Alternate Tunnel Encapsulation for Data Frames in CAPWAP:
draft-zhang-opsawg-capwap-cds-01

R. Zhang (China Telecom)
H. Deng (CMCC)
Z. Cao (CMCC)
R. Pazhyannur (Cisco)
S. Gundavelli (Cisco)
Problem Statement

**Supported Tunnel Modes**

- **User Traffic Locally Bridged**
  - Access Controller
  - WTP
  - Data Channel
  - Control Channel

- **User Traffic Tunneled**
  - Access Controller
  - WTP
  - Data Channel
  - Control Channel

**Desired Tunnel Mode**

- Separate Control Plane from Data Plane
- Why Local Bridging is not an option
  - SP may not be same as Access Network Provider
- Extend Local MAC mode
  - CAPWAP Data channel for 802.11 Mgmt frames and security
  - User Traffic tunneled to AR instead of AC
- Multiple Additional Tunnel Encapsulations supported
Proposal

• Incorporated changes based on last meeting discussion
  • Generalized tunnel types to include additional tunnel encapsulation

• Defined new IEEE 802.11 Message Elements
  • Supported Alternate Tunnel Encapsulations
  • Alternate Tunnel Encapsulation

• WTP announces capability in Discover/Join request
  • Support for additional Tunnel Encapsulation (L2TP, PMIPv6-IP/GRE, etc)

• AC may configure Tunnel Encapsulation during WLAN configuration
  • AC may also configure WTP with additional parameters to setup tunnel (for example, IP address of Access Router, shared secret, etc). This is not described in the current draft.
Discussion

• Feedback on mailer
  ✓ Add descriptive text on why this is needed
  ✓ Describe how AR will be discovered
  ✓ Document impact to RFC 5415 and RFC 5416
  ✓ Editorial changes

• Next steps
  • This is the third version (second major revision after original submission). Is it on track to get it adopted?