You make **possible**

Deploying ISE in a Dynamic Environment

(Best Practice)

Clark Gambrel, CCIE #18179
@clarkgambrel

BRKSEC-2059

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

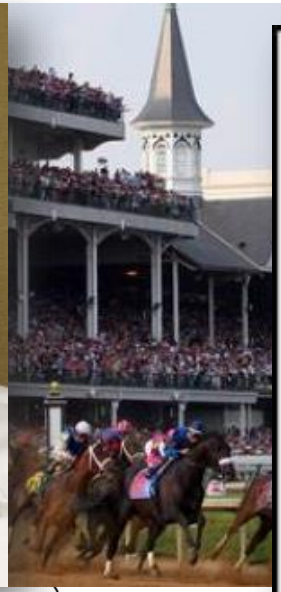
Clark

~~Bruce~~ Gambrel, CCIE #18179

Technical Leader – Engineering

cgambrel@cisco.com

@ClarkGambrel



KENTUCKY

"I might be a redneck"

Kentucky is known for...

Housekeeping

You make networking **possible**

Cisco live!

Cisco Policy and Access Sessions: Building Blocks

Sunday	Monday	Tuesday	Wednesday	Thursday
08:00 **TECSEC-3672** Implementing Identity Services Engine 2.6	16:00 **BRKSEC-1003** Cisco Platform Exchange Grid (pxGrid) Inside Out	08:00 **BRKSEC-2059** Deploying ISE in a Dynamic Environment (Best Practices)	08:00 **BRKSEC-3229** ISE under magnifying glass. How to troubleshoot ISE	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

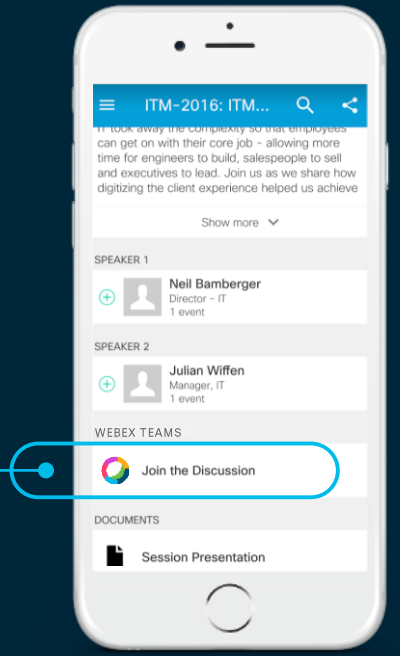
Questions?

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

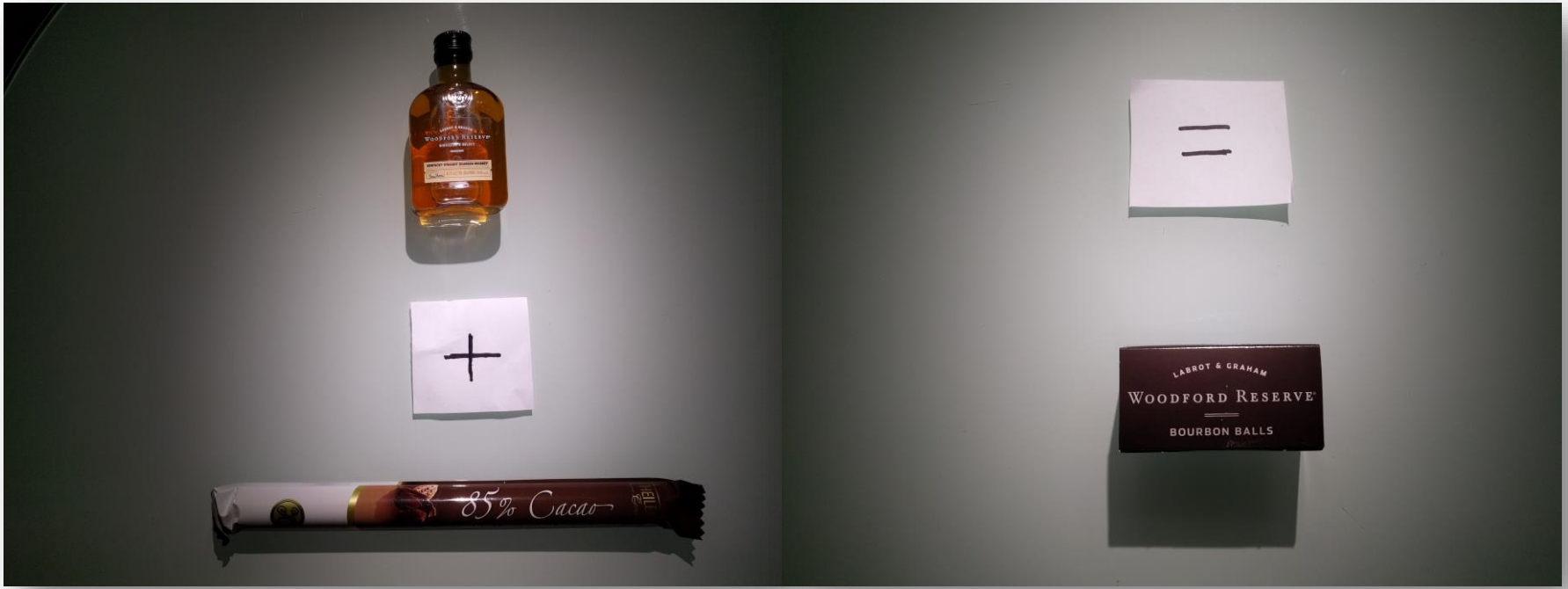
Webex Teams will be moderated by the speaker until June 16, 2019.



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

Kenny Louie under Creative Commons License

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://tvtropes.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)

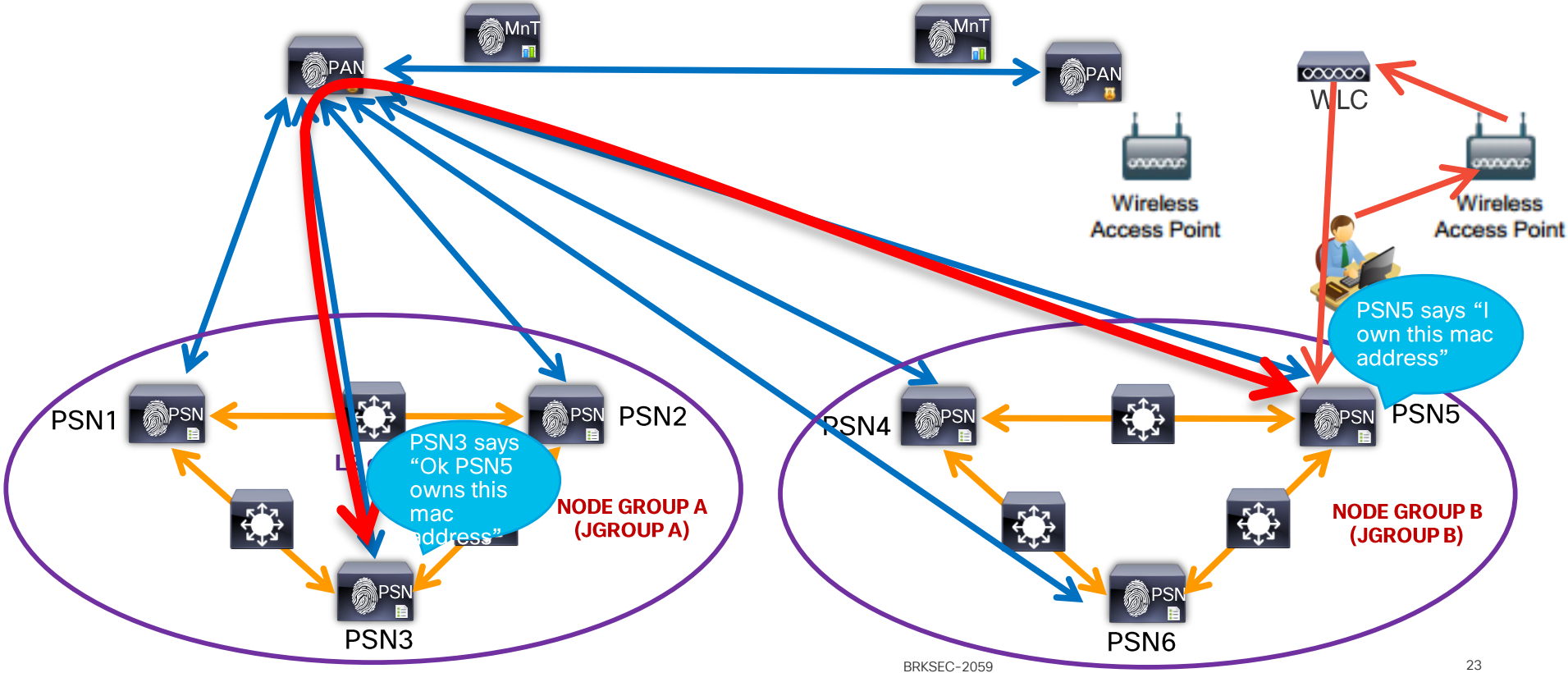
You make networking **possible**

Cisco live!

Inter-Node Communications

Radius Flapping can be a real mess!

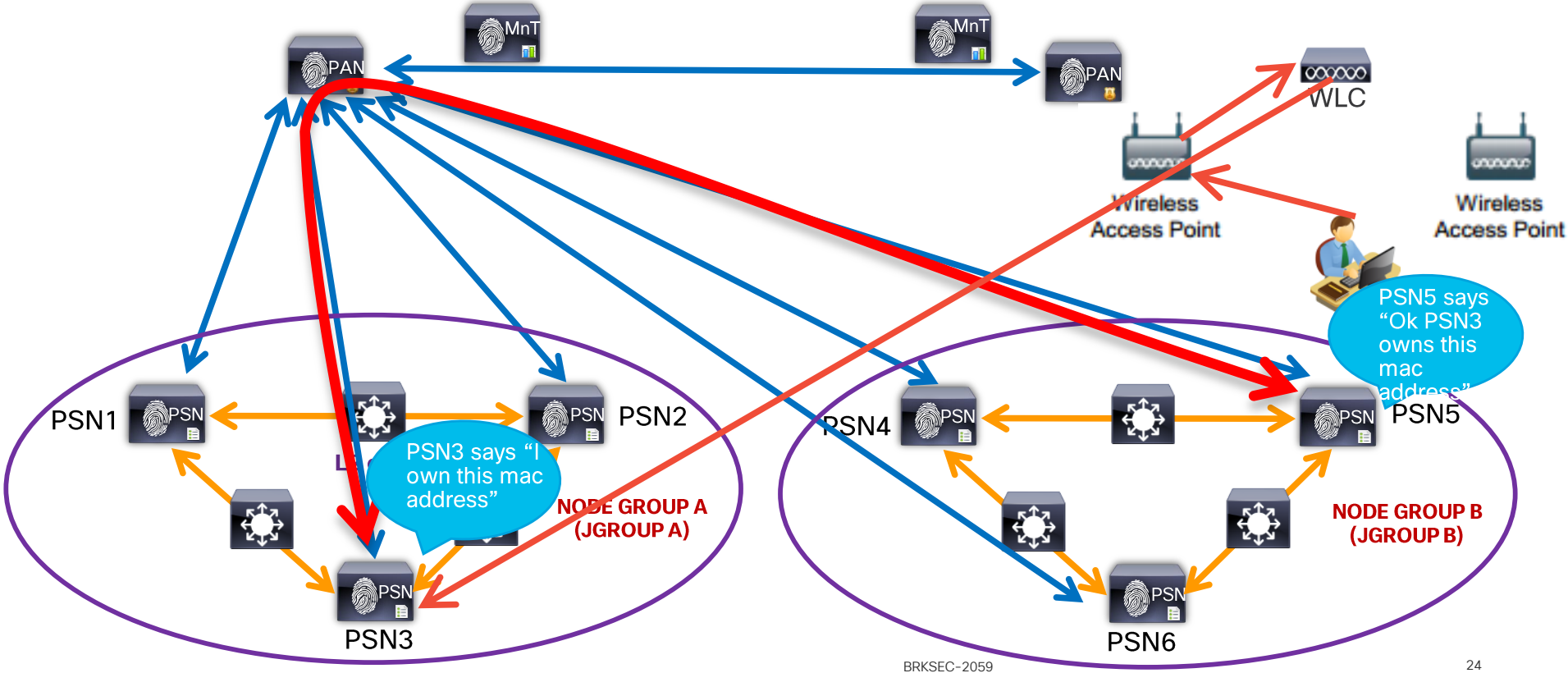
- Profiling sync leverages JGroup channels
- All replication outside node group must traverse PAN–including Ownership Change!
- If Local JGroup fails, then nodes fall back to Global JGroup communication channel.



Inter-Node Communications

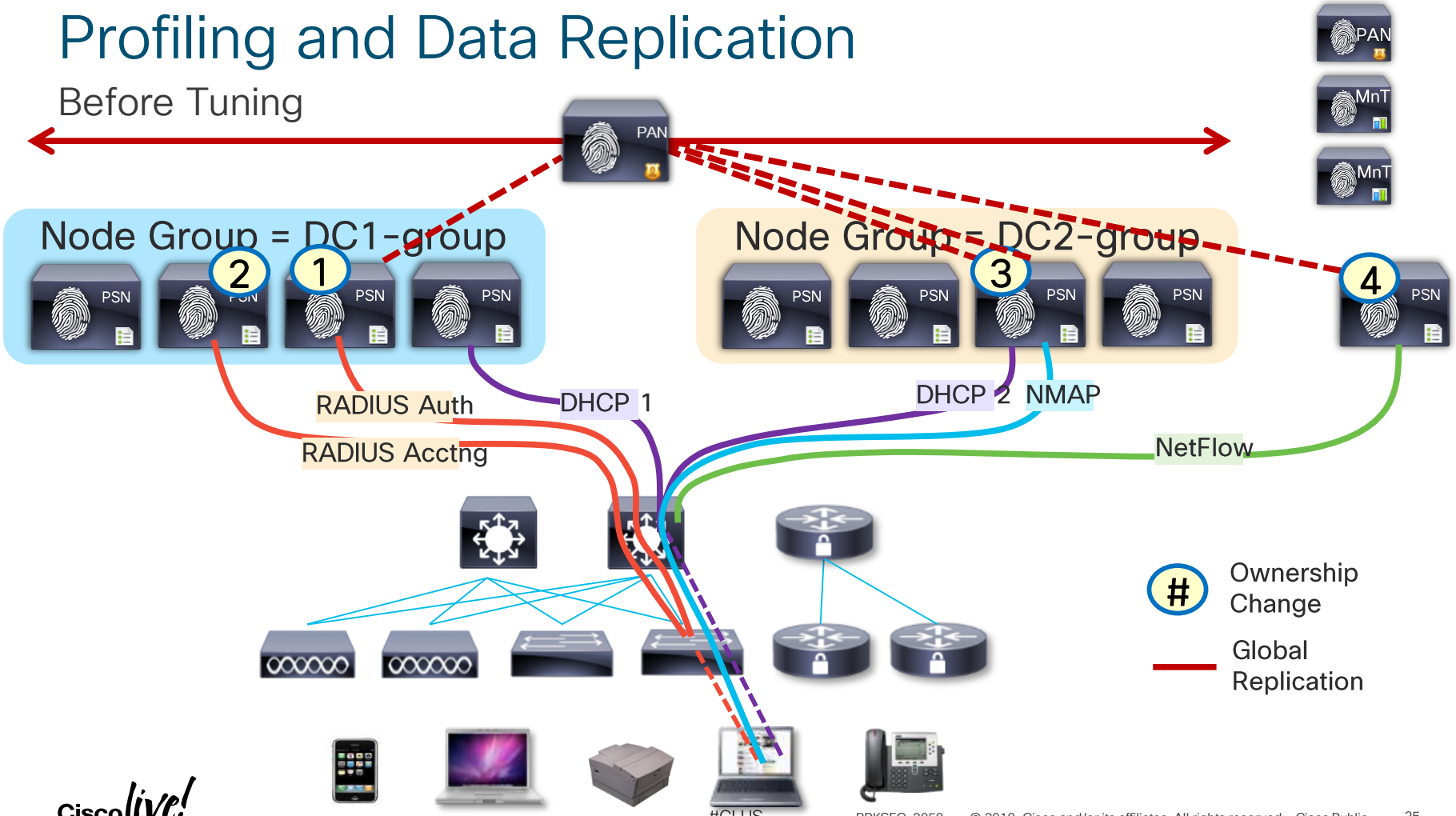
Radius Flapping can be a real mess!

- 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



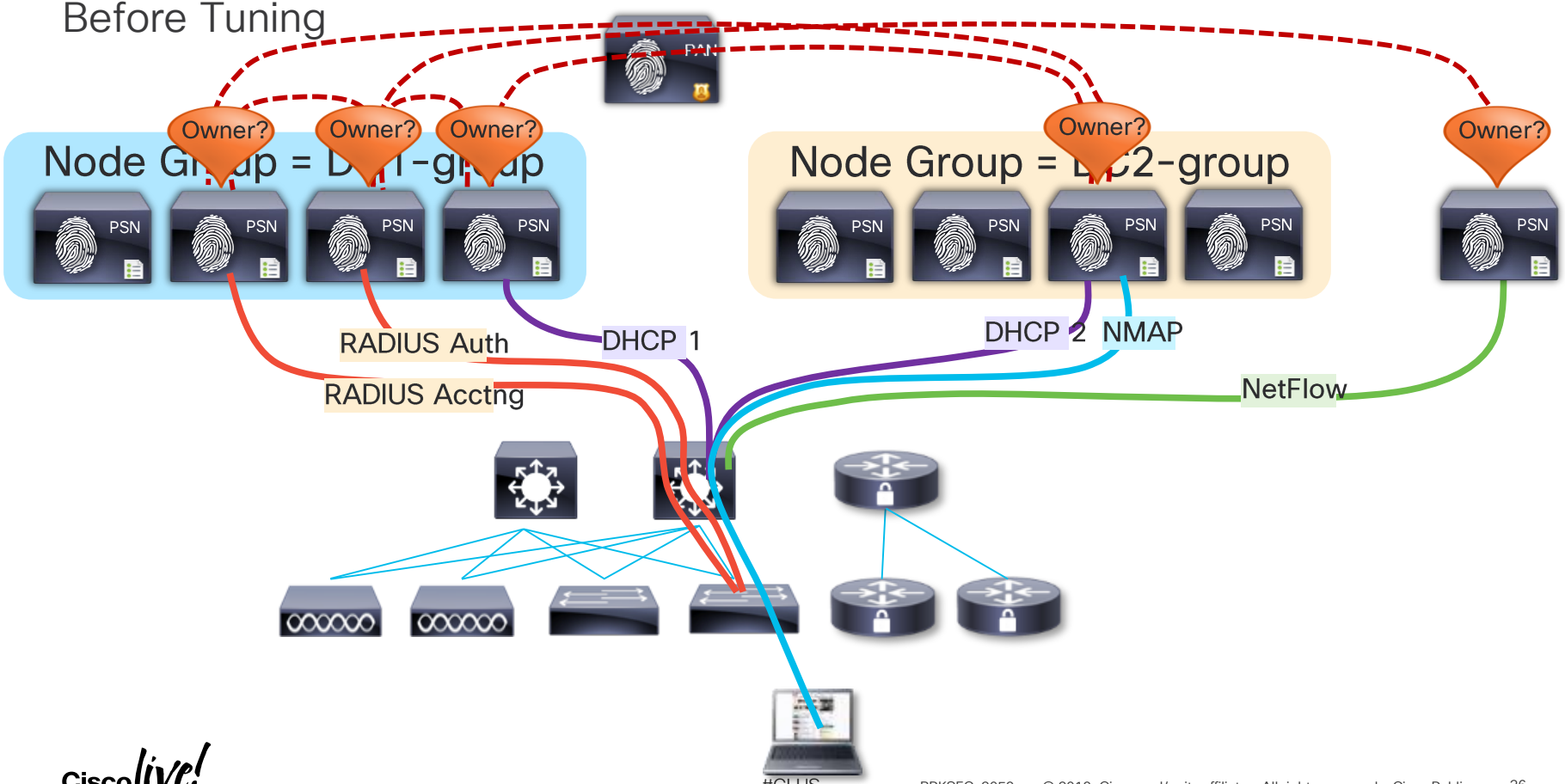
Profiling and Data Replication

Before Tuning



Impact of Ownership Changes

Before Tuning



WLC Best Practice Check List

You make networking **possible**

Cisco live!

