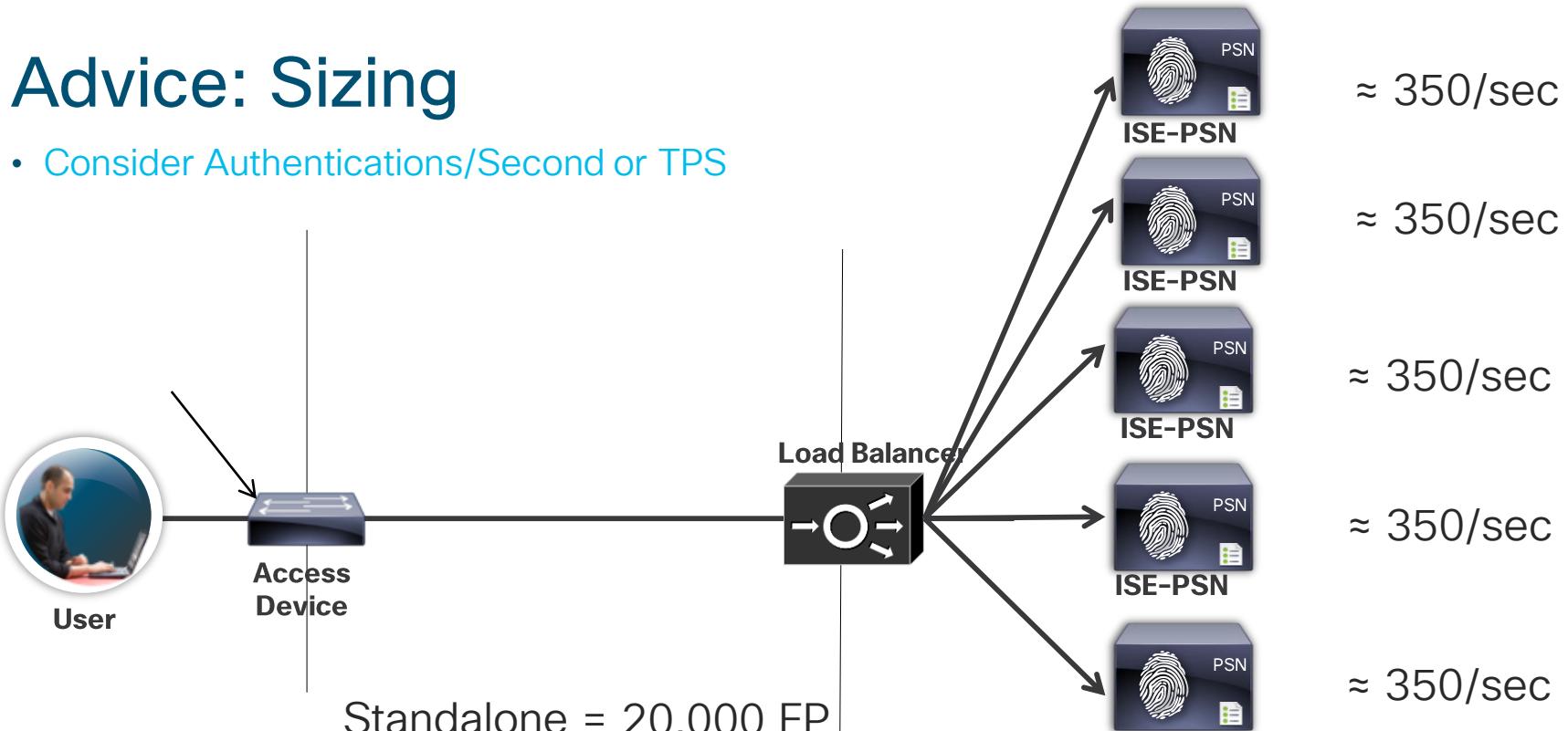
Authentications per second with PSN only persona (Approximate values)

Authentication Method	Identity Store	Cisco SNS-3595 (auths / second)	Cisco SNS-3615 (auths / second)	Cisco SNS-3655 (auths / second)	Cisco SNS-3695 (auths / second)
PAP	Internal	1256	1281	1478	1531
PAP	Active Directory	443	513	545	571
PAP	LDAP	1557	1463	1537	1604
PEAP (MSCHAPv2)	Internal	439	467	491	513
PEAP (MSCHAPv2)	Active Directory	356	373	387	407
PEAP (GTC)	Internal	421	434	461	496
PEAP (GTC)	Active Directory	334	371	404	431
EAP-FAST (MSCHAPv2)	Internal	557	643	661	703
EAP-FAST (MSCHAPv2)	Active Directory	417	457	471	489

