cisco Live!

Let’s go

The bridge to possible

Unleashing the Art of Troubleshooting authentication latency issues

Surendra Reddy Kanala, Technical Leader, ISE

BRKSEC-3412

Your Speaker

Surendra Reddy Kanala

Technical Leader – ISE/AAA

“Better Late Than Never - works in Life, but not networks”

Agenda

- Authentication Latencies
- External Latencies
- Internal Latencies
- Let’s Troubleshoot
- Conclusion

Authentication Latencies

Is the latency concerning?

- Baseline Latency

  Consistent
  No impact to business

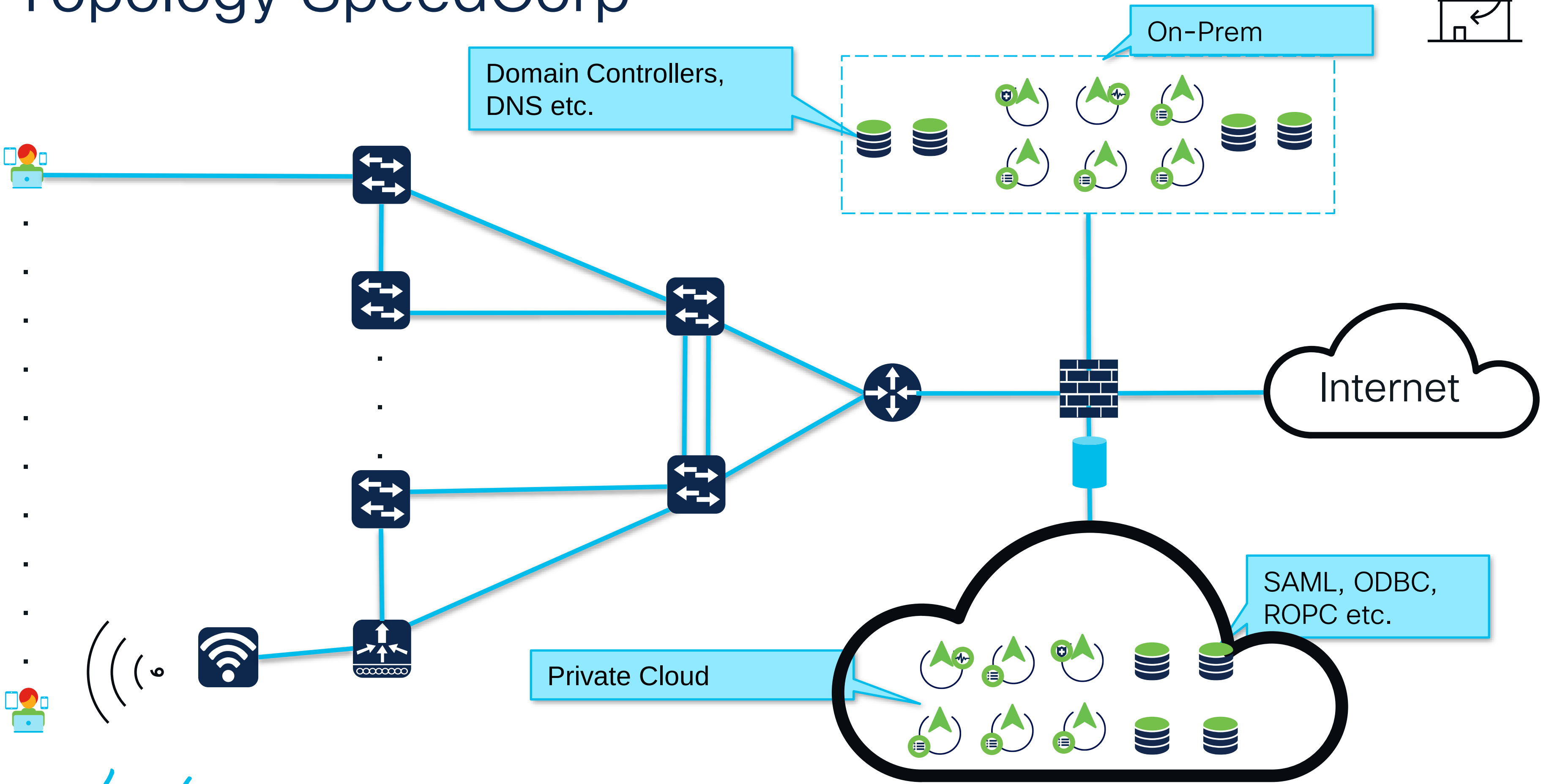
- Expected Latency

  Sporadic but expected spikes
  No to little impact to business

- Actual Latency

  Unpredictable
  Actual Impact to business

Topology SpeedCorp



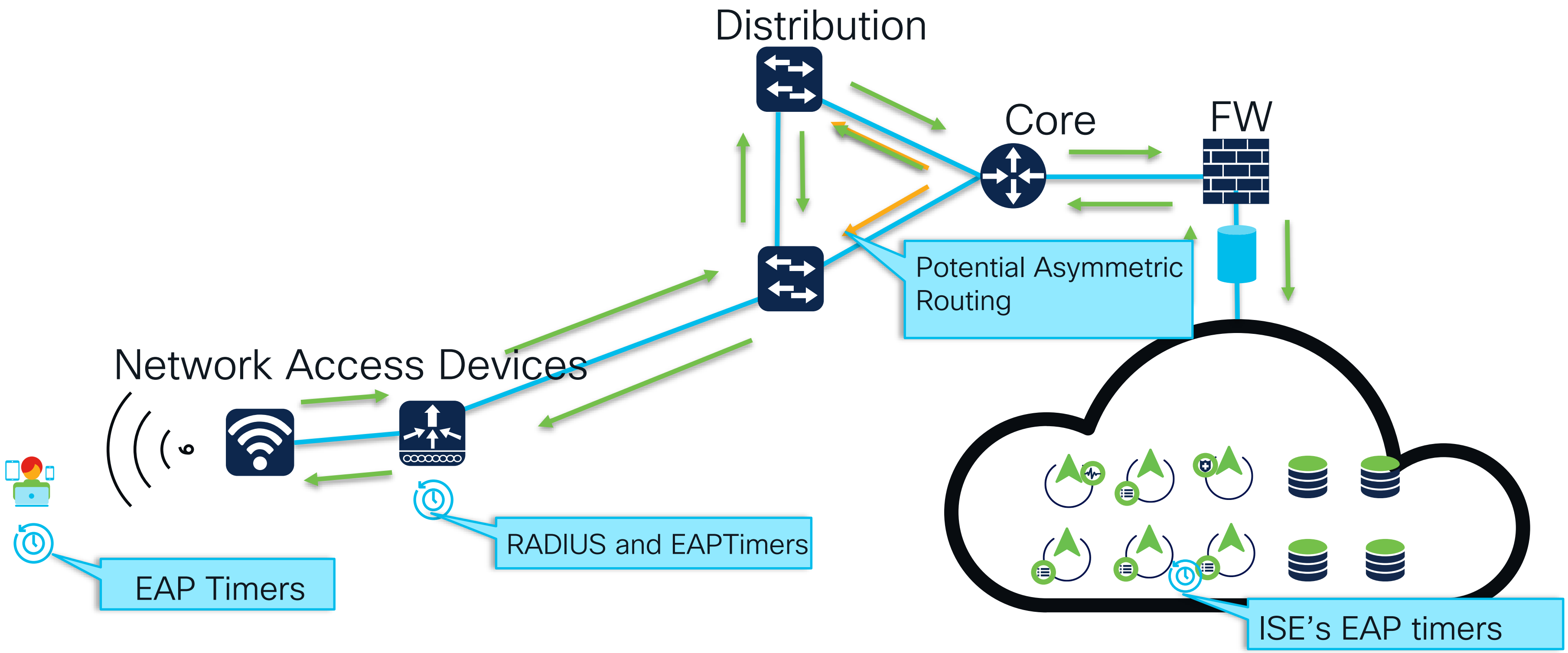
Domain Controllers, DNS etc.

On-Prem

SAML, ODBC, ROPC etc.

Private Cloud

Typical Authentication Flow and timers

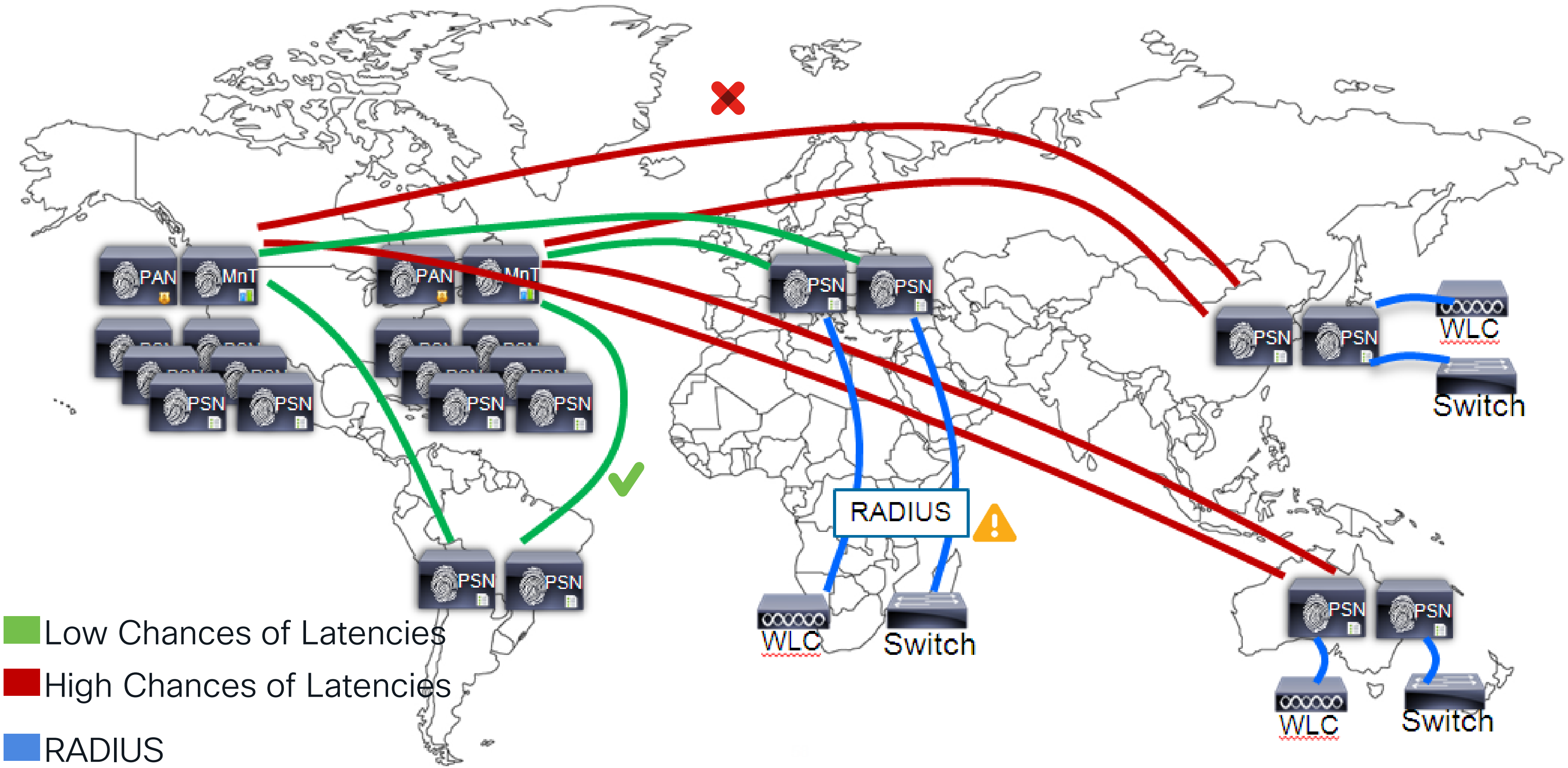


External Latencies

Potential Break Point –External Identity Sources

- Domain Controllers and their locations.
- Cloud based identity Providers
- Proxy flows
- Other external identity sources that are used for MFA such as DUO, RSA Token Servers, SAML , MDM Servers, OCSP Responders etc.

Potential Break Points – Distributed Persona/Network Devices



🟩 Low Chances of Latencies

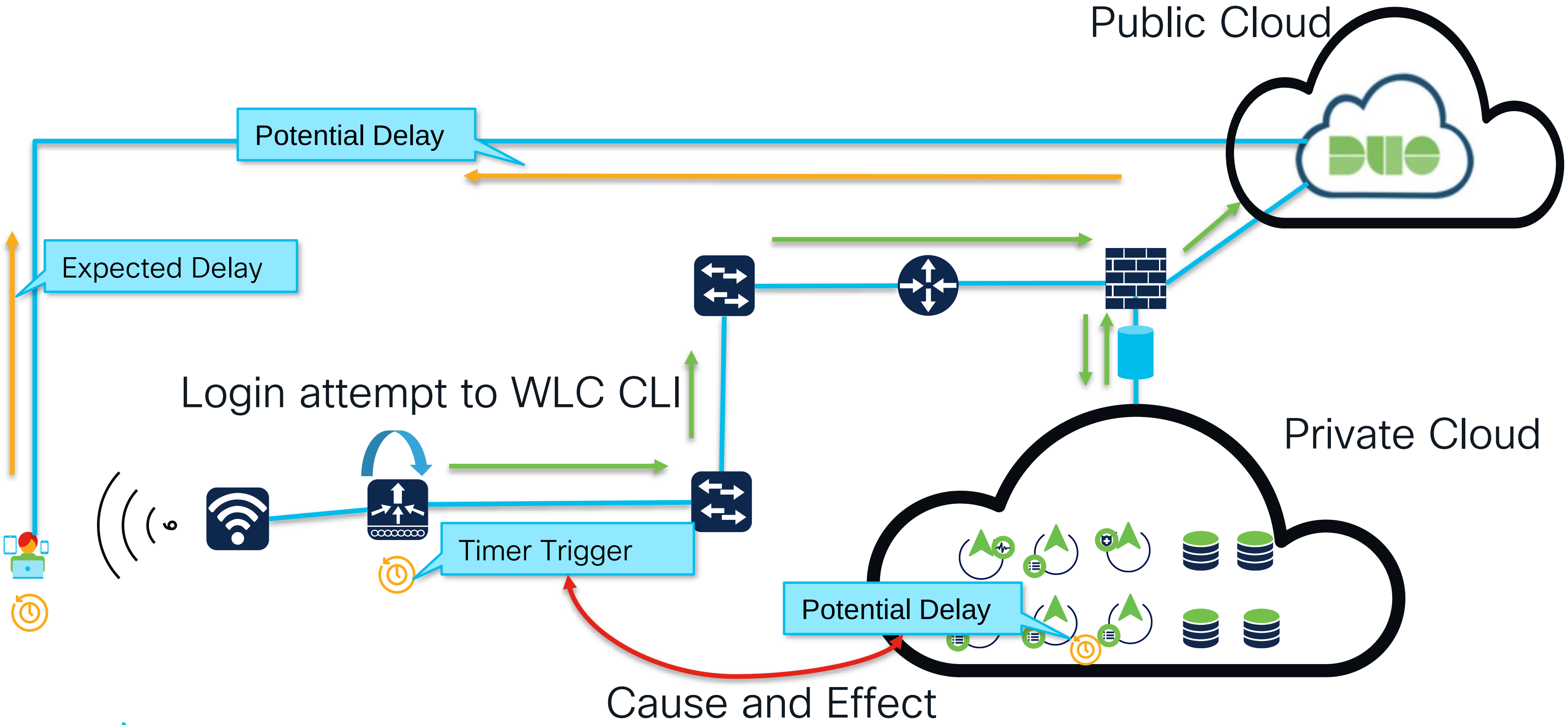
🟥 High Chances of Latencies

🟦 RADIUS

Potential Break Point -Endpoints and Users

- Authentication flows that require user input like username/password
- MFA flows such as Push notifications or OTP
- Supplicant network interface configurations

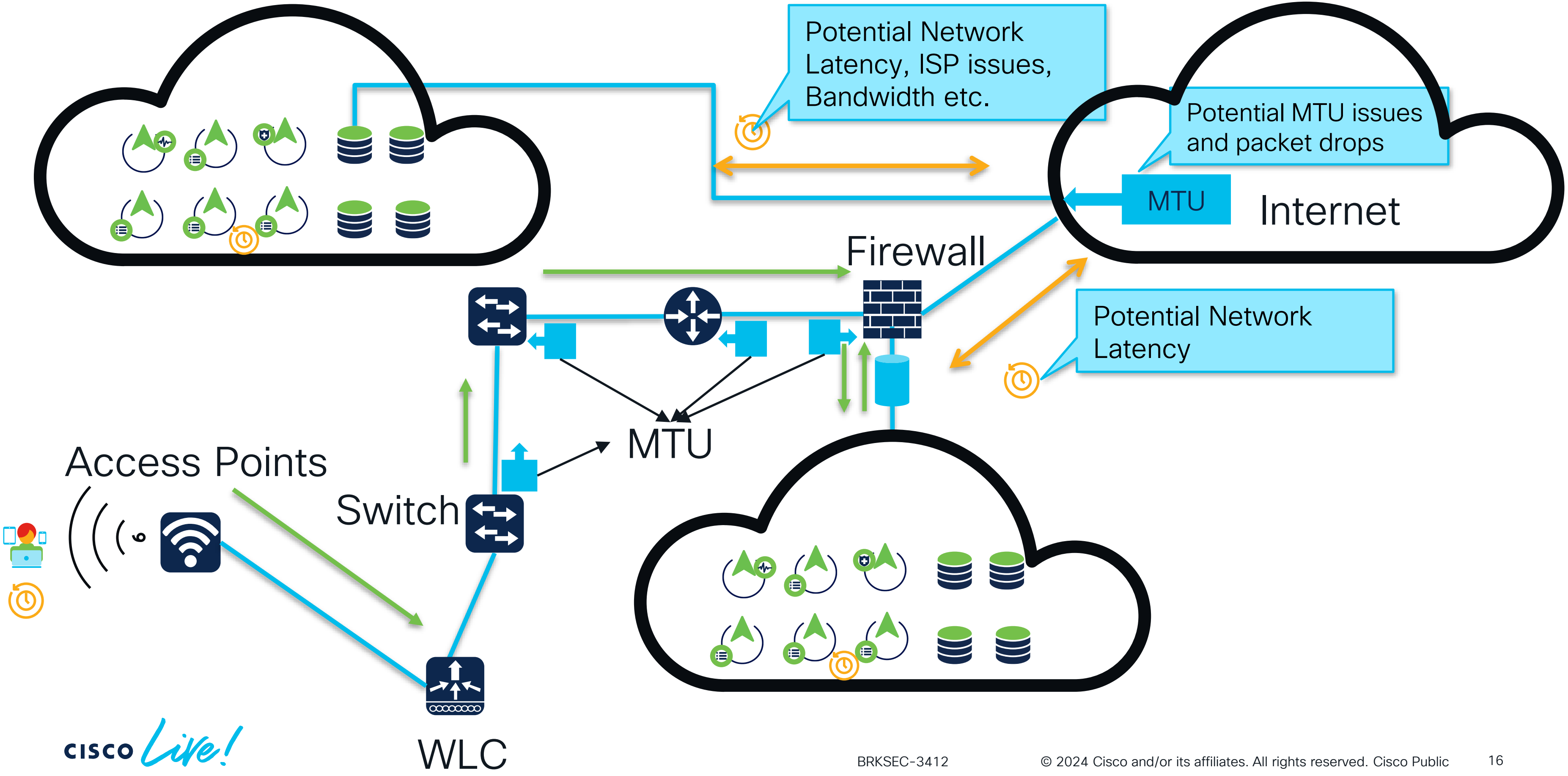
Potential Break Points – User intervention



Potential Break Point –Network Latencies

- Assymtric Routing.
- MTU issues.
- Packet Drops.
- Latency between ISE nodes.