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

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

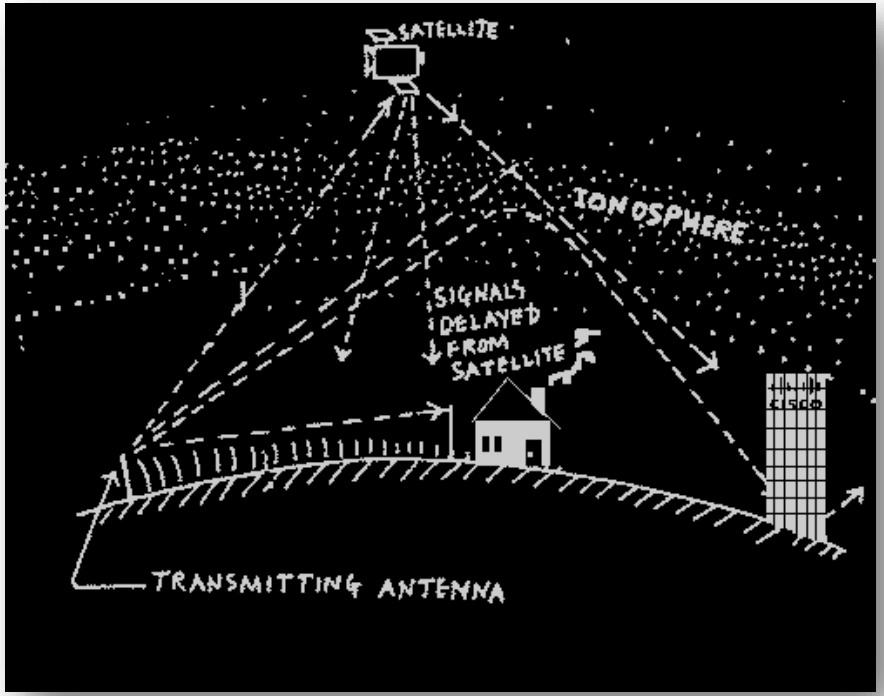
Advice: Timers

WLC: Radius

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

Advice: Timers

WLC: Radius



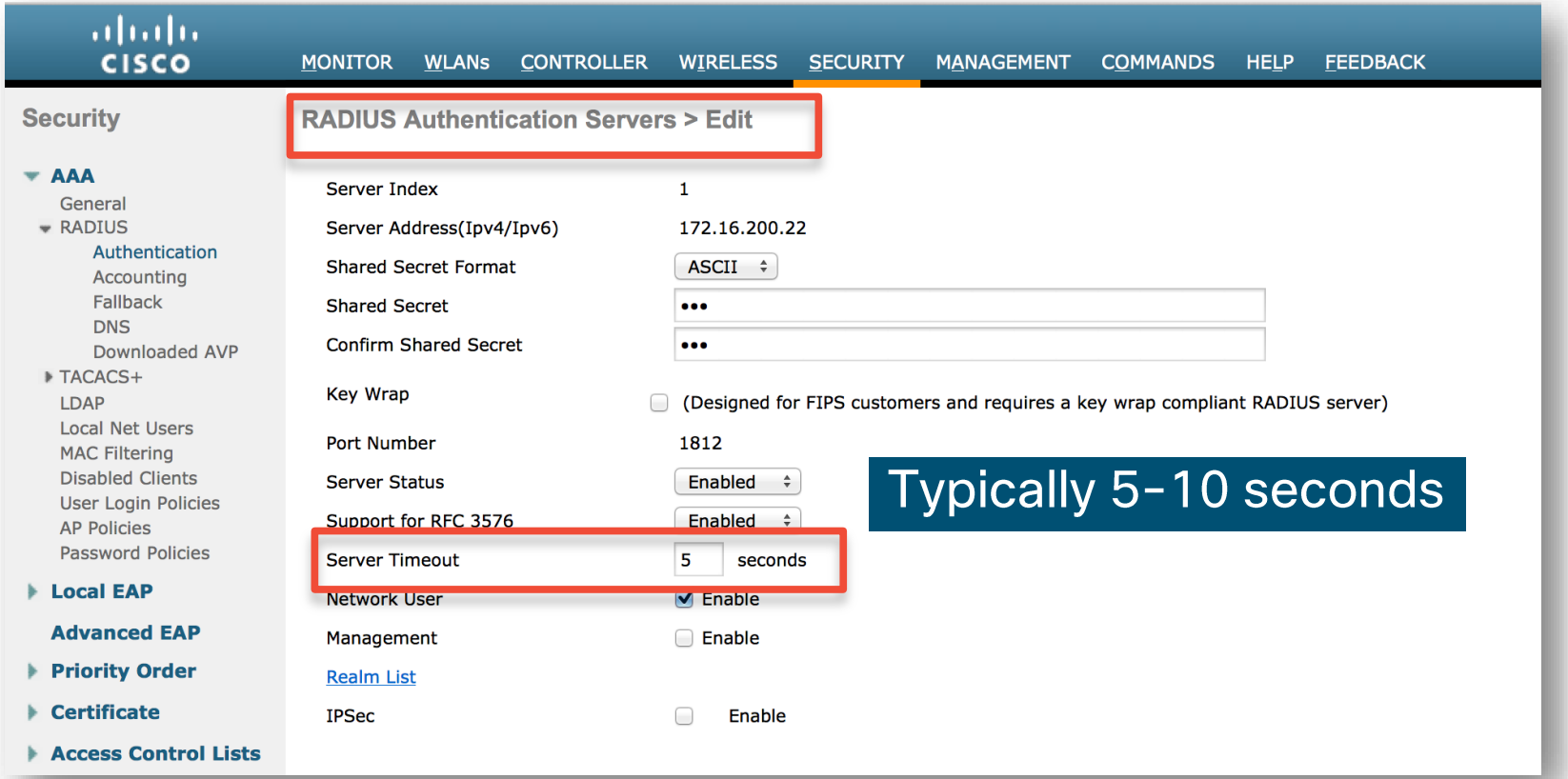
- Use timers appropriate to the environment (tune for your environment)
- Some remote/cloud based radius servers may have higher authentication latency and require some tweaking.

Advice: Timers

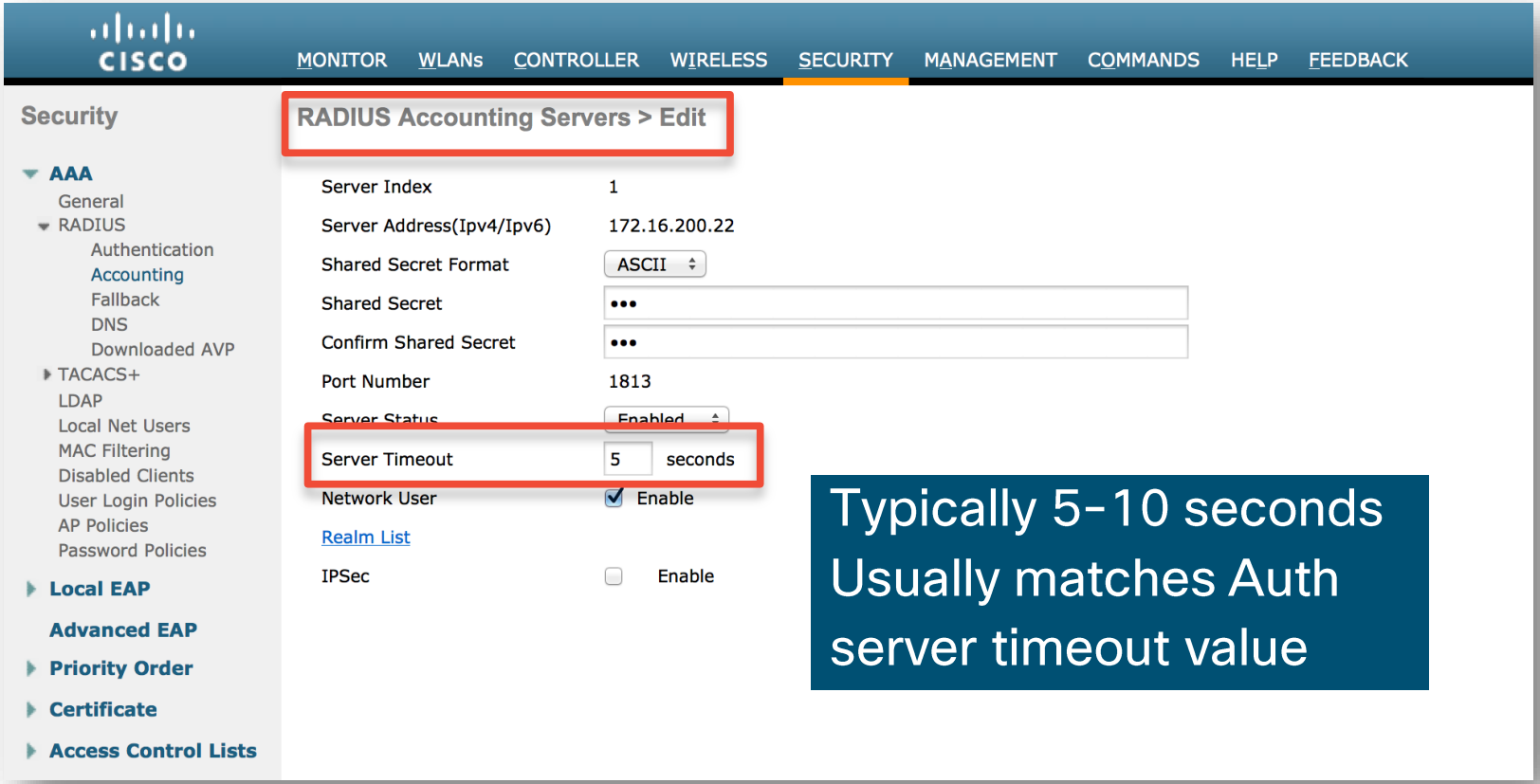
WLC: Radius – Continued

- Setting timers too long and the client might restart its session, retries from radius server will be dropped
- Avoid unnecessary radius server flaps with timers that are too short
- Radius **flapping** can have some major impacts on an ISE deployment

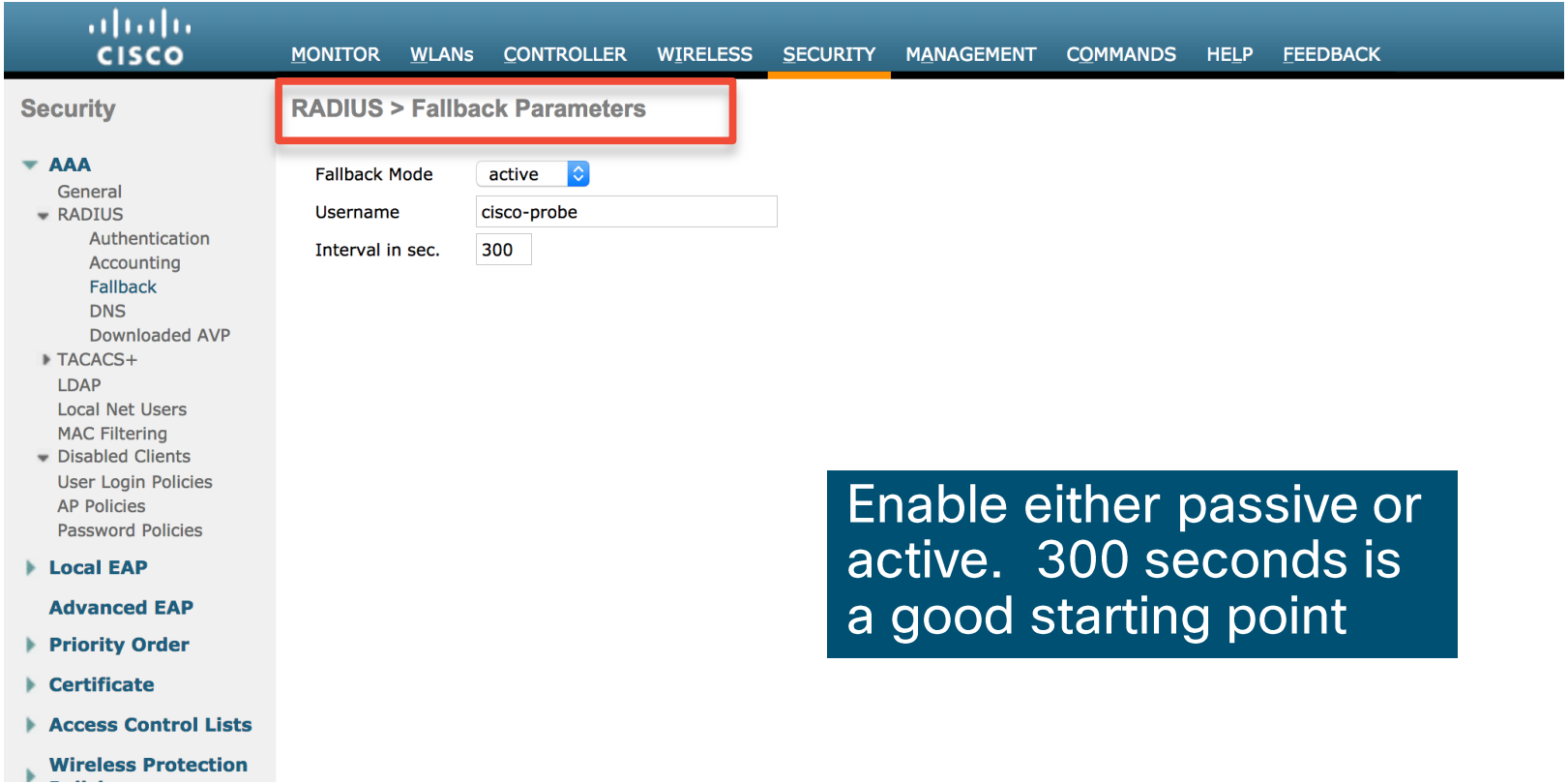
Advice: Timers – Radius



Advice: Timers – Radius



Advice: Timers – Radius



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

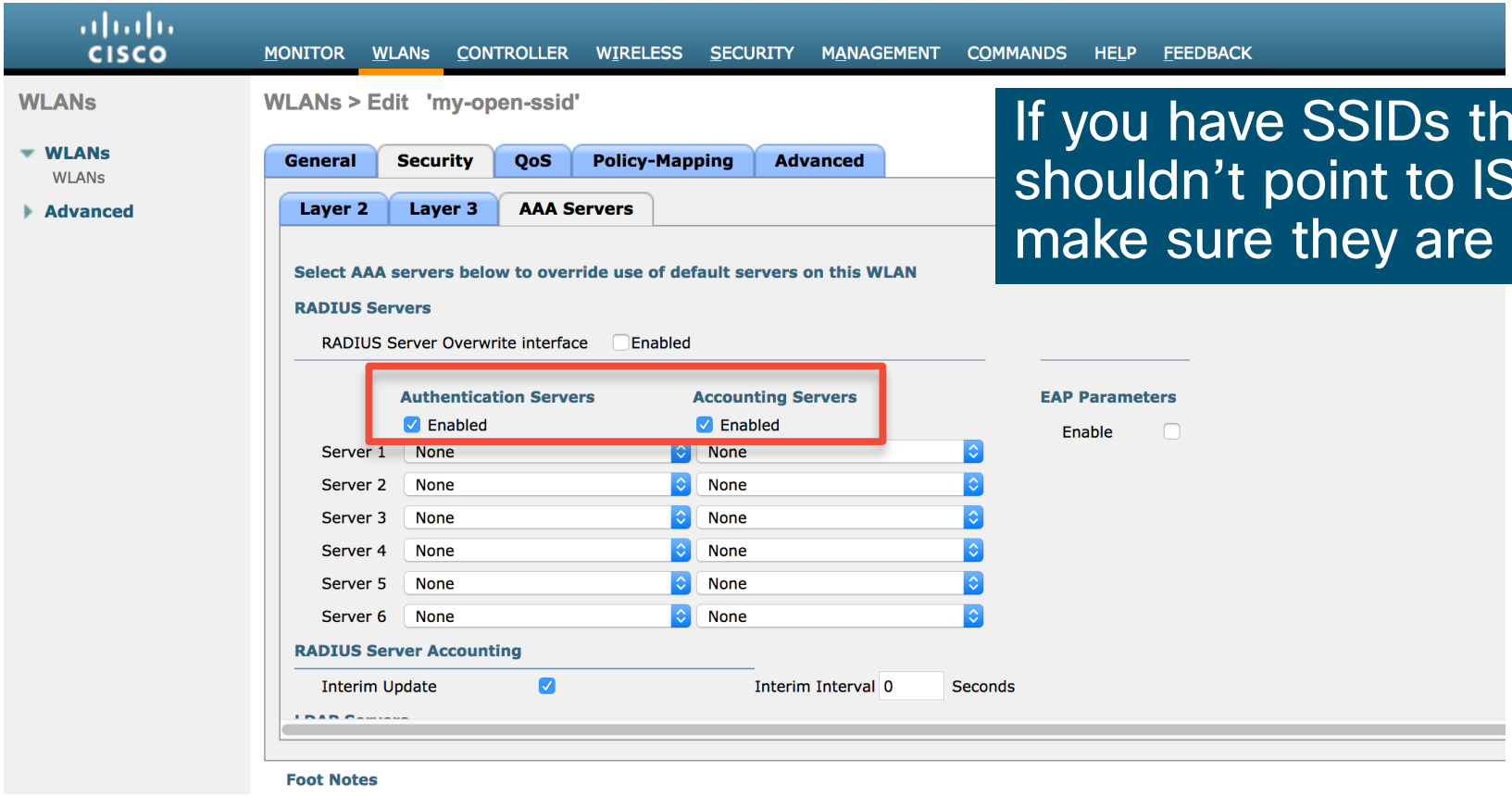
This can have a big impact on ISE and Wireless Auths in general

```
(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
```

(Cisco Controller) >config radius aggressive-failover disable

Advice: Timers – WLANs

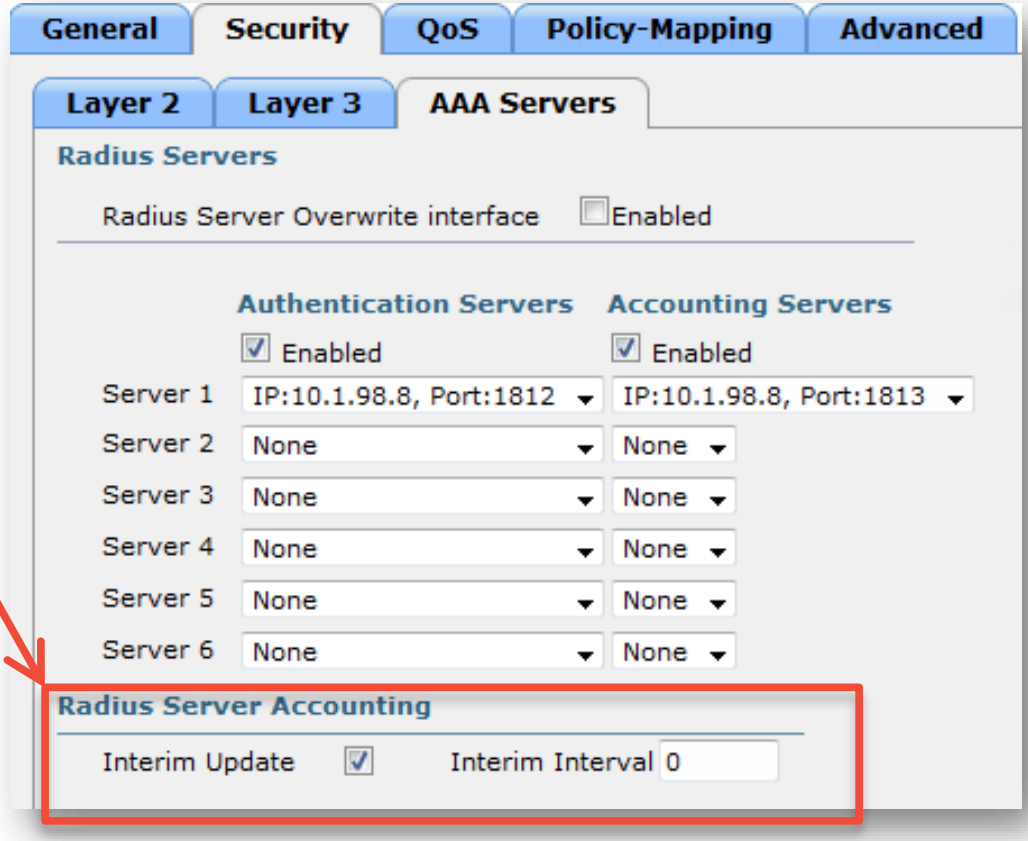


If you have SSIDs that shouldn't point to ISE, make sure they are not!