ISE Performance and Scale - <https://cs.co/ise-perf-scale>

Advice: Sizing

- Consider Authentications/Second or TPS



Standalone = 20,000 EP

Small Distributed Deployment = 20,000 EP

Medium Distributed Deployment = 20,000 EP

PEAP MSChapv2(AD)
Total ≈ 1300/sec

Advice: Avoid Meltdowns

ISE Settings

- Make sure that you have **Anomalous Suppression Detection** enabled, suppress misbehaving clients as well as repeated successful authentications



Advice: Avoid Meltdowns

ISE Settings

- Make sure that you have Anomalous Suppression Detection enabled, suppress misbehaving clients as well as repeated successful authentications

The screenshot shows the Cisco Identity Services Engine (ISE) web interface. The navigation bar includes Home, Context Visibility, Operations, Policy, Administration, Work Center, System, Identity Management, Network Resources, Device Portal Management, pxGrid Services, Feed Service, and Thread. The main menu on the left lists Client Provisioning, FIPS Mode, Alarm Settings, Posture, Profiling, Protocols (EAP-FAST, EAP-TLS, PEAP, EAP-TTLS, RADIUS), IPSec, Security Settings, and Proxy. The RADIUS Settings page is displayed under the Protocols section. The 'Suppression & Reports' tab is active. Three specific settings are highlighted with red boxes:

- Suppress Repeated Failed Clients:** Includes a checkbox for 'Suppress repeated failed clients' (checked) and a setting 'Detect two failures within' followed by a dropdown menu showing '5' minutes (1 - 30).
- Reject RADIUS requests from clients with repeated failures:** Includes a checkbox for 'Reject RADIUS requests from clients with repeated failures' (checked) and a setting 'Failures prior to automatic rejection' followed by a dropdown menu showing '5' (2-100) minutes (15 - 60).
- Suppress Successful Reports:** Includes a checkbox for 'Suppress repeated successful authentications' (checked).

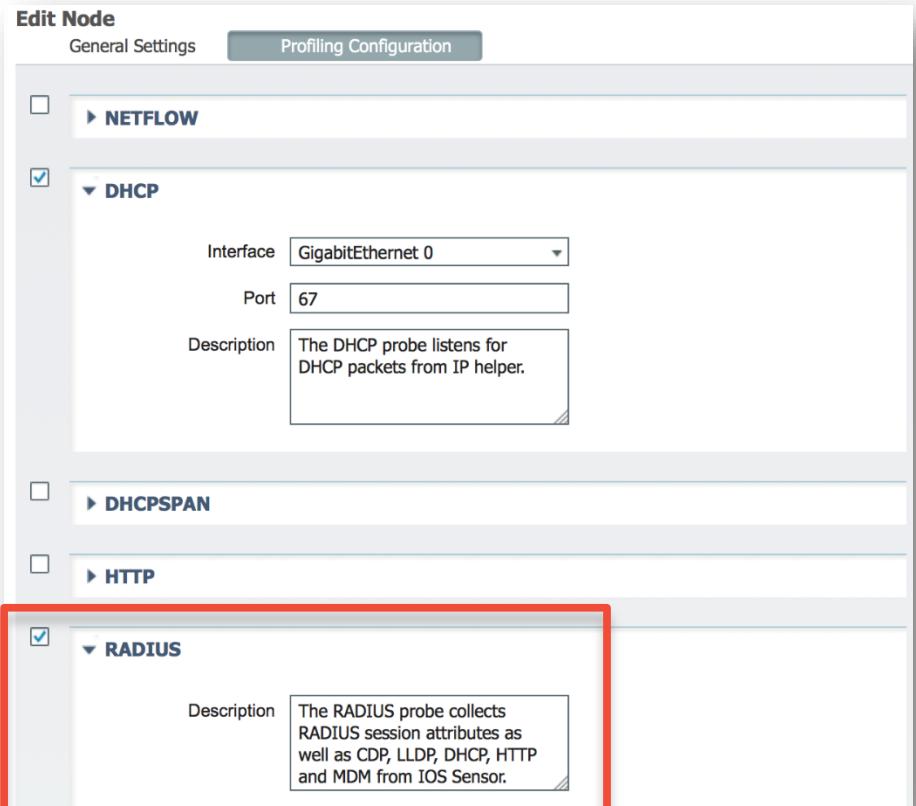
A large blue banner at the bottom of the page reads 'Administration→Settings→Protocols→Radius'.

Administration→Settings→Protocols→Radius

Advice: Avoid Meltdowns

ISE Settings

- Make sure that you have Anomalous Suppression Detection enabled, suppress misbehaving clients as well as repeated successful authentications
- Only use the profiling probes/information that you need. Don't have information overload. Avoid probes that use SPAN. Start with Radius only first. Use device sensors in network access device



Administration → Deployment → Profiling

Advice: Avoid Meltdowns

ISE Settings

- Enable EndPoint Attribute Filter

Administration→Settings→Profiling

Profiler Configuration

* CoA Type: Reauth

Current custom SNMP community strings: ••••• Show

Change custom SNMP community strings: (For NMAP, comma separated. Field will be cleared on successful saved change.)