Potential Break Points – Network Components



Potential Network Latency, ISP issues, Bandwidth etc.

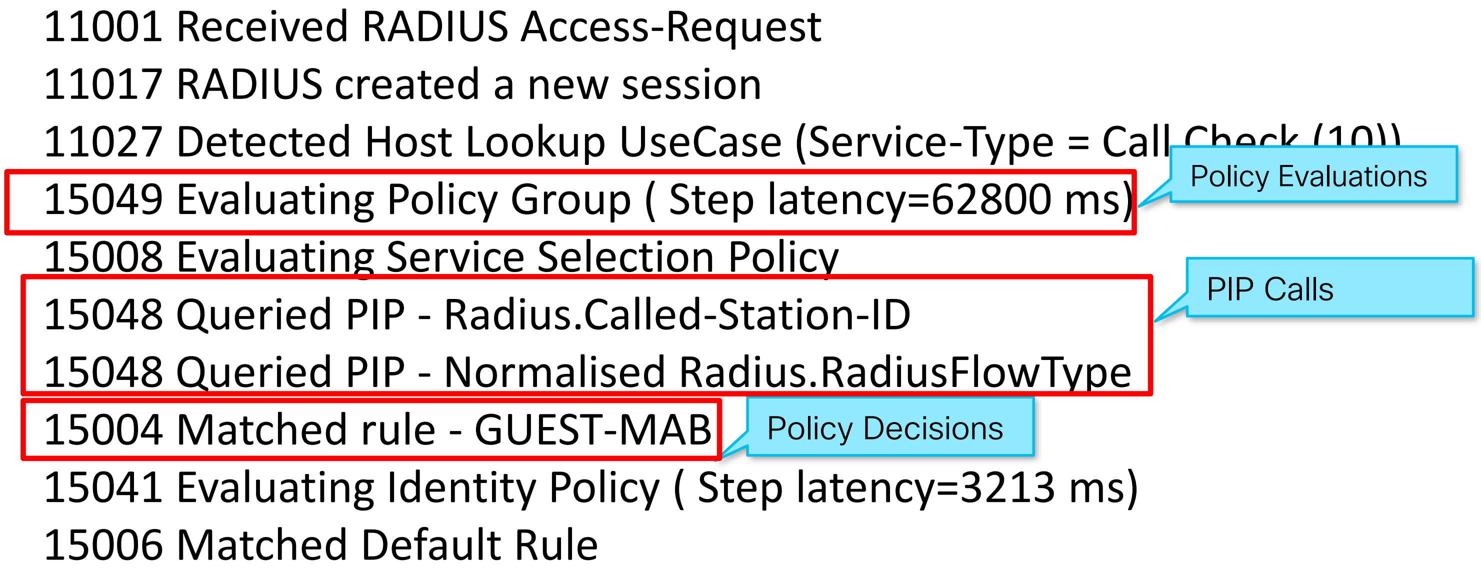
Potential MTU issues and packet drops

Potential Network Latency

Internal Latencies

ISE and Logs

ISE Architecture – different components.

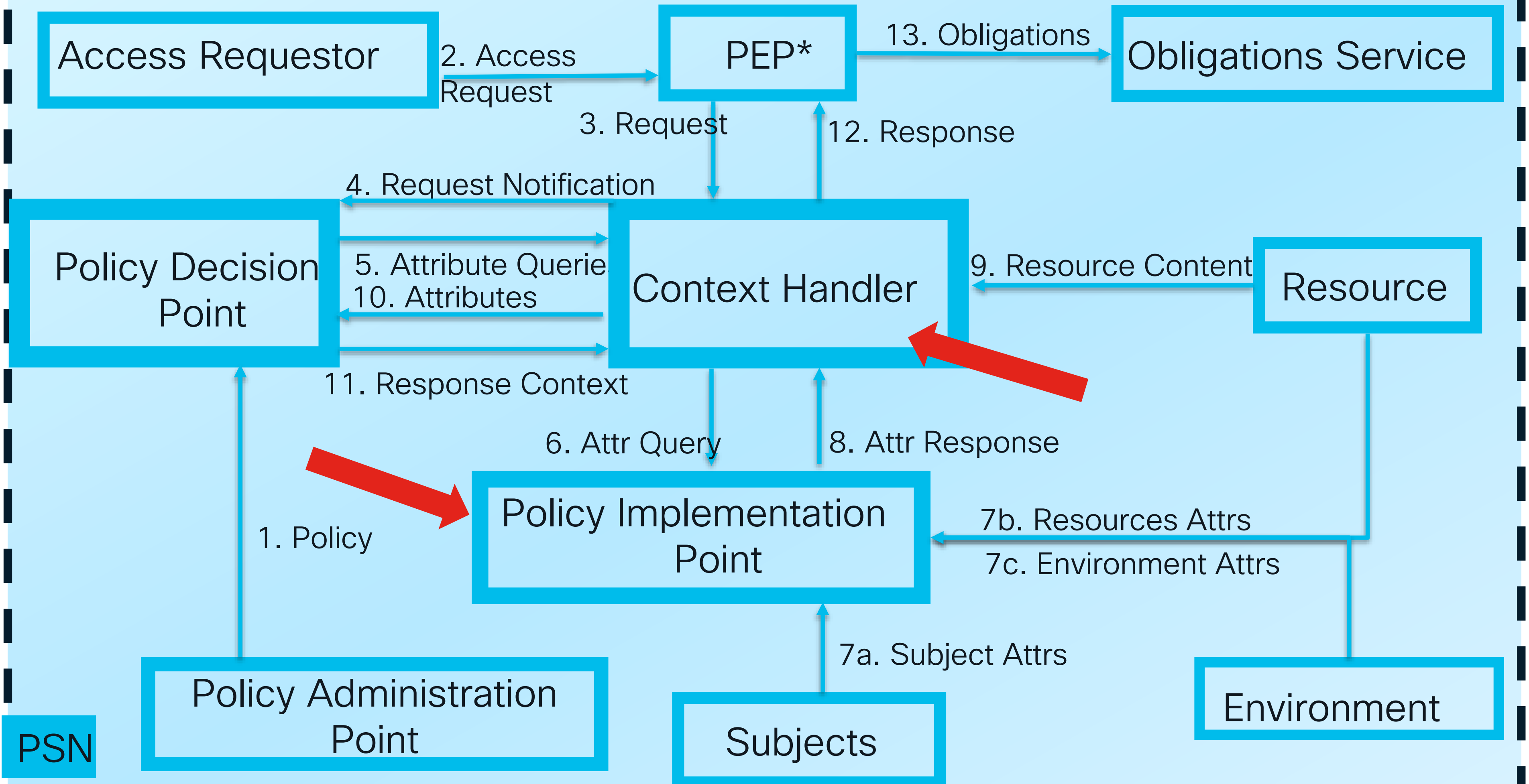


```
11001 Received RADIUS Access-Request
11017 RADIUS created a new session
11027 Detected Host Lookup UseCase (Service-Type = Call Check (10))
15049 Evaluating Policy Group ( Step latency=62800 ms)
15008 Evaluating Service Selection Policy
15048 Queried PIP - Radius.Called-Station-ID
15048 Queried PIP - Normalised Radius.RadiusFlowType
15004 Matched rule - GUEST-MAB
15041 Evaluating Identity Policy ( Step latency=3213 ms)
15006 Matched Default Rule
```

Policy Evaluations

PIP Calls

Policy Decisions



Access Requestor

2. Access Request

PEP*

13. Obligations

Obligations Service

3. Request

12. Response

4. Request Notification

Policy Decision Point

5. Attribute Querie

10. Attributes

11. Response Context

Context Handler

9. Resource Content

Resource

6. Attr Query

8. Attr Response

1. Policy

Policy Implementation Point

7b. Resources Attrs

7c. Environment Attrs

7a. Subject Attrs

Policy Administration Point

Subjects

Environment

PSN

*PEP – Policy Evaluation Point

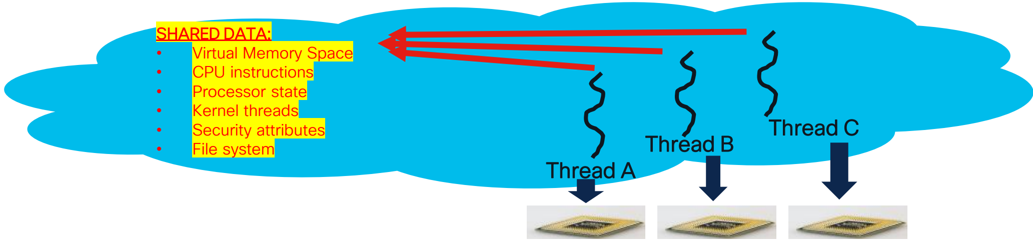
Thread Pools for Policy Events

Important thread pools for policy evaluation

- Main – Resposbile for receiving and sending RADIUS content to PEP and in/out of ISE.
- Policy – Responsible for sending the events to PDP for policy evaluation within which Pip calls are executed
- Reactor – Called in to pass events from one pool to another pool within the same context.
- NsfFetcher – Called when session cache and internal objects need an operation.
- InternalUsers – Called for an operation on the internal user store.
- EapTls – Called for processing TLS conversations.
- ADIDStore – Called when interaction with Active Directory is required.
- RestFetcher – Responsible for calling REST ID Store when required.

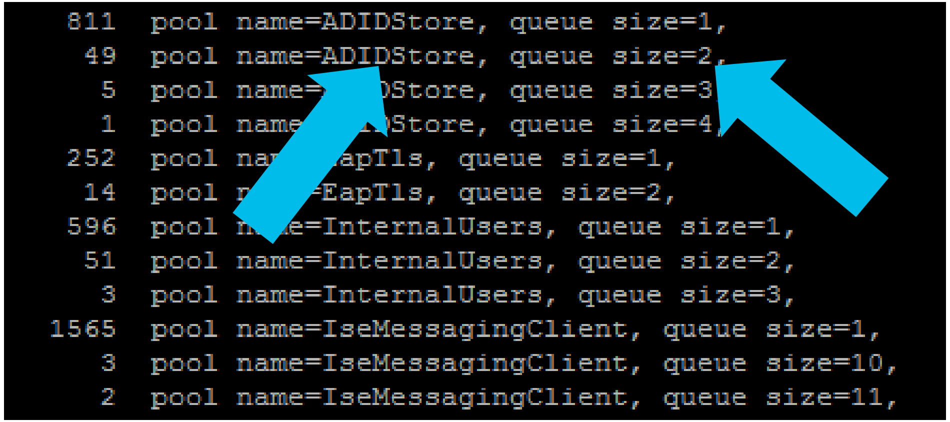
ISE command for Thread and Heap dumps:
"*application configure ise*" and choose

[22]Generate Heap Dump
[23]Generate Thread Dump

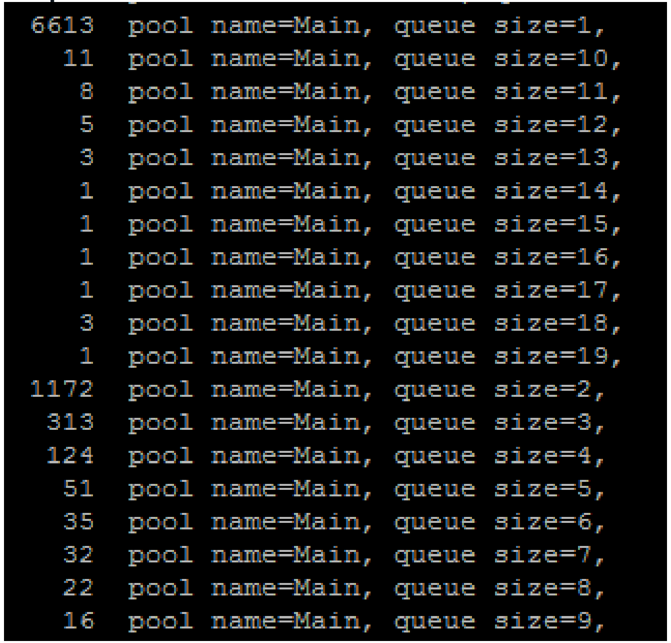


Analyzing the thread pool queues

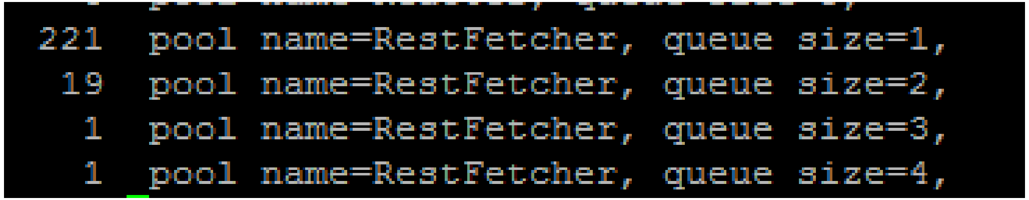
cat prrt-server.log | grep -Eo " pool .*?,"|sort|uniq -c



```
    811  pool name=ADIDStore, queue size=1,
     49  pool name=ADIDStore, queue size=2,
      5  pool name=ADIDStore, queue size=3,
      1  pool name=ADIDStore, queue size=4,
    252  pool name=EapTls, queue size=1,
     14  pool name=EapTls, queue size=2,
    596  pool name=InternalUsers, queue size=1,
     51  pool name=InternalUsers, queue size=2,
      3  pool name=InternalUsers, queue size=3,
   1565  pool name=IseMessagingClient, queue size=1,
      3  pool name=IseMessagingClient, queue size=10,
      2  pool name=IseMessagingClient, queue size=11,
```



```
   6613  pool name=Main, queue size=1,
     11  pool name=Main, queue size=10,
      8  pool name=Main, queue size=11,
      5  pool name=Main, queue size=12,
      3  pool name=Main, queue size=13,
      1  pool name=Main, queue size=14,
      1  pool name=Main, queue size=15,
      1  pool name=Main, queue size=16,
      1  pool name=Main, queue size=17,
      3  pool name=Main, queue size=18,
      1  pool name=Main, queue size=19,
   1172  pool name=Main, queue size=2,
    313  pool name=Main, queue size=3,
    124  pool name=Main, queue size=4,
     51  pool name=Main, queue size=5,
     35  pool name=Main, queue size=6,
     32  pool name=Main, queue size=7,
     22  pool name=Main, queue size=8,
     16  pool name=Main, queue size=9,
```



```
    221  pool name=RestFetcher, queue size=1,
     19  pool name=RestFetcher, queue size=2,
      1  pool name=RestFetcher, queue size=3,
      1  pool name=RestFetcher, queue size=4,
```

