Issues on the CAPWAP list

CAPWAP session

7 Nov 2005

IETF64, Vancouver

Eval Rec: Base Protocol

Issue / Recommendation	R0
Description	Base Protocol
Reference	Evaluation Draft-00
Comments/Concerns	Primary recommendation Questions on why any candidate protocol with different auxiliary recommendations would not meet Objectives. LWAPP meets most of objectives. Known implementation variants. Thus evaluation team decided based on its set goals. Recommendations-set should be treated in their entirety and not just for the base protocol recommendation Recent poll indicating notable level of concern related to IPR.
Evaluation Recommendation	Use LWAPP as the base protocol: the most complete (in meeting objectives) & considered most flexible & extensible.
Consensus	<WG Agreement on the Base Protocol recommendation> Status: Open
[Notes]	

Eval Rec: Information Elements

Issue / Recommendation	R1
Description	Information Elements: Change request to expand the size of the type field in the message element header from 8 to 16 bits
Reference	Evaluation Draft-00, section 9.1.1
Comments/Concerns	No known concerns.
Evaluation Recommendation	As above in description
Consensus	Agreement on recommendation. Status: Closed?
[Notes]	

Eval Rec: Control Channel Security

Issue / Recommendation	R2
Description	Control Channel Security: evaluation team recommends use of DTLS (upcoming standard) as the security mechanism to protect in place of the proprietary method proposed by LWAPP
Reference	Evaluation draft-00, section 9.1.2
Comments/Concerns	pre-Discovery DTLS – establish DTLS with each AC to interrogate the rght AC to load-balance post-discovery DTLS: take the potential minimal risk of unprotected load-balance discovery and then establish based on chosen AC. question on security properties of DTLS that better meet
Evaluation Recommendation	None.
Consensus	Post-discovery DTLS is benign and does not pose a risk that is not already present in the initial ("client hello") exchange phase. Further – the sanity of AC-discovery can be validated after the fact (DTLS) – as necessary.
[Notes]	

Eval Rec: Local-MAC data tunneling

Issue / Recommendation	R3
Description	Support for Local-MAC user-data tunneling. This change request is to allow for 802.3 tunneling of user data in local bridging mode
Reference	9.1.3.1
Comments/Concerns	While this is achievable – it introduces yet another mode to support leading CAPWAP protocol to have to support three modes (as opposed to two earlier). AC can be realized as software-based module on a server platform (non-appliance). Avoids overhead of .11 (encryption, QoS) processing at AC. AC still needs .11 usage/control information to decide/enforce policies.
Evaluation Recommendation	Recommendation is to support this third mode
Consensus	support this third mode – tunnel user data in local bridging mode. Open w.r.t. whether it is a mandatory mode. Status:
[Notes]	

Eval Rec: L2 encapsulation

Issue / Recommendation	R4
Description	Removal of L2 encapsulation for data tunneling. Removal of L2 encapsulation from CAPWAP protocol specifications
Reference	Eval-draft-00 section: 9.2.2
Comments/Concerns	• No objections raised. • Can this remain in specifications as informational/optional?
Evaluation Recommendation	As above
Consensus	General Agreement to remove. Status:
[Notes]	

Eval Rec: GRE/L2TP Data Encap.

Issue / Recommendation	R5
Description	Data encapsulation standard: to make use of the L2TP or GRE encapsulation protocols instead of the proposed encapsulation in base protocol. The goal stated is re-use of code.
Reference	Eval-draft-00 section 9.2.3
Comments/Concerns	• GRE is fitter as alternative to UDP rather than alternative to LWAPP. • Unix-operating environ.'s 1:1 module dependency makes configuring same daemon difficult • LWAPP hdr. still needed to transport SNR/RSSI information
Evaluation Recommendation	As described above in the <description>
Consensus	Status: open.
[Notes]	<No counter-objections to LWAPP author's disagreement>

Eval Rec: Firmware Triggers

Issue / Recommendation	R6
Description	Firmware Triggers. Protocol state machine must support the ability to initiate the process for checking and performing a firmware update independently of other functions
Reference	Evaluation Draft (section 6.5); mailing list discussions
Comments/Concerns	Firmware operations have to be independent of other operations. Firmware check and update procedures should be able to be invoked at any operational state
Evaluation Recommendation	As per section 6.5
Consensus	<open>
[Notes]	