Confirm changed custom SNMP community strings: (For NMAP, comma separated. Field will be cleared on successful saved change.)

EndPoint Attribute Filter: Enabled 

Enable Anomalous Behaviour Detection: Enabled 

Enable Anomalous Behaviour Enforcement: Enabled

Load Balancer for ISE Best Practice Check List



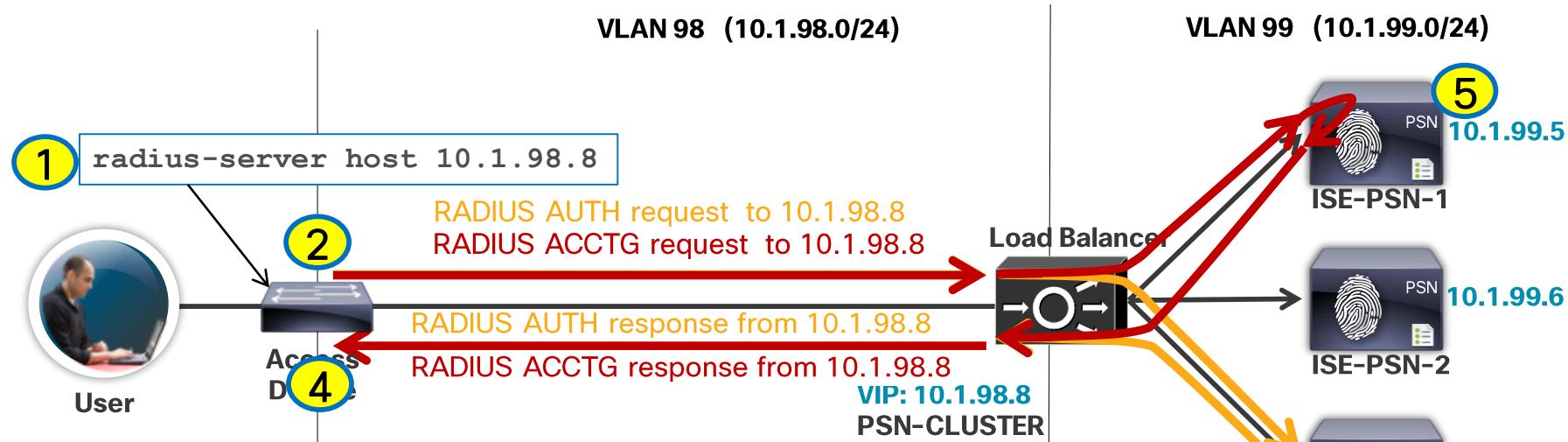
You make networking **possible**

Load Balancer for ISE Best Practice Check List

- Persistence (Stickyness) is a must!
- Sticky Timers need to be at least 1 hour
- DO NOT Round Robin Traffic
- Persistence based on Calling-Station-ID is best
- Avoid using Source-IP address for sticky value

Load Balancing RADIUS

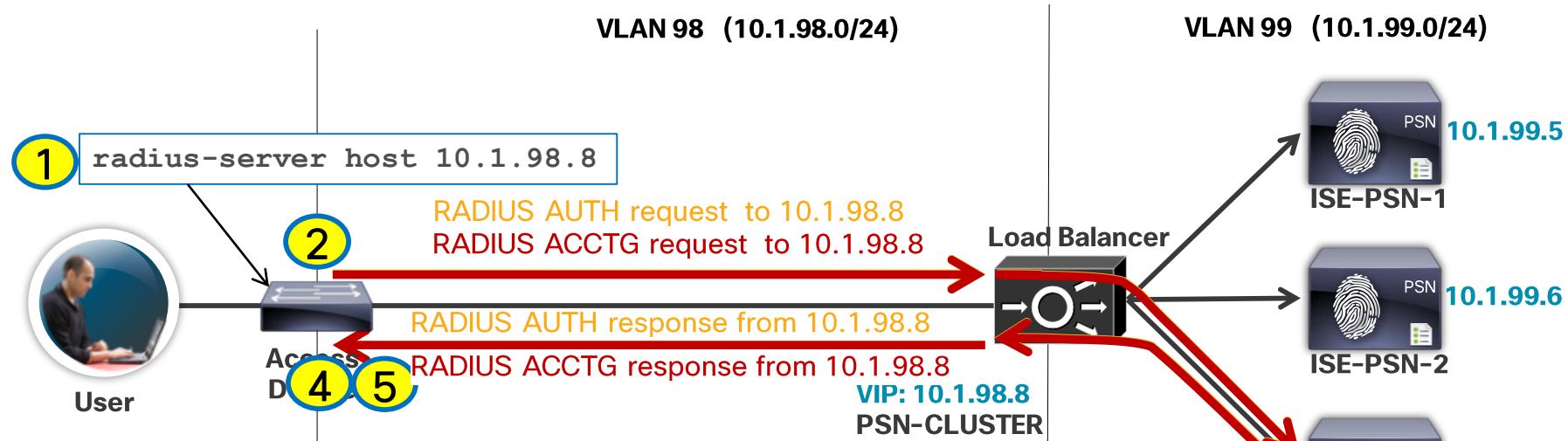
Sample Flow



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 different PSN because round-robin(RR) load balancing is used without persistency (sticky).
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 different PSN based on RR and no sticky