*Debugs for runtime-AAA component should be enabled

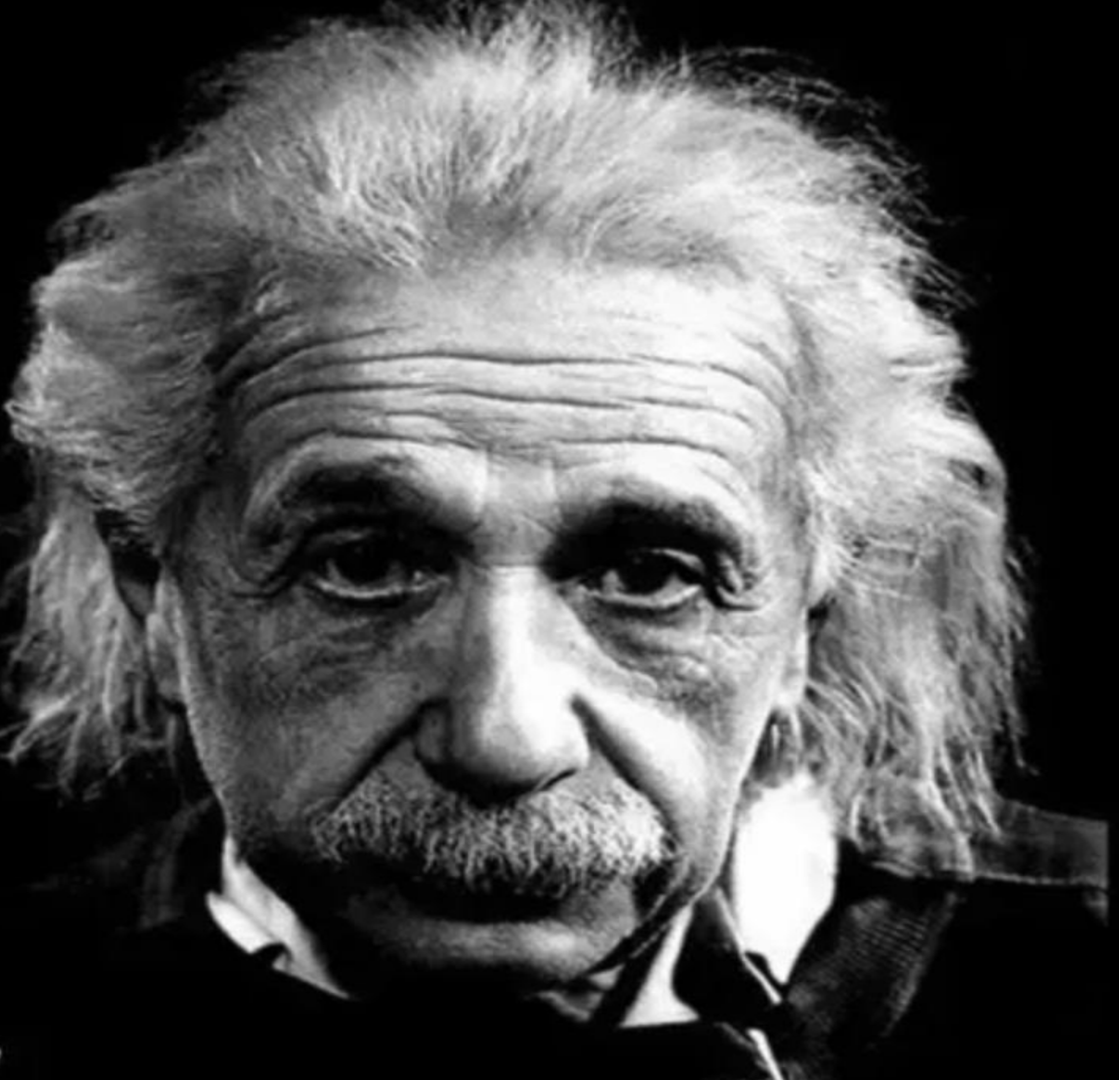
Troubleshooting Latency Issues

Troubleshooting Strategies

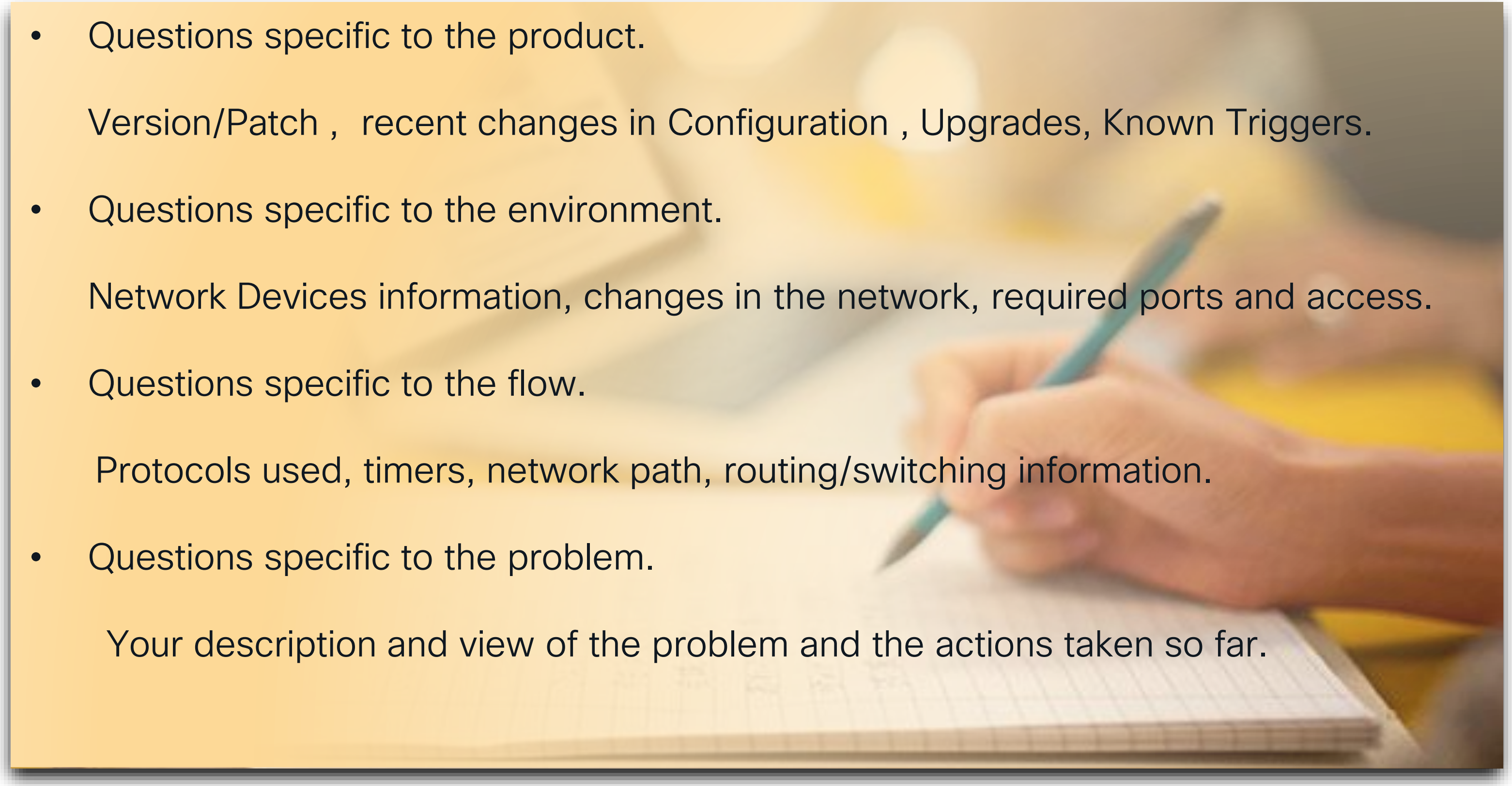
- Shoot from the hip/ Bottom Up approaches
- Ready the tools.
- Isolate the point of failure.

"If I had an hour to solve a problem and my life depended on the solution, I would spend the first 55 minutes determining the proper question to ask, for once I know the proper question, I could solve the problem in less than 5 minutes.”

- *Albert Einstein*



The TAC Approach – Define Problem Description



- Questions specific to the product.

  Version/Patch , recent changes in Configuration , Upgrades, Known Triggers.

- Questions specific to the environment.

  Network Devices information, changes in the network, required ports and access.

- Questions specific to the flow.

  Protocols used, timers, network path, routing/switching information.

- Questions specific to the problem.

  Your description and view of the problem and the actions taken so far.

The TAC Approach – Gathering Information and Debugs

- Assess the possibility of workarounds for temporary relief by looking at livelogs/Reports/Dashboards.

- Gathering essential information to troubleshoot the problem.

  User details, MAC Addresses, Timestamps etc., setting the debugs to required level, recreate/reproduce the
  problem and collect the logs.

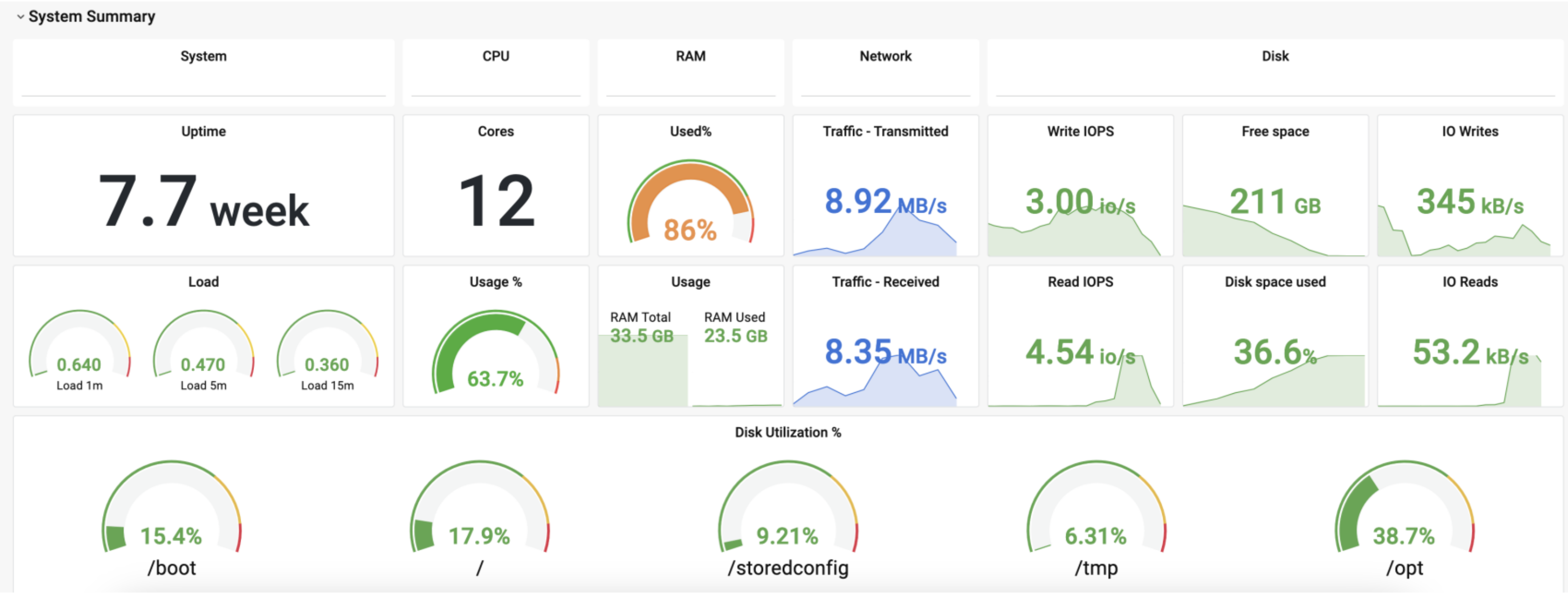
- Analyze the logs to find the cause of the problem.

ISE Live Logs and Reports

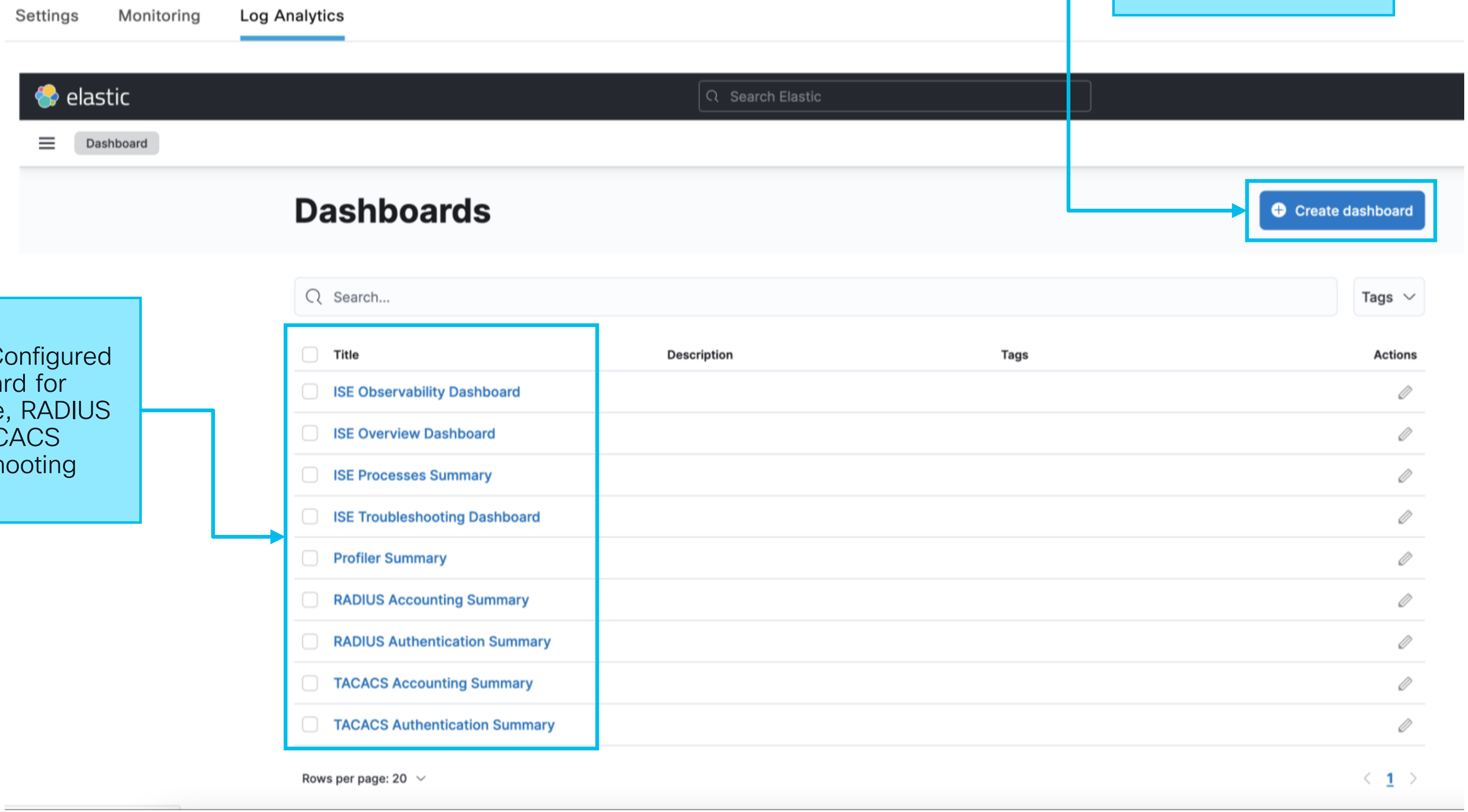
- System 360
- Common errors seen during latencies
- Step Latencies in live logs – New in 3.3!
- Key Performance Metrics (KPM) Reports
- Approach to follow.

System 360

ISE Monitoring – The New Way.



System 360 – Log Analytics



Dashboards

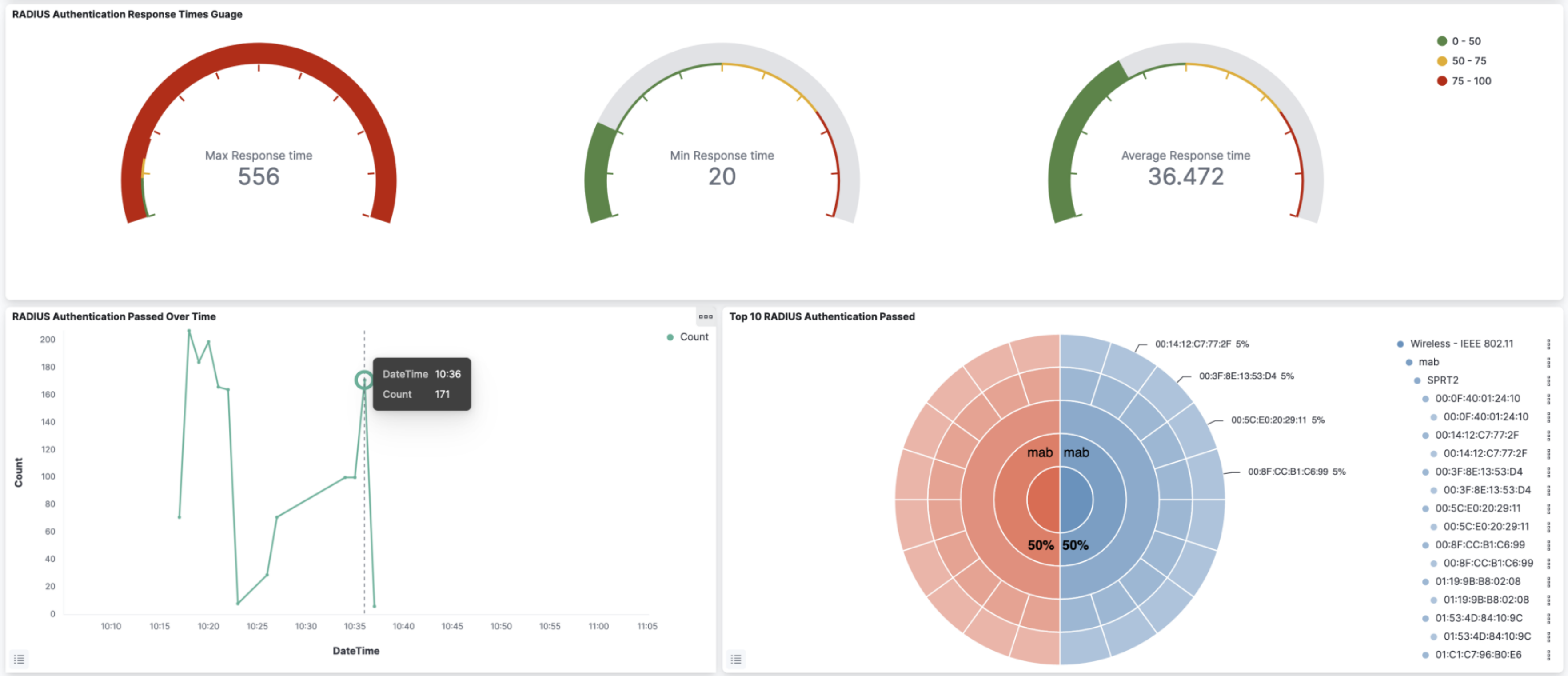
☐ Title	Description	Tags	Actions
☐ ISE Observability Dashboard			✎
☐ ISE Overview Dashboard			✎
☐ ISE Processes Summary			✎
☐ ISE Troubleshooting Dashboard			✎
☐ Profiler Summary			✎
☐ RADIUS Accounting Summary			✎
☐ RADIUS Authentication Summary			✎
☐ TACACS Accounting Summary			✎
☐ TACACS Authentication Summary			✎

Create Custom Dashboard

Set of Pre-Configured Dashboard for Performance, RADIUS and TACACS Troubleshooting

