Advanced eduroam Service Engineering Components (pre-introduction to Tech Spec)

It is recommended that organisations providing eduroam services should introduce the features/adjust their services as described below. It is intended that the elements will ultimately make their way into the Technical Specification.

Network segregation

While the Technical Specification requires the segregation of guests and home users onto separate networks, this requirement has not included recent cyber security advice to segregate different classes of home users into separate networks as well.

Therefore, it is eduroam(UK)'s recommendation to follow security advice in this regard and separate classes of home users (such as students/learners and staff) into different networks by functional requirement. The cyber security landscape evolves faster than the technical specification does (or needs to), and perceived threats should inform the design of your network infrastructure.

For example, learners and students do not require (and probably would never need to) access core infrastructure such as domain controllers, switches, wireless controllers, or finance systems, and as such should be segregated onto a network that does not provide access to such core infrastructure. Similar requirements may be applied to staff also; network engineering and IT staff may require access to network infrastructure but business administrative staff do not, and as such, additional staff networks may be defined for staff segregation.

Components that were included in Technical Specification v1.5 - released Q3 2023

The eduroam(UK) Technical Specification was updated to include:

- a) Organisations providing Wi-Fi Visited services in the 2.4GHz or 5GHz RF bands MAY implement WPA3-Enterprise in transition mode; Protected Management Frames (PMFs) MAY be implemented but MUST be set to ‘Supported’ rather than ‘Required’.
- b) Organisations providing a Wi-Fi Visited service in the 6GHz RF band, which requires implementation of WPA3-Enterprise, MUST NOT enable 192-bit security.
- c) ?Recommendation - WPA3-Enterprise in transition mode SHOULD be implemented in the 2.4GHz and 5GHz RF bands.

What RF bands (2.4GHz, 5GHz and 6GHz) eduroam organisations use to provide Wi-Fi services and how these are set up remains at the discretion of the individual participating member organisations. It is recommended that if organisations deploy 6GHz Wi-Fi, eduroam should in addition continue be provided at least over the 5GHz band.

Components that were included in Technical Specification v1.4 - released 2014

NAPTR Records for organisations using non-country-code realms - mandatory. Due to the growing number of organisations using non-country-code realm names (e.g. camford.org and ja.net rather than camford.ac.uk) it will be a requirement that any new request to utilise such realms will only be accepted on condition that the organisation creates a NAPTR record in DNS to support RadSec DD. This is to enable NREN federation RADIUS servers (or the European TLRs if necessary) to perform RadSec Dynamic Discovery lookups to forward authentication requires directly to the UK NRPS, thereby reducing the number of RADIUS hops involved.

An implication of this is that the DNS Management servers for such organisations will have to support NAPTR records. This means that Microsoft Windows Server 2003 DNS Server and Windows 2008 non-R2 DNS Servers, which lack NAPTR record capability, will not be suitable and so affected organisations will need to deploy alternatives.

It will be a stong recommendation that existing members with non-country-code realms should also create NAPTR records. This will become a mandatory requirement from January 2016, after which date there is no guarantee that the existing European special RADIUS routing settings will not be disabled. This notice period provides organisations with a sufficently long period of time to implement NAPTR-capable DNS management servers.

The rationale for the change from recommendation to requirement is that in order to support organisations requiring such realm names using standard RADIUS routing, the European top level RADIUS servers have to include specific routing for each and every realm and this is now becoming unmanageable. Nb the requirement will NOT apply to organisations using

realms ending in .uk, although such organisations would also benefit from the establishment of NATPR records and this remains a strong recommendation.

Accounting - RADIUS Accounting will be removed in Tech Spev v1.4

- -

Components that are or became strong recommendations in Technical Specification 1.3

WPA/TKIP - strongly recommended NOT to be supported. WPA/TKIP is deprecated. Permission to support this cipher will be withdrawn in the medium term. Whilst established members of eduroam(UK) may still offer support for this, new joiners MUST ONLY provide WPA2/AES. Any organisation still providing WPA/TKIP should seriously consider withdrawing it from their networks as soon as possible. (Appeared in v1.3)

NAPTR Records in DNS - recommended. This cannot be made mandatory since some organisations employ DNS Servers that do not support such records (appeared in v1.3).