Load Balancing RADIUS

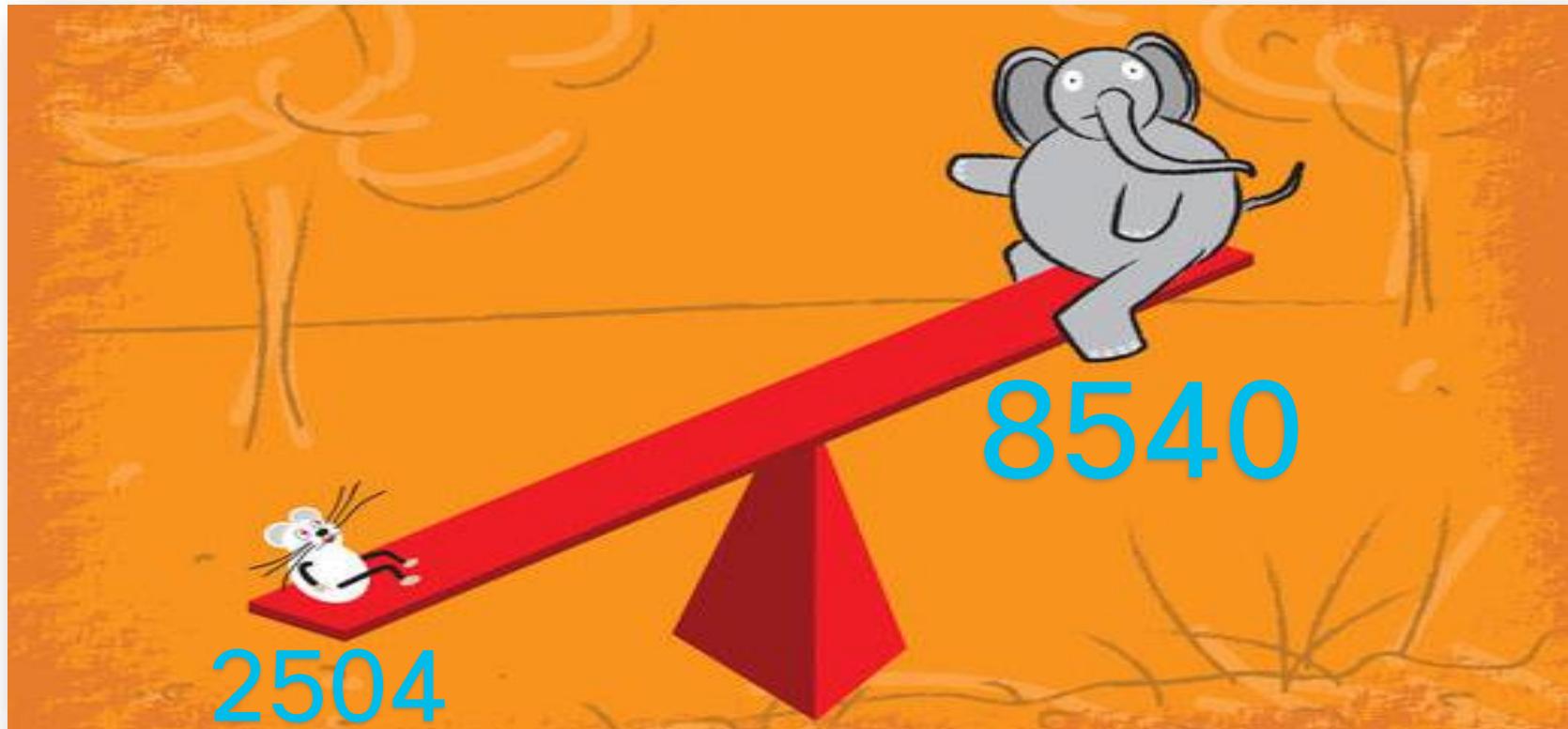
Sample Flow



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

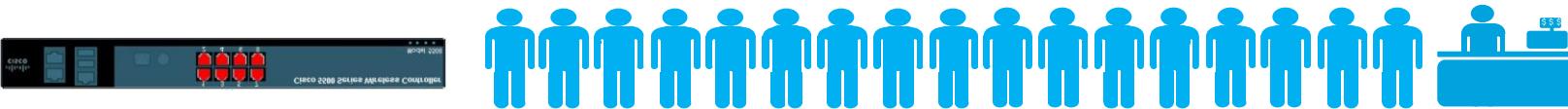
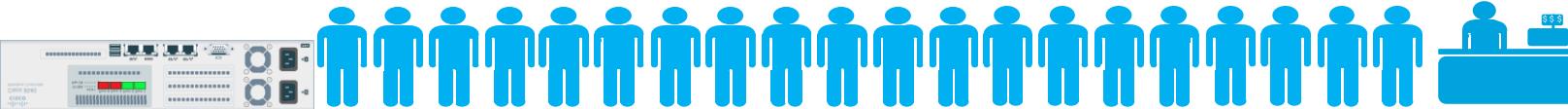
Load Balancing RADIUS

All NADs are not created equal!



