

RADIUS Conference 2026, 15th of June 2026

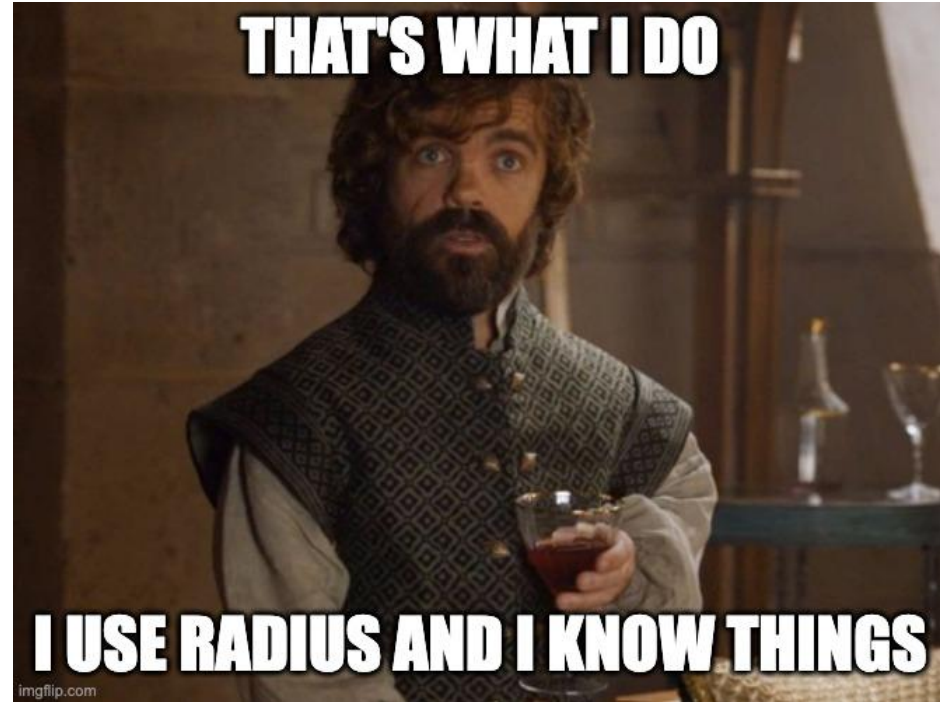
Expand your awareness RADIUS

Using RADIUS to improve network situational awareness

Karri Huhtanen (Radiator Software)

The access edge knows things

- Identity, device, location and policy meet at the access edge
- VPNs, Wired 802.1X and Wi-Fi already produce useful events even before IP connectivity
- Security tools often see access results, but they do not see the full context
- RADIUS can help fill that gap



RADIUS is usually treated as a gatekeeper

- Access-Request: may I enter?
- Access-Accept: yes, with this policy
- Access-Reject: no (and sometimes why)
- VLANs, filters, roles and session controls

Useful, but incomplete as a mental model.



RADIUS is also an access event stream

Each authentication and accounting exchange can describe:

- **Who** authenticated, or from which organisation
- **What** device appeared
- **Where** it attached: switch, port, AP, SSID, VPN, NAS identifier / IP address ...
- **When** sessions started, changed and ended
- **How** access was authorised
- **How much traffic** was observed
- **Why access** failed or stopped