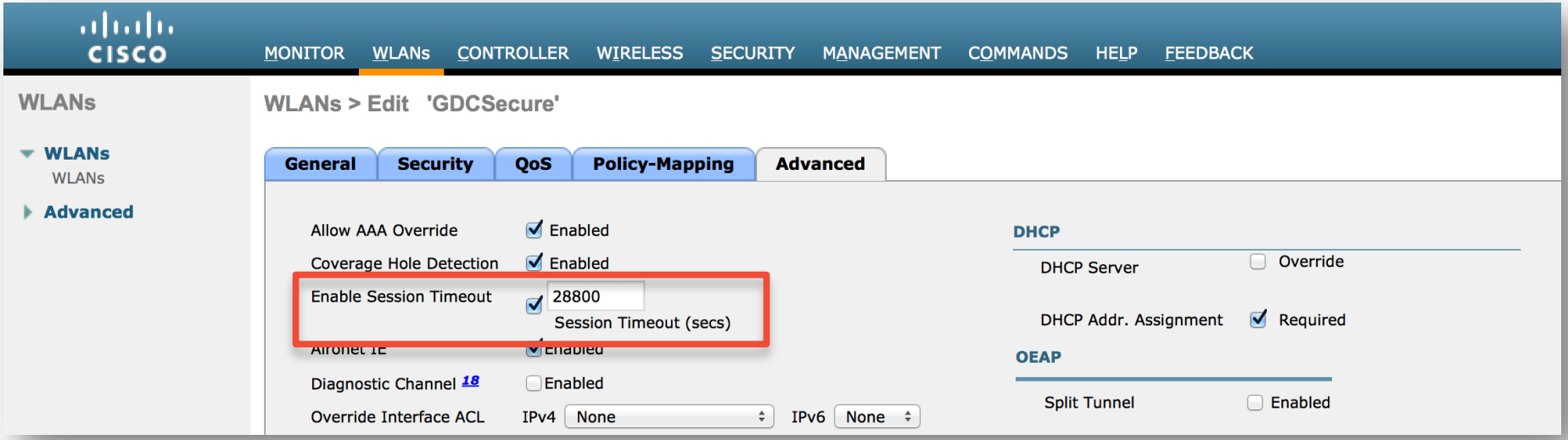
Advice: Timers – WLANs

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

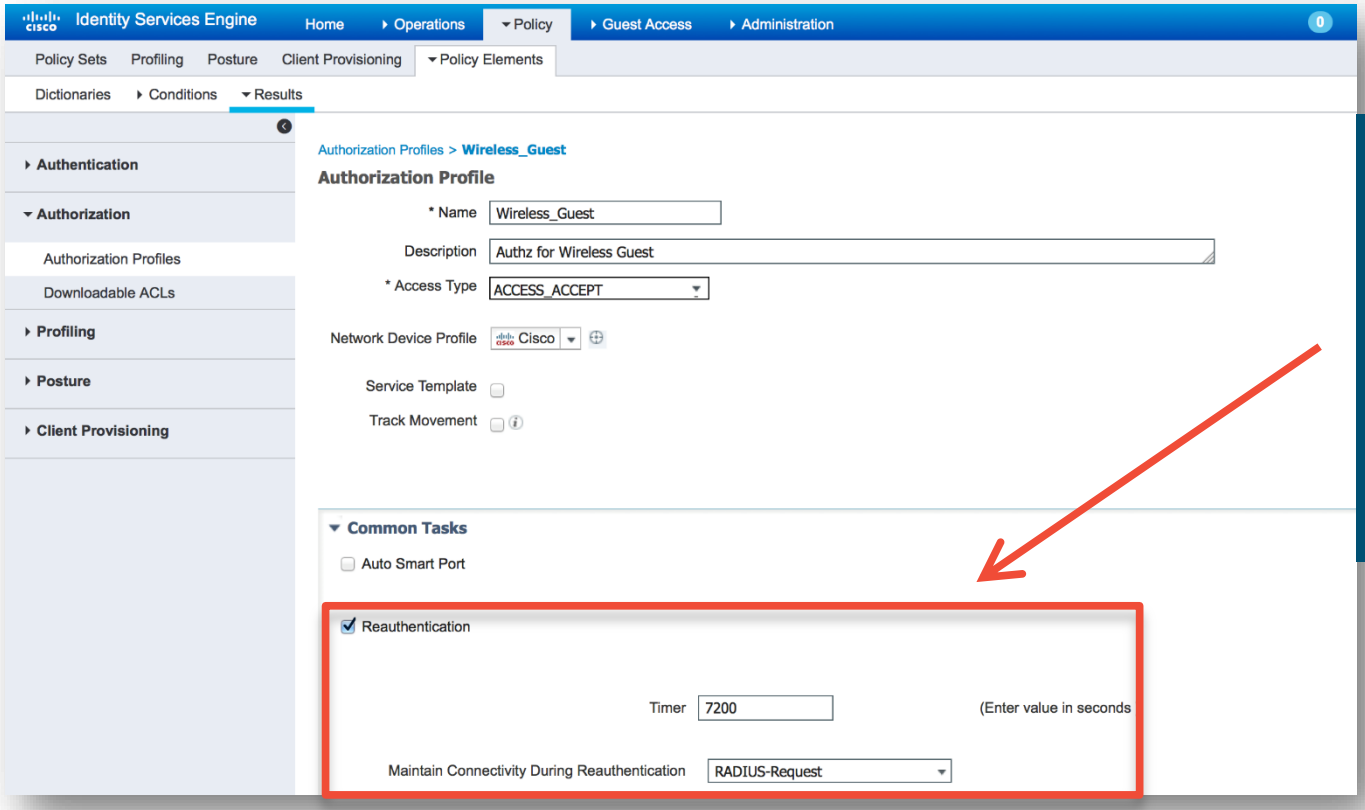


Advice: Timers – WLANs



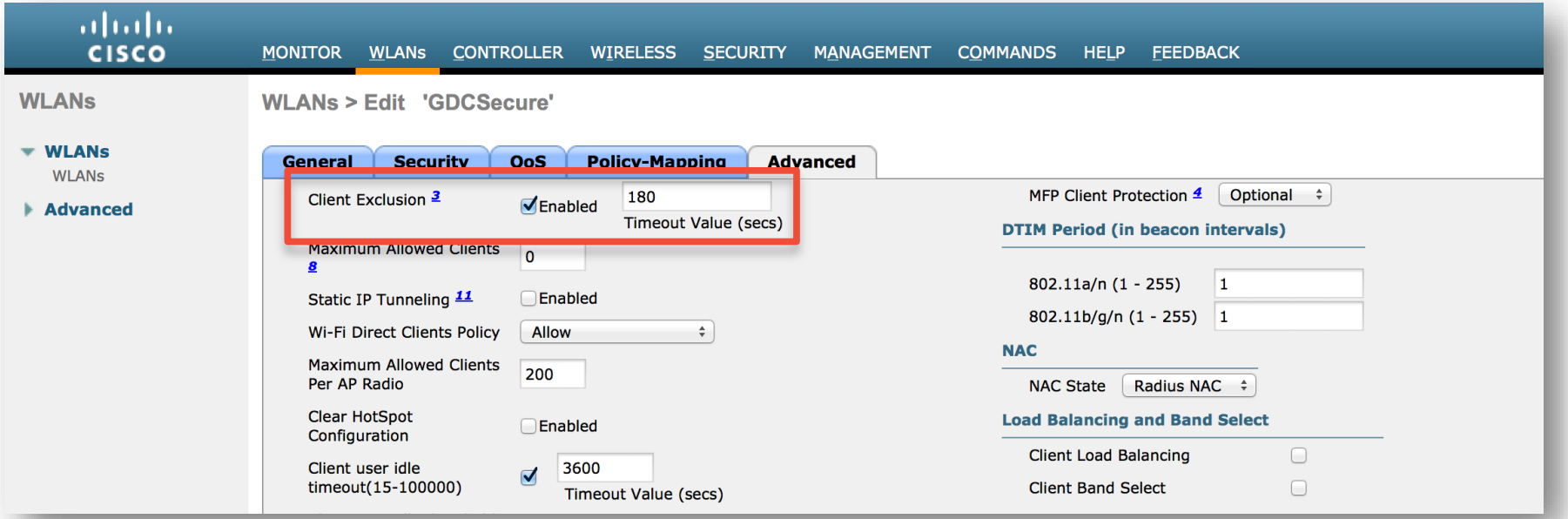
Increase Session Timeout to 2+ hours (7200+ sec), if Enabled (recommended)

Advice: Timers – WLANs



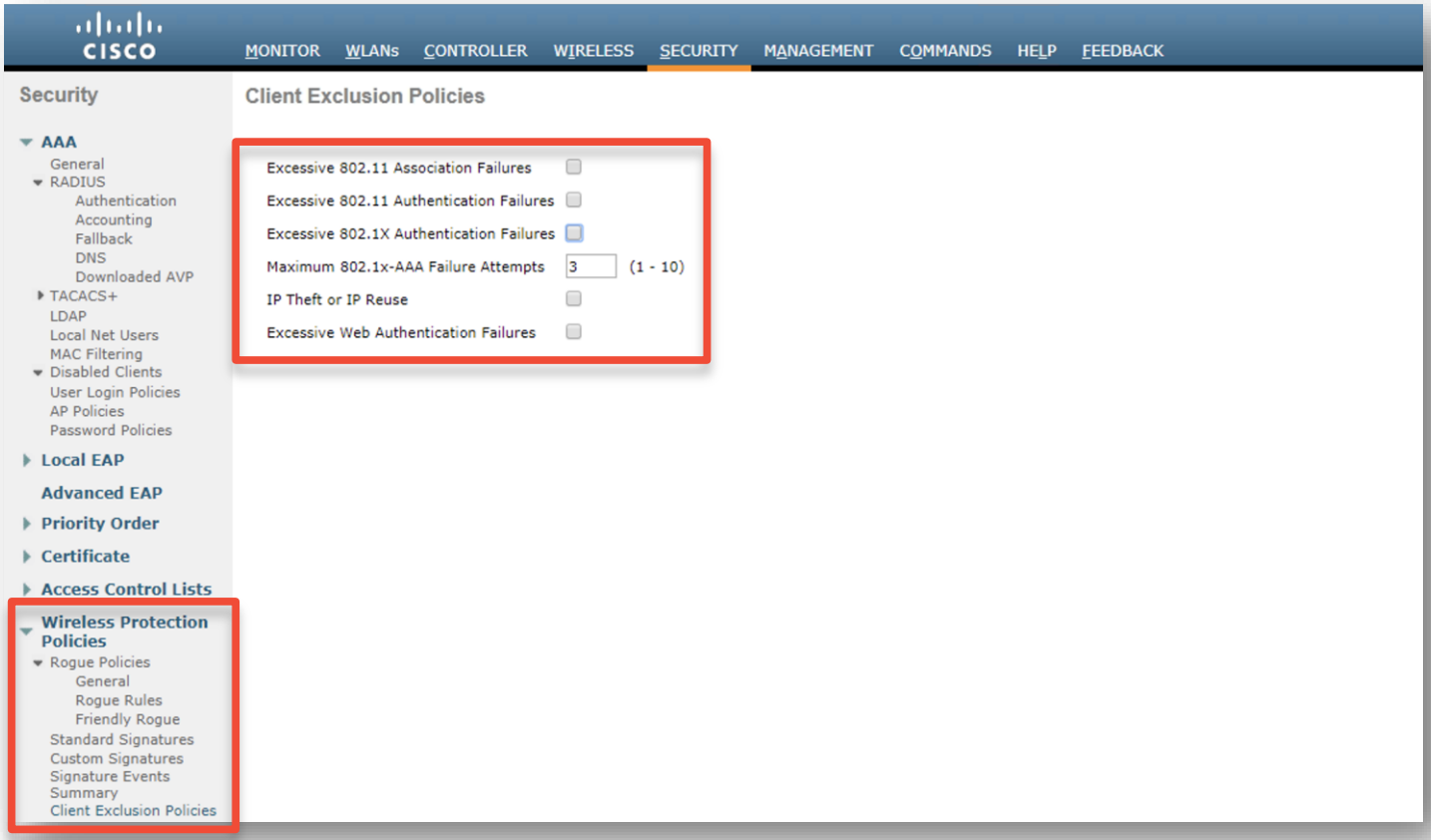
This can also be sent as a Radius attribute in ISE under the AuthZ Profile

Advice: Timers – WLANs

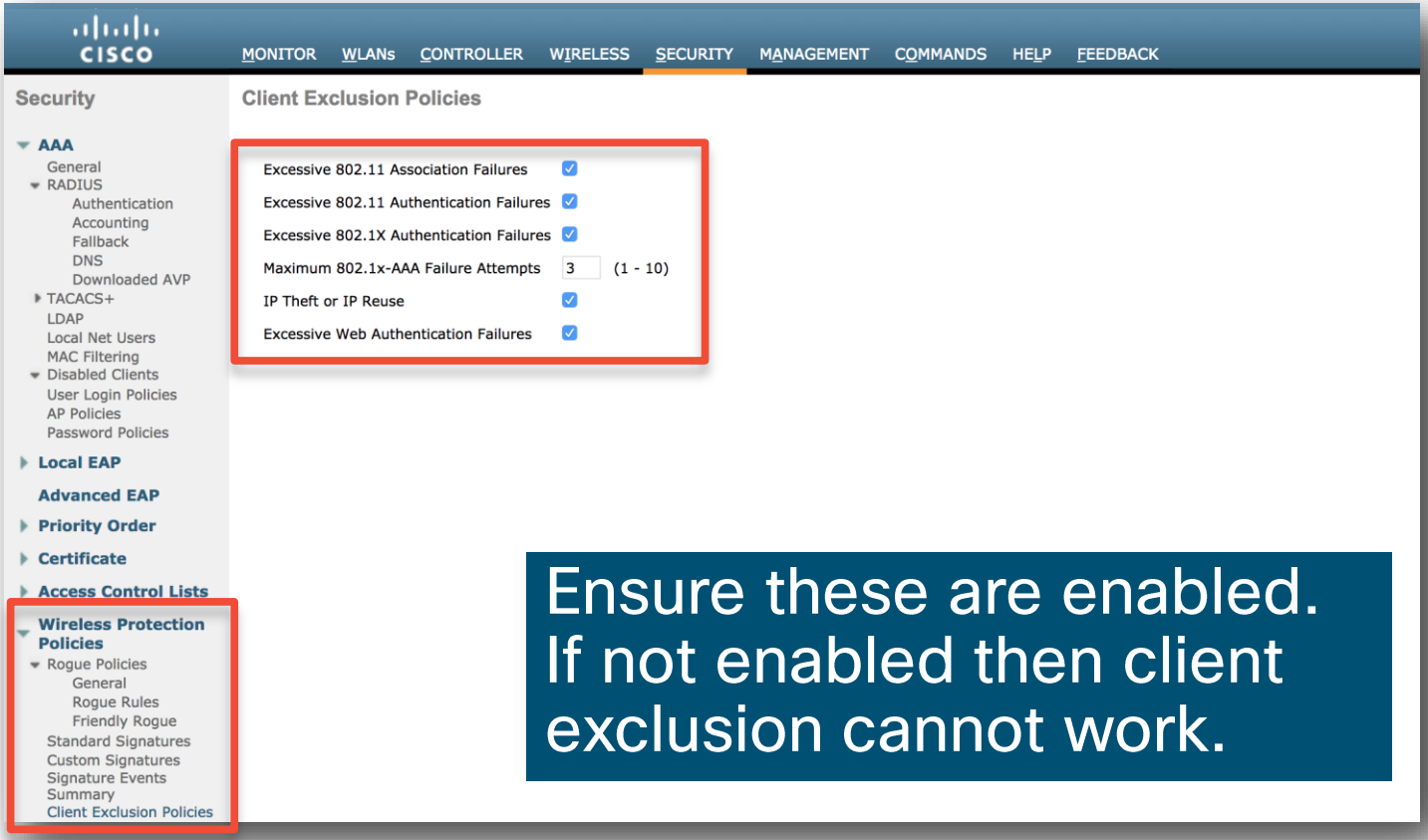


Increase Client Exclusion to 180+ seconds (3+ mins)