System 360 – Log Analytics

Latency within Authentications

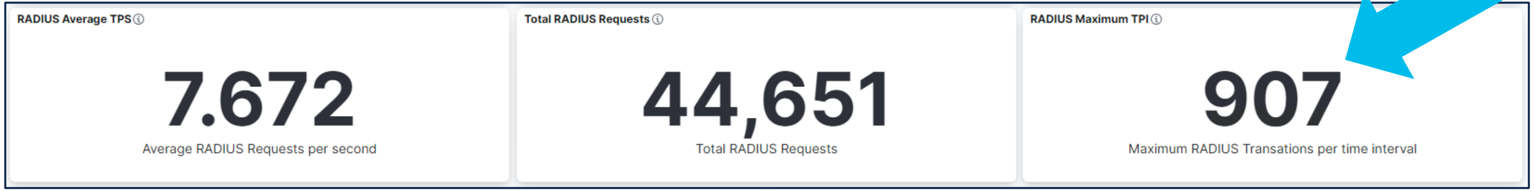


Authentication Rates over Time

Top Authenticating Endpoints

System 360 – Log Analytics

Max TPI



RADIUS Average TPS ⓘ

7.672

Average RADIUS Requests per second

Total RADIUS Requests ⓘ

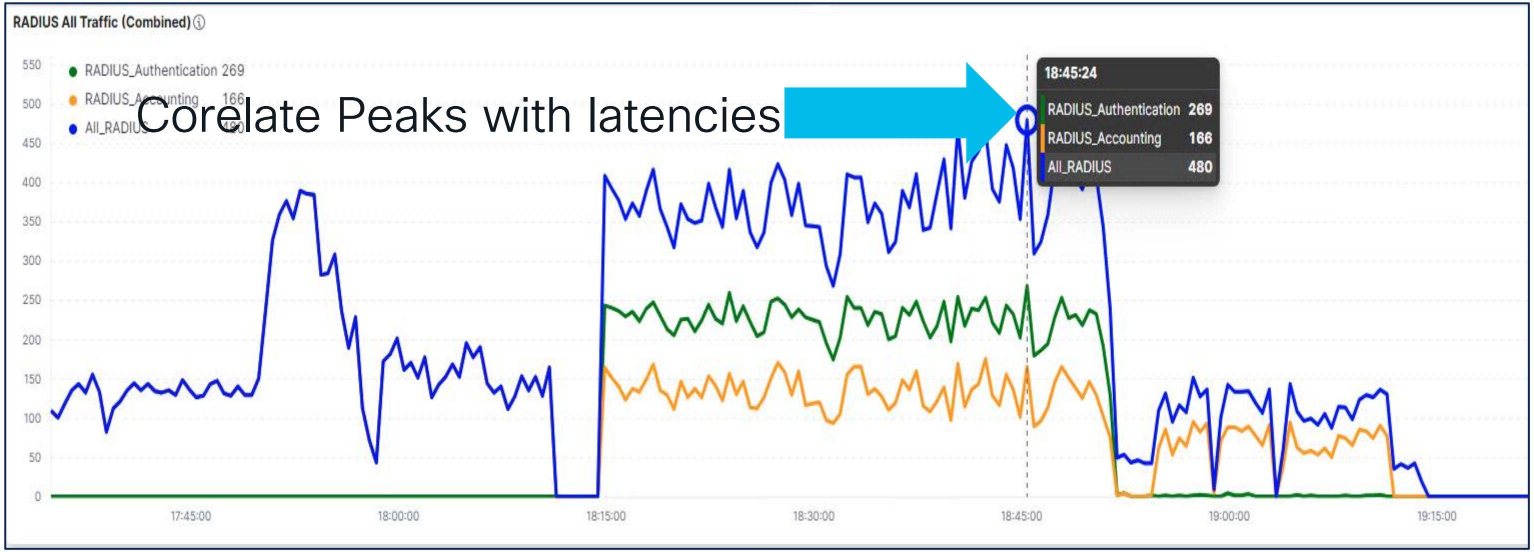
44,651

Total RADIUS Requests

RADIUS Maximum TPI ⓘ

907

Maximum RADIUS Transations per time interval

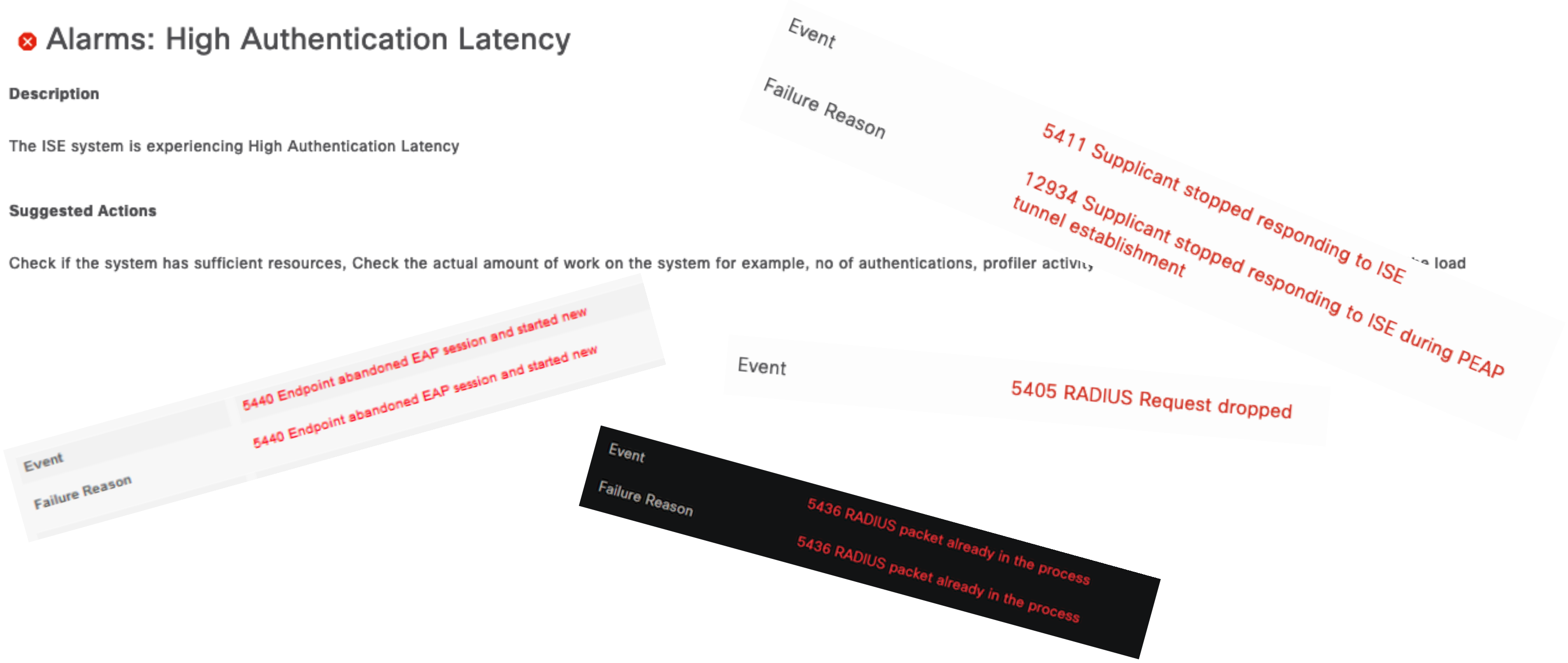


RADIUS All Traffic (Combined) ⓘ

Corelate Peaks with latencies

Common Errors related to Authentication Latencies

Failure Reasons 1293x, 1294x, 54xx



Alarms: High Authentication Latency

Description

The ISE system is experiencing High Authentication Latency

Suggested Actions

Check if the system has sufficient resources, Check the actual amount of work on the system for example, no of authentications, profiler activi load

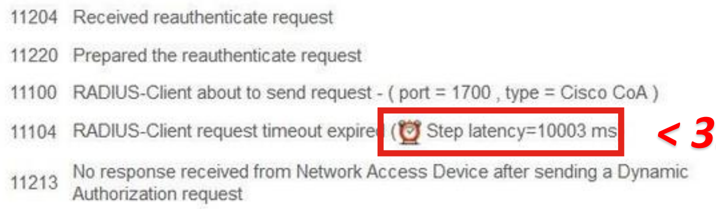
Event	
Failure Reason	5411 Supplicant stopped responding to ISE 12934 Supplicant stopped responding to ISE during PEAP tunnel establishment

Event	5440 Endpoint abandoned EAP session and started new
Failure Reason	5440 Endpoint abandoned EAP session and started new

Event	5405 RADIUS Request dropped

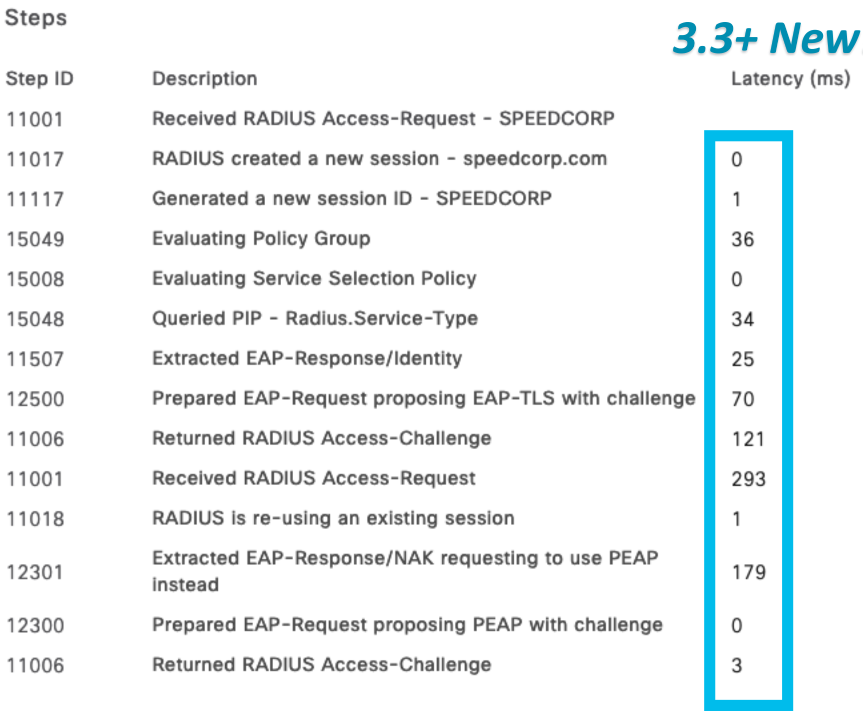
Event	5436 RADIUS packet already in the process
Failure Reason	5436 RADIUS packet already in the process

Step Latencies



11204	Received reauthenticate request
11220	Prepared the reauthenticate request
11100	RADIUS-Client about to send request - (port = 1700 , type = Cisco CoA)
11104	RADIUS-Client request timeout expired (⏰ Step latency=10003 ms
11213	No response received from Network Access Device after sending a Dynamic Authorization request

< 3.3

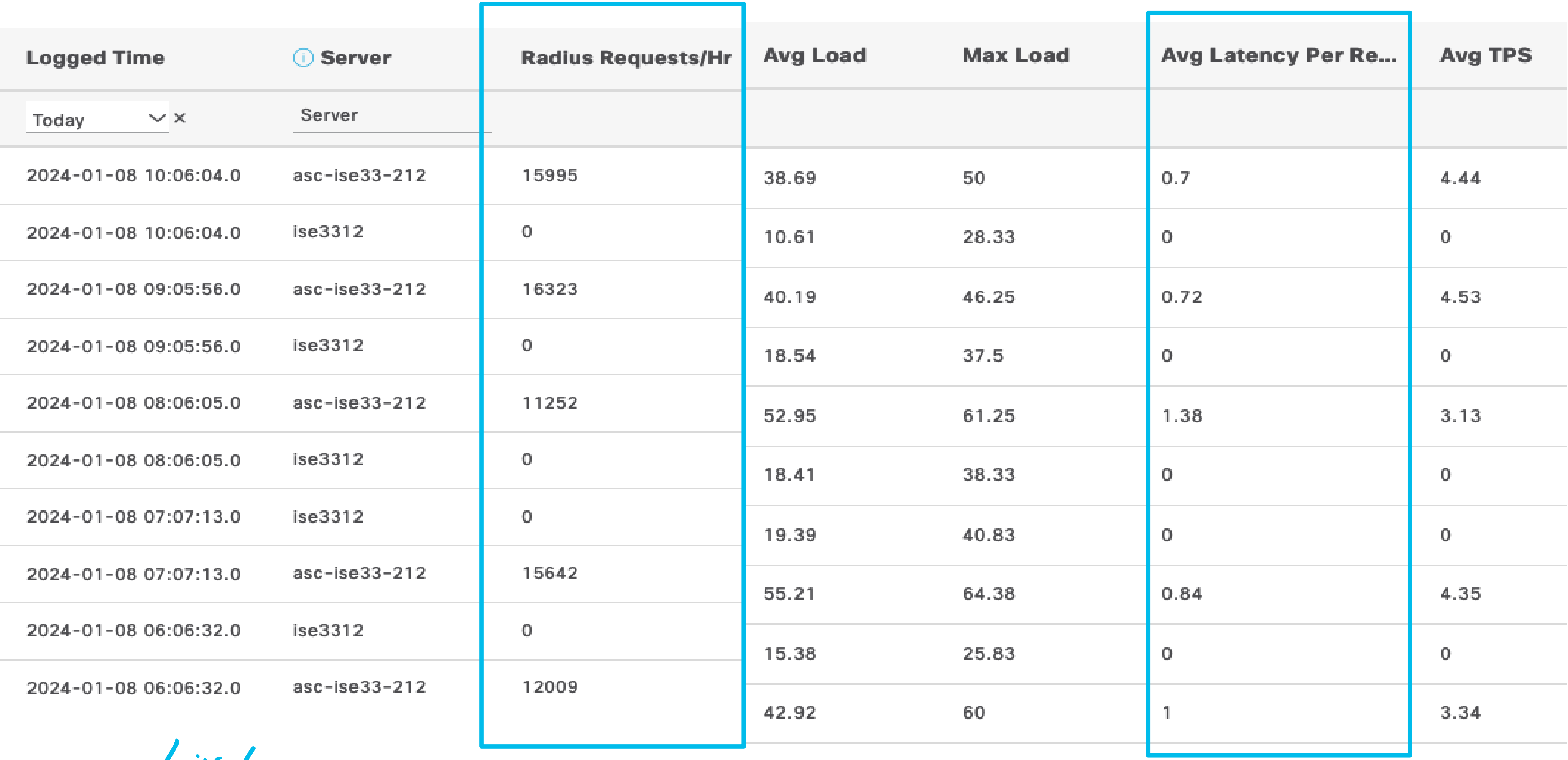


Steps

3.3+ New!

Step ID	Description	Latency (ms)
11001	Received RADIUS Access-Request - SPEEDCORP	
11017	RADIUS created a new session - speedcorp.com	0
11117	Generated a new session ID - SPEEDCORP	1
15049	Evaluating Policy Group	36
15008	Evaluating Service Selection Policy	0
15048	Queried PIP - Radius.Service-Type	34
11507	Extracted EAP-Response/Identity	25
12500	Prepared EAP-Request proposing EAP-TLS with challenge	70
11006	Returned RADIUS Access-Challenge	121
11001	Received RADIUS Access-Request	293
11018	RADIUS is re-using an existing session	1
12301	Extracted EAP-Response/NAK requesting to use PEAP instead	179
12300	Prepared EAP-Request proposing PEAP with challenge	0
11006	Returned RADIUS Access-Challenge	3

Key Performance Metrics Report

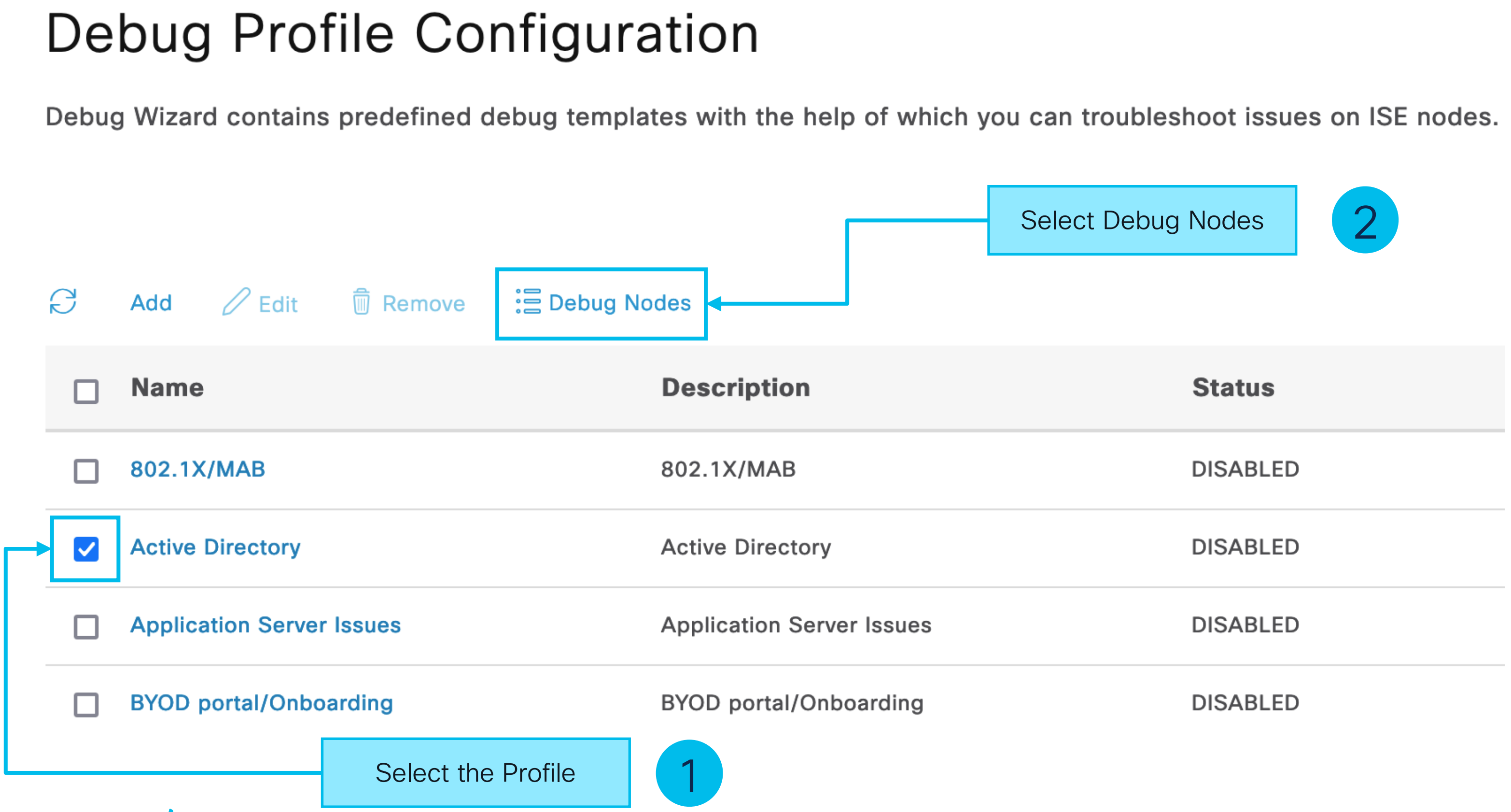


Logged Time	ⓘ Server	Radius Requests/Hr	Avg Load	Max Load	Avg Latency Per Re...	Avg TPS
Today ⌄ ×	Server					
2024-01-08 10:06:04.0	asc-ise33-212	15995	38.69	50	0.7	4.44
2024-01-08 10:06:04.0	ise3312	0	10.61	28.33	0	0
2024-01-08 09:05:56.0	asc-ise33-212	16323	40.19	46.25	0.72	4.53
2024-01-08 09:05:56.0	ise3312	0	18.54	37.5	0	0
2024-01-08 08:06:05.0	asc-ise33-212	11252	52.95	61.25	1.38	3.13
2024-01-08 08:06:05.0	ise3312	0	18.41	38.33	0	0
2024-01-08 07:07:13.0	ise3312	0	19.39	40.83	0	0
2024-01-08 07:07:13.0	asc-ise33-212	15642	55.21	64.38	0.84	4.35
2024-01-08 06:06:32.0	ise3312	0	15.38	25.83	0	0
2024-01-08 06:06:32.0	asc-ise33-212	12009	42.92	60	1	3.34

ISE Debugs and Logs

- Debug Wizard on ISE
- Debugs for different use cases
- Thread Pools
- Lets follow a session in the logs