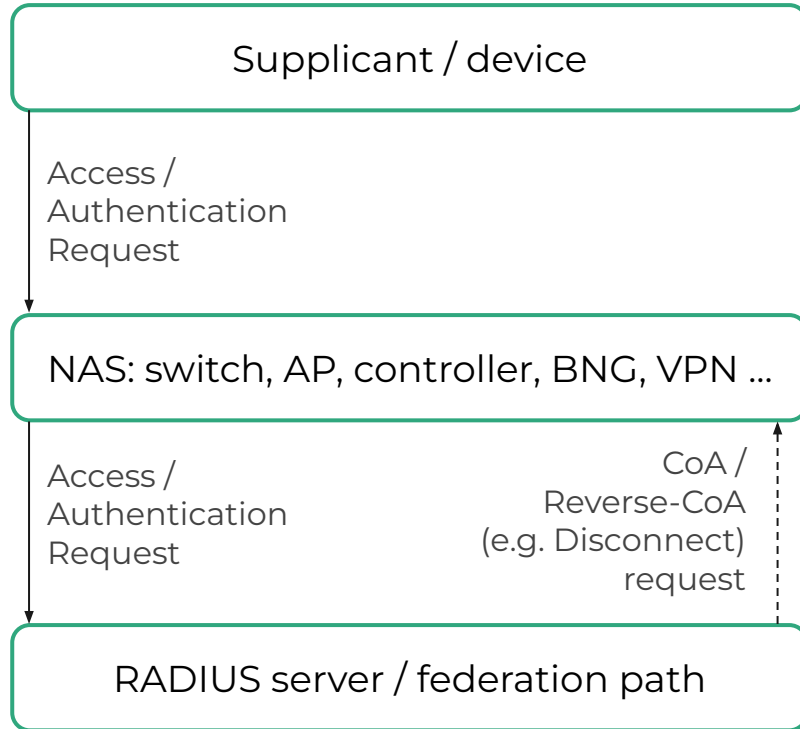


Questions RADIUS can help answer

- Which user or device was connected where at this time?
- What was their path if they were roaming around?
- Did it use wired, Wi-Fi, VPN or some other access type?
- Which AP, SSID, port, VPN endpoint or IP addresses were involved?
- What policy result and response did it receive?
- Did the session volume and duration look normal?
- Did failure or some other patterns change?



RADIUS AAA flow



Authentication

Access-Request -> Accept / Reject

Accounting

Start -> Interim-Update -> Stop

Dynamic authorisation

CoA/Reverse CoA, where supported

From dial-up records to access telemetry

RADIUS accounting started with practical questions:

- When did the session start and stop?
- How long did it last?
- How much input and output traffic was recorded?
- Why did it terminate?

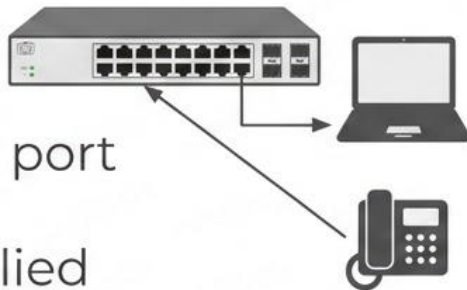
The same pattern still matters in 802.1X networks and in any access.



Wired 802.1X: fixed ports should not be blind spots

Secured Ethernet ports can tell you

- Which user/device authenticated on which switch port
- Whether a fixed port suddenly became active
- Whether the expected VLAN, filter or role was applied
- Whether reauthentication or termination behaviour changed
- Traffic amounts, IP addresses sometimes even without authentication



Timestamp	User	Device	Port	VLAN	Traffic
16.05.2021	User 1	Laptop	4	30	1300p
16.05.2023	User 2	Device	8	30	291p
16.05.2022	User 3	VoIP	10	30	1300p
16.05.2022	User 4	computer	12	30	120p
...

Example RADIUS attributes:

NAS-Identifier, NAS-IP-Address, NAS-Port-Type , NAS-Port-Id ,
Called-Station-Id, Calling-Station-Id , ...

Wi-Fi 802.1X context



Wi-Fi RADIUS attributes can add:

- User, realm and device context
- AP, BSSID, SSID information
- RF band and WLAN security attributes, where reported
- Roaming and accountable but private identity context
- Failure and disconnect reason information

Example RADIUS attributes: cisco-avpair, Called-Station-Id, Called-Station-Id, Chargeable-User-Identity, WLAN-RF-Band, WBA-Identity-Provider, Operator-Name ...

Passpoint and roaming add federation context



Wi-Fi roaming information may provide:

- Home identity provider, visited network details on AP level
- Identifiers: both privacy-preserving and identity disclosing
- Operator, venue and attachment-point context
- Roaming policy, service tier and clearing context
- Connection quality (IETF draft about Connect-Info)

RADIUS helps connect the access event to the roaming story.