- -

Components that are or became strong recommendations in Technical Specification 1.2

The following components are strongly recommended but cannot be made mandatory due to lack of universal support in systems deployed for eduroam services

Chargeable User Identity should be requested in Access-Requests by Visited organisations if possible (appeared in v1.2)

Chargeable User Identity should be added if possible to RADIUS responses by Home organisations in accordance with RFC4372 when solicited in Access-Requests from Visited organisations (appeared in v1.2)

IPv6 should be implemented (appeared in v1.2)

Inclusion of VLAN assignment attribute in Access-Accepts should be avoided where no bilateral agreement exists (appeared in v1.2)

Load balancing of traffic to NRPS should be implemented on NRPS (appeared in v1.2)

Operator-Name should be inserted wherever possible in Access-Requests (appeared in v1.2)

Elements that became mandatory requirements in Technical Specification 1.2

Main mandatory requirements changes introduced in 1.2:

1 Emphasised that only RFC 4282 compliant usernames (of the form userID@realm [1]) to be employed for user authentication both for roaming users and for users when at the Home site.

2 Mandatory requirement that Visited sites must not forward malformed usernames to the NRPS (e.g. usernames with realms that are malformed, typos, bad higher level domain).

3 Specification of RADIUS parameters to be logged now include User-ID, CUI and CSI.

4 Improvement in service status information that must be published on the orgs eduroam service information web site.

5 Removed the different tiers of technical standards from the specification (JRS2/JRS3).

6 Range of Tiers replaced with a ‘base engineering standards’ together with evolutionary progression path for introduction of enhanced standards.

7 Relating to ORPS using RadSec (TLS over TCP) to NRPS i) definition of use of TCP 2083 ii) only Geant eduPKI certificates to be used.

8 Home organisation ORPS must not reject based on NAS-Port-Type not matching a specific value and must process all auth requests against a user database.

9 It is now permitted that NASs can connect multiple users to a single port (to accommodate controller-based systems).

10 Due to simplification of Tiers, although not recommended, NAT permitted regardless of whether or not IPv6 supported.

11 Mandatory ports and protocols additions:

- IP 41 (IPv6 Tunnel Broker ServiceTCP/50)
- TCP/3128(SQUID Proxy)
- TCP 8080(HTTP Proxy)
- TCP/50 (ESP)
- TCP/51(AH)
- UDP/500(ISAKMP)

12 Removed requirement to support WPA/TKIP – replaced with permission that existing deployments may continue to do so until end December 2014, recommend to phase out asap.

13 All Visited sites MUST now support WPA2/AES and new joiners can only offer WPA2/AES.

14 Emphasized that all NASs must include CSI and NAS-IP-Address.

15 Broadcasting of eduroam SSID at non-operational sites must be limited to test environment.

16 Due to deprecation of PAP authentication, test accounts must now use the EAP method normally used at the organisation and not PAP.

17 List of attributes that must not be filtered out updated to reflect recommendation to use Operator-Name and CUI (ie O-N and CUI must not be filtered out).

The eduroam(UK) Technical Specification will shortly be updated to include:

.

- a) Organisations providing Wi-Fi Visited services in the 2.4GHz or 5GHz RF bands MAY implement WPA3-Enterprise in transition mode; Protected Management Frames (PMFs) MAY be implemented but MUST be set to ‘Supported’ rather than ‘Required’.
-
- b) Organisations providing a Wi-Fi Visited service in the 6GHz RF band, which requires implementation of WPA3-Enterprise, MUST NOT enable 192-bit security.
-
- c) ?Recommendation - WPA3-Enterprise in transition mode SHOULD be implemented in the 2.4GHz and 5GHz RF bands.

What RF bands (2.4GHz, 5GHz and 6GHz) eduroam organisations use to provide Wi-Fi services and how these are set up remains at the discretion of the individual participating member organisations. It is recommended that if organisations deploy 6GHz Wi-Fi, eduroam should in addition continue be provided at least over the 5GHz band.

Source URL: https://community.jisc.ac.uk/library/janet-services-documentation/advanced-eduroam-service-engineering-components-pre

Links
[1] mailto:userID@realm