Eval: Default Mode - Logical Groups

Issue / Recommendation	R7
Description	Default mode for logical groups.
Reference	mailing list discussions; objectives draft section 5.1.1; evaluation draft(-00) section 6.1
Comments/Concerns	“The final CAPWAP protocol needs a default operation for logical groups for wired and wireless sections. The basic case is to map VLANs to BSSIDs which is simplest and most common. Logical group configuration must cover setup on both wired and wireless aspects of the network and include a link between the two.”
Evaluation Recommendation	Nothing specific.
Consensus	Status: closed?
[Notes]	

Issue: PMK Sharing

Issue / Recommendation	I0
Description	PMK sharing: when PMK is shared between WTPs running over an AC; the client has no way to distinguish this situation at transition-time between this genuine case and one of possible WTP compromise. PMK sharing is justified in the sense of
Reference	RFC4118 – security considerations section
Comments/Concerns	Security Reviewers and IESG asserted this situation must be resolved either by reference to any solution in IEEE or within realm of IETF/CAPWAP. None of the candidate protocols have addressed this concern.
Evaluation Recommendation	No recommendations on this matter.
Consensus/Status	<open>
[Notes]	

Issue: 802.11i operations

Issue / Recommendation	I1
Description	CAPWAP operations for IEEE 802.11i when encryption/decryption is located in WTP and authenticator function is located in AC.
Reference	Mailing list discussions & Objectives draft (5.1.10)
Comments/Concerns	• KeyRSC and KeyMIC values are maintained at point of encryption/decryption. 4-way exchanges and group-key exchanges from AC require accurate values. • This design issue can be accommodated by having the AC send the particular message of the 4-way exchange or group-key exchange to the WTP with unassigned KeyRSC and KeyMIC fields. The WTP then updates the fields with the prevailing counter values and forwards the message to the terminal.
Evaluation Recommendation	n/a
Consensus	<open>
[Notes]	

Issue: Local & Split-MAC Negotiations

Issue / Recommendation	I2
Description	Local & Split-MAC negotiations
Reference	Mailing list discussions & Objectives 5.1.11
Comments/Concerns	• Major distinguishing characteristics of WTP must be negotiated during WTP initialization. • Including (i) type of MAC (split, local), (ii) type of frames exchanged (native, 802.3, no frames) and (iii) type of IEEE 802.11i design (encryption and authenticator function on separate devices or on same device)
Evaluation Recommendation	N/A
Consensus	Status: <open>
[Notes]	

Issue: Firmware Download

Issue / Recommendation	I3
Description	In-band / out-of-band firmware downloads. Use the control channel path and the protection it offers or use other ‘out-of-band’ mechanisms such as ftp/sftp/scp.
Reference	mailing list discussions
Comments/Concerns	• Efficient recovery from (transfer) errors cited as favorable factor for out-of-band protocols. • Piggybacking the (download) function over existing SA of the CAPWAP channel transport has value.
Evaluation Recommendation	<As per evaluation draft section 6.5 & Objectives>
Consensus (open/resolved/non-issue)	<open>
[Notes]	<may be similar to R6>

Misc.: IPR claims

Issue / Recommendation	M0
Description	LWAPP IPR clear in disclosure and royalty-free offer if accepted for standardization
Reference	[mailing list series of discussions]
Comments/Concerns	• Not clear if that clause is impacted by subsequent Cisco declaration. • Still an open-source concern unless fashioned along RFC1822 or similar. • The recent poll for consensus on LWAPP as base protocol recommendation is seeing objections related almost solely to IPR concerns.
Evaluation Recommendation	N/A
Consensus	• WG has done its work of calling for and clearing up details to the extent the process allows • The claiming parties have met the IETF IPR reporting requirements <closed>
[Notes]	

Misc.: Firmware & RF certification

Issue / Recommendation	M1
Description	FCC certification of firmware downloads: firmware from one vendor used on another vendor hardware needs to re-qualify for FCC certification for RF.
Reference	[mailing list series of discussions]
Comments/Concerns	
Evaluation Recommendation	N/A
Consensus (open/resolved/non-issue)	Closed: Non-issue in the context of evaluation team recommendation of base protocol.
[Notes]	