Policy and access information



RADIUS can provide, assign and enforce settings such as:

- VLAN assignment
- Filter or ACL name
- Role or service class
- Quarantine or restricted access
- Priority or QoS-related policy

One can then match the access decision result to the intent.

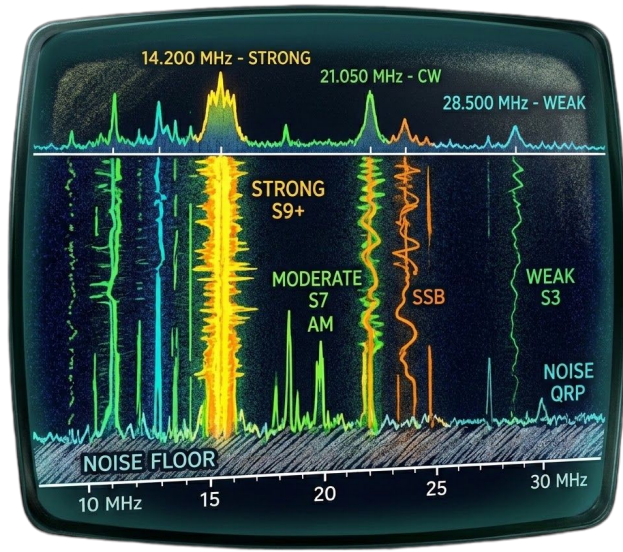
Accounting as behaviour telemetry

Accounting records can show:

- IP address information
- Start, interim update and stop lifecycle
- Session duration
- Traffic amounts: Input/output octets
- Termination causes
- Location changes, movement paths (Called-Station-Id), connection points
- Signal / connection quality information / statistics



Detection examples: small signals, useful context



- Same identity appears in unlikely locations
- Connections happening outside working hours
- Endpoint appears on an unexpected fixed port
- Wi-Fi session uses an unexpected settings or VLAN
- Roaming rejects spike for one provider or venue
- Low-use device suddenly transfers high volume
- Reauthentication failures at a switch, AP or site

Vendor-specific attributes: useful, but messy

VSAs can add valuable context:

- Endpoint category, posture, role or site metadata
- Controller or NAC-specific policy results
- Roaming service, provider and charging context
- More precise failure classification

But the goal is consistent access context, not vendor analytics.

```
Chargeable-User-Identity-Request:
  "58327a4e566a524443455f7a50372d75765f354e7a6f3836765f476144382
  26f63335048386a5f6b656b7036466d6c34"
Operator-Name: NULL
✓ RADIUS-Request-Attrs: [ 40 items
  ✓ 0: { 3 items
    name: "cisco-avpair"
    type: "string"
    value: "dc-profile-name=Linux-Workstation"
  }
  ✓ 1: { 3 items
    name: "cisco-avpair"
    type: "string"
    value: "dc-device-name=Unknown Device"
  }
  ✓ 2: { 3 items
    name: "cisco-avpair"
    type: "string"
    value: "dc-device-class-tag=Workstation:Linux-Workstation"
  }
  ✓ 3: { 3 items
    name: "cisco-avpair"
    type: "string"
    value: "dc-certainty-metric=10"
  }
}
```

WBA / OpenRoaming VSA examples

Public WBA VSAs illustrate the enrichment pattern:

- WBA-Offered-Service: service tier context
- WBA-Identity-Provider: identity provider attribution
- WBA-Financial-Clearing-Provider /
WBA-Data-Clearing-Provider
- WBA-Linear-Volume-Rate: charging model context
- Enhanced Reply-Message: richer reject reasons

These are vendor-specific attributes, not IETF-standard RADIUS attributes.