Debug Wizard by Function



Debug Profile Configuration

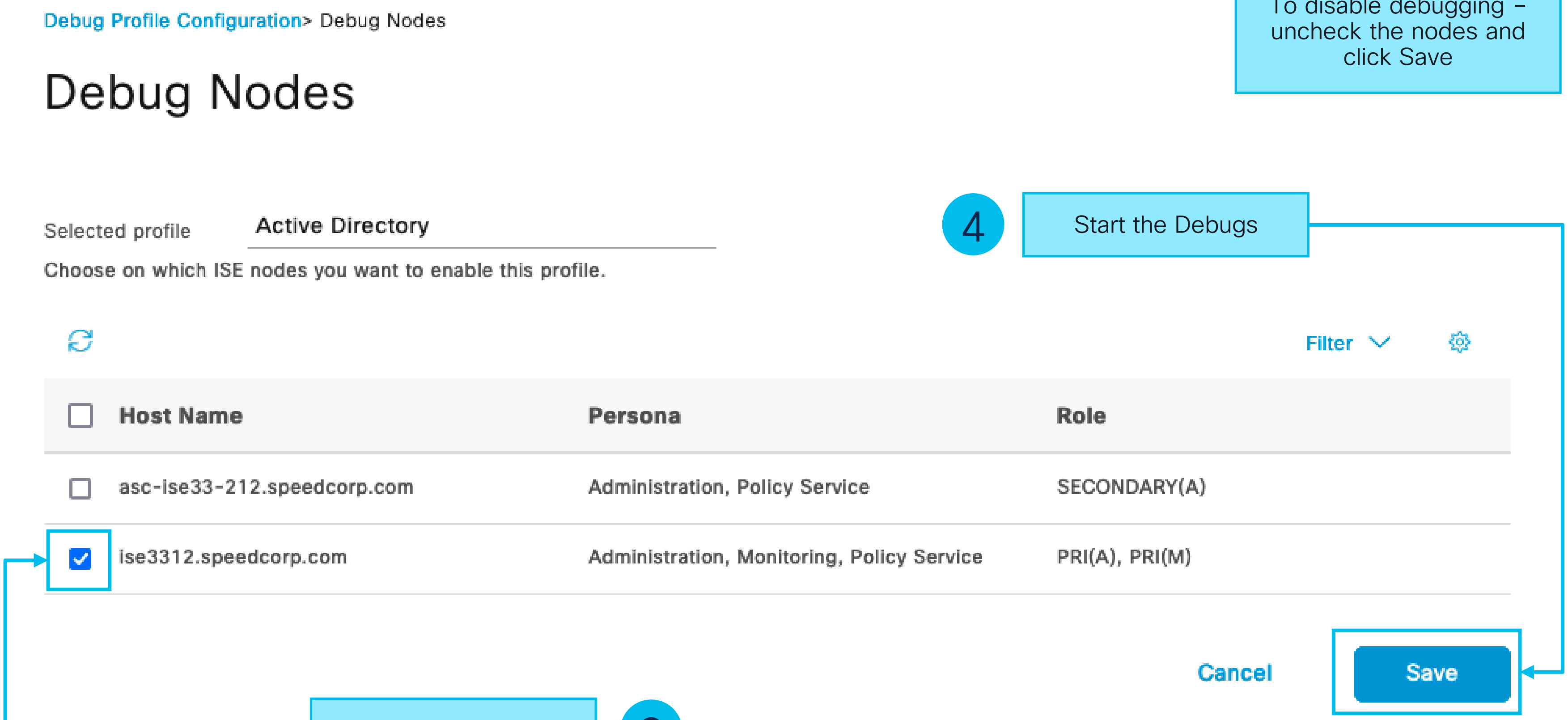
Debug Wizard contains predefined debug templates with the help of which you can troubleshoot issues on ISE nodes.

□	Name	Description	Status
□	802.1X/MAB	802.1X/MAB	DISABLED
☑	Active Directory	Active Directory	DISABLED
□	Application Server Issues	Application Server Issues	DISABLED
□	BYOD portal/Onboarding	BYOD portal/Onboarding	DISABLED

1 Select the Profile

2 Select Debug Nodes

Debug Wizard by Function



Debug Profile Configuration> Debug Nodes

Debug Nodes

Selected profile: Active Directory

Choose on which ISE nodes you want to enable this profile.

□	Host Name	Persona	Role
□	asc-ise33-212.speedcorp.com	Administration, Policy Service	SECONDARY(A)
☑	ise3312.speedcorp.com	Administration, Monitoring, Policy Service	PRI(A), PRI(M)

To disable debugging – uncheck the nodes and click Save

4 Start the Debugs

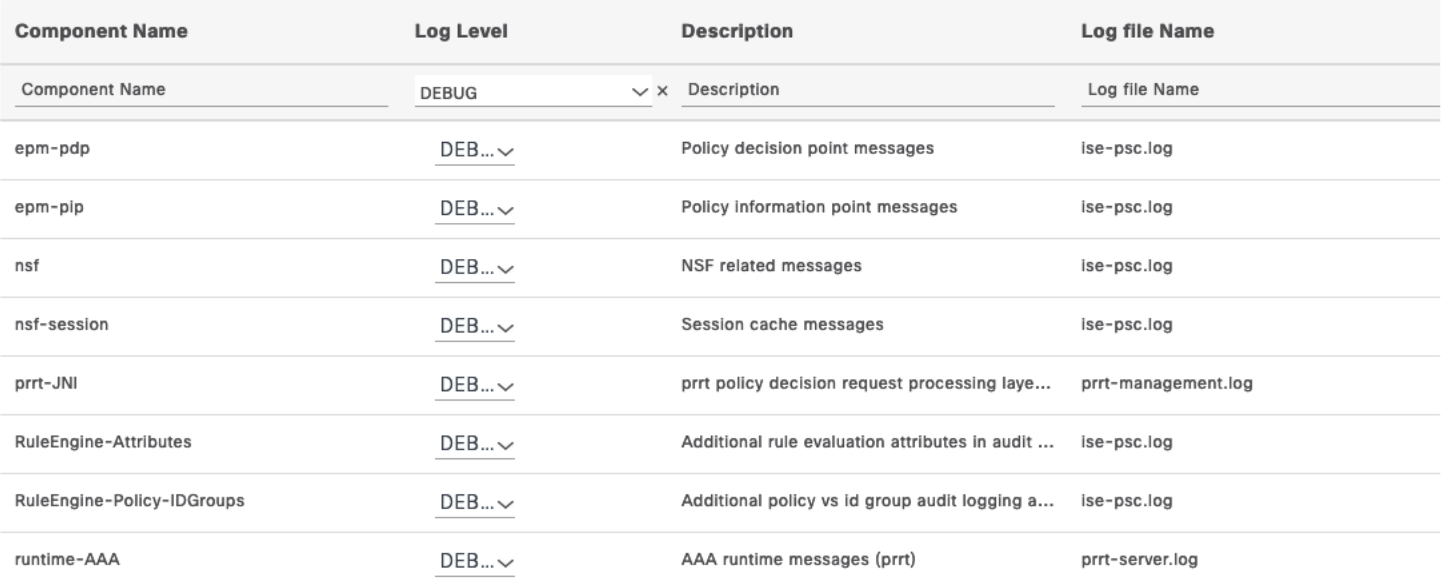
3 Select the Nodes

Debug Components and Logs for common use cases

- **Infrastructure (ise-psc.log)** - Platform, Patches, Upgrades, Certificates, Backup/Restore/Repositories etc. related issues.
- **runtime-aaa (prrt-server.log, prrt-management.log)** - AAA related issues. If requested by TAC as they are performance heavy, then nsf* (Network Service Framework) debugs.
- **Profiler (Profiler.log)** – For issues related to Profiling.
- **posture, provisioning, portal-web-action, portal-session (ise-psc.log, guest.log)** – For Posture related issues.
- **guestaccess (Guest.log)** – For Guest related issues.

Debug Components and Logs

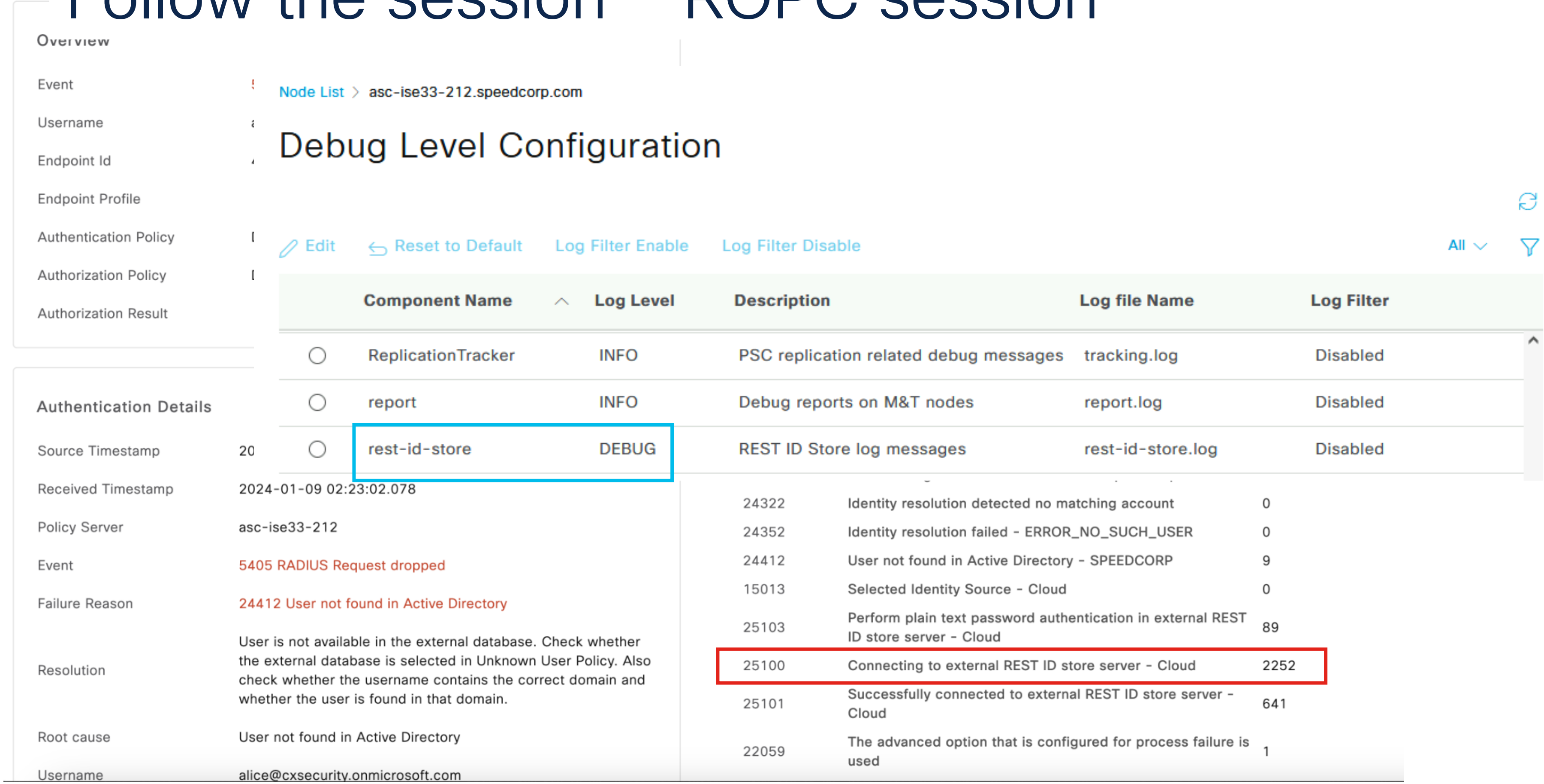
Alternatively navigate to **Operation > Troubleshoot > Debug Wizard > Debug Profile Configuration** or **Debug Log Configuration** and view the components and log files.



Component Name	Log Level	Description	Log file Name
Component Name	DEBUG ˅ ×	Description	Log file Name
epm-pdp	DEB... ˅	Policy decision point messages	ise-psc.log
epm-pip	DEB... ˅	Policy information point messages	ise-psc.log
nsf	DEB... ˅	NSF related messages	ise-psc.log
nsf-session	DEB... ˅	Session cache messages	ise-psc.log
prrt-JNI	DEB... ˅	prrt policy decision request processing laye...	prrt-management.log
RuleEngine-Attributes	DEB... ˅	Additional rule evaluation attributes in audit ...	ise-psc.log
RuleEngine-Policy-IDGroups	DEB... ˅	Additional policy vs id group audit logging a...	ise-psc.log
runtime-AAA	DEB... ˅	AAA runtime messages (prrt)	prrt-server.log

Let’s follow a Session

Follow the session – ROPC session



Overview

Event

Username

Endpoint Id

Endpoint Profile

Authentication Policy

Authorization Policy

Authorization Result

Node List > asc-ise33-212.speedcorp.com

Debug Level Configuration

	Component Name	Log Level	Description	Log file Name	Log Filter
○	ReplicationTracker	INFO	PSC replication related debug messages	tracking.log	Disabled
○	report	INFO	Debug reports on M&T nodes	report.log	Disabled
○	rest-id-store	DEBUG	REST ID Store log messages	rest-id-store.log	Disabled

Authentication Details

Source Timestamp	20
Received Timestamp	2024-01-09 02:23:02.078
Policy Server	asc-ise33-212
Event	5405 RADIUS Request dropped
Failure Reason	24412 User not found in Active Directory
Resolution	User is not available in the external database. Check whether the external database is selected in Unknown User Policy. Also check whether the username contains the correct domain and whether the user is found in that domain.
Root cause	User not found in Active Directory
Username	alice@cxsecurity.onmicrosoft.com

24322	Identity resolution detected no matching account	0
24352	Identity resolution failed - ERROR_NO_SUCH_USER	0
24412	User not found in Active Directory - SPEEDCORP	9
15013	Selected Identity Source - Cloud	0
25103	Perform plain text password authentication in external REST ID store server - Cloud	89
25100	Connecting to external REST ID store server - Cloud	2252
25101	Successfully connected to external REST ID store server - Cloud	641
22059	The advanced option that is configured for process failure is used	1

Check runtime logs in prrt-server.log

Major JavaBridge Events in ROPC flow filtered with session ID in green

```
JavaEventHandler,2024-01-09 02:22:58,596,DEBUG,0x7f04d1789700,cntx=0004342415,sesn=asc-ise33-
212/494073967/247050,CPMSessionID=c0a8295d5UBshnQ2Qt010in2tSWeYjYY1xzLmHMCZa7PcTtRVxg,
user=alice@cxsecurity.onmicrosoft.com,CallingStationID=41:F3:C9:B1:97:8D,JavaEventHandler::onEvent:
class=com.cisco.cpm.prrt.policy.PolicyEngine event=EvaluatePolicyEvent,JavaEventHandler.cpp:191

JavaEventHandler,2024-01-09 02:22:59,163,DEBUG,0x7f04bfd0a700, cntx=0004342415, sesn=asc-
ise33-
212/494073967/247050,CPMSessionID=c0a8295d5UBshnQ2Qt010in2tSWeYjYY1xzLmHMCZa7PcTtRVxg,
user=alice@cxsecurity.onmicrosoft.com,CallingStationID=41:F3:C9:B1:97:8D,JavaEventHandler::onEvent:
class=com.cisco.cpm.prrt.idstores.RestUserFetcher event=RestAuthenticateUser,JavaEventHandler.cpp:191

JavaEventHandler,2024-01-09 02:23:02,059,DEBUG,0x7f04d5bab700, cntx=0004342415,sesn=asc-
ise33-
212/494073967/247050,CPMSessionID=c0a8295d[illegible]shnQ2Qt010in2tSWeYjYY1xzLmHMCZa7PcTtRVxg,
user=alice@cxsecurity.onmicrosoft.com,CallingSta[illegible]D=41:F3:C9:B1:97:8D,JavaEventHandler::onEvent:
class=com.cisco.cpm.prrt.eventhandlers.Session[illegible]dater
event=SessionUpdateEvent,JavaEventHandler[illegible]:191
```

Thread Id

Check PolicyEngine Invocation logs in prrt-server.log

```
AuthenStateManager,2024-01-09 02:22:58,478,DEBUG,0x7f04d67b1700,acquireOrCreateState:
created sessionID=asc-ise33-212/494073967/247050,AuthenStateManager.cpp:112

Ra    ,2024-01-09 02:22:58 530,DEBUG,0x7f04d67b1700,cntx=0004342415,sesn=asc-ise33-
                         50,CP    ssionID=c0a8295d5UBshnQ2Qt010in2tSWeYjYY1xzLmHMCZa7PcTtR
Vxg,user=alice@cxsecurity.onmi
nRadiusPacketEvent invoking polic

JavaBridge,2024-01-09 02:2 :58,59
212/494073967/247050,CPMSessionID=c0a8295d5UBshnQ2Qt010in2tSWeYjYY1xzLmHMCZa7PcTtR
Vxg,user=alice@cxsecurity.onmicrosoft.com,CallingStationID=41:F3:C9:B1:97:8D,JavaBridge::invoke:
class=com.cisco.cpm.prrt.policy.PolicyEngine event=EvaluatePolicyEvent,JavaBridge.cpp:537

Radius,2024-01-09 02:22:58,720,DEBUG,0x7f04d65b0700,cntx=0004342415,sesn=asc-ise33-
212/494073967/247050,CPMSessionID=c   295d5UBshnQ2Qt010in2t  eYjYY1xzLm   CZa7PcTtR
Vxg,user=alice@cxsecurity.onmicrosoft.c  ,CallingStationID=41:F3:C9:B1:  8D,Radiu   questFlow::o
nResponseEvaluatePolicyEvent process   result of policy e
```

Session ID Creation

If there is internal latency on the ISE application itself It will be evident here with a bigger time delta. Keep an eye out for these PolicyEngine events.