Advice: Timers – WLANs

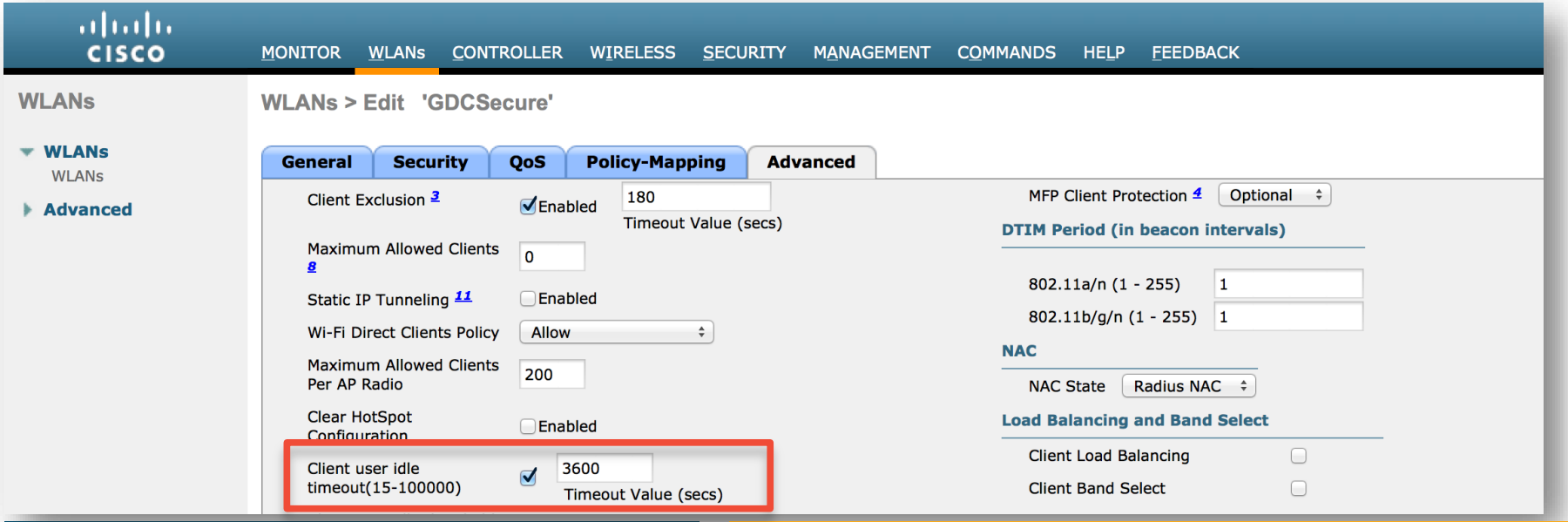


Advice: Timers – WLANs



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

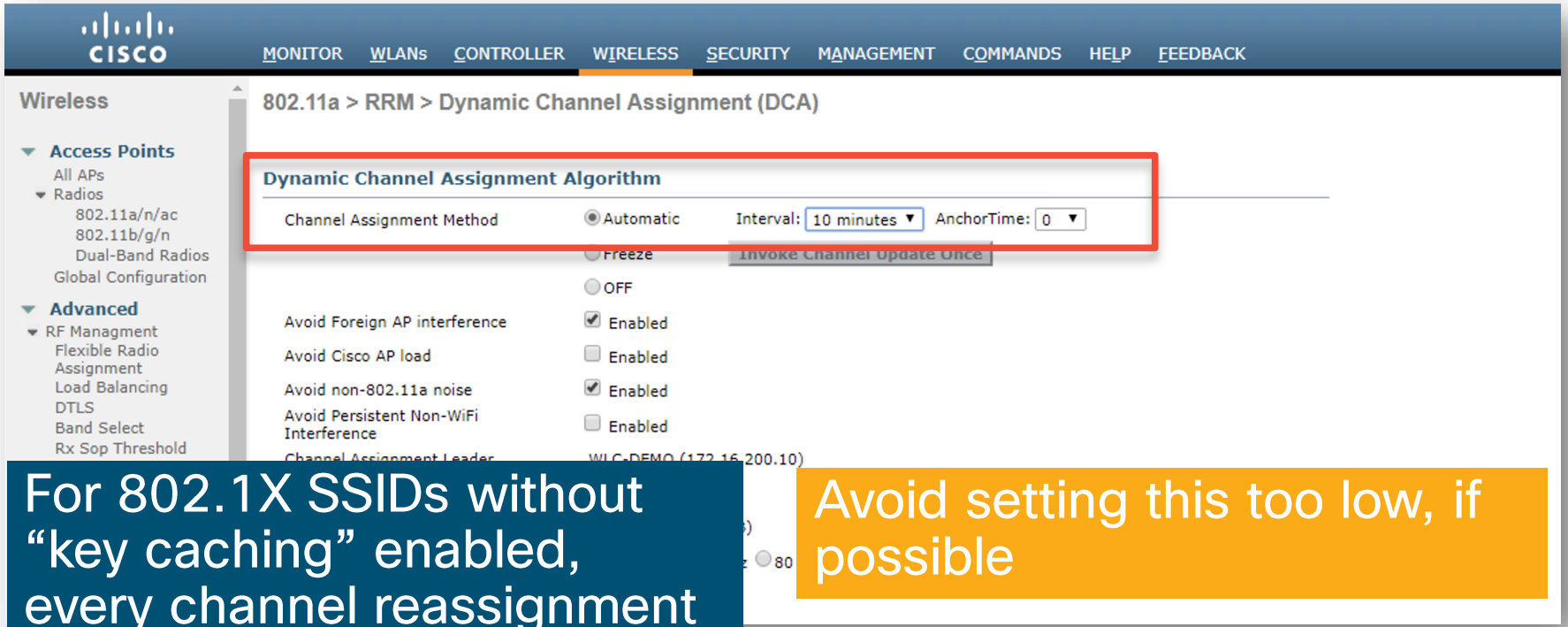
Advice: Timers – WLANs



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

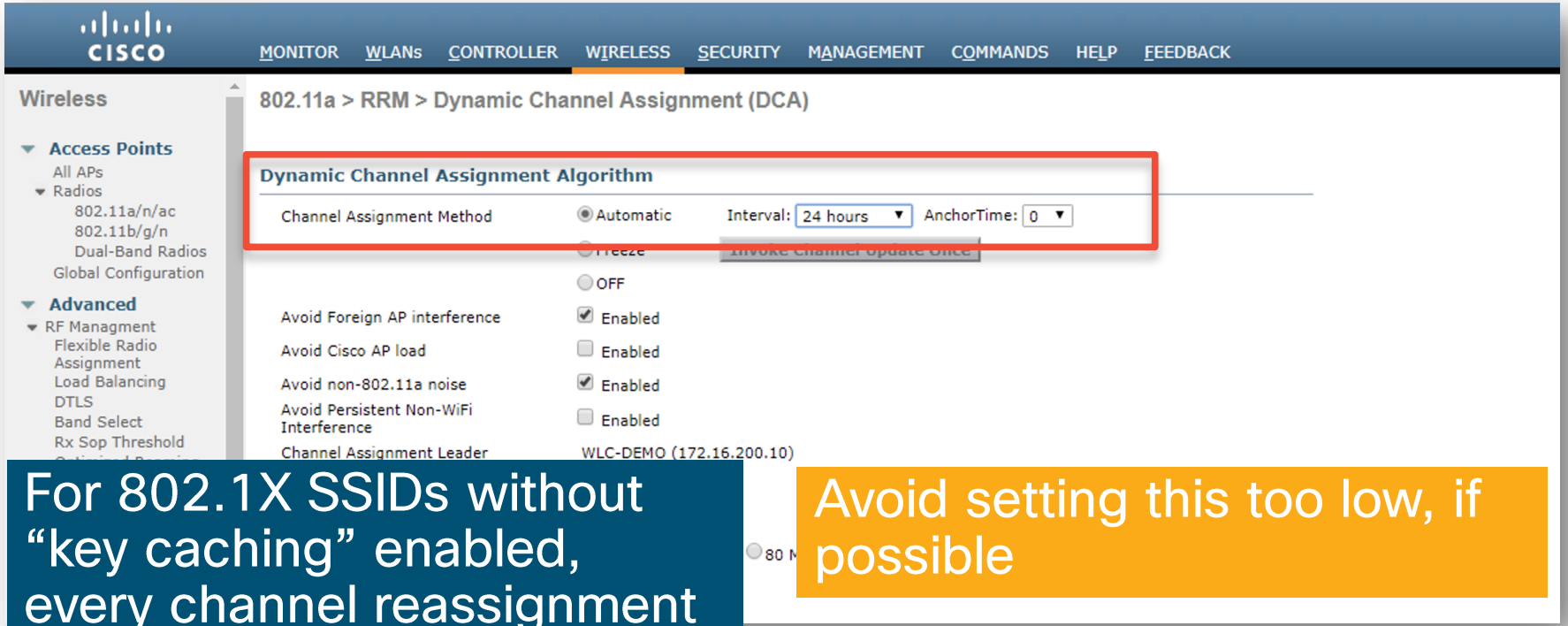
Advice: Timers – WLANs



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

Advice: Timers – WLANs



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**

Cisco live!

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)	Large VM Appliance (based on SNS-3495)
Processor	4 total cores (at 2.0 GHz or above) or a total minimum CPU allocation of 8000 MHz.	8 total cores (at 2.0 GHz or above) or a total minimum CPU allocation of 16000 MHz.
Memory	16 GB	32 GB
Total Disk Space	200 GB to 2 TB. See Disk Space Requirements for more information.	200 GB to 2 TB. See Disk Space Requirements for more information.
Ethernet NICs	Up to 4 Gigabit Ethernet NICs	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 [illegible] Installation Guide

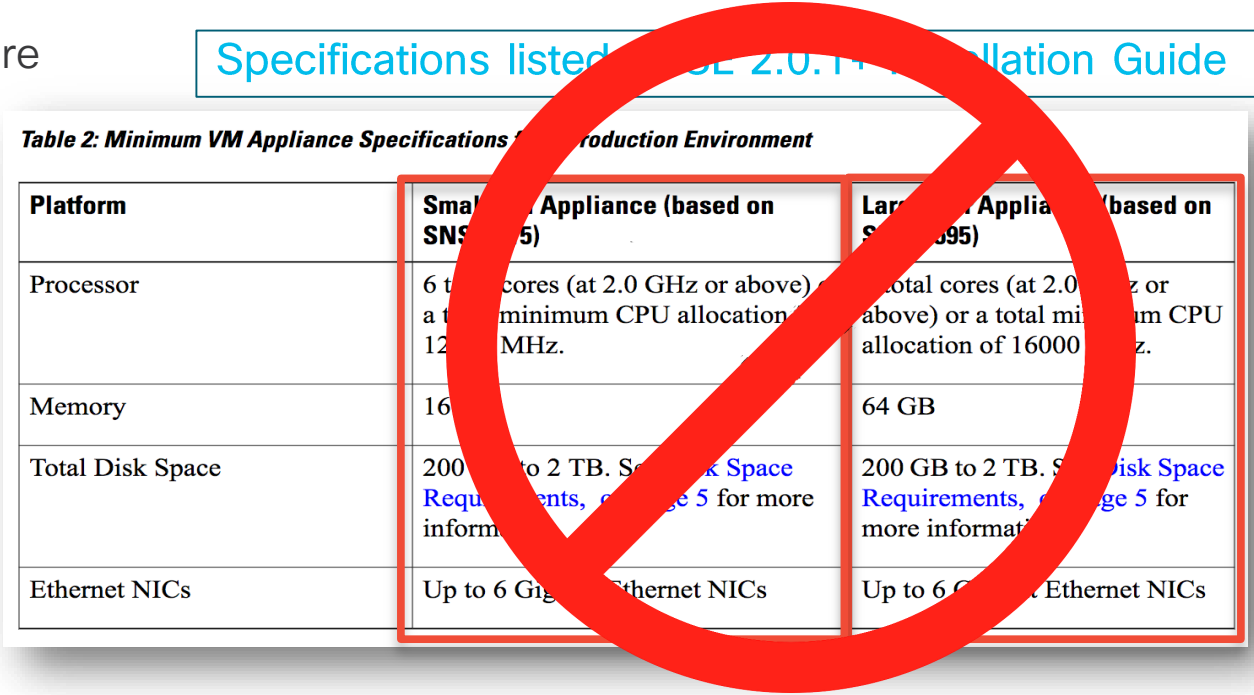


Table 2: Minimum VM Appliance Specifications [illegible] Production Environment

Platform	Small [illegible] Appliance (based on SNS [illegible]5)	Large [illegible] Appliance [illegible] based on S[illegible]595)
Processor	6 t[illegible] cores (at 2.0 GHz or above) [illegible] a t[illegible] minimum CPU allocation [illegible] 12[illegible] MHz.	[illegible] total cores (at 2.0[illegible]z or above) or a total mi[illegible]m CPU allocation of 16000 [illegible]z.
Memory	16[illegible]	64 GB
Total Disk Space	200 [illegible]to 2 TB. S[illegible]k Space Requ[illegible]ents, [illegible]ge 5 for more inform[illegible]	200 GB to 2 TB. S[illegible]isk Space Requirements, [illegible]ge 5 for more informati[illegible]
Ethernet NICs	Up to 6 Gig[illegible]thernet NICs	Up to 6 G[illegible] 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 wih 16 GB RAM and 8 cores is created; which doesnt 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.

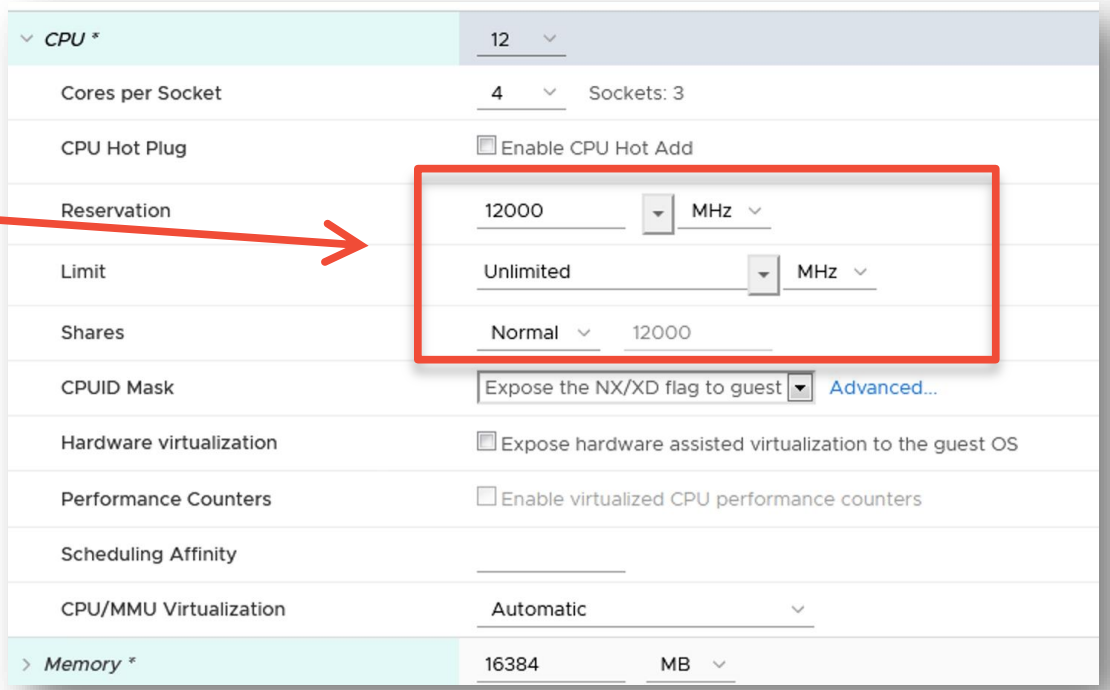
Specifications listed in ISE 2.0.1+ Installation Guide

Platform	Small VM Appliance (based on SNS-3515)	Medium VM Appliance (based on SNS-3595)	Large VM Appliance (Super MnT)
Processor	**12** total cores (2 GHz or above) with a minimum CPU allocation of 12000MHz.	**16** total cores (2 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

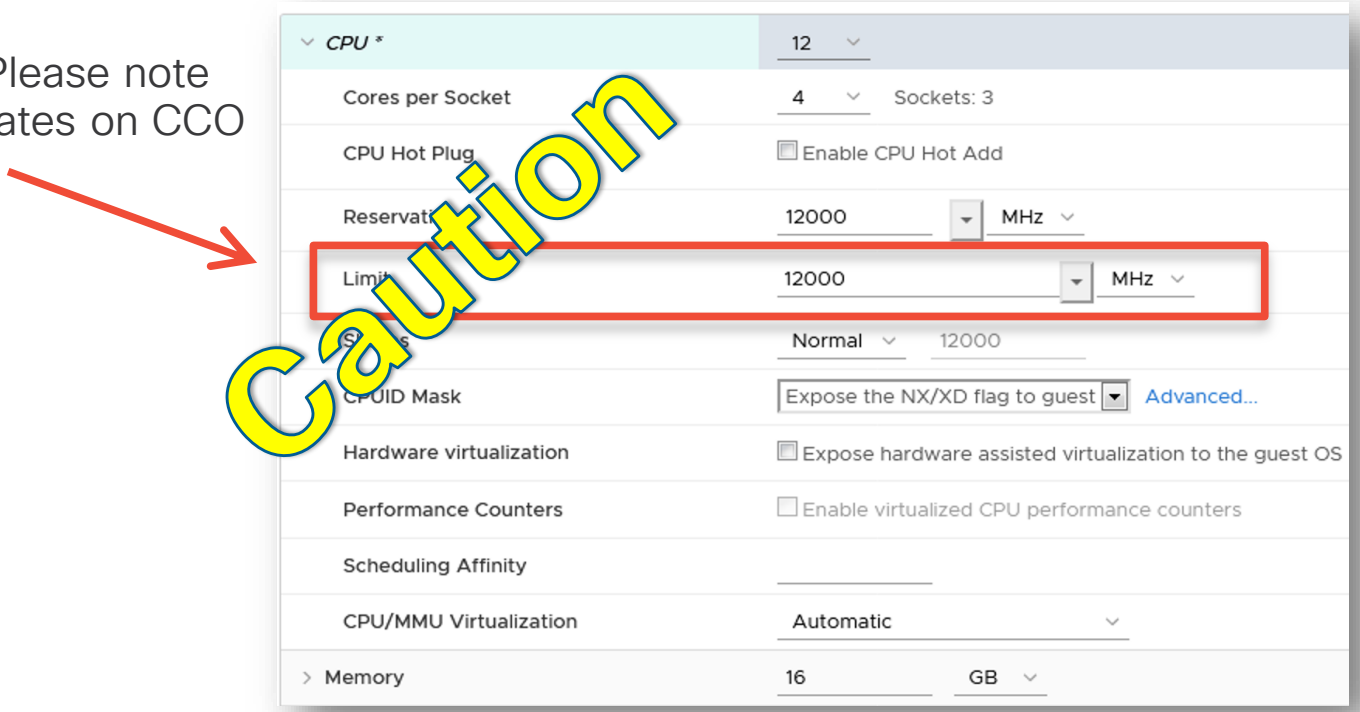
- To be successful (and **supported**) ISE VMs must be built with Dedicated Resources that are equivalent to the hardware appliance.



Advice: VM Resources

Reservations

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



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.