Normalisation of the RADIUS attributes

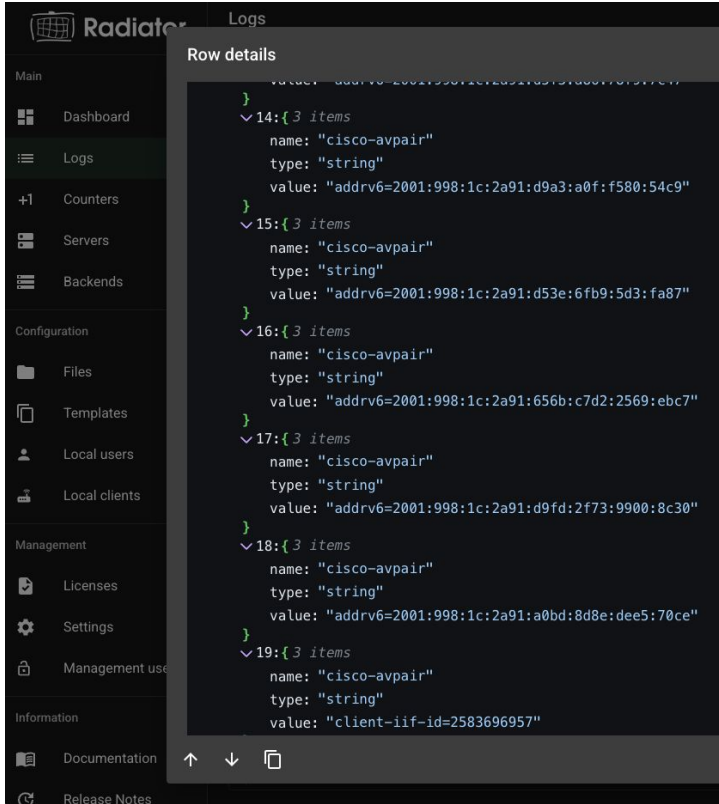
To refine RADIUS information:

- Decode standard and selected vendor dictionaries
- Parse inconsistent MAC, SSID, port and Connect-Info formats
- (combine authentication and accounting records into sessions)
- Preserve raw and unknown attributes for troubleshooting
- (re-)map to stable fields for analytics

Packets -> **Decoded attributes** -> **Normalised format** -> **Enriched log context**



Example: Converting RADIUS to JSON



The screenshot shows the Radiator web interface. A 'Row details' modal window is open, displaying a list of RADIUS log entries. The entries are numbered 14 through 19, each containing a 'name' and a 'value' field. The 'name' field is consistently 'cisco-avpair' and the 'value' field contains various RADIUS attributes.

```
Row details
value: "addrv6=2001:998:1c:2a91:d9a3:a0f:f580:54c9"
}
14: { 3 items
  name: "cisco-avpair"
  type: "string"
  value: "addrv6=2001:998:1c:2a91:d9a3:a0f:f580:54c9"
}
15: { 3 items
  name: "cisco-avpair"
  type: "string"
  value: "addrv6=2001:998:1c:2a91:d53e:6fb9:5d3:fa87"
}
16: { 3 items
  name: "cisco-avpair"
  type: "string"
  value: "addrv6=2001:998:1c:2a91:656b:c7d2:2569:ebc7"
}
17: { 3 items
  name: "cisco-avpair"
  type: "string"
  value: "addrv6=2001:998:1c:2a91:d9fd:2f73:9900:8c30"
}
18: { 3 items
  name: "cisco-avpair"
  type: "string"
  value: "addrv6=2001:998:1c:2a91:a0bd:8d8e:dee5:70ce"
}
19: { 3 items
  name: "cisco-avpair"
  type: "string"
  value: "client-iiif-id=2583696957"
```

```

  0: "service-type=Framed"
  1: "audit-session-id=F7FFFF0A00031F4C929F7B8D"
  2: "method=dot1x"
  3: "addrv6=fe80::203:7fff:fec2:43"
  4: "addrv6=2001:998:1c:2a91:280b:4ee8:b7ae:26d9"
  5: "addrv6=2001:998:1c:2a91:d5f3:a86:78f9:7c47"
  6: "addrv6=2001:998:1c:2a91:d9a3:a0f:f580:54c9"
  7: "addrv6=2001:998:1c:2a91:d53e:6fb9:5d3:fa87"
  8: "addrv6=2001:998:1c:2a91:656b:c7d2:2569:ebc7"
  9: "addrv6=2001:998:1c:2a91:d9fd:2f73:9900:8c30"
 10: "addrv6=2001:998:1c:2a91:a0bd:8d8e:dee5:70ce"
 11: "client-iiif-id=2583696957"
 12: "vlan-id=145"
 13: "cisco-wlan-ssid=roam.fi"
 14: "wlan-profile-name=roam.fi"
]
```