Thread Id changes

Context/SessionID remain the same

Check Flow invocation in prrt-server.log

```
RadiusMSCHAPFlow,2024-01-09 02:22:58,830,DEBUG,0x7f04d65b0700,cntx=0004342415,sesn=asc-ise33-
212/494073967/247050,CPMSessionID=c0a8295d5UBshnQ2Qt010in2tSWeYjYY1xzLmHMCZa7PcTtRVxg,user=al
ice@cxsecurity.onmicrosoft.com,CallingStationID=41:F3:C9:B1:97:8D,RadiusMSCHAPv2Flow::validateContext,Radi
usMSCHAPv2Flow.cpp:90
RadiusMSCHAPFlow,2024-01-09 02:22:58,830,DEBUG,0x7f04d65b0700,cntx=0004342415,sesn=asc-ise33-
212/494073967/247050,CPMSessionID=c0a8295d5UBshnQ2Qt010in2tSWeYjYY1xzLmHMCZa7PcTtRVxg,user=al
ice@cxsecurity.onmicrosoft.com,CallingStationID=41:F3:C9:B1:97:8D,RadiusMSCHAPv1Flow::validateContext,Radi
usMSCHAPv1Flow.cpp:84
RadiusCHAPFlow,2024-01-09 02:22:58,830,DEBUG,0x7f04d65b0700,cntx=0004342415,sesn=asc-ise33-
212/494073967/247050,CPMSessionID=c0a8295d5UBshnQ2Qt010in2tSWeYjYY1xzLmHMCZa7PcTtRVxg,user=al
ice@cxsecurity.onmicrosoft.com,CallingStationID=41:F3:C9:B1:97:8D,RadiusCHAPFlow::validateContext,RadiusCH
APFlow.cpp:79
RadiusPAPFlow,2024-01-09 02:22:58,830,DEBUG,0x7f04d65b0700,cntx=0004342415,sesn=asc-ise33-
212/494073967/247050,CPMSessionID=c0a8295d5UBshnQ2Qt010in2tSWeYjYY1xzLmHMCZa7PcTtRVxg,user=al
ice@cxsecurity.onmicrosoft.com,CallingStationID=41:F3:C9:B1:97:8D,RadiusPAPFlow::validateContext,RadiusPAPF
low.cpp:142
RadiusPAPFlow,2024-01-09 02:22:58,830,DEBUG,0x7f04d65b0700,cntx=0004342415,sesn=asc-ise33-
212/494073967/247050,CPMSessionID=c0a8295d5UBshnQ2Qt010in2tSWeYjYY1xzLmHMCZa7PcTtRVxg,user=al
ice@cxsecurity.onmicrosoft.com,CallingStationID=41:F3:C9:B1:97:8D,All mandatory attributes are
present,RadiusPAPFlow.cpp:130
```

Different flows are checked as configured in Allowed Protocols

PAP is selected based on the attributes in the request

Check Identity Store Selection in prrt-server.log

```
IdentitySequence,2024-01-09 02:22:58,959,DEBUG,0x7f04d53a7700,cntx=0004342415,sesn=asc-ise33-
212/494073967/247050,CPMSessionID=c0a8295d5UBshnQ2Qt010in2tSWeYjYY1xzLmHMCZa7PcTtRVxg,user=alice@cxsecurit
y.onmicrosoft.com,CallingStationID=41:F3:C9:B1:97:8D,***** Going to run authentication policy for IDStore
selection.,IdentitySequenceWorkflow.cpp:302

IdentitySequence,2024-01-09 02:22:58,959,DEBUG,0x7f04d53a7700,cntx=00
212/494073967/247050,CPMSessionID=c0a8295d5UBshnQ2Qt010in2tSWeYjY
y.onmicrosoft.com,CallingStationID=41:F3:C9:B1:97:8D,******* Authen
IDStoreName:SPEEDCORP,IdentitySequenceWorkflow.cpp:377
IdentitySequence,2024-01    02:22:58,959,DEBUG,0x7f04d53a7700,cntx=0004342415,sesn=asc-ise33-
212/494073967/247050,C    sionID=c0a8295d5UBshnQ2Qt010in2tSWeYjYY1xzLmHMCZa7PcTtRVxg,user=alice@cxsecurit
y.onmicrosoft.com,CallingStatio    1:F3:C9:B1:97:8D,******* Authen IDStoreName:Cloud,IdentitySequenceWorkflow.cpp:377
IdentitySequence,2024-01-09 02:2    959,DEBUG,0x7f04d    700,cntx=0004342415,sesn=asc-ise33-
212/494073967/247050,CPMSession    a8295d5UBshn    10in2tSWeYjYY1xzLmHMCZa7PcTtRVxg,user=alice@cxsecurit
y.onmicrosoft.com,CallingStationID=41:F    1:97:8D,*    workflow is calling:<PAPAuthenticator>
************,IdentitySequenceWorkflo

IDStore,2024-01-09 02:22:58,959,DEBUG,0x7f04d5    a7700,cntx=0004342415,sesn=asc-ise33-
212/494073967/247050,CPMSessionID=c0a8295d5UBshnQ2Qt010in2tSWeYjYY1xzLmHMCZa7PcTtRVxg,user=alice@cxsecurit
y.onmicrosoft.com,CallingStationID=41:F3:C9:B1:97:8D,ActiveDirectoryIDStore::shouldInvoke ADDomain =
speedcorp.com,A    eDirectoryIDStore.cpp:571
CiscoAD,2024-0    2:59,000,DEBUG,0x7f04d218e700,cntx=0004342415,sesn=asc-ise33-
212/494073967/2470    sionID=c0a8295d5UBshnQ2Qt010in2tSWeYjYY1xzLmHM    Z
y.onmicrosoft.com,Cal    : cad_ResolveIdentity :
Start,ActiveDirectoryID
prrt-server.log.2:Cisco    f04d218e700,cntx=0004342
```

Authentication Policy Selection

IDStores in IDStore Sequence

First IDStore in sequence

Resolve identity with AD

```
ADClient,2024-01-09 02:22:59,074,DEBUG,0x7f04d218e700,cntx=0004342415,sesn=asc-ise33-
212/494073967/247050,CPMSessionID=c0a8295d5UBshnQ2Qt010in2tSWeYjYY1xzLmHMCZa7PcTtRVxg,user=alice@cxsec
urity.onmicrosoft.com,CallingStationID=41:F3:C9:B1:97:8D,[ActiveDirectoryClient::plainTextAuthenticate] PAP authentication
for user alice@cxsecurity.onmicrosoft.com has failed due to error 40008:LW_ERROR_NO_SUCH_USER:No such user, please
refer to Test user option to get further information,ActiveDirectoryClient.cpp:817

IdentitySequence,2024-01-09 02:22:59,074,DEBUG,0x7f04d67b1700,cntx=0004342415,sesn=asc-ise33-
212/494073967/247050,CPMSessionID=c0a8295d5UBshnQ2Qt010in2tSWeYjYY1xzLmHMCZa7PcTtRVxg,us alice@cxsec
urity.onmicrosoft.com,CallingStationID=41:F3:C9:B1:97:8D,******* workflow continues, calling
authenticator=<PAPAuthenticator> with CurrentIDStoreName=<Cloud>************,Id tySequenceWorkflow 59
PAPAuthenticator,2024-01-09 02:22:59,074,DEBUG,0x7f04d67b1700,cntx=000434 5,sesn=asc-ise33-
212/494073967/247050,CPMSessionID=c0a8295d5UBshnQ2Qt010in2tSWeYjYY1xz
urity.onmicrosoft.com,CallingStationID=41:F3:C9:B1:97:8D,Attempting calling Cloud
IDStore,../../../../build/lnx418_64/include/Authenticator.h:142

JavaBridge,2024-01-0
212/494073967/24705
urity.onmicrosoft.com,(
class=com.cisco.cpm.prrt.idstores.RestUserFetcher event=RestAuthenticateUser,JavaBridge.cpp:537
Logging,2024-01-09 02:23:01,415,WARN ,0x7f04bfd0a700,cntx=0004342415,sesn=asc-ise33-
212/494073967/247050,CPMSessionI =c0a onID=4
1:F3:C9:B1:97:8D,Long step latency ;
RESTIDStore,2024-01-09 02:23:02,05 DEE
212/494073967/247050,CPMSessionID=c0a8295d5UBshnQ2Qt010in2tSWeYjYY1xzLmHMCZa7PcTtRVxg,user=alice@cxsec
urity.onmicrosoft.com,CallingStationID=41:F3:C9:B1:97:8D,RESTIDStore - authentication/lookup status:
Error,RESTIDStore.cpp:150
```

Active Directory returned that there is no such user.

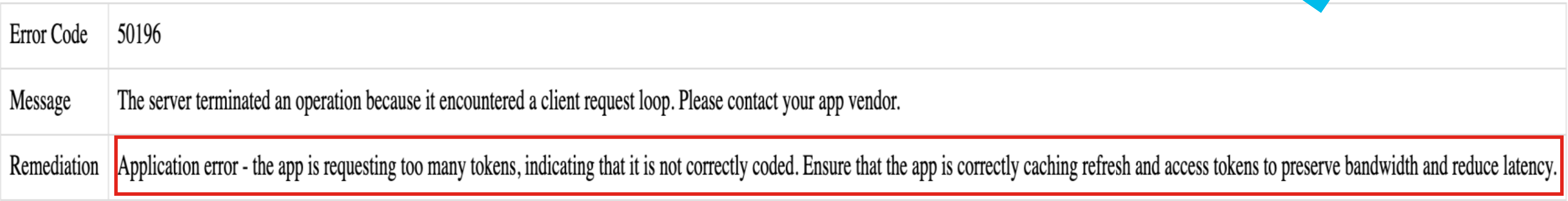
So ISE continues with the next ID Store based on the configuration for user not found usecase in Identity Store Sequence settings

Long Step Latency noticed by ISE when trying to lookup user in the Cloud ID Store

Authentication resulted in Error

Check ROPC logs at ropc/rest-id-store.log

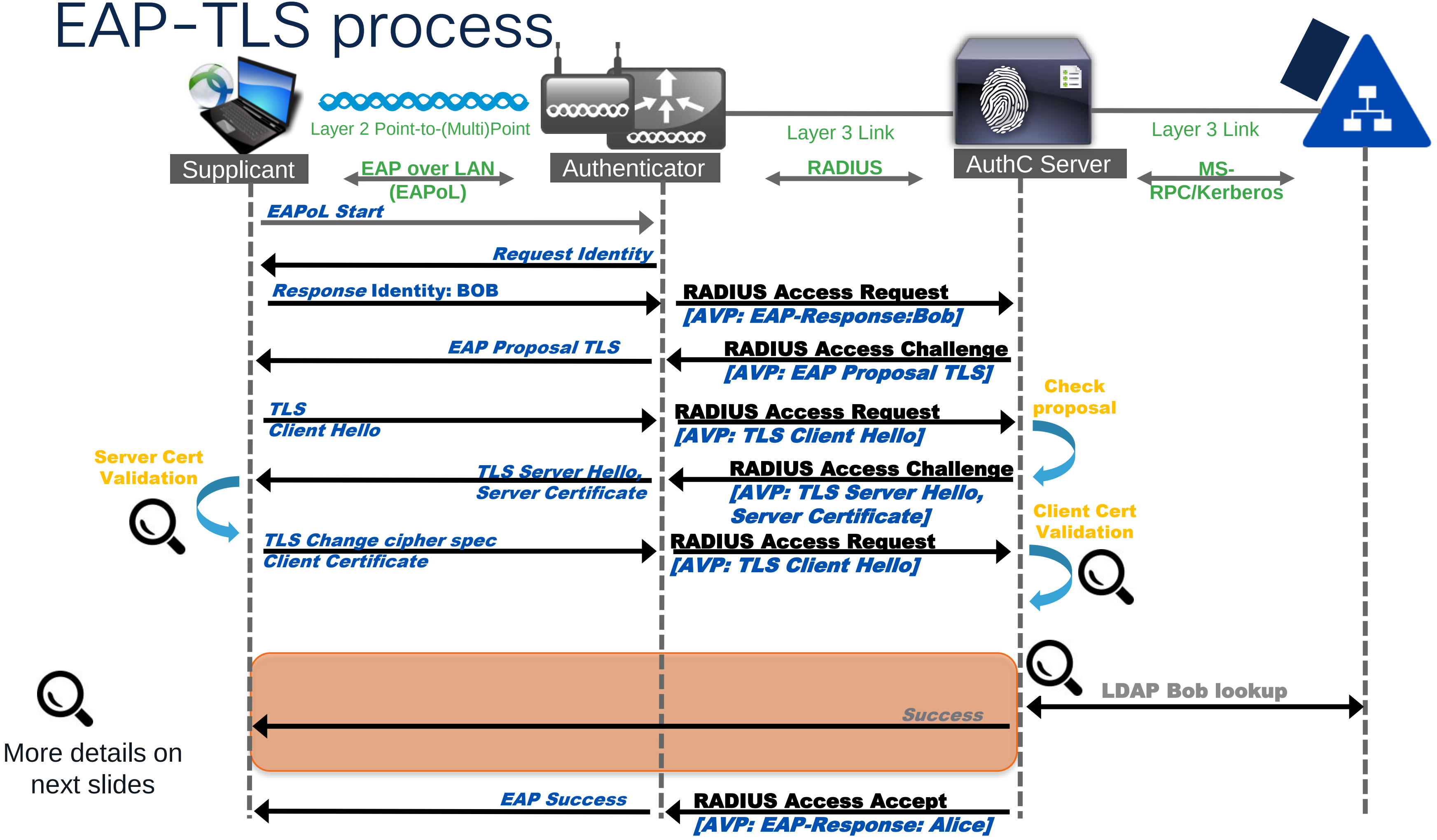
```
2024-01-09 02:23:02,049 DEBUG  [I/O dispatcher 116][[]] cisco.ise.ropc.utilities.HttpClientWrapper -:::::-
userGrpProcessTtls Start ......
2024-01-09 02:23:02,050 DEBUG  [I/O dispatcher 116][[]] cisco.ise.ropc.utilities.HttpClientWrapper -:::::-  Async
Group process for Ttls I/O dispatcher 116
2024-01-09 02:23:02,050 ERROR  [I/O dispatcher 116][[]] cisco.ise.ropc.utilities.HttpClientWrapper -:::::- Error
occured to fetch user authenticate for TTLS {"error":"invalid_grant","error_description":"AADSTS50196: The server
terminated an operation because it encountered a client request loop. Please contact your app vendor. Trace ID:
55dd87eb-50ac-4597-99be-5d5f09a98100 Correlation ID: df376c1b-c6ea-4c80-80cc-5daccbf83875
Timestamp: 2024-01-09 02:23:48Z","error_codes":[50196],"timestamp":"2024-01-09
02:23:48Z","trace_id":"55dd87eb-50ac-4597-99be-5d5f09a98100","correlation_id":"df376c1b-c6ea-4c80-
80cc-5daccbf83875","error_uri":"https://login.microsoftonline.com/error?code=50196"}
2024-01-09 02:23:02,050 DEBUG  [I/O dispatcher 116][[]] cisco.ise.ropc.utilities.HttpClientWrapper -:::::-
userGrpProcessTtls End ......
```



Error Code	50196
Message	The server terminated an operation because it encountered a client request loop. Please contact your app vendor.
Remediation	Application error - the app is requesting too many tokens, indicating that it is not correctly coded. Ensure that the app is correctly caching refresh and access tokens to preserve bandwidth and reduce latency.

EAP TLS and Capture Analysis

EAP-TLS process



Supplicant

Layer 2 Point-to-(Multi)Point

EAP over LAN (EAPoL)

Authenticator

Layer 3 Link

RADIUS

AuthC Server

Layer 3 Link

MS-RPC/Kerberos

EAPoL Start

Request Identity

Response **Identity: BOB**

RADIUS Access Request
[AVP: EAP-Response:Bob]

EAP Proposal TLS

RADIUS Access Challenge
[AVP: EAP Proposal TLS]

Check proposal

TLS Client Hello

RADIUS Access Request
[AVP: TLS Client Hello]

Server Cert Validation

TLS Server Hello, Server Certificate

RADIUS Access Challenge
[AVP: TLS Server Hello, Server Certificate]

Client Cert Validation

TLS Change cipher spec Client Certificate

RADIUS Access Request
[AVP: TLS Client Hello]

LDAP Bob lookup

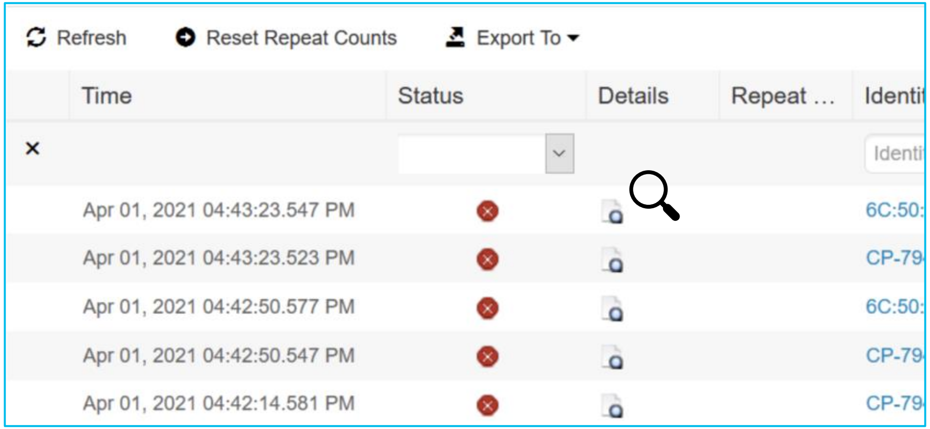
Success

More details on next slides

EAP Success

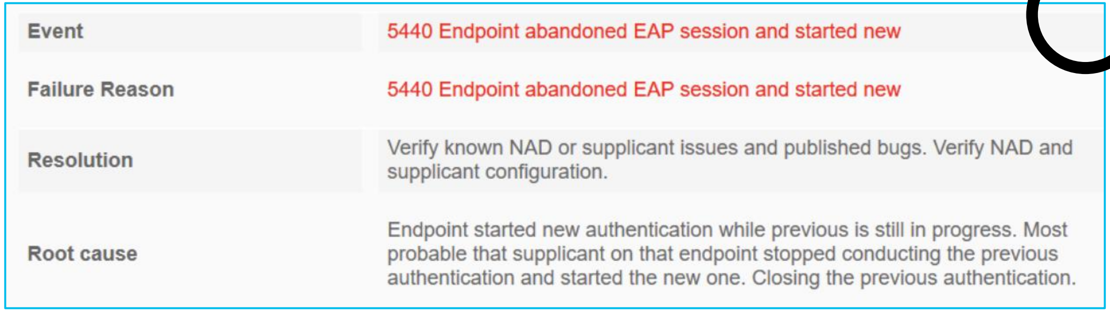
RADIUS Access Accept
[AVP: EAP-Response: Alice]

ISE RADIUS Live Logs



Refresh   Reset Repeat Counts   Export To ▾

	Time	Status	Details	Repeat ...	Identi
✕					Identi
	Apr 01, 2021 04:43:23.547 PM	⊗	🔍		6C:50:
	Apr 01, 2021 04:43:23.523 PM	⊗	🔍		CP-79
	Apr 01, 2021 04:42:50.577 PM	⊗	🔍		6C:50:
	Apr 01, 2021 04:42:50.547 PM	⊗	🔍		CP-79
	Apr 01, 2021 04:42:14.581 PM	⊗	🔍		CP-79

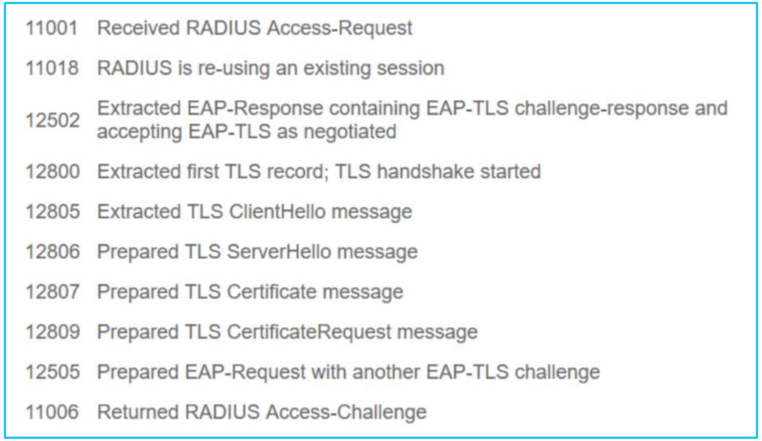


Event	5440 Endpoint abandoned EAP session and started new
Failure Reason	5440 Endpoint abandoned EAP session and started new
Resolution	Verify known NAD or supplicant issues and published bugs. Verify NAD and supplicant configuration.
Root cause	Endpoint started new authentication while previous is still in progress. Most probable that supplicant on that endpoint stopped conducting the previous authentication and started the new one. Closing the previous authentication.