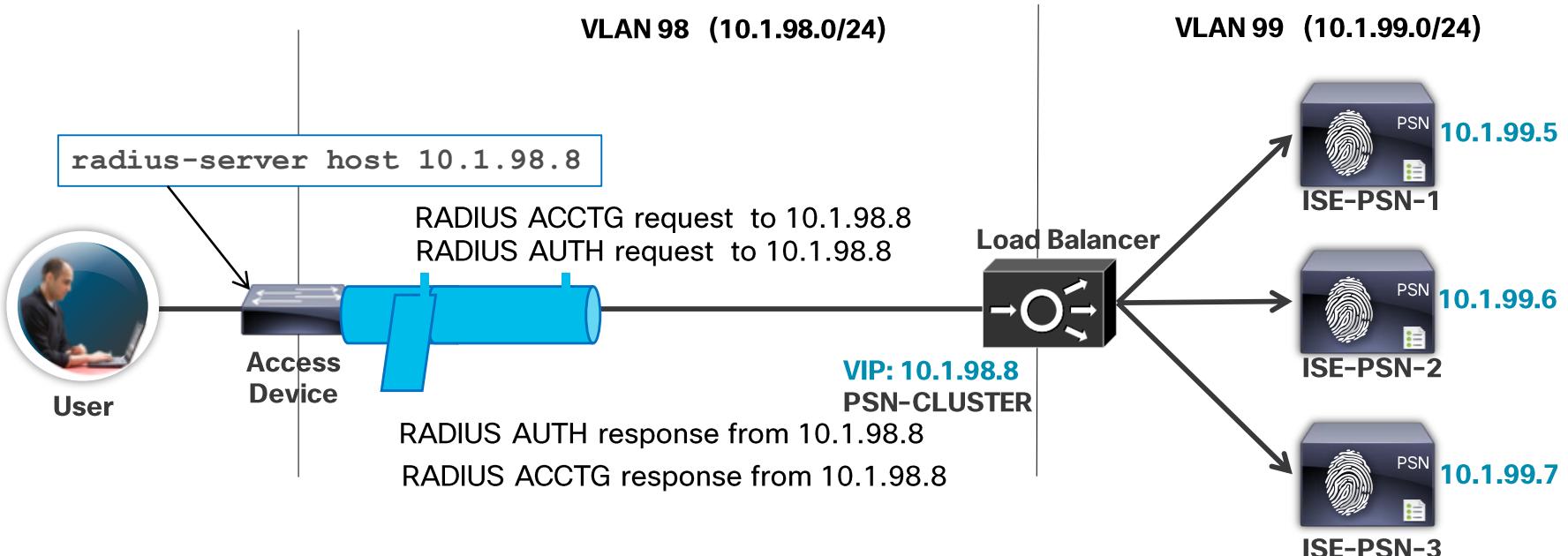
Load Balancing RADIUS

IP vs Calling Station ID Stickiness



