CoA Proxying

RADEXT - IETF 95
Alan DeKok
FreeRADIUS
Open Issues

• Proxy spoofing is always possible
• Can be minimized, but not prevented
• Mandatory attributes need to be removed before being sent to the NAS
• Comments from Peter Deacon
A CoA proxy MUST NOT send the NAS an attribute in a CoA packet, unless the NAS sent the attribute in an Access-Request or Accounting-Request packet.

or

All “server” attributes MUST be removed by the final proxy before the packet is sent to the NAS. This includes, but is not limited to, Proxy-State, Operator-Name, NAS-Identifier
Explanation

- When the NAS sends a packet to a local server, that server may add attributes to the packet
- Those attributes are NOT understood by the NAS
- The local server do the inverse process with CoA proxy
- i.e. remove any attributes it had added
Discussion?