# 802.1X and DHCP

RADEXT - IETF 97

Alan DeKok
FreeRADIUS

# The Problem

- DHCP is entirely unsecured.
- There are no ties between 802.1X and DHCP

# The proposal

- Create a DHCP signing key from the 802.1X MSK
- Use it to sign DHCP packets

# How does it work?

- RADIUS server generates the keys
- DHCP server uses them to verify / sign packets

# Exchanging keys

- The keys need to be exchanged
- This is done securely…
- via implementation-defined methods

# What does this mean?

- The AAA / DHCP servers can talk to each other
- They are run by people who talk to each other
- issues of “trust” are open to discussion

# Problems

- Many details not worked out.
- DHCP does not provide for capability negotiation
- 802.1X does not provide for capability negotiation
- No way for either end to signal that this is happening

# Questions

- Is this a good idea?
- Does it help security?
- Does it not hurt security?
- Can it be implemented?
- Will people implement it?

# Discussion?