

draft-ietf-radext-radius-fragmentation-04

draft-ietf-radext-radius-fragmentation-04

- Received comments from Jim Schaad
- Some corrections regarding RFC 2119 language
- Some minor changes and typos
- Added new section dedicated to the flag “T”
 - Draft now updates RFC 6929
 - Describes how the Long Extended Type attribute format is updated

draft-ietf-radext-radius-fragmentation-04

- State attribute value uniqueness
 - Changed from “globally and temporally unique” to “temporally unique to the server”
- Added recommendation
 - Servers to include a State attribute on their Access-Accept packets
 - To allow clients to perform further interactions (e.g. more authorization exchanges)

draft-ietf-radext-radius-fragmentation-04

- We found an issue that affected previous versions
 - RFC 2865 specifies that :
 - *An Access-Request MUST contain either a User-Password or a CHAP-Password or a State.*
 - *If future extensions allow other kinds of authentication information to be conveyed, the attribute for that can be used in an Access-Request instead of User-Password or CHAP-Password.*
 - But the first chunk of the pre-authorization phase :
 - May not contain any
 - Depends on the type of the authorization attribute being transported , and the specific distribution of the attributes along the chunks.
 - The rest of the chunks will contain at least an State attribute, and thus they'd not be a problem

draft-ietf-radext-radius-fragmentation-04

- Fragmentation draft already stated that compliant servers will postpone all authorization and authentication handling until all of the chunks have been received.
- 04 version has added some lines clarifying that this postponement also affects to the verification of the inclusion of authentication attributes, which will be delayed until the original large packet has been rebuilt.
- We expect proxies to not drop these packets, as they will be precluding future extensions otherwise

draft-ietf-radext-radius-fragmentation-04

- If this is considered insufficient, then we would need to include some kind phony authentication attribute on the first chunk of the pre-authorization phase:
 - Eg. Empty EAP-Message attribute (RFC 3579 EAP-Start)
 - Eg. Phony CHAP-Password
 - Eg. Disposable State
 - Other?

draft-ietf-radext-radius-fragmentation-04

- 04 version prepared for LC