Securing RADIUS information

```
Files
Instance Id R00

← 30_backends-radsec-roaming.radconf

3  backends {
5    radius "radsec-auth.fi-eduroam" {
101
102      post-proxying {
103        filter {
104          # do not accept the following attributes in the RADIUS reply
105          Acct-Interim-Interval;
106          Airespace-WLAN-Id;
107          cisco-avpair;
108          Tunnel-Type;
109          Tunnel-Medium-Type;
110          Tunnel-Private-Group-ID;
111        }
112      }
113    }
}
```

RADIUS-requests and replies may contain identity, device, location and policy data.

RADIUS replies and CoA requests may also contain instructions to alter user/device network access parameters.

Integration considerations:

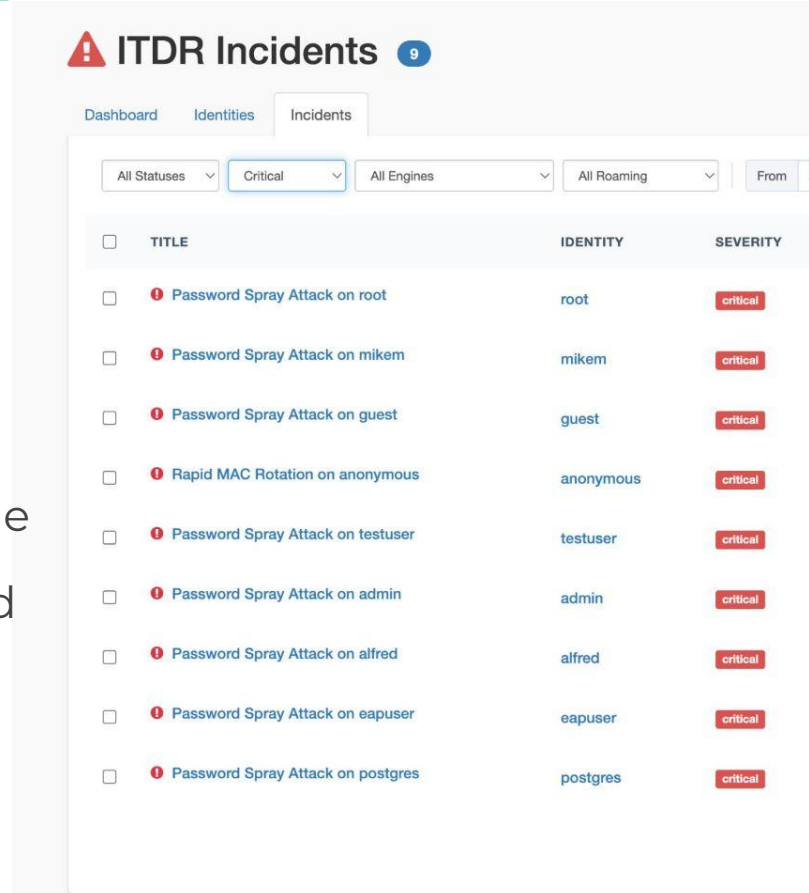
- Use RadSec / RADIUS over TLS where paths cross untrusted or administrative boundaries
- Filter all inbound and outbound information and instructions you do not want get
- Move RADIUS information and logs quickly to a log processing / analytics / storage solution, which has role-based access control, retention times and audit logs to secure the information

Using RADIUS to expand your awareness

RADIUS context can enrich:

- SOC timelines and incident information
- SIEM and log analysis and searches
- xDR, DHCP, DNS, VPN and identity correlation
- Asset-inventory validation
- Anomaly models for movement, access type, access times, policy and traffic volume

AI solutions can help identifying anomalies and processing all this information. Some (e.g. IronWiFi ITDR) can be configured to do active response as well.