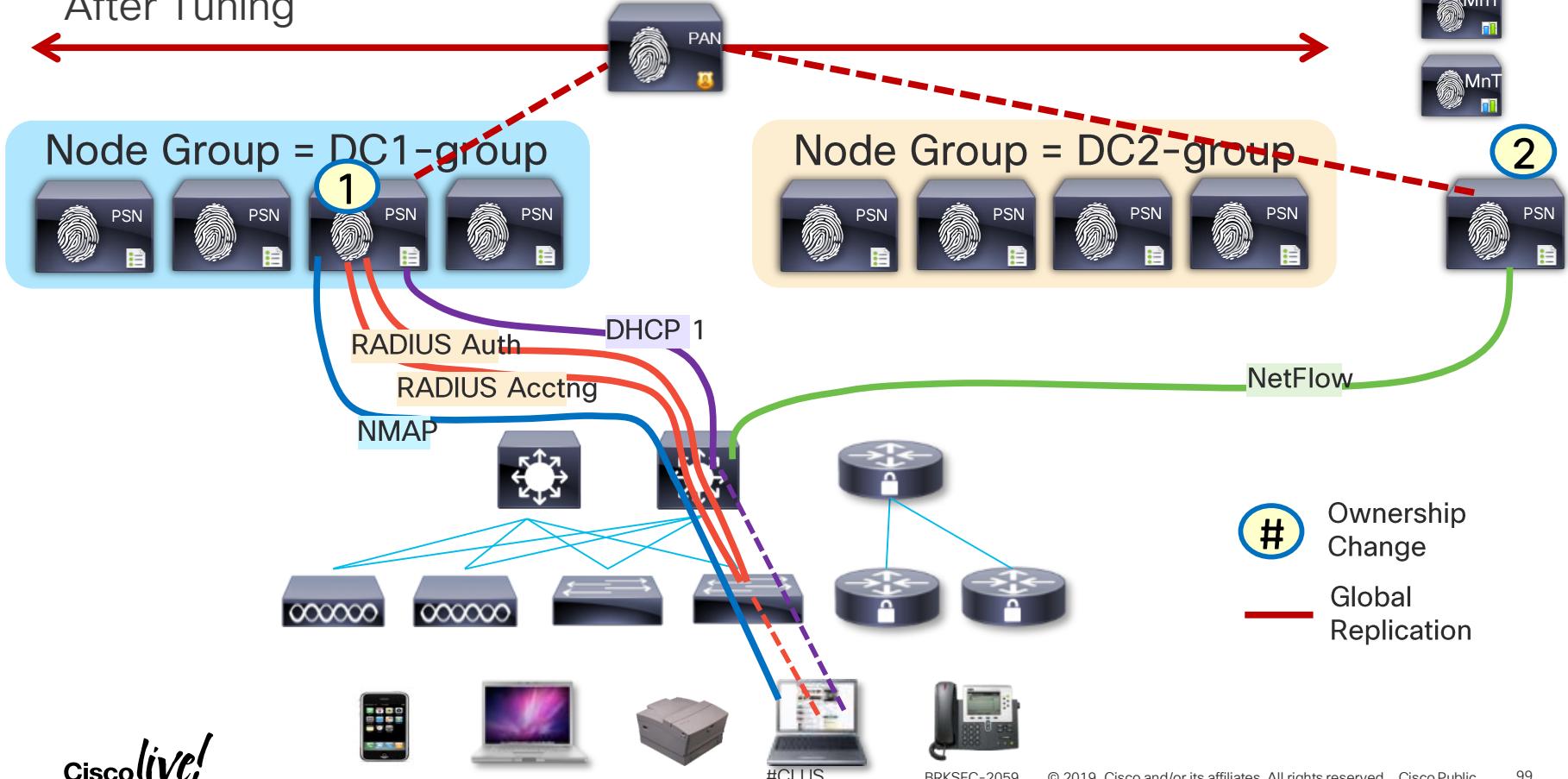
Load Balancing RADIUS

Avoid spraying packets!!!