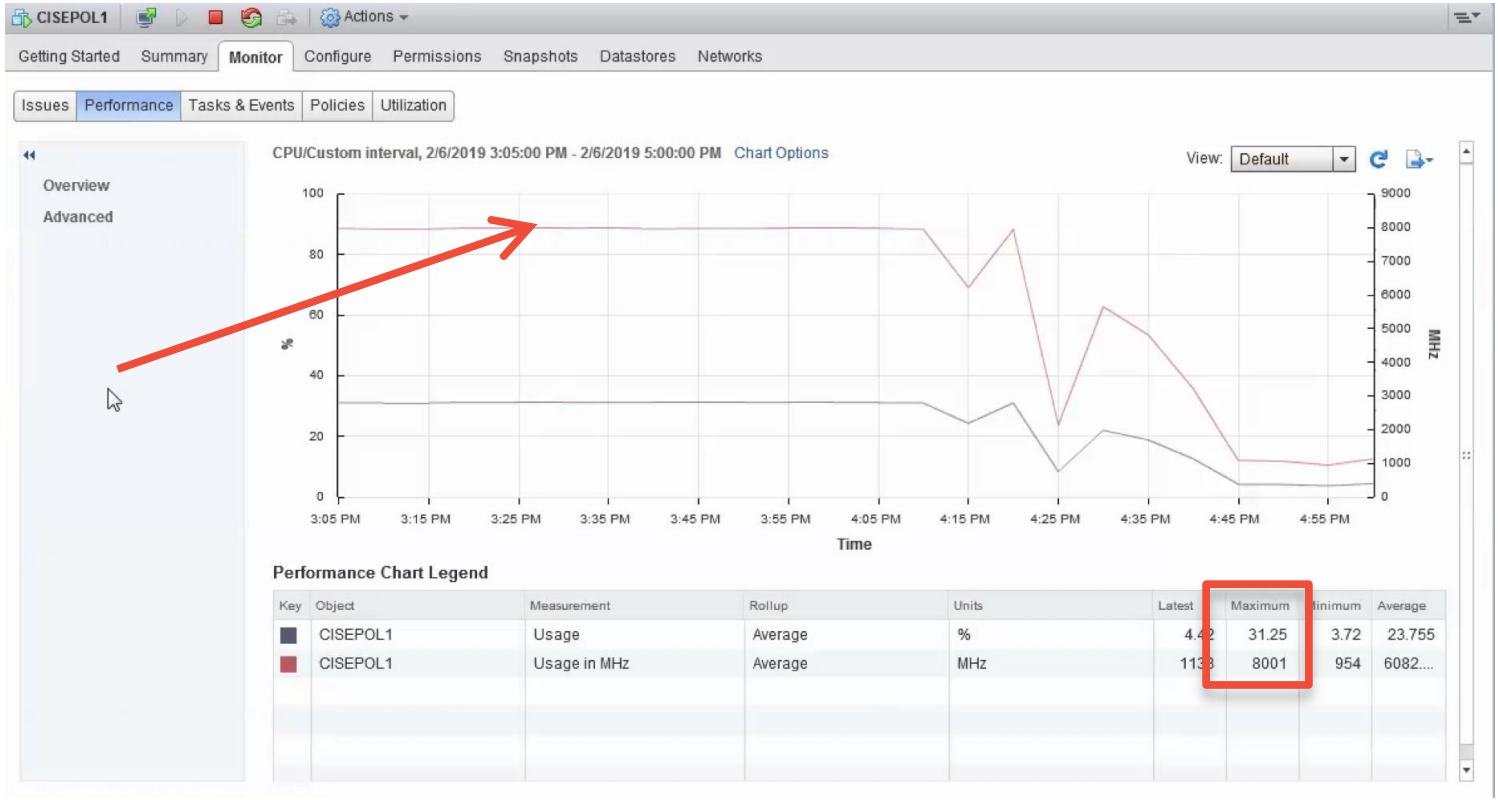
Workaround:
Customer can shutdown the ISE VM client, remove the limit and restart the ISE VM.

Further Problem Description:

Not Resolved: New Templates are needed. Workaround available.

Advice: VM Resources

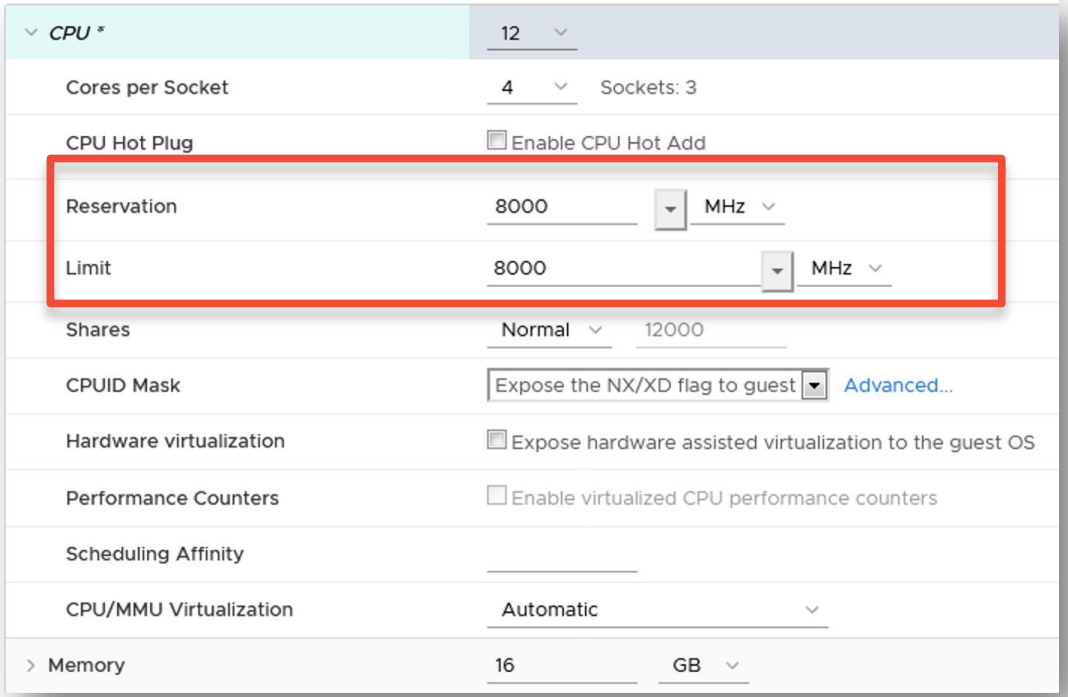
Reservations



Advice: VM Resources

Reservations

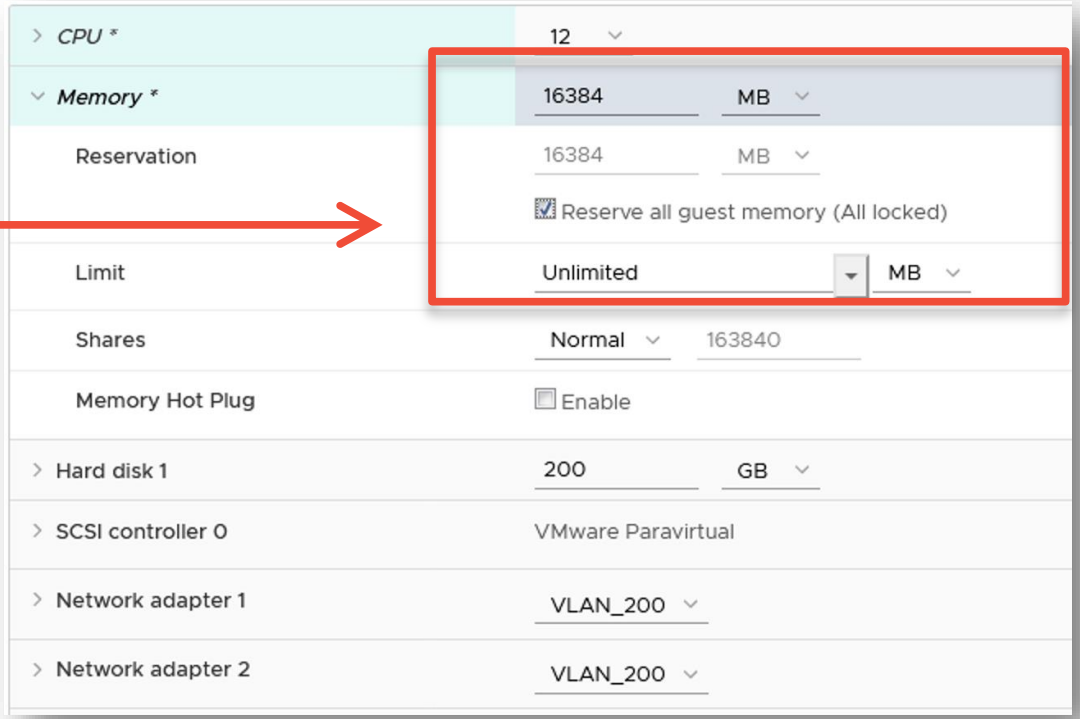
- Avoid setting limits. Please note that some OVA templates on CCO contain this issue.



Advice: VM Resources

Reservations

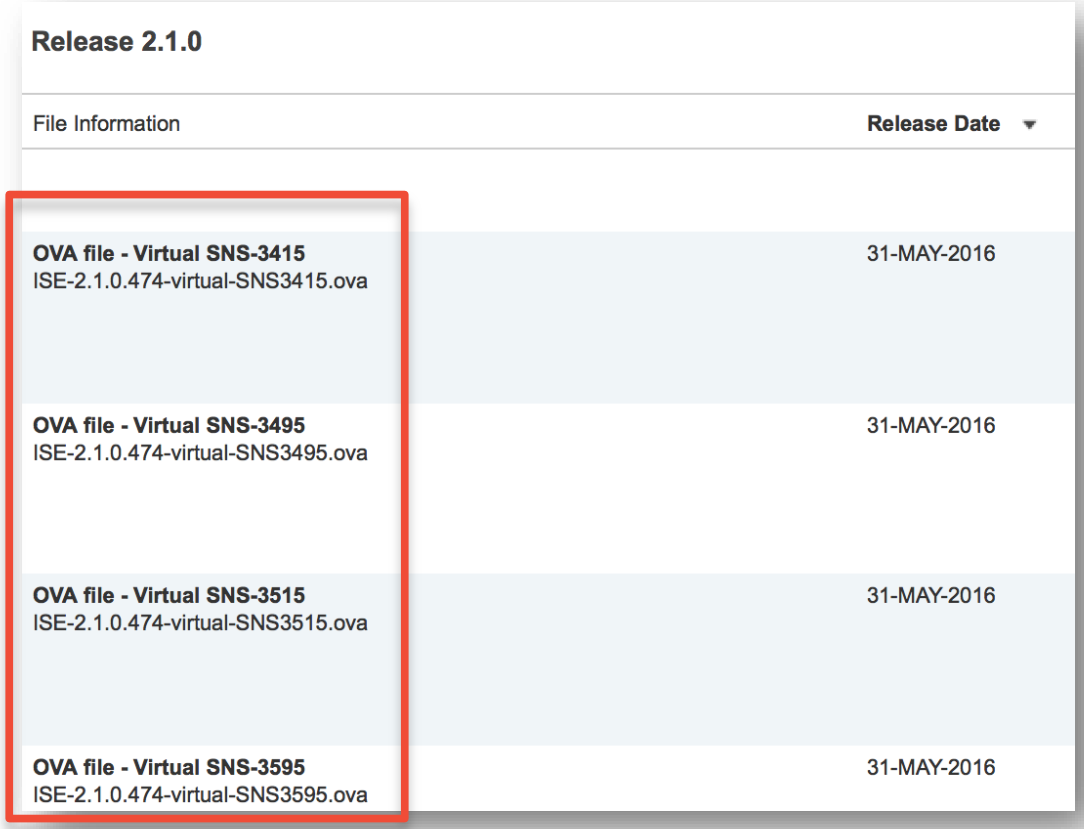
- To be successful (and **supported**) ISE VMs must be built with Dedicated Resources that are equivalent to the hardware appliance.



Advice: VM Resources

Reservations

- 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!



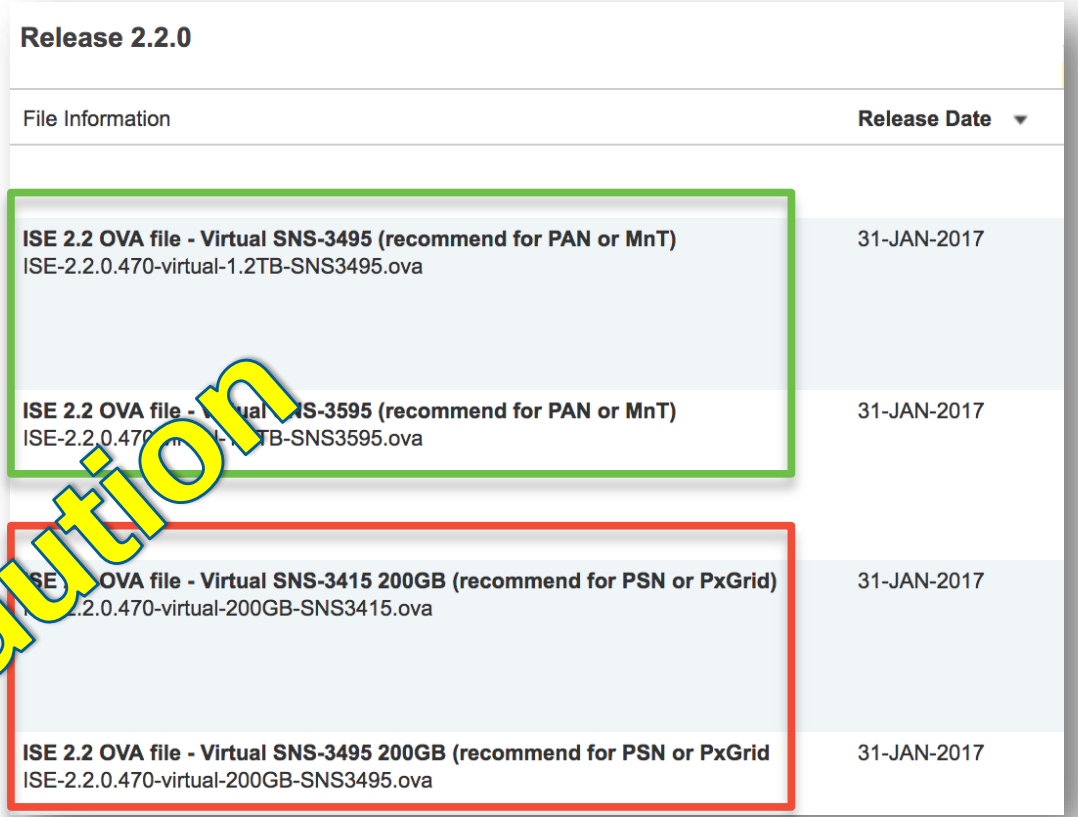
Release 2.1.0

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

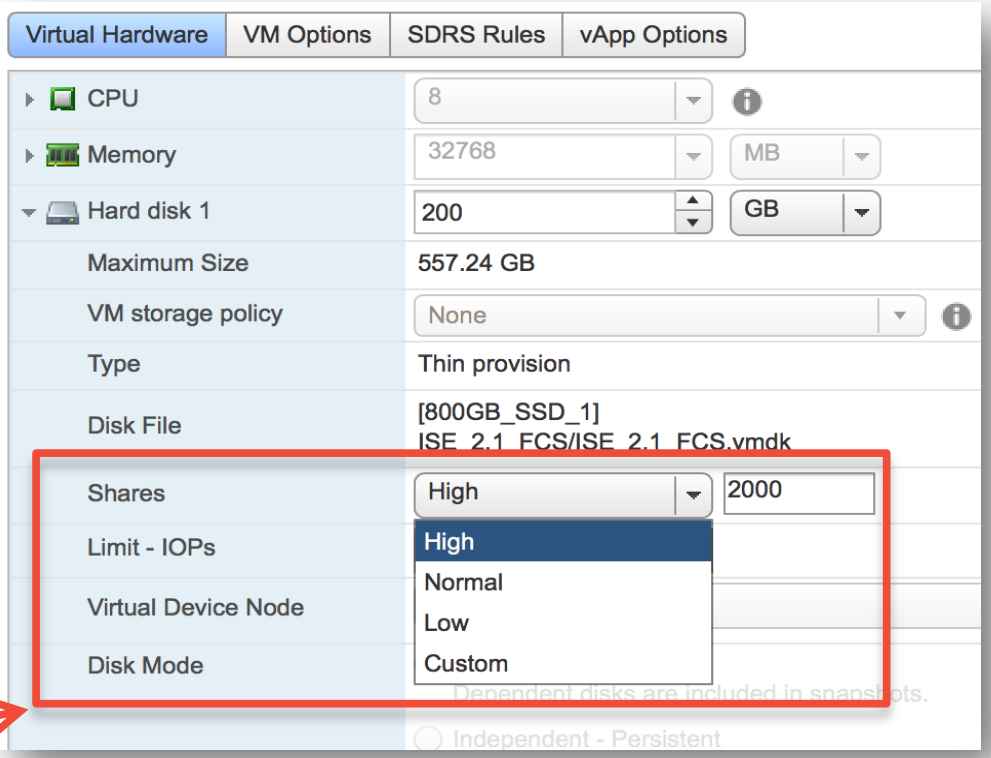
- To be successful (and **supported**) ISE VMs must be built with Dedicated Resources that are equivalent to the hardware appliance.
- In 1.3 we added OVA Templates for deploying SNS-3415 and SNS-3495 equivalent hardware. That has been expanded to include the SNS-3515 and SNS-3595 platforms as well.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



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

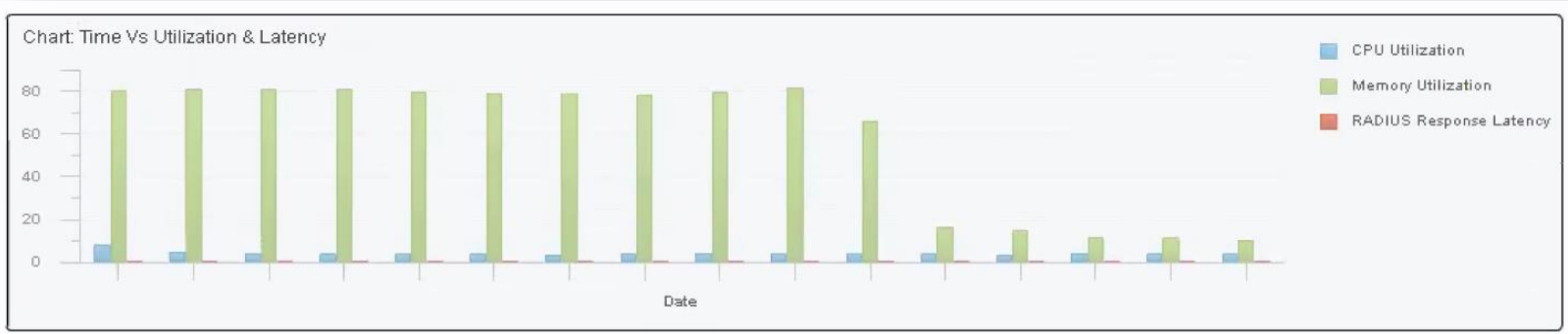
Generated at 2016-05-26 15:58:56.55

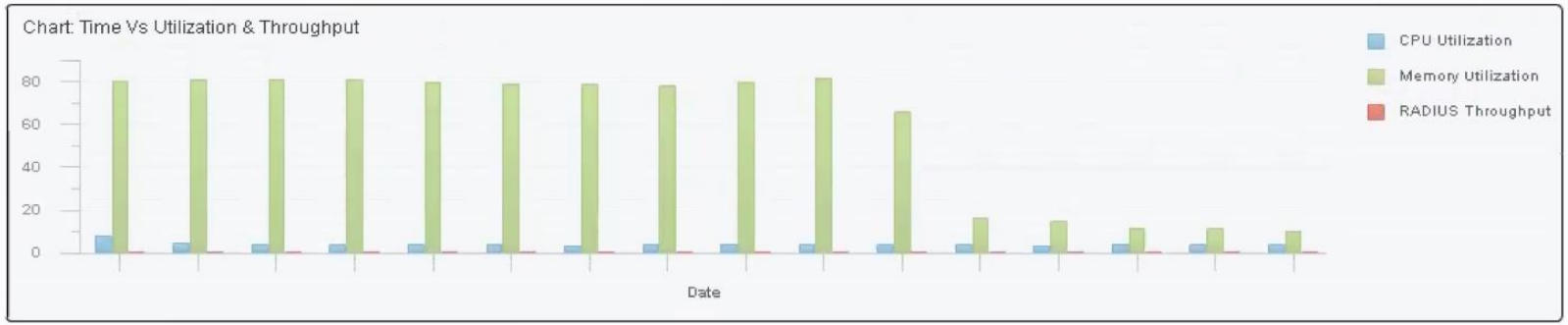
Health Summary

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
[illegible]	[illegible]	[illegible]	[illegible]	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
[illegible]	[illegible]	[illegible]	[illegible]	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

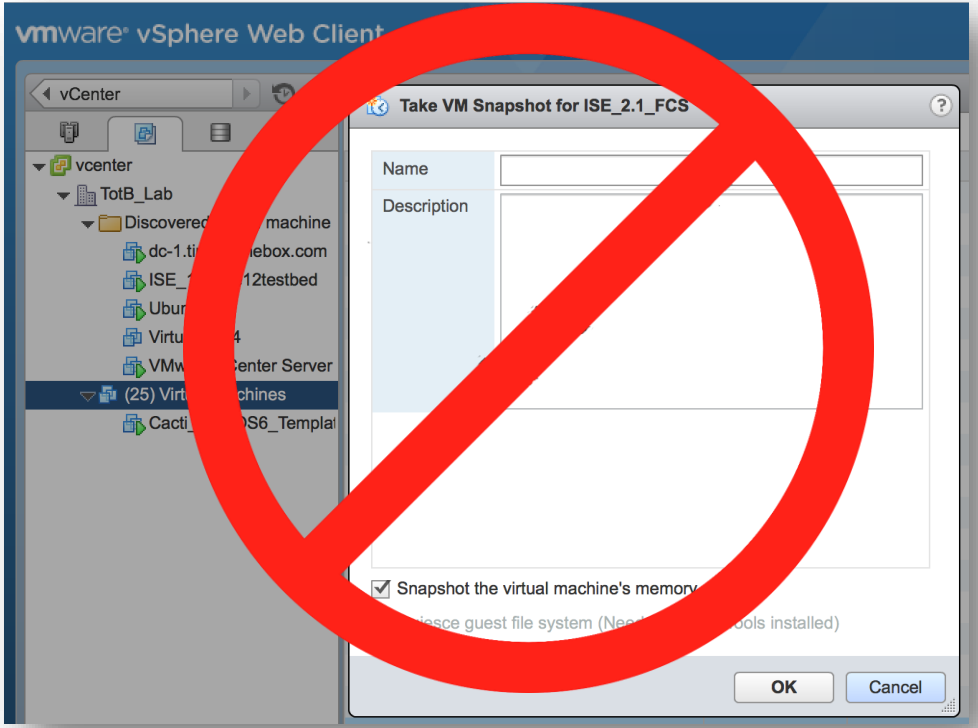




Advice: VM Settings

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**

Cisco live!