The screenshot displays the 'ITDR Incidents' dashboard. At the top, there is a navigation bar with 'Dashboard', 'Identities', and 'Incidents' tabs. Below the tabs are several filter dropdowns: 'All Statuses', 'Critical', 'All Engines', 'All Roaming', and 'From'. The main content area is a table with columns for 'TITLE', 'IDENTITY', and 'SEVERITY'. The table lists ten incidents, all of which are 'critical' in severity. Each incident title starts with a red exclamation mark icon and describes a 'Password Spray Attack' on a specific user or a 'Rapid MAC Rotation' on an anonymous user.

<input type="checkbox"/>	TITLE	IDENTITY	SEVERITY
<input type="checkbox"/>	🚨 Password Spray Attack on root	root	critical
<input type="checkbox"/>	🚨 Password Spray Attack on mikem	mikem	critical
<input type="checkbox"/>	🚨 Password Spray Attack on guest	guest	critical
<input type="checkbox"/>	🚨 Rapid MAC Rotation on anonymous	anonymous	critical
<input type="checkbox"/>	🚨 Password Spray Attack on testuser	testuser	critical
<input type="checkbox"/>	🚨 Password Spray Attack on admin	admin	critical
<input type="checkbox"/>	🚨 Password Spray Attack on alfred	alfred	critical
<input type="checkbox"/>	🚨 Password Spray Attack on eapuser	eapuser	critical
<input type="checkbox"/>	🚨 Password Spray Attack on postgres	postgres	critical

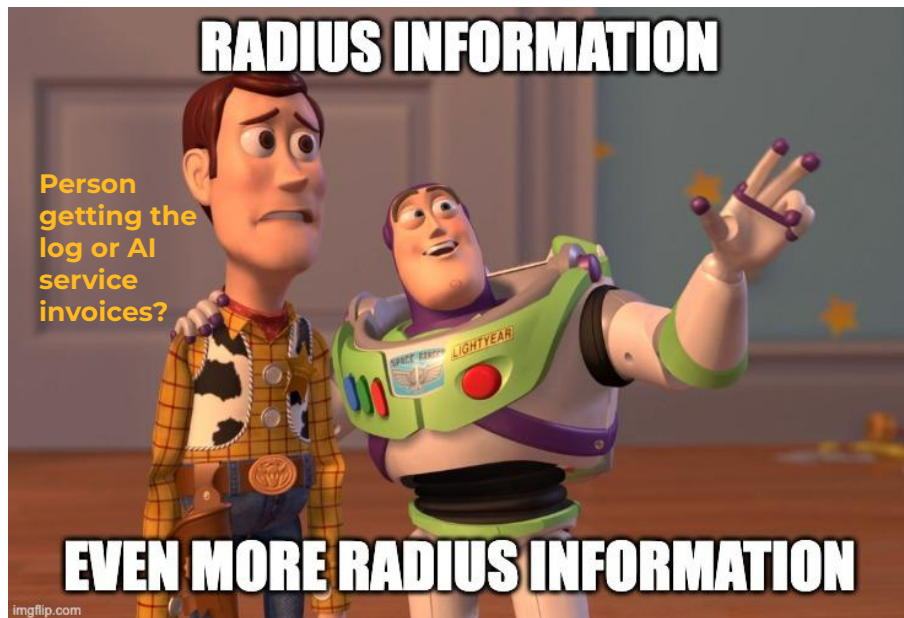
Automated, active response with RADIUS

With dynamic authorisation (CoA, Reverse-CoA, Passpoint attributes) with RADIUS you can:

- Terminate or authorise connections
- Assign quarantine VLAN or filters
- Policy updates during a session
- Disconnect misbehaving, suspicious devices / users

But use guardrails: authorisation, audit, testing and check the trust borders.

Future directions



- Common RADIUS as JSON format
- Wi-Fi Quality Metrics (Connect-Info)
- Wi-Fi Sensing?
- Emergency services and location support
- Privacy improvement, but at the same time even more options for location (tracking)
- Privacy first EAPs (EAP-PPT?)
- RADIUS information from the home access points (Per Device Credentials from external RADIUS)

RADIUS provides much more than just Authentication, Authorisation and Accounting.

RADIUS provides also information to monitor your infrastructure, identify and detect anomalies and means to take action to handle them.