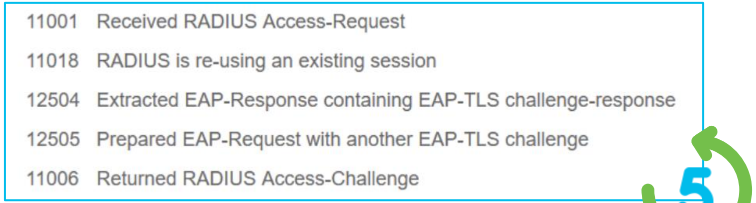
What does it mean?

- Either ISE has not received response from the endpoint for initial authentication session or the endpoint has never received the response from the ISE.
- Endpoint started a new session before the initial one timed out on ISE.

Troubleshooting – detailed report steps.



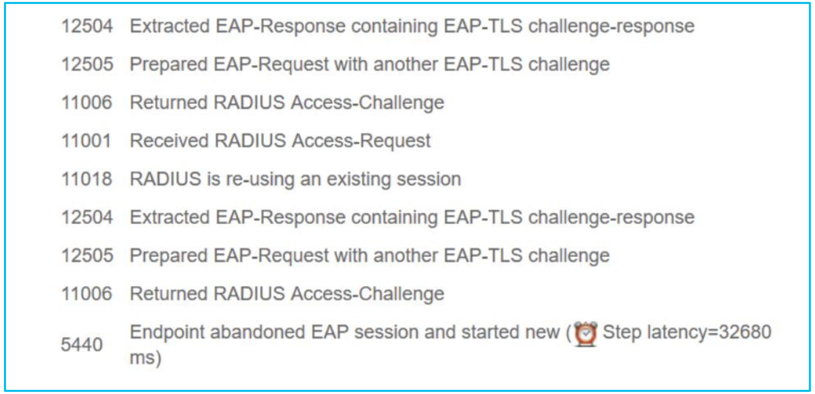
```
11001  Received RADIUS Access-Request
11018  RADIUS is re-using an existing session
12502  Extracted EAP-Response containing EAP-TLS challenge-response and
       accepting EAP-TLS as negotiated
12800  Extracted first TLS record; TLS handshake started
12805  Extracted TLS ClientHello message
12806  Prepared TLS ServerHello message
12807  Prepared TLS Certificate message
12809  Prepared TLS CertificateRequest message
12505  Prepared EAP-Request with another EAP-TLS challenge
11006  Returned RADIUS Access-Challenge
```



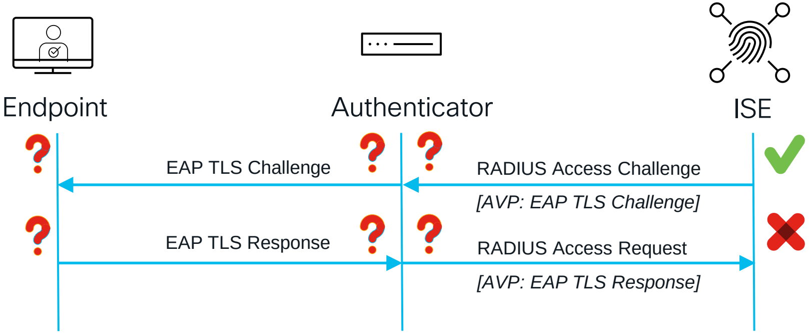
```
11001  Received RADIUS Access-Request
11018  RADIUS is re-using an existing session
12504  Extracted EAP-Response containing EAP-TLS challenge-response
12505  Prepared EAP-Request with another EAP-TLS challenge
11006  Returned RADIUS Access-Challenge
```

5

step keeps repeating



```
12504  Extracted EAP-Response containing EAP-TLS challenge-response
12505  Prepared EAP-Request with another EAP-TLS challenge
11006  Returned RADIUS Access-Challenge
11001  Received RADIUS Access-Request
11018  RADIUS is re-using an existing session
12504  Extracted EAP-Response containing EAP-TLS challenge-response
12505  Prepared EAP-Request with another EAP-TLS challenge
11006  Returned RADIUS Access-Challenge
5440   Endpoint abandoned EAP session and started new (⏰ Step latency=32680
       ms)
```



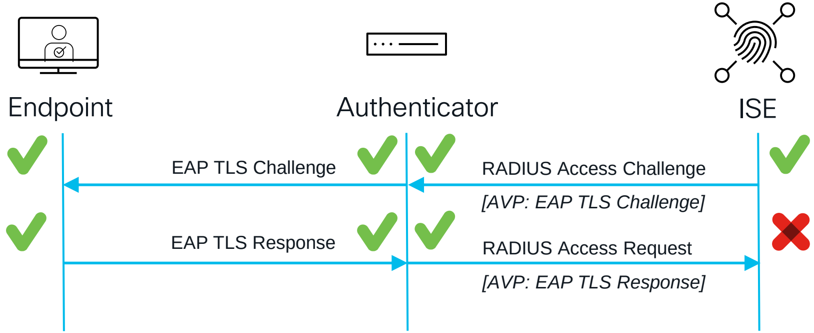
Troubleshooting – authenticator

```
#set platform software trace smd switch active R0 dot1x-all debug
#set platform software trace smd switch active R0 radius debug

2021/04/01 14:46:00.142097 {smd_R0-0}{1}: [radius] [22809]: (debug): RADIUS(00000000): Sending a
IPv4 Radius Packet
2021/04/01 14:46:00.142144 {smd_R0-0}{1}: [radius] [22809]: (info): RADIUS: Started 4 sec
timeout
2021/04/01 14:46:04.142283 {smd_R0-0}{1}: [radius] [22809]: (debug):
RADIUS(00000000): Request timed out!
```

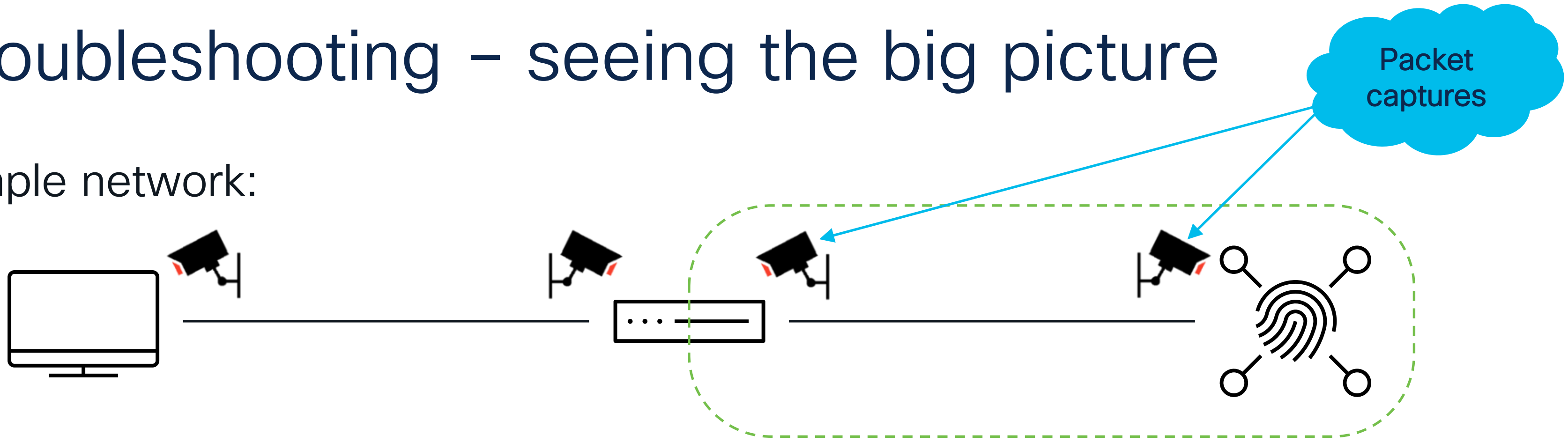
Usually 3 retries

```
2021/04/01 14:46:16.146327 {smd_R0-0}{1}: [radius] [22809]: (debug): RADIUS-RADIUS_DEAD:
RADIUS server 10.91.32.21:1812,1813 is not responding.
```

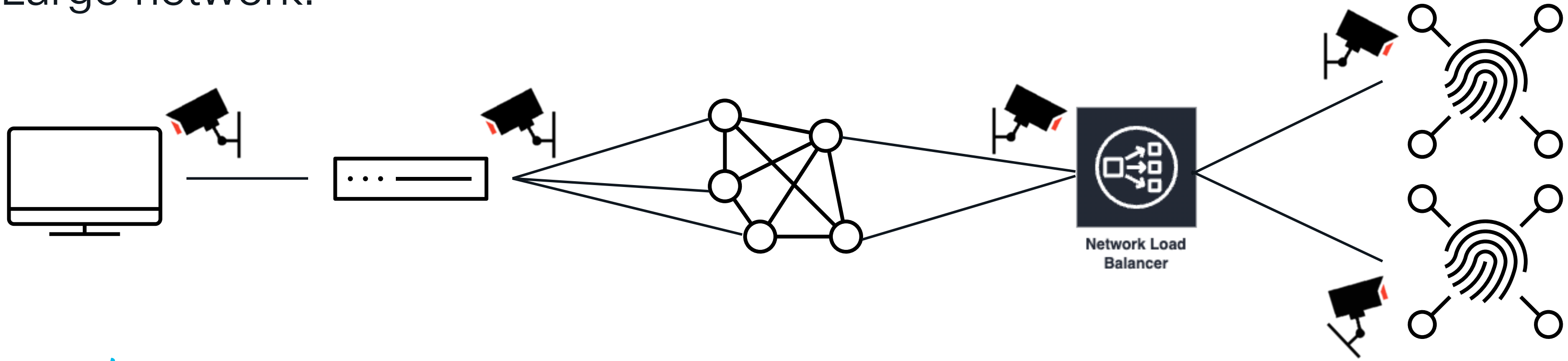


Troubleshooting – seeing the big picture

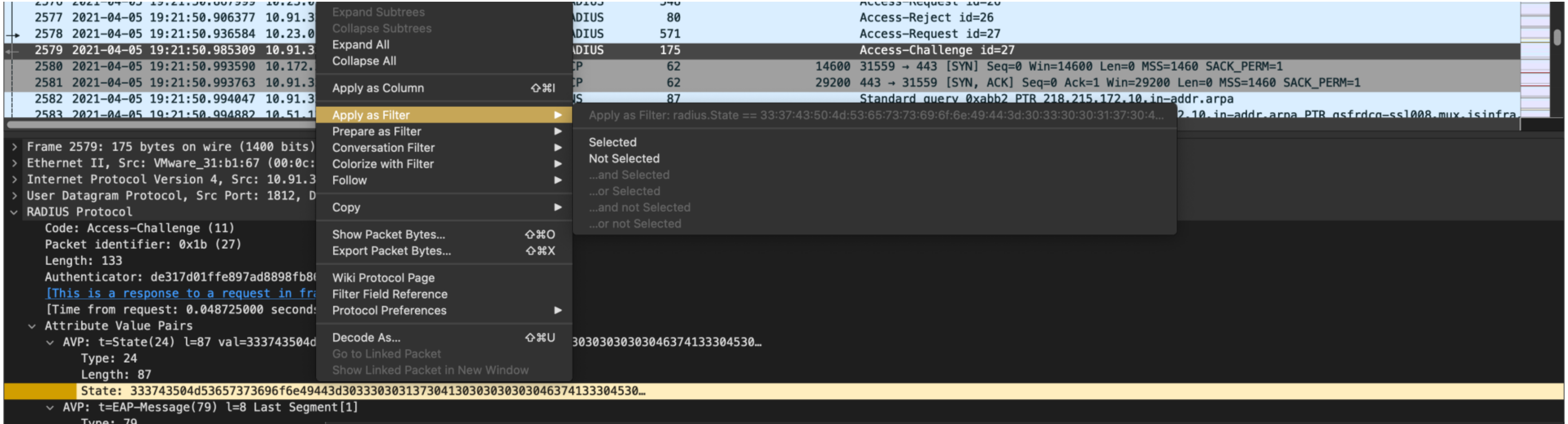
Simple network:



Large network:



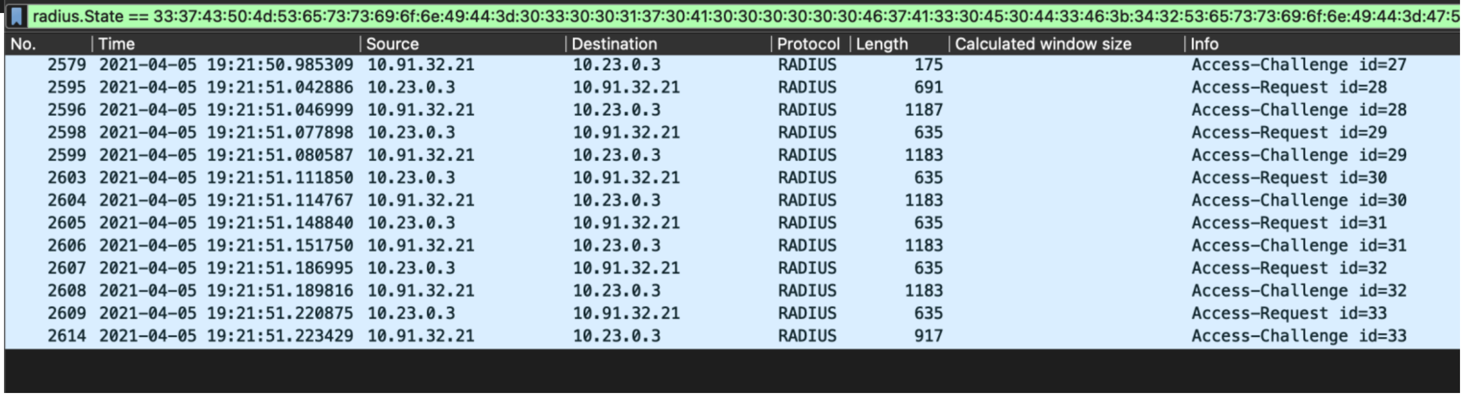
Packet captures - ISE



```
2577  2021-04-05 19:21:50.906377  10.91.3   ADIUS    80           Access-Reject id=26
2578  2021-04-05 19:21:50.936584  10.23.0   ADIUS   571           Access-Request id=27
2579  2021-04-05 19:21:50.985309  10.91.3   ADIUS   175           Access-Challenge id=27
2580  2021-04-05 19:21:50.993590  10.172.   CP       62    14600  31559 → 443 [SYN] Seq=0 Win=14600 Len=0 MSS=1460 SACK_PERM=1
2581  2021-04-05 19:21:50.993763  10.91.3   CP       62    29200  443 → 31559 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM=1
2582  2021-04-05 19:21:50.994047  10.91.3   IS       87           Standard query 0xabb2 PTR 218.215.172.10.in-addr.arpa
2583  2021-04-05 19:21:50.994882  10.51.1                         2.10.in-addr.arpa PTR gsfrdcg-ssl008.mux.isinfra
```

```
> Frame 2579: 175 bytes on wire (1400 bits)
> Ethernet II, Src: VMware_31:b1:67 (00:0c:
> Internet Protocol Version 4, Src: 10.91.3
> User Datagram Protocol, Src Port: 1812, D
v RADIUS Protocol
    Code: Access-Challenge (11)
    Packet identifier: 0x1b (27)
    Length: 133
    Authenticator: de317d01ffe897ad8898fb8
    [This is a response to a request in fra
    [Time from request: 0.048725000 second
  v Attribute Value Pairs
    v AVP: t=State(24) l=87 val=333743504d                     303030303046374133304530…
        Type: 24
        Length: 87
        State: 333743504d53657373696f6e49443d3033303031373041303030303030463741333045 30…
    v AVP: t=EAP-Message(79) l=8 Last Segment[1]
        Type: 79
```