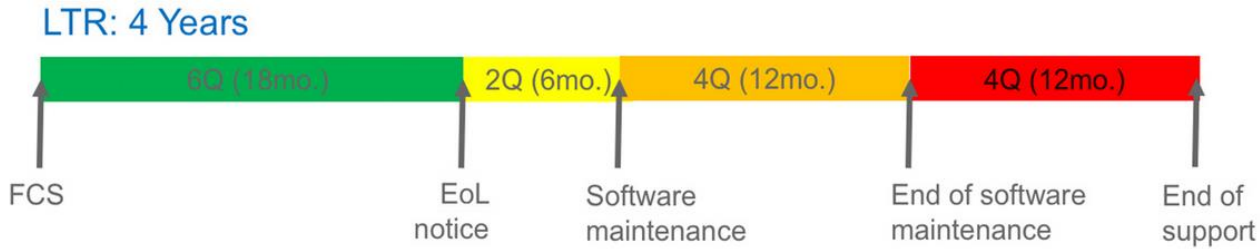
ISE Best Practice Check List

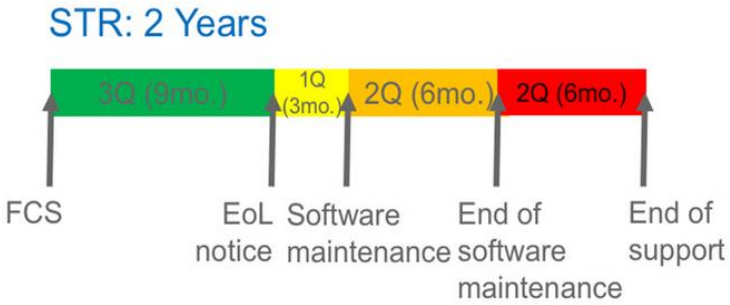
- Long vs Short lived releases
- Size correctly
- Know your clients
- Ensure suppression with rejection is enabled
- Enable Endpoint Attribute Filter
- Avoid ordering policy in a way that does unnecessary lookups (AD)
- Reduce the number of Endpoint Map Ownership Changes
- Watch out for misbehaving clients!

Advice: Versions

Information

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





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

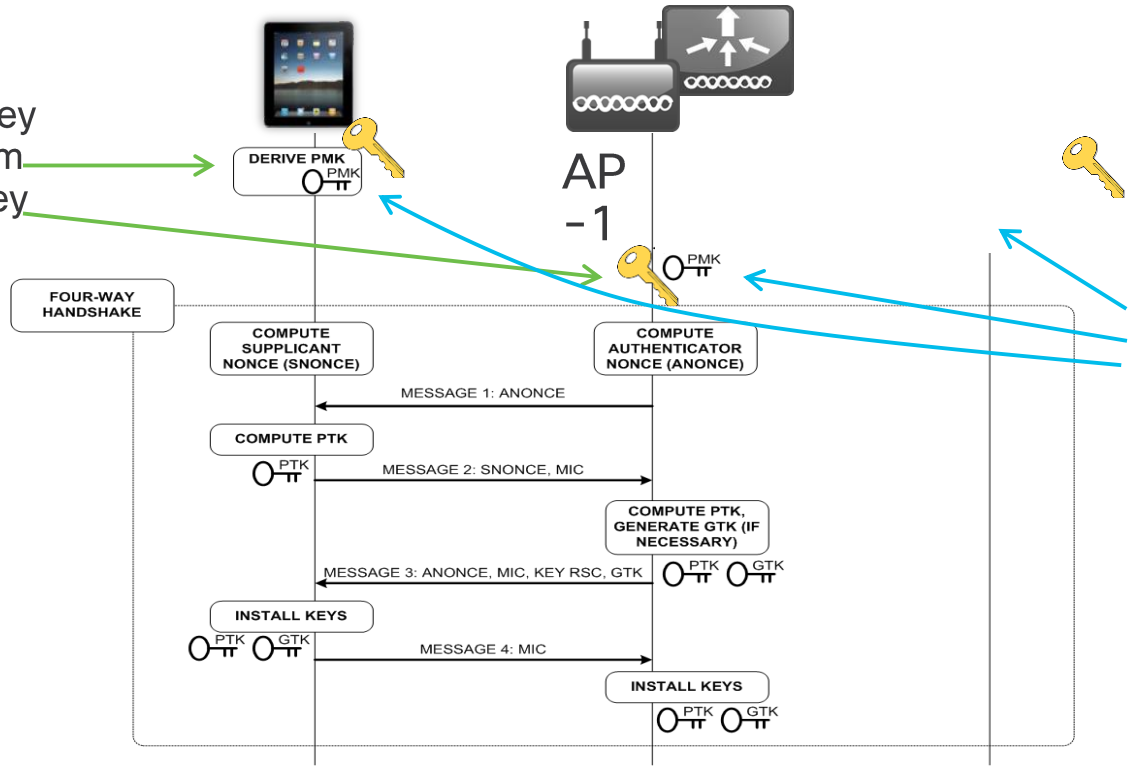
- ISE releases have a ”Long lived”-“Short lived” cadence
- Releases follow currently an even/odd or every other pattern

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)

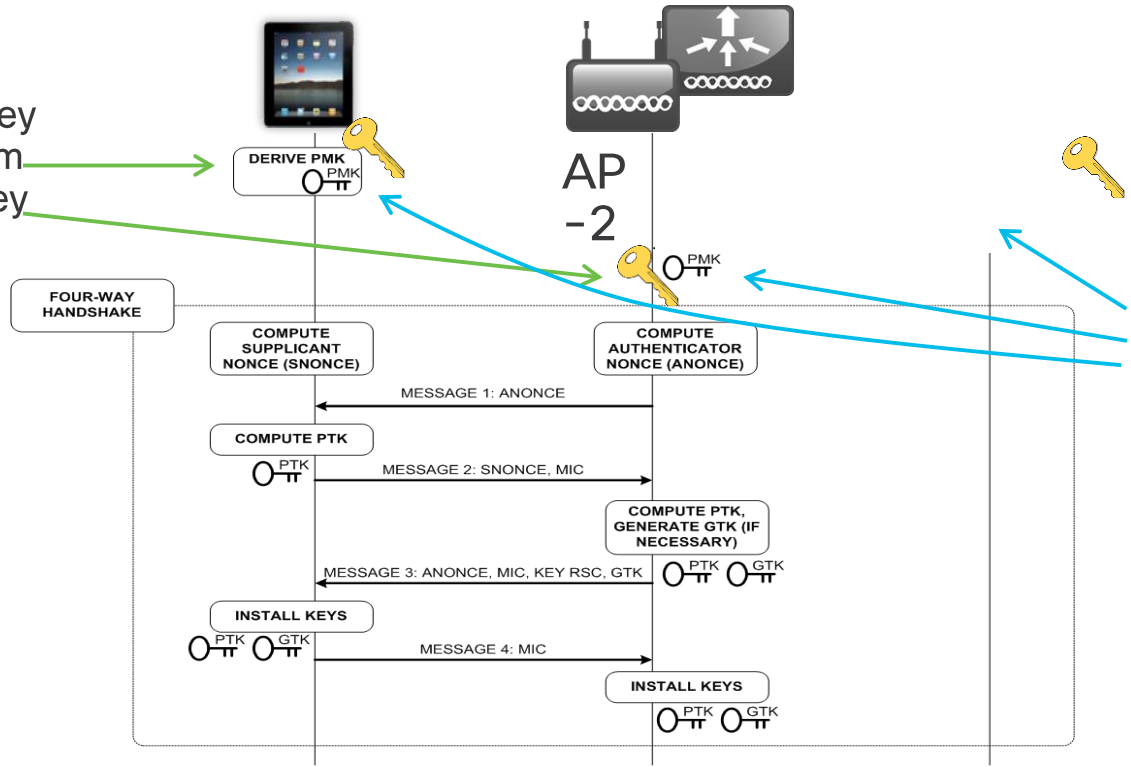


- PMK derived from 802.1X

Advice: Sizing

Without key caching, this happens on every 802.1x roam

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

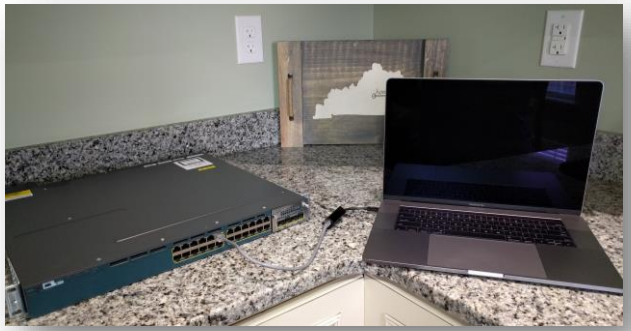


- PMK derived from 802.1X

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

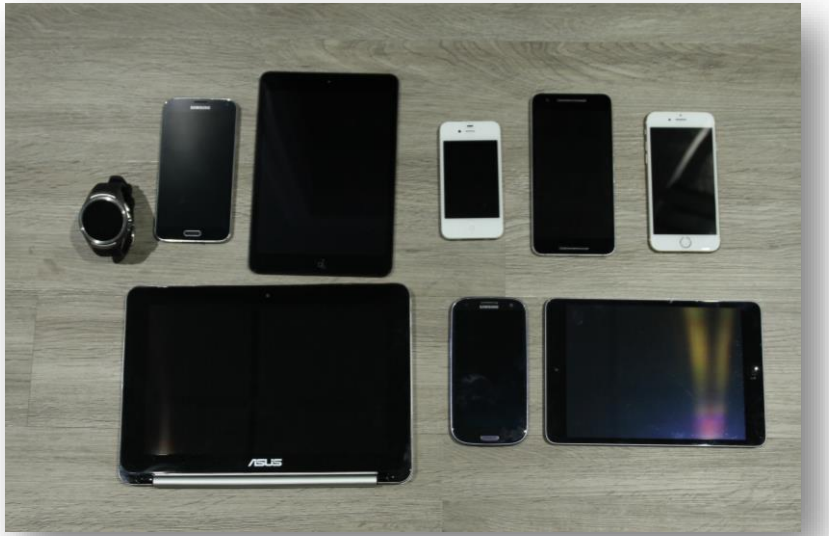
=2X

=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

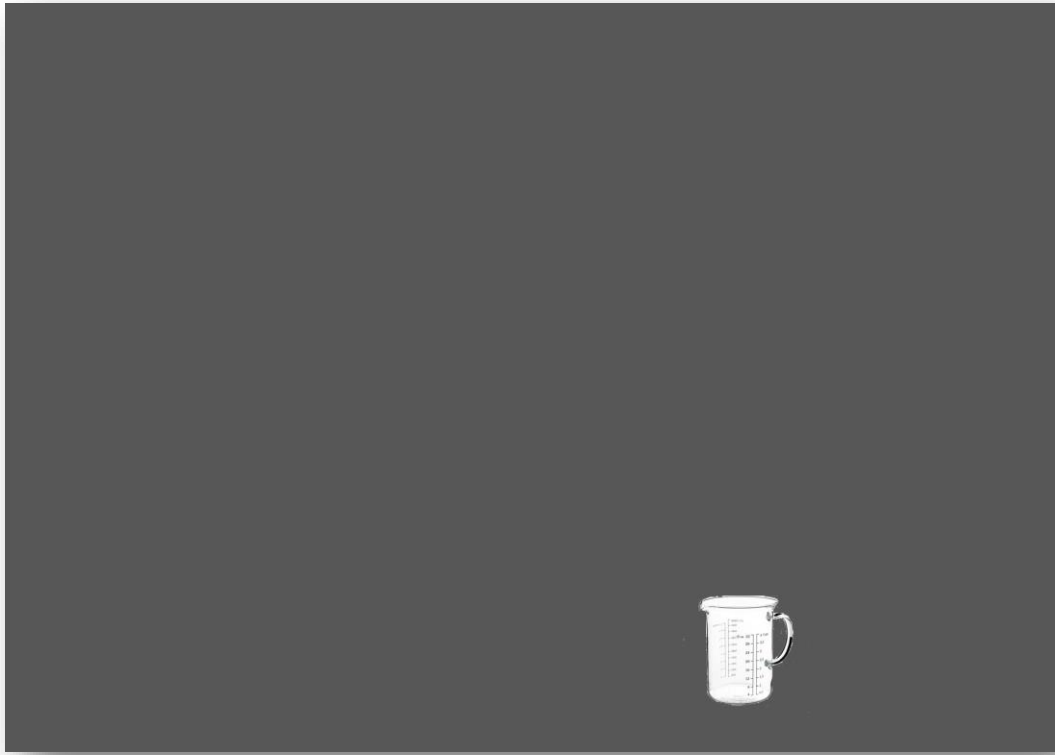
Scaling per PSN[1]	Max Active Sessions
SNS 3615	10,000
SNS 3655	50,000
SNS 3695	100,000
SNS 3515	7,500
SNS 3595	40,000

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.

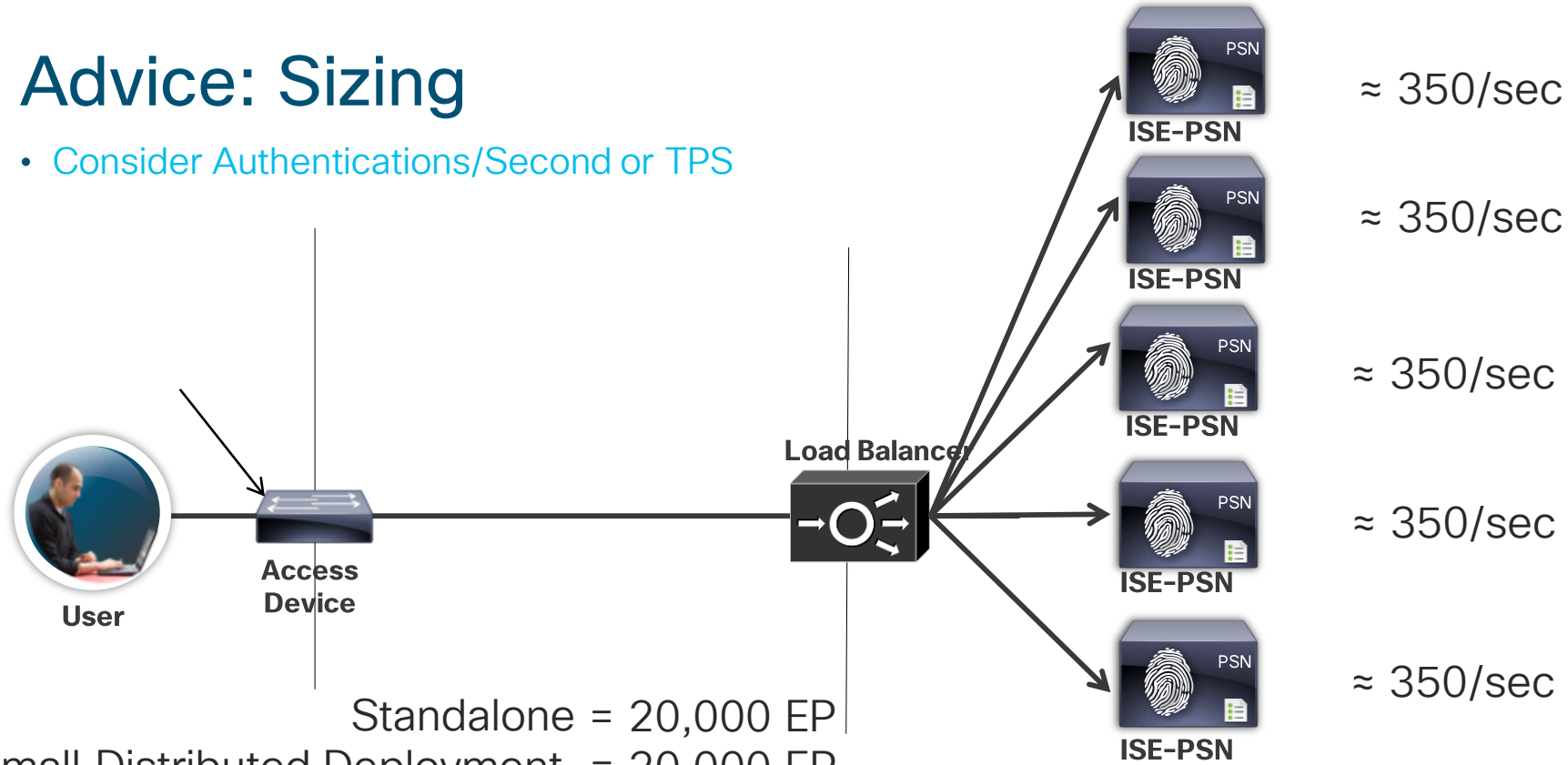
Authentications per second with PSN only persona (Approximate values)