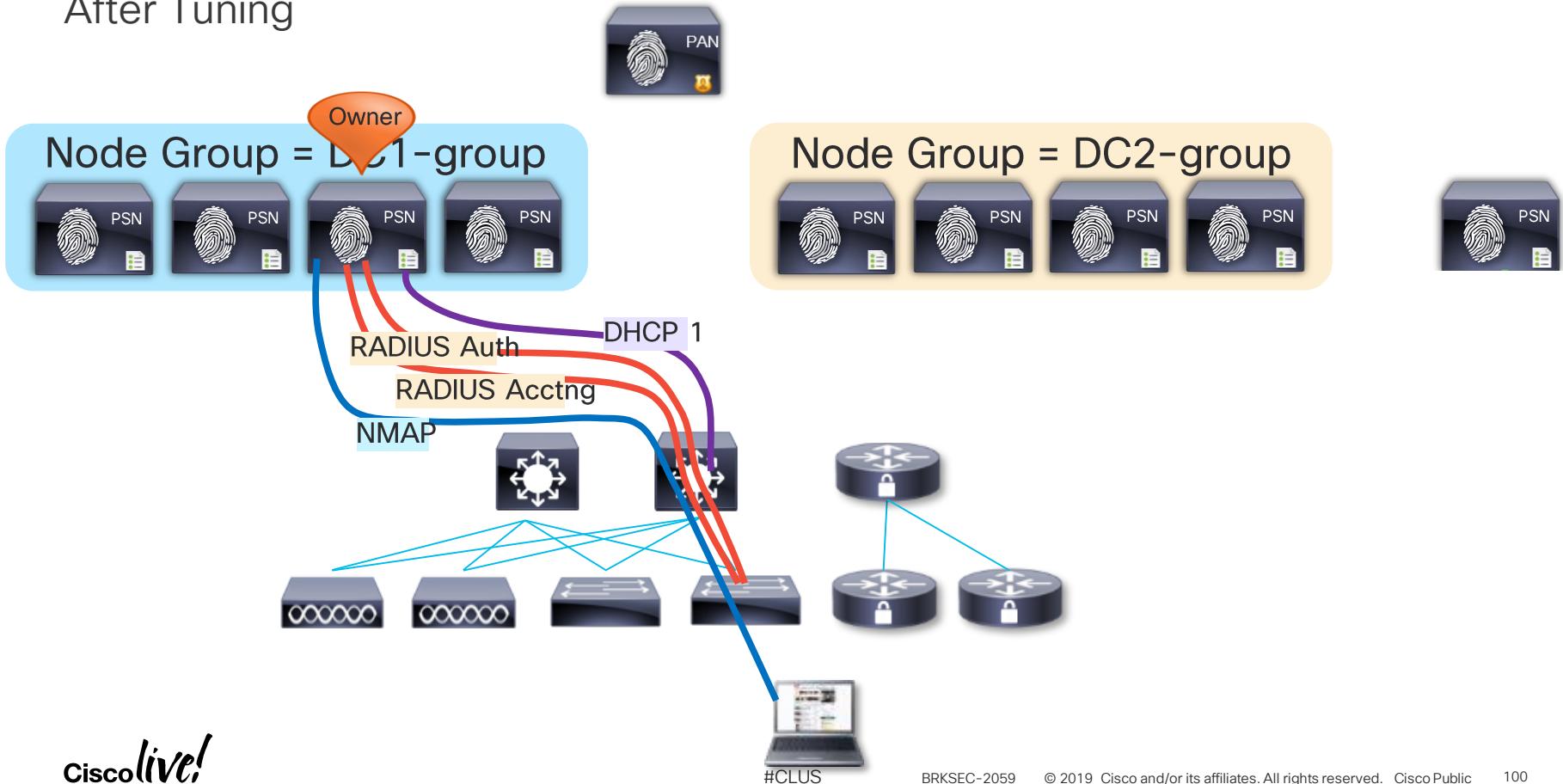
Profiling and Data Replication

After Tuning



Impact of Ownership Changes

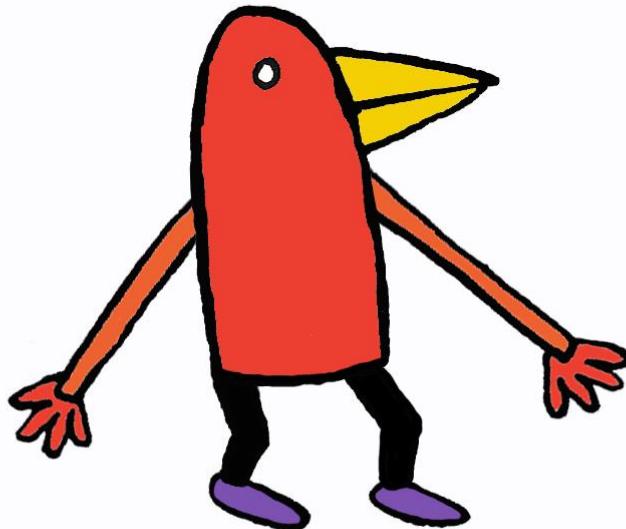
After Tuning



Advice: Avoid Meltdowns

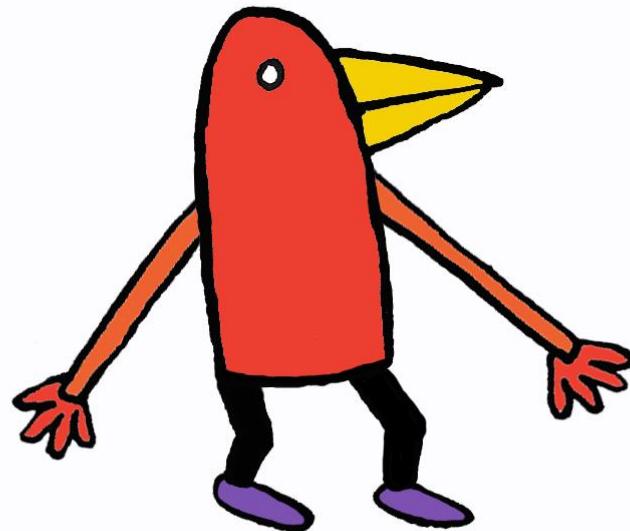
ISE Settings

- Enable EndPoint Attribute Filter
- Avoid Radius Flapping



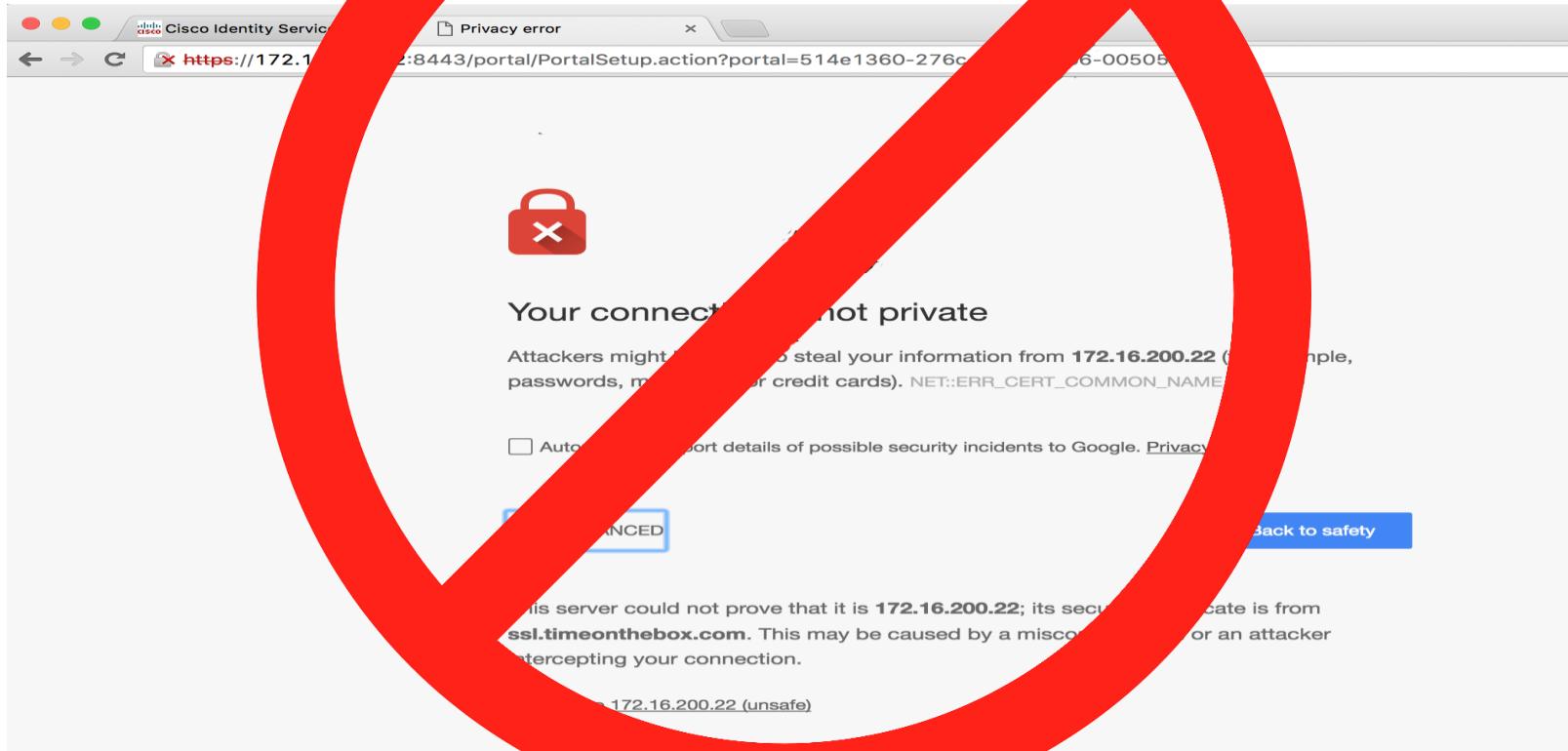
Avoid Radius Flapping...

USE BEST PRACTICE!!!



Soapbox: Buy Public Certificate

Stop teaching users to accept Man-in-the-middle attacks!



Conclusion

- Public Environments can be challenging
- Avoid ISE “meltdowns”
- Keep up to date with versions and patches, be aware of software defects that might affect your environment
- Use advice in this guide to solve challenges in your environment
- Learn from the experiences of others and avoid their mistakes

Complete your online session evaluation



- Please complete your session survey after each session. Your feedback is very important.
- Complete a minimum of 4 session surveys and the Overall Conference survey (starting on Thursday) to receive your Cisco Live water bottle.
- All surveys can be taken in the Cisco Live Mobile App or by logging in to the Session Catalog on ciscolive.cisco.com/us.

Cisco Live sessions will be available for viewing on demand after the event at ciscolive.cisco.com.

Continue your education



Demos in the
Cisco campus



Walk-in labs



Meet the engineer
1:1 meetings



Related sessions



Thank you





A horizontal sequence of nine stylized lowercase 'i' characters, each composed of a colored dot at the top and a vertical bar below. The colors alternate and include blue, green, orange, and red.

You make **possible**