Narrow down the capture to single flow

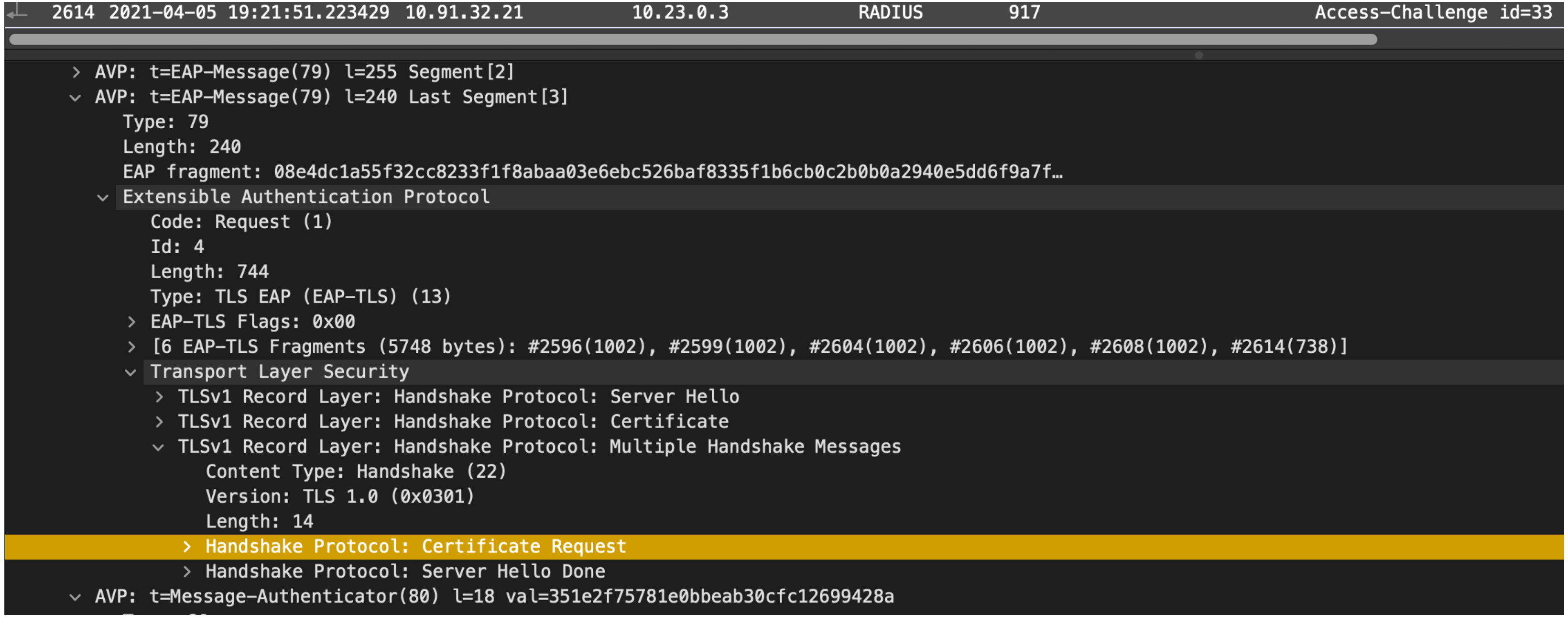


```
radius.State == 33:37:43:50:4d:53:65:73:73:69:6f:6e:49:44:3d:30:33:30:30:31:37:30:41:30:30:30:30:30:30:46:37:41:33:30:45:30:44:33:46:3b:34:32:53:65:73:73:69:6f:6e:49:44:3d:47:5
```

```
No.   Time                        Source        Destination   Protocol  Length  Calculated window size  Info
2579  2021-04-05 19:21:50.985309  10.91.32.21   10.23.0.3     RADIUS       175                          Access-Challenge id=27
2595  2021-04-05 19:21:51.042886  10.23.0.3     10.91.32.21   RADIUS       691                          Access-Request id=28
2596  2021-04-05 19:21:51.046999  10.91.32.21   10.23.0.3     RADIUS      1187                          Access-Challenge id=28
2598  2021-04-05 19:21:51.077898  10.23.0.3     10.91.32.21   RADIUS       635                          Access-Request id=29
2599  2021-04-05 19:21:51.080587  10.91.32.21   10.23.0.3     RADIUS      1183                          Access-Challenge id=29
2603  2021-04-05 19:21:51.111850  10.23.0.3     10.91.32.21   RADIUS       635                          Access-Request id=30
2604  2021-04-05 19:21:51.114767  10.91.32.21   10.23.0.3     RADIUS      1183                          Access-Challenge id=30
2605  2021-04-05 19:21:51.148840  10.23.0.3     10.91.32.21   RADIUS       635                          Access-Request id=31
2606  2021-04-05 19:21:51.151750  10.91.32.21   10.23.0.3     RADIUS      1183                          Access-Challenge id=31
2607  2021-04-05 19:21:51.186995  10.23.0.3     10.91.32.21   RADIUS       635                          Access-Request id=32
2608  2021-04-05 19:21:51.189816  10.91.32.21   10.23.0.3     RADIUS      1183                          Access-Challenge id=32
2609  2021-04-05 19:21:51.220875  10.23.0.3     10.91.32.21   RADIUS       635                          Access-Request id=33
2614  2021-04-05 19:21:51.223429  10.91.32.21   10.23.0.3     RADIUS       917                          Access-Challenge id=33
```

Packet captures – ISE cont.

- The last Access-Challenge **(id=33)** sent by ISE contains Server Hello (for the server certificate validation) with user certificate request.
- No response is received on the ISE.

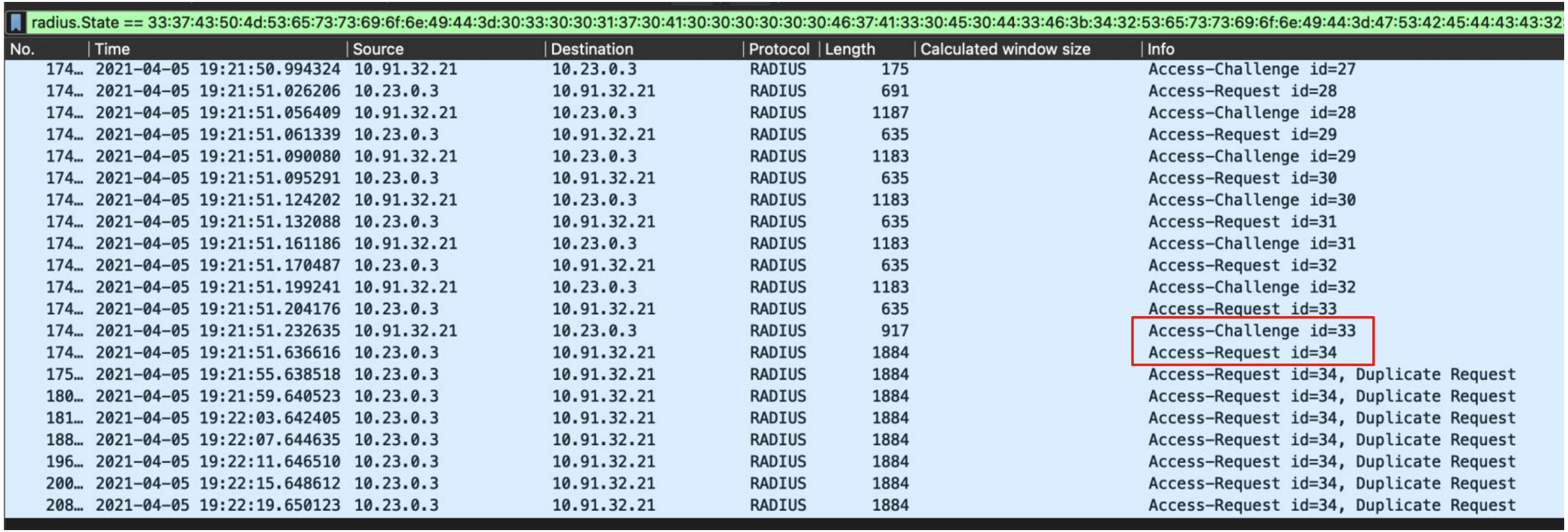


```
2614  2021-04-05 19:21:51.223429  10.91.32.21        10.23.0.3        RADIUS     917              Access-Challenge id=33

   › AVP: t=EAP-Message(79) l=255 Segment[2]
   ⌄ AVP: t=EAP-Message(79) l=240 Last Segment[3]
       Type: 79
       Length: 240
       EAP fragment: 08e4dc1a55f32cc8233f1f8abaa03e6ebc526baf8335f1b6cb0c2b0b0a2940e5dd6f9a7f…
     ⌄ Extensible Authentication Protocol
         Code: Request (1)
         Id: 4
         Length: 744
         Type: TLS EAP (EAP-TLS) (13)
       › EAP-TLS Flags: 0x00
       › [6 EAP-TLS Fragments (5748 bytes): #2596(1002), #2599(1002), #2604(1002), #2606(1002), #2608(1002), #2614(738)]
       ⌄ Transport Layer Security
         › TLSv1 Record Layer: Handshake Protocol: Server Hello
         › TLSv1 Record Layer: Handshake Protocol: Certificate
         ⌄ TLSv1 Record Layer: Handshake Protocol: Multiple Handshake Messages
             Content Type: Handshake (22)
             Version: TLS 1.0 (0x0301)
             Length: 14
           › Handshake Protocol: Certificate Request
           › Handshake Protocol: Server Hello Done
   ⌄ AVP: t=Message-Authenticator(80) l=18 val=351e2f75781e0bbeab30cfc12699428a
```

Packet captures - Switch

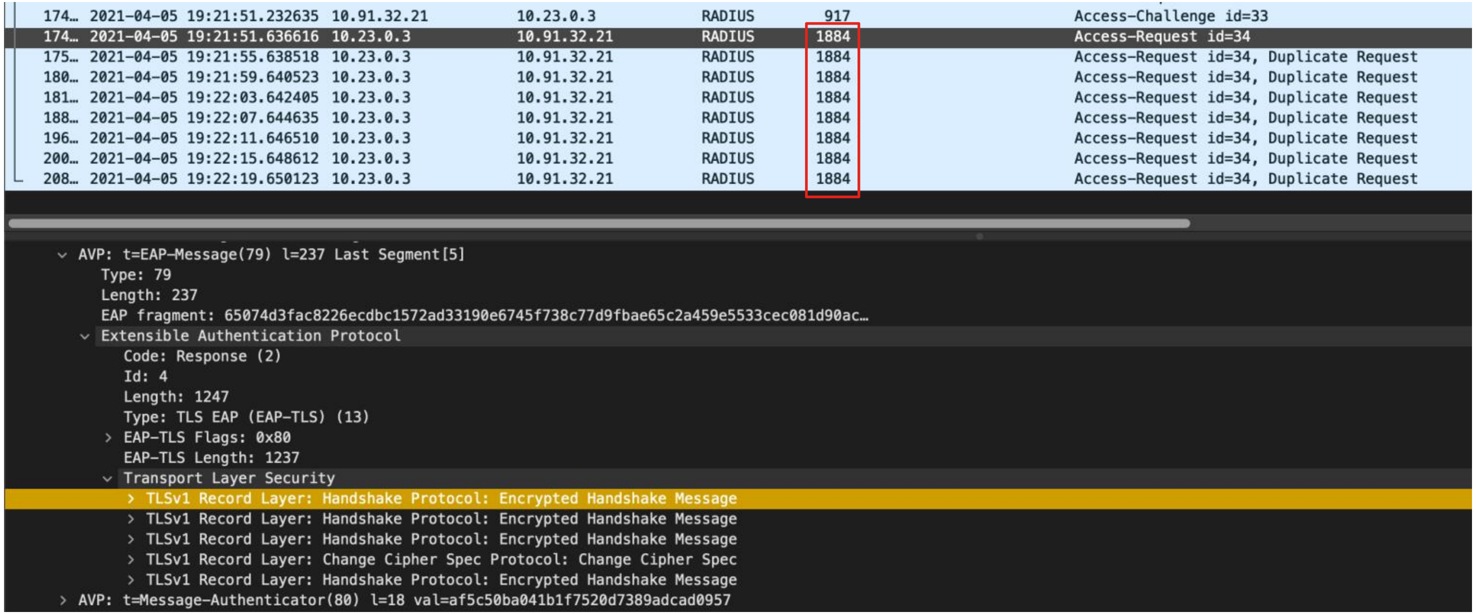
- Packet capture was collected at the same time from ISE and Switch.
- Can be filtered with the same “radius.State” filter.
- At first glance it’s visible that there are more messages.



```
radius.State == 33:37:43:50:4d:53:65:73:73:69:6f:6e:49:44:3d:30:33:30:30:31:37:30:41:30:30:30:30:30:30:46:37:41:33:30:45:30:44:33:46:3b:34:32:53:65:73:73:69:6f:6e:49:44:3d:47:53:42:45:44:43:43:32
No.   Time                        Source       Destination  Protocol Length Calculated window size  Info
174…  2021-04-05 19:21:50.994324  10.91.32.21  10.23.0.3    RADIUS    175                           Access-Challenge id=27
174…  2021-04-05 19:21:51.026206  10.23.0.3    10.91.32.21  RADIUS    691                           Access-Request id=28
174…  2021-04-05 19:21:51.056409  10.91.32.21  10.23.0.3    RADIUS   1187                           Access-Challenge id=28
174…  2021-04-05 19:21:51.061339  10.23.0.3    10.91.32.21  RADIUS    635                           Access-Request id=29
174…  2021-04-05 19:21:51.090080  10.91.32.21  10.23.0.3    RADIUS   1183                           Access-Challenge id=29
174…  2021-04-05 19:21:51.095291  10.23.0.3    10.91.32.21  RADIUS    635                           Access-Request id=30
174…  2021-04-05 19:21:51.124202  10.91.32.21  10.23.0.3    RADIUS   1183                           Access-Challenge id=30
174…  2021-04-05 19:21:51.132088  10.23.0.3    10.91.32.21  RADIUS    635                           Access-Request id=31
174…  2021-04-05 19:21:51.161186  10.91.32.21  10.23.0.3    RADIUS   1183                           Access-Challenge id=31
174…  2021-04-05 19:21:51.170487  10.23.0.3    10.91.32.21  RADIUS    635                           Access-Request id=32
174…  2021-04-05 19:21:51.199241  10.91.32.21  10.23.0.3    RADIUS   1183                           Access-Challenge id=32
174…  2021-04-05 19:21:51.204176  10.23.0.3    10.91.32.21  RADIUS    635                           Access-Request id=33
174…  2021-04-05 19:21:51.232635  10.91.32.21  10.23.0.3    RADIUS    917                           Access-Challenge id=33
174…  2021-04-05 19:21:51.636616  10.23.0.3    10.91.32.21  RADIUS   1884                           Access-Request id=34
175…  2021-04-05 19:21:55.638518  10.23.0.3    10.91.32.21  RADIUS   1884                           Access-Request id=34, Duplicate Request
180…  2021-04-05 19:21:59.640523  10.23.0.3    10.91.32.21  RADIUS   1884                           Access-Request id=34, Duplicate Request
181…  2021-04-05 19:22:03.642405  10.23.0.3    10.91.32.21  RADIUS   1884                           Access-Request id=34, Duplicate Request
188…  2021-04-05 19:22:07.644635  10.23.0.3    10.91.32.21  RADIUS   1884                           Access-Request id=34, Duplicate Request
196…  2021-04-05 19:22:11.646510  10.23.0.3    10.91.32.21  RADIUS   1884                           Access-Request id=34, Duplicate Request
200…  2021-04-05 19:22:15.648612  10.23.0.3    10.91.32.21  RADIUS   1884                           Access-Request id=34, Duplicate Request
208…  2021-04-05 19:22:19.650123  10.23.0.3    10.91.32.21  RADIUS   1884                           Access-Request id=34, Duplicate Request
```

Packet captures – Switch cont.

- Endpoint responded to ISE Access-Challenge **(id=33)** and authenticator is trying to send the Access-Request **(id=34)** to ISE however, it seems as if either ISE did not receive them or the responses from the ISE are not getting back to the switch.

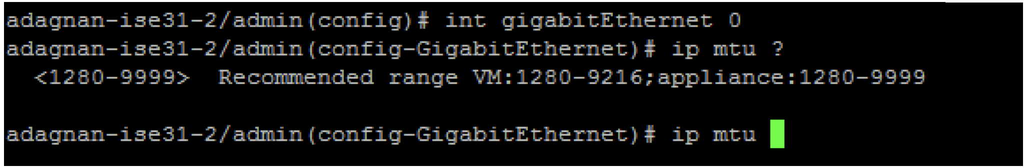


```
174… 2021-04-05 19:21:51.232635 10.91.32.21   10.23.0.3    RADIUS   917    Access-Challenge id=33
174… 2021-04-05 19:21:51.636616 10.23.0.3     10.91.32.21  RADIUS   1884   Access-Request id=34
175… 2021-04-05 19:21:55.638518 10.23.0.3     10.91.32.21  RADIUS   1884   Access-Request id=34, Duplicate Request
180… 2021-04-05 19:21:59.640523 10.23.0.3     10.91.32.21  RADIUS   1884   Access-Request id=34, Duplicate Request
181… 2021-04-05 19:22:03.642405 10.23.0.3     10.91.32.21  RADIUS   1884   Access-Request id=34, Duplicate Request
188… 2021-04-05 19:22:07.644635 10.23.0.3     10.91.32.21  RADIUS   1884   Access-Request id=34, Duplicate Request
196… 2021-04-05 19:22:11.646510 10.23.0.3     10.91.32.21  RADIUS   1884   Access-Request id=34, Duplicate Request
200… 2021-04-05 19:22:15.648612 10.23.0.3     10.91.32.21  RADIUS   1884   Access-Request id=34, Duplicate Request
208… 2021-04-05 19:22:19.650123 10.23.0.3     10.91.32.21  RADIUS   1884   Access-Request id=34, Duplicate Request
```

```
⌄ AVP: t=EAP-Message(79) l=237 Last Segment[5]
    Type: 79
    Length: 237
    EAP fragment: 65074d3fac8226ecdbc1572ad33190e6745f738c77d9fbae65c2a459e5533cec081d90ac…
  ⌄ Extensible Authentication Protocol
      Code: Response (2)
      Id: 4
      Length: 1247
      Type: TLS EAP (EAP-TLS) (13)
    › EAP-TLS Flags: 0x80
      EAP-TLS Length: 1237
    ⌄ Transport Layer Security
      › TLSv1 Record Layer: Handshake Protocol: Encrypted Handshake Message
      › TLSv1 Record Layer: Handshake Protocol: Encrypted Handshake Message
      › TLSv1 Record Layer: Handshake Protocol: Encrypted Handshake Message
      › TLSv1 Record Layer: Change Cipher Spec Protocol: Change Cipher Spec
      › TLSv1 Record Layer: Handshake Protocol: Encrypted Handshake Message
› AVP: t=Message-Authenticator(80) l=18 val=af5c50ba041b1f7520d7389adcad0957
```

ISE MTU

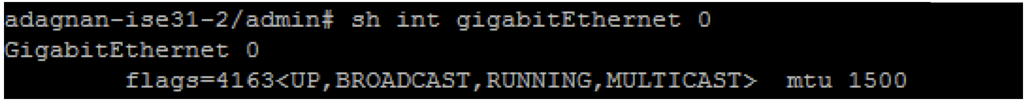
Jumbo frames are supported since version 3.1:



```
adagnan-ise31-2/admin(config)# int gigabitEthernet 0
adagnan-ise31-2/admin(config-GigabitEthernet)# ip mtu ?
  <1280-9999>  Recommended range VM:1280-9216;appliance:1280-9999

adagnan-ise31-2/admin(config-GigabitEthernet)# ip mtu
```

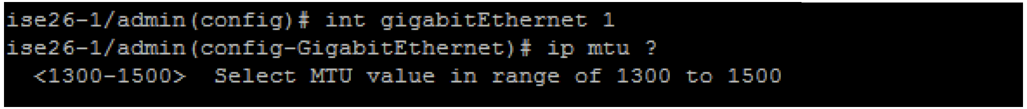
The default value is still 1500:



```
adagnan-ise31-2/admin# sh int gigabitEthernet 0
GigabitEthernet 0
        flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
```

⚠

Pre 3.1:



```
ise26-1/admin(config)# int gigabitEthernet 1
ise26-1/admin(config-GigabitEthernet)# ip mtu ?
  <1300-1500>  Select MTU value in range of 1300 to 1500
```

Conclusion

Summary and Call for Action

- Define base line latencies in normal network operation.
- Latency peaks are expected based on start/resumption of business hours.
- Follow Step Latencies in Live Log details page to determine potential break points.
- Enable the required debugs and pick an authentication attempt that experienced latency to follow the session.
- If you see internal latencies, collect thread and heap dumps along with debugs.
- Ensure packet captures are taken at potential breakpoints for faster resolution.

The bridge to possible

Thank you

cisco Live!

cisco Live!

Let's go