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 ≈ 1750/sec

Advice: Avoid Meltdowns

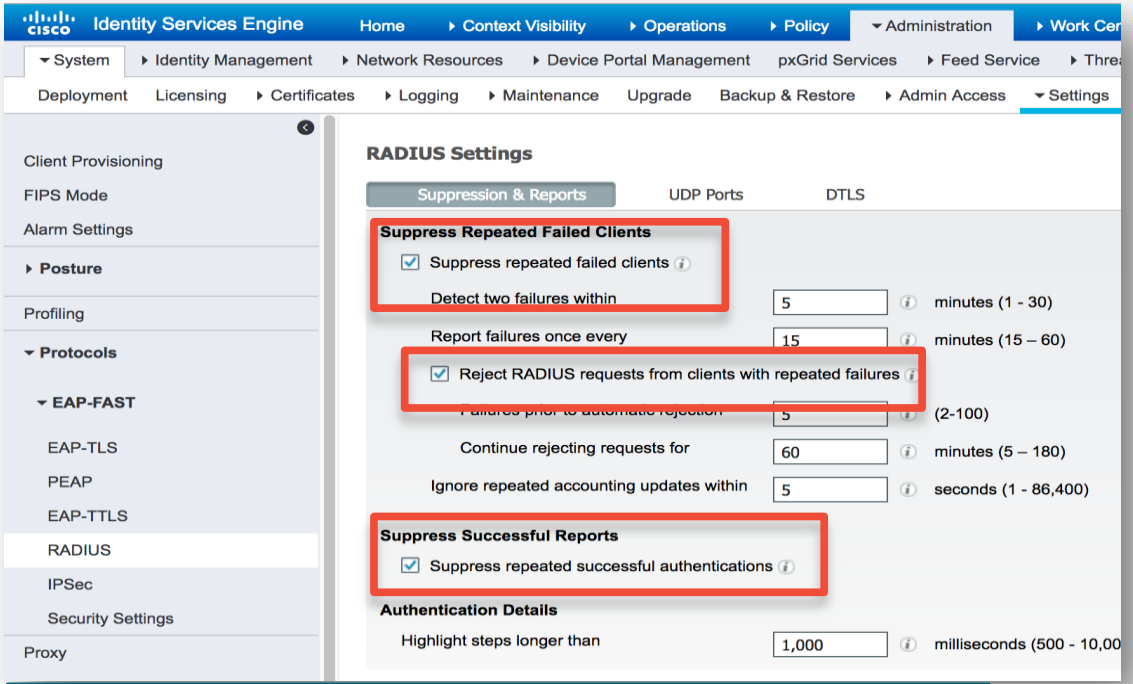
ISE Settings

- 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

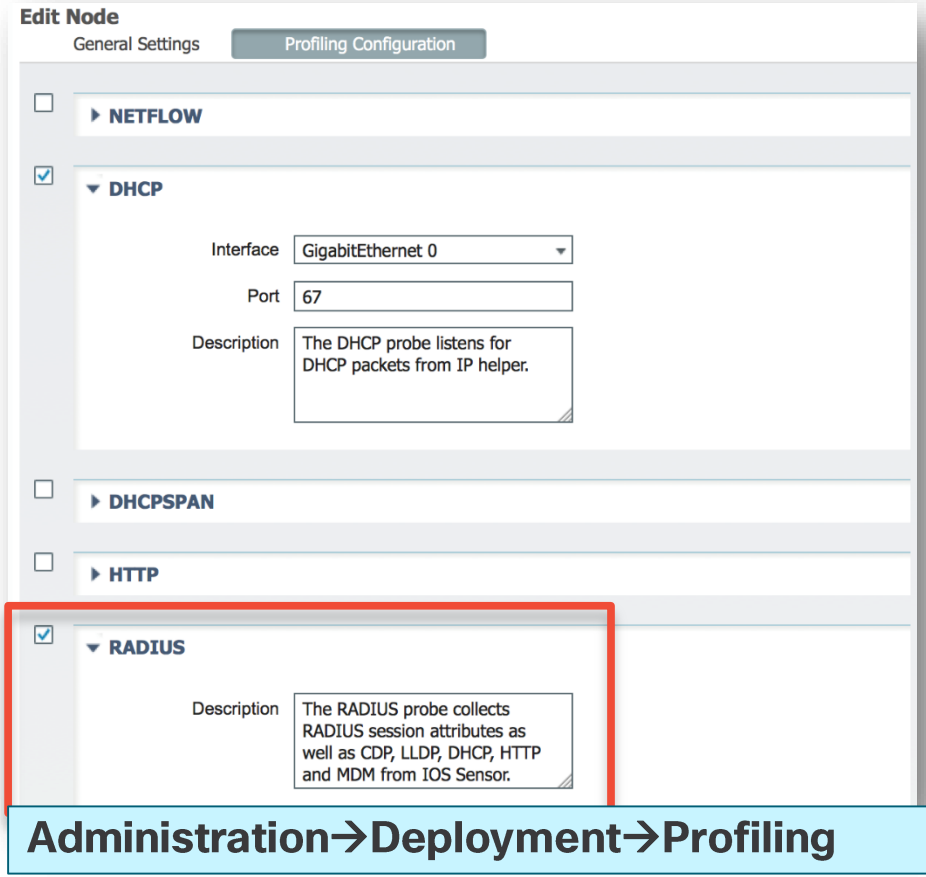


Administration→Settings→Protocols→Radius

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

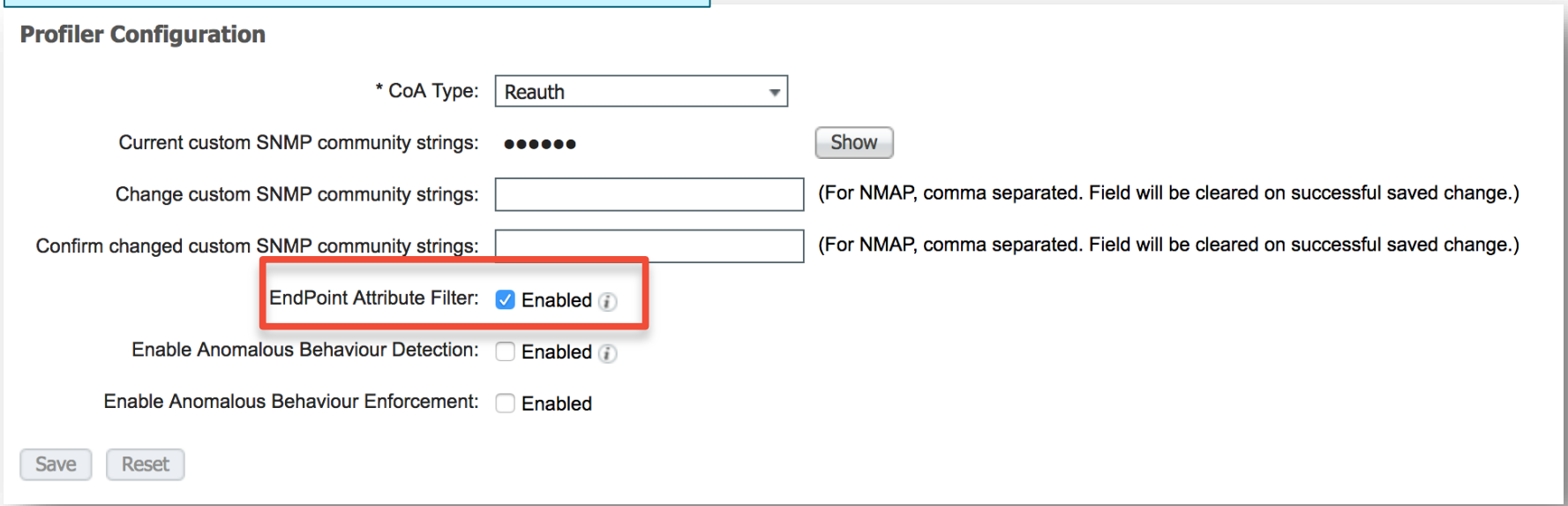


Advice: Avoid Meltdowns

ISE Settings

- Enable EndPoint Attribute Filter

Administration→Settings→Profiling



Load Balancer for ISE Best Practice Check List

You make networking **possible**

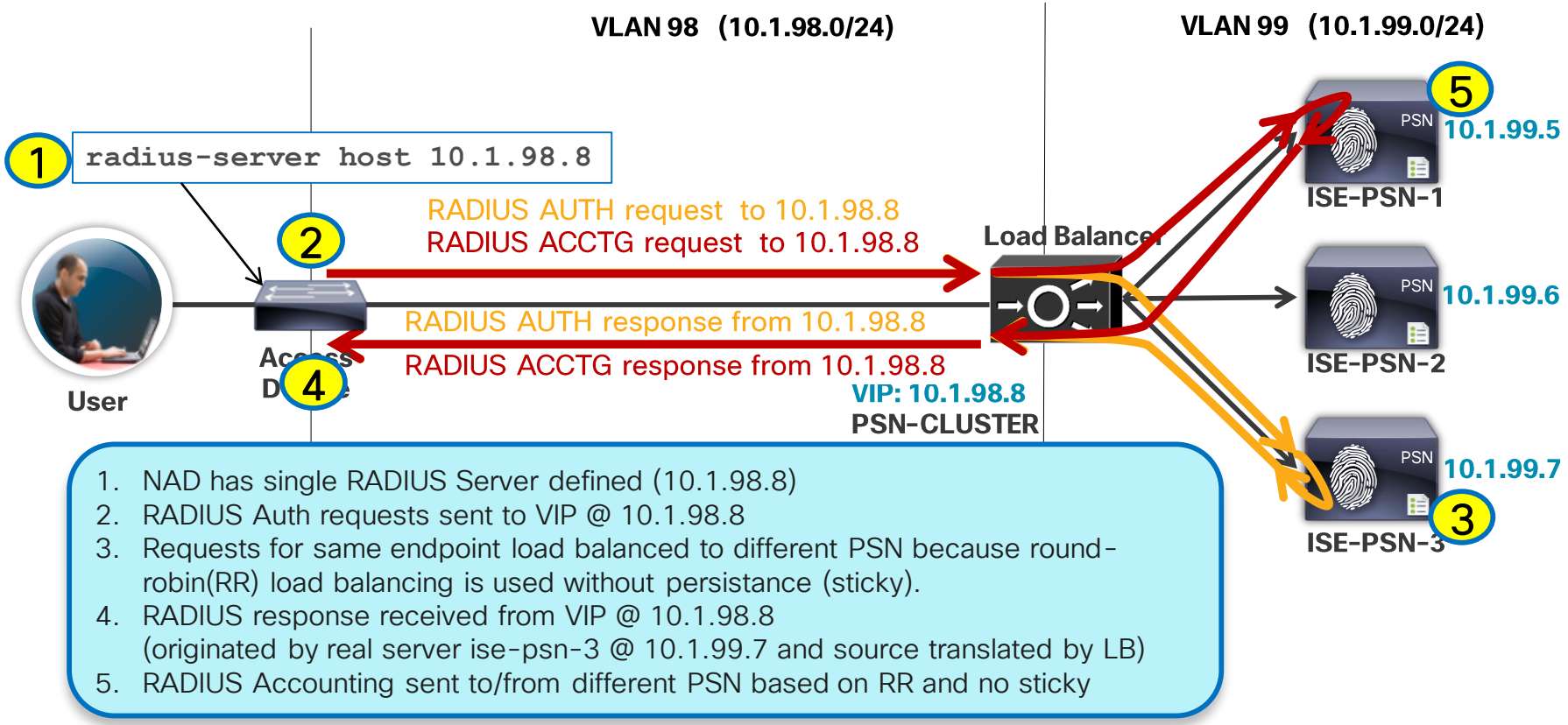
Cisco live!

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

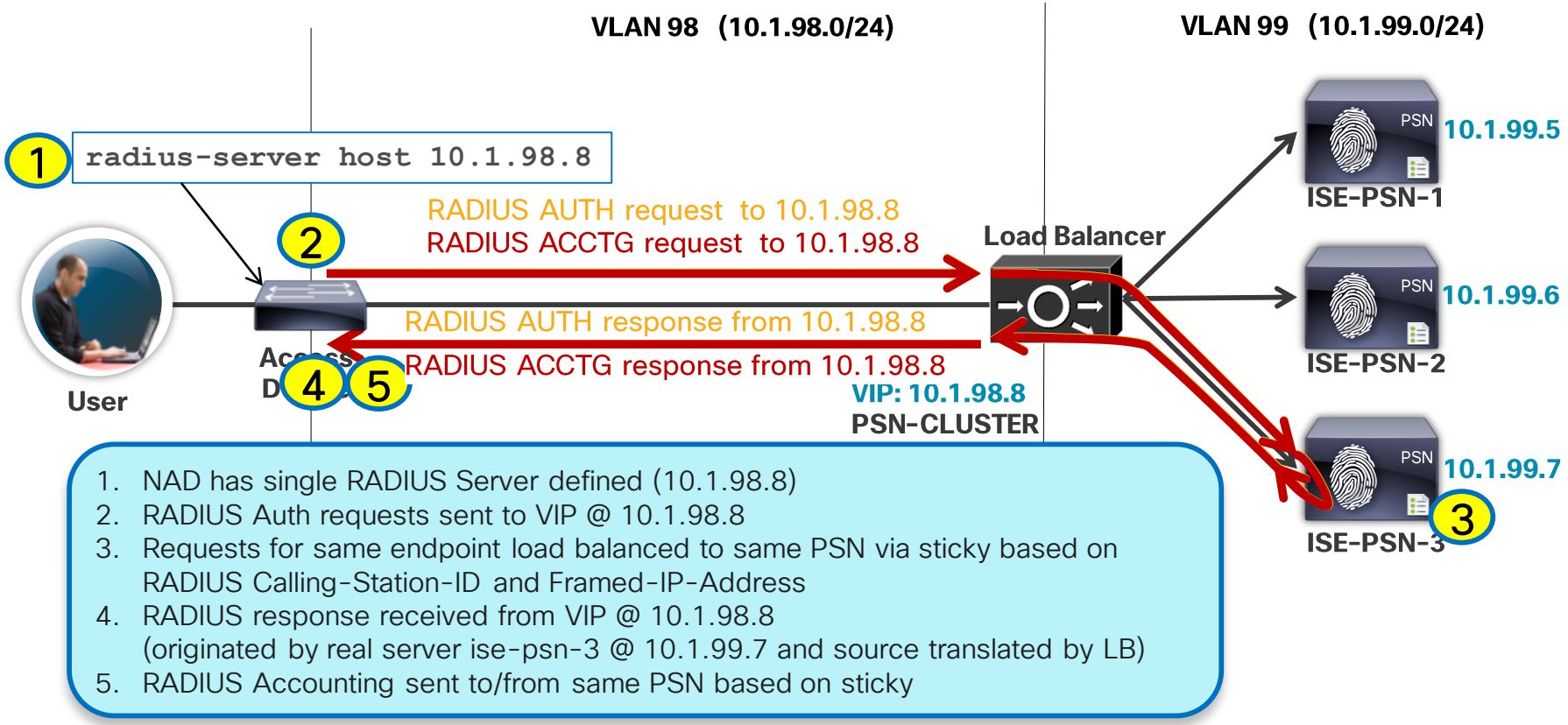
Sample Flow



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 persistance (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

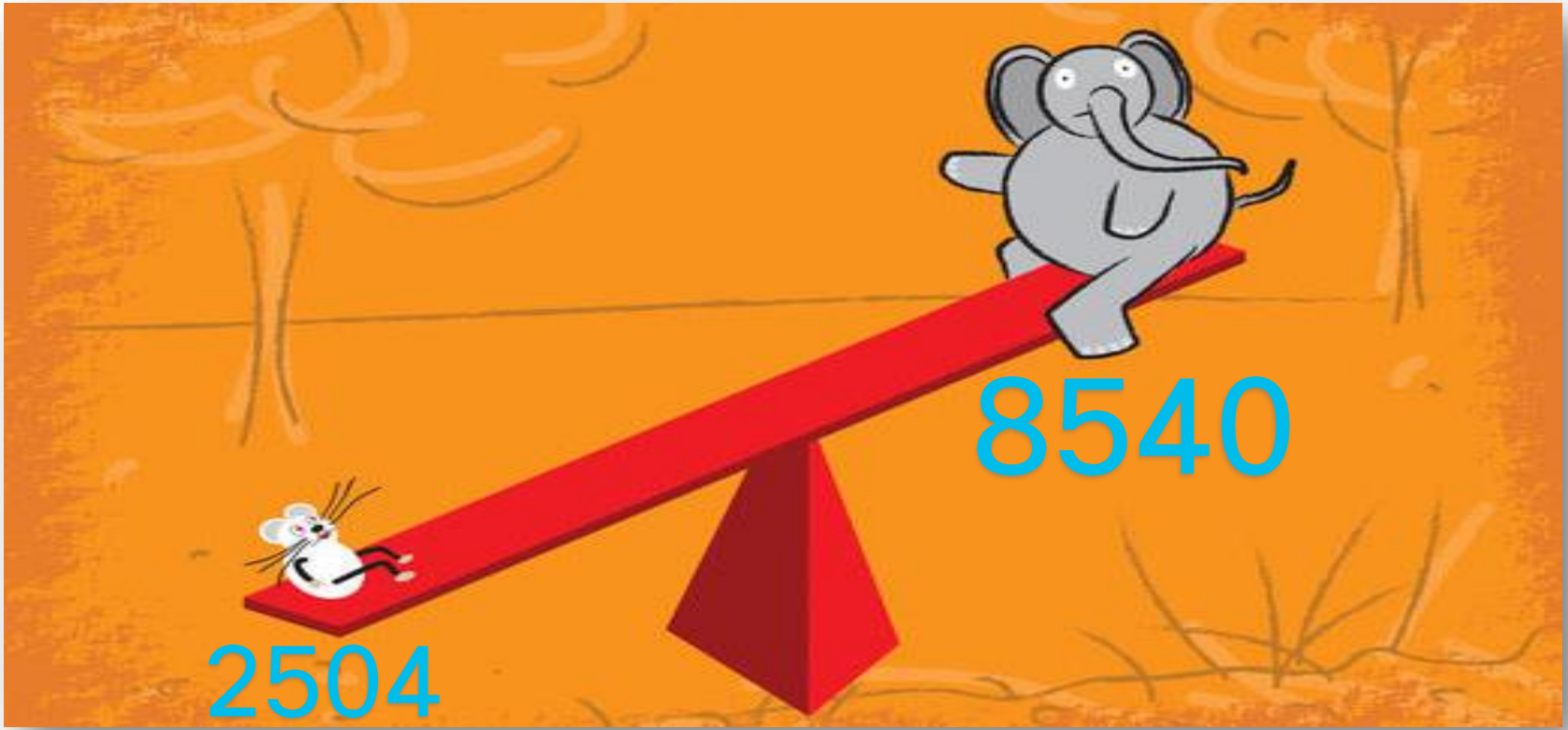
Sample Flow



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

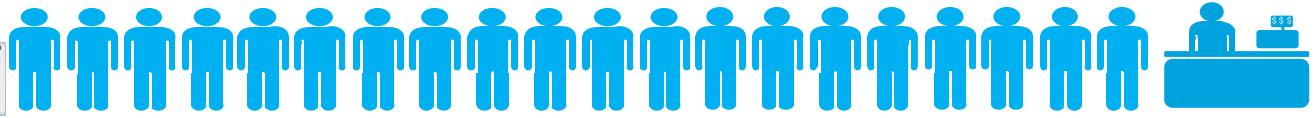
Load Balancing RADIUS

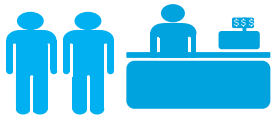
All NADs are not created equal!

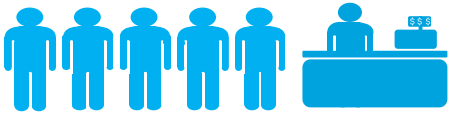


Load Balancing RADIUS

IP vs Calling Station ID Stickiness

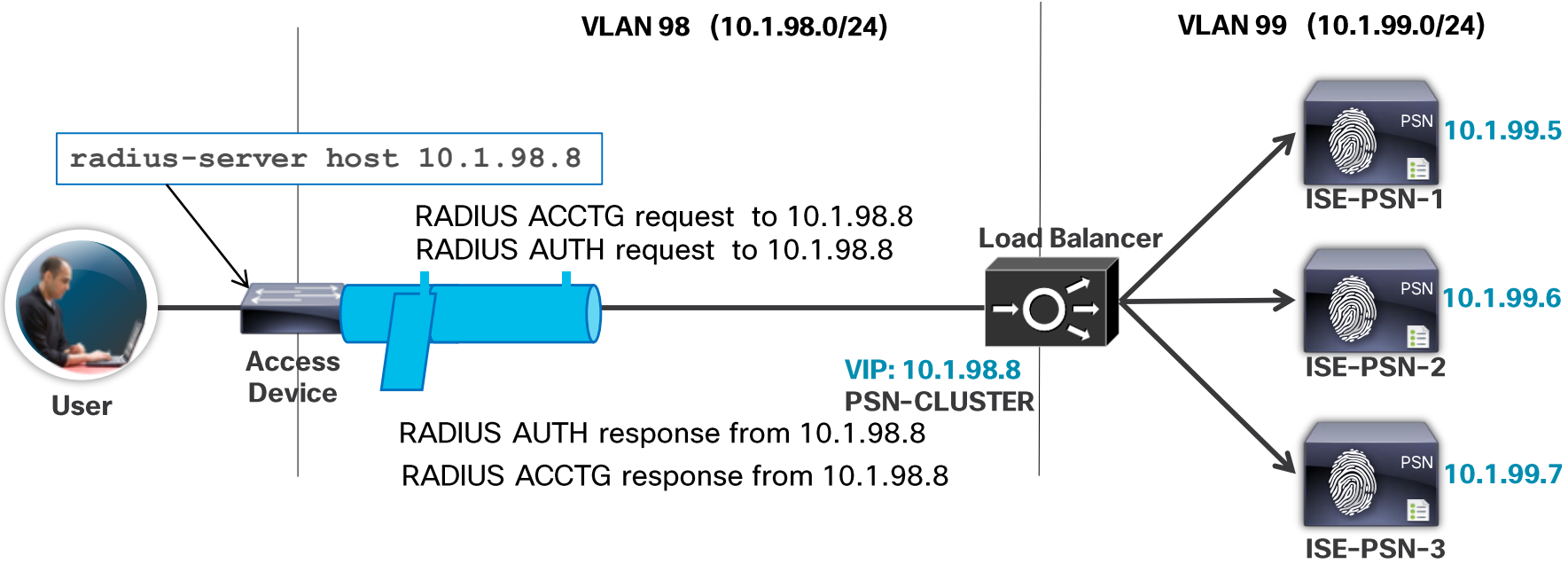






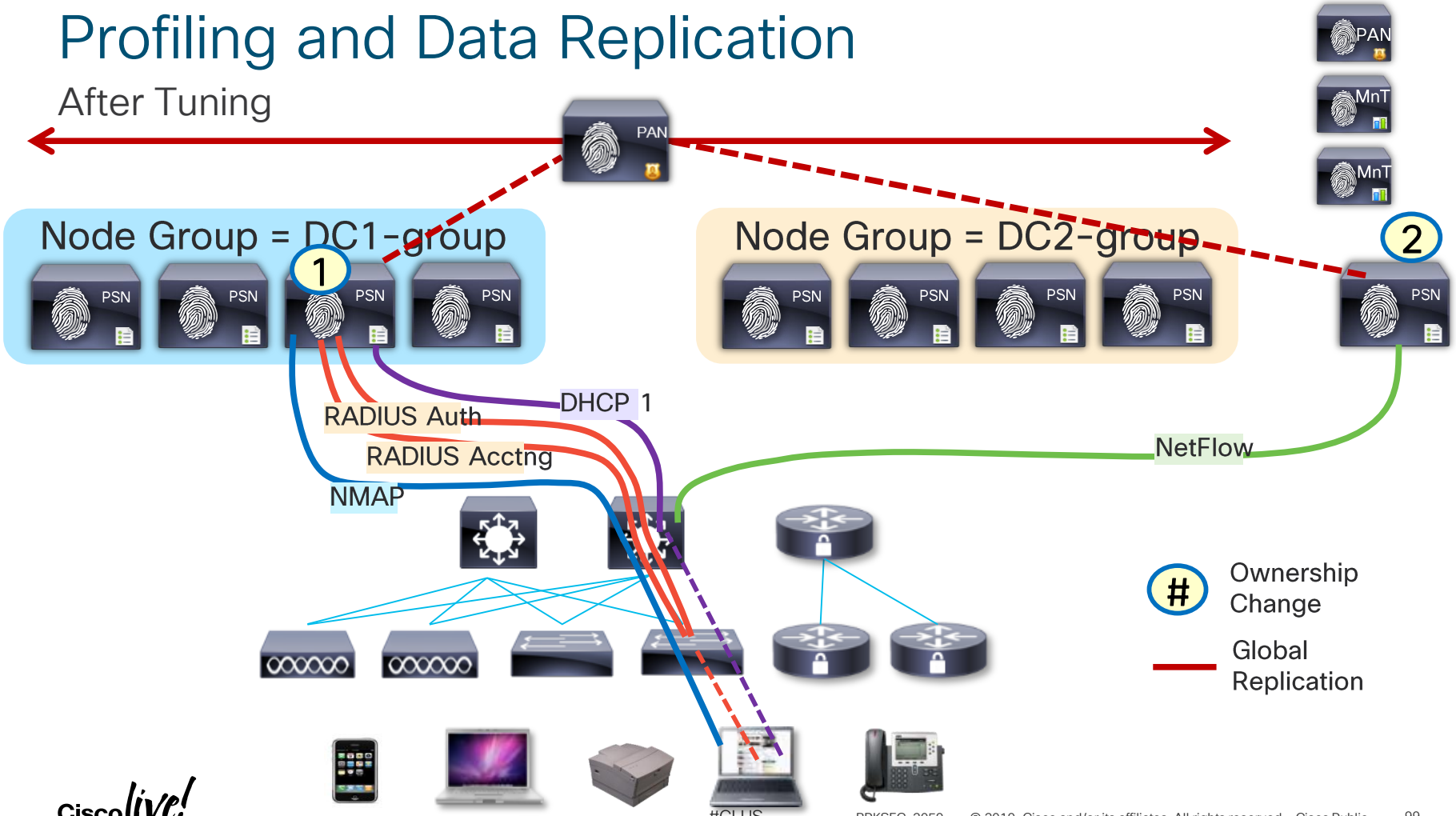
Load Balancing RADIUS

Avoid spraying packets!!!



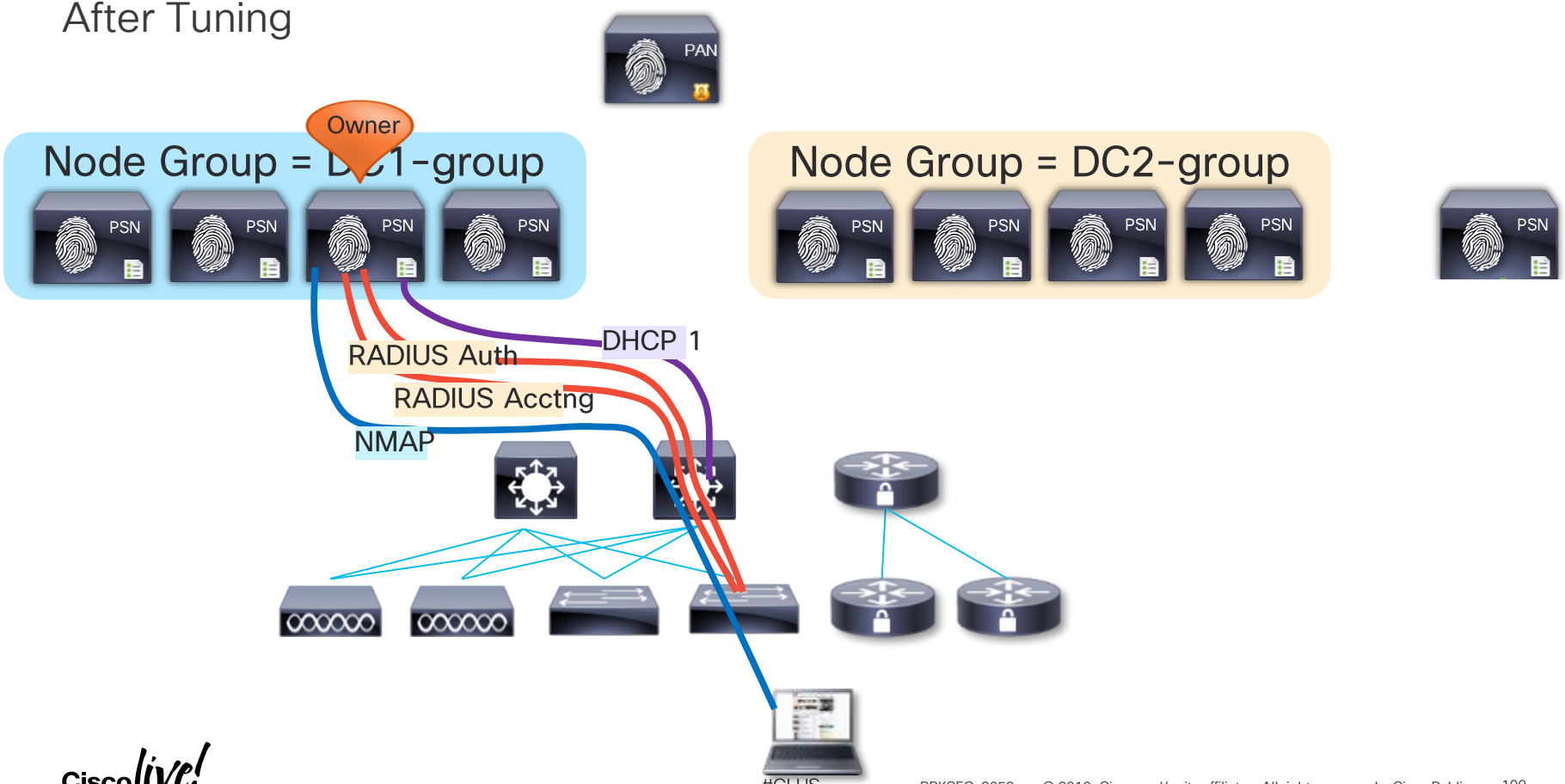
Profiling and Data Replication

After Tuning



Impact of Ownership Changes

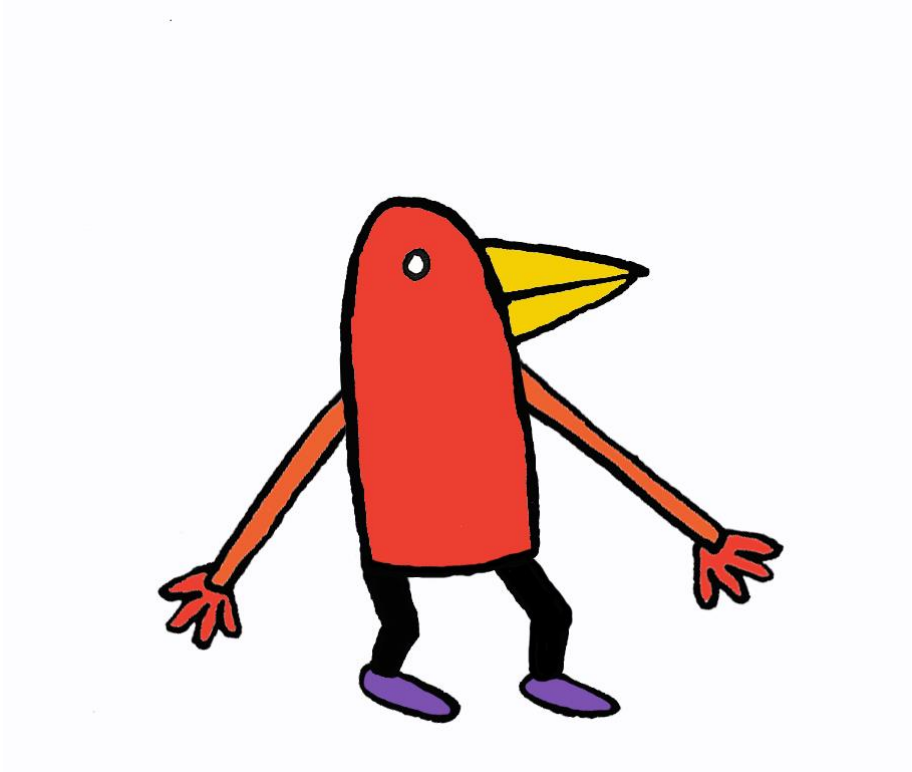
After Tuning



Advice: Avoid Meltdowns

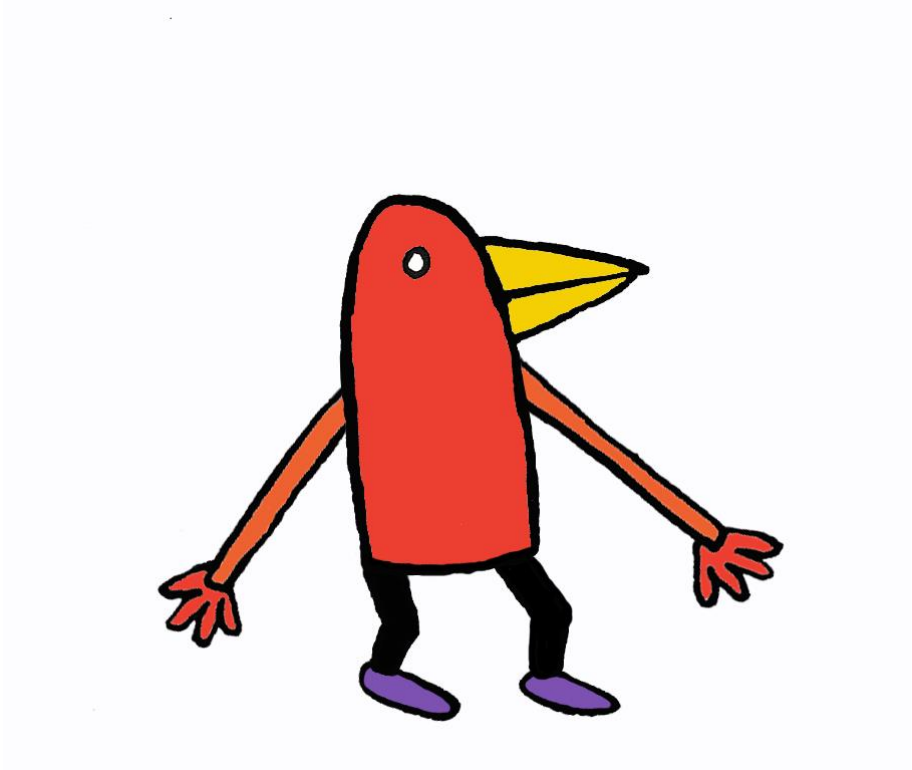
ISE Settings

- Enable **EndPoint Attribute Filter**
- **Avoid** Radius Flapping



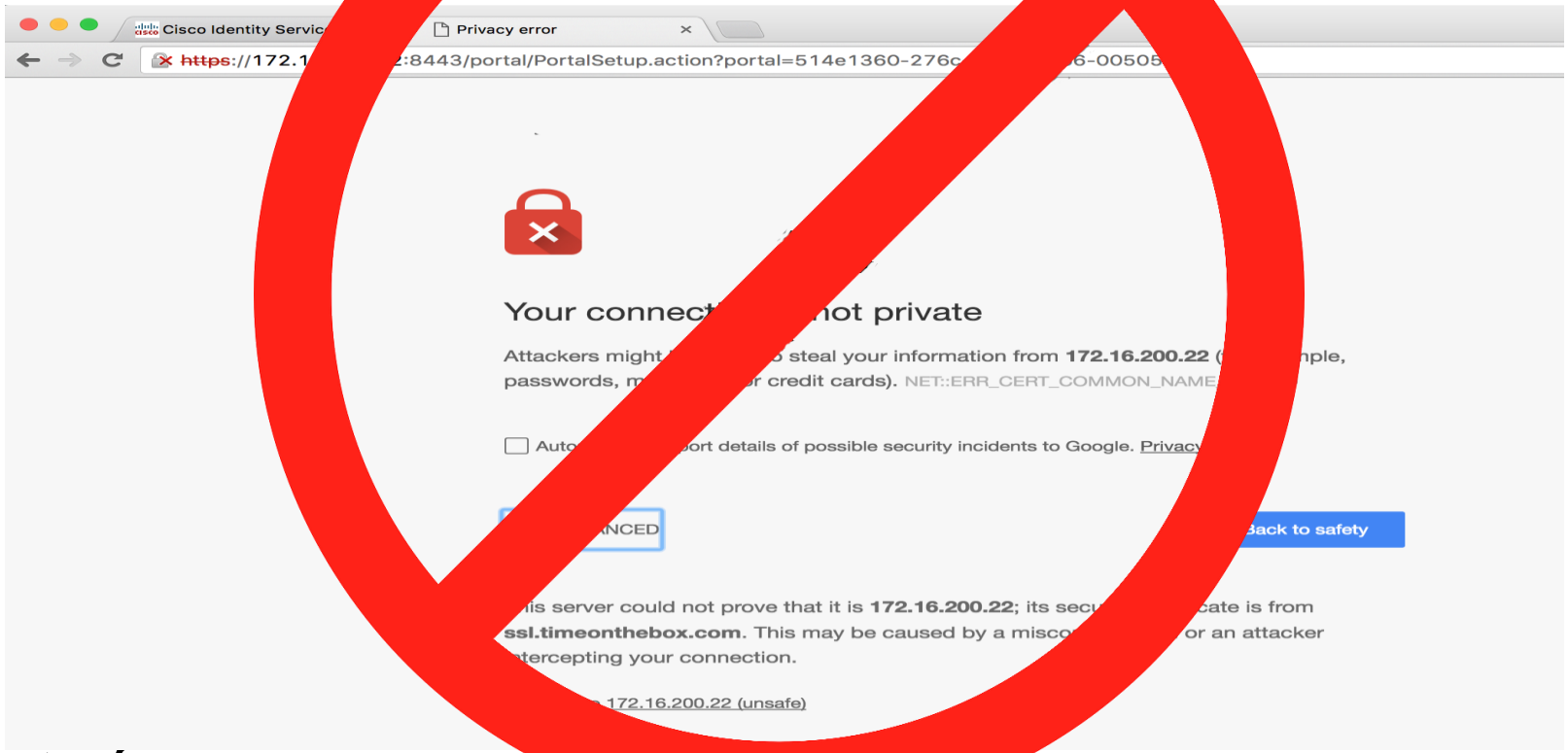
Avoid Radius Flapping...

USE BEST PRACTICE!!!



Soapbox: Buy P[illegible]lic Certificate

Stop teaching users [illegible]ccept Man-in-the-middle a[illegible]s!



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

You make **possible**