Network Advertisement and Selection Proposal for IEEE 802.1af

1 Introduction

Network Advertisement and selection are enhancements to 802.1X defined in 802.1af to provide information about what is available to entities accessing the network and to facilitate the selection of a particular type of access.

Two types of messages are defined to provide network advertisement functionality. The first is a request which is used to probe a network to determine what types of access are available. The second is a response which indicates what is available from the network. It is possible for an authenticator to send an unsolicited advertisement response.

The primary piece of information that is conveyed in the network advertisement is the network identity (NID). The network identity is a string that identifies a network. A supplicant will typically associate a NID with a configuration profile that contains the parameters necessary to successfully use the network.

Network selection is carried using request response messages. In the network selection request the supplicant indicates the network it wishes to join. The network selection response provides the result of the selection. After the selection is complete network access may be granted or the authenticator may be prepared to begin execution of 802.1af or some other authentication protocol.

While this document focuses on new EAPOL packets types to support network advertisement and selection some of the TLVs defined for the network advertisement and selection messages can be used in other EAPOL frames or other protocols such as LLDP [802.1AB].

Note that all protocol messages defined here are carried within packet types of EAPOL-NASP. Extending EAPOL-EAP packets to carry the selection response has the potential of decreasing the MTU available to EAP which could complicate existing mechanisms.

2 Protocol Operation and State Machine

2.1 Network Advertisement Operation

The network advertisement protocol is a request response protocol that is triggered by the supplicant accessing the network. This protocol should not require any state to be maintained on the authenticator. The network advertisement protocol is carried out

using messages of packet type EAPOL-NASP. This exchange is carried out in clear text packets.

The advertisement request (AD-REQ) may be sent by the supplicant to a unicast address of an authenticator or a multicast address specified in 802.1af at any time. This includes while an authentication is in progress.

The advertisement response (AD-REP) from the authenticator consists of two sections. The first is the authentication information section that contains information about the authenticator and the second section is the Network Identity (NID) entries. The AD-REP may be sent unsolicited by the authenticator to inform the supplicant of its choices.

The currently defined information for the authenticator is a key management domain. The key management domain is used by the supplicant to determine which cached keys it may have are usable with a particular authenticator. A supplicant key cache would typically be organized by NID name and key management domain.

The NID entries are a list of NIDs with associated optional attributes. A NID consists of a NID name that a supplicant associates with a configuration profile and a list of NID properties.

NID properties include:

> Default network – this indicates to the supplicant that this is the NID to select if it does not recognize any of the other NIDs in the AD-REP. This is the network that would be selected if no network selection is explicitly performed.
> Fallback available – this indicates to the supplicant that a fallback network providing limited access is available even if authentication fails.
> 802.1X – this indicates that 802.1X is supported by this NID
> 802.1af – this indicates that 802.1af is supported by this NID
> Higher layer authentication – this indicates that some higher layer authentication protocol can be used for authentication

[Q: do we want to include properties for MKA and/or 802.1AE?]

In an advertisement only one NID each of the following types may be marked default: 802.1X, 802.1af, and Higher layer authentication. Additional NID properties, such as proprietary extensions, can be included as TLVs in the NID entry.

2.2 Network Advertisement State Machine

TBD

2.3 Network Selection Operation

The network selection protocol is a request response protocol initiated by the supplicant. The network advertisement protocol is carried out using messages of packet type EAPOL-NASP. This exchange is carried out in clear text packets.

The supplicant sends a network selection request (SEL-REQ) containing a NID that is wishes to attempt to use with the properties set that the supplicant wishes. The SEL-REQ message is used to select any type of network including one with 802.1X and 802.1af capabilities.

The network then responds with a network selection response (SEL-REP) that indicates if the selection is successful and what NID was selected. The selection process may change the state of the authenticator such that it optimizes for the selected network profile type. The authenticator ignores the default network and fallback available properties. If more than one of 802.1X, 802.1af or higher layer authentication properties is set then the authenticator returns a failure of 'conflicting selection' to the supplicant. If the authenticator is currently involved in an authentication exchange with the supplicant it may return a status of 'busy'.

It is valid for the supplicant to skip the selection process and go straight into 802.1X, 802.1af or a higher layer mechanism, in this case a default NID will be assumed by the authenticator.

2.4 Network Selection State Machine

TBD: Note: We'll need to reconcile the state machine for collisions (or floods) when a NAD may get both or multiple new network selection requests

3 Network Advertisement and Selection Messages

Network advertisement and selections messages are defined within a new 802.1X EAPOL PDUs with a Packet Type of EAPOL-NASP.

The encoding, validation and decoding of each NASP-PDU is consistent with the general rules for EAPOL PDUs specified in 9.2 and 9.5. Each NASP-PDU contains a message type followed by one or more pieces of information in Type-Length-Value format. The TLV format and TLV processing rules are consistent with 802.1AB although the type space is separate. Where a particular TLV is useful in both LLDP and NASP coordination between TLV types is desirable.

Protocol Version
Packet-Type EAPOL-NASP

Packet Body Length
Message Type (1 byte)
TLV 1
TLV 2
…
TLV n

There are 4 NASP message types defined in this specification: Advertisement request (AD-REQ), Advertisement Response (AD-REP), selection request (SEL-REQ) and selection response (SEL-REP). The specific format for these messages is defined in following sections.

The TLVs following the message type are identical in format to the 802.1AB TLVs as follows:

TLV Type (7 bits)	TLV information string length (9 bits)	TLV information String (0 <= n <= 511)

The order of the TLVs is important since they may be grouped together within the context of a message.

3.1 AD-REQ Format

The NASP-PDU of the AD-REQ is as follows:

AD-REQ message type
List of optional TLVs

There are no required TLVs for the AD-REQ message so any of the optional TLVs should be ignored if not understood by the receiver.

3.2 AD-REP Format

The NASP-PDU portion of the AD-REP is as follows:

AD-REP message type
Optional authenticator TLVs
NID TLV (1)
Optional TLVs for NID (1)
NID TLV (2)

Optional TLVs for NID (2)
…
NID TLV (n)
Optional TLVs for NID (n)

The AD-REP consists of two main sections: authenticator information and Network Identity entries. The authenticator information is optional and consists of the TLVs at the beginning of the message before the Network Identity Entries. The beginning of the network TLVs section is indicated by the first NID TLV in the message. Each Network Identity entry starts with a NID TLV followed by 0 or more optional TLVs that describe the network identity. The end of a network Identity entry is indicated by the next NID TLV or the end of the message. Any TLVs that are not recognized should be ignored.

The following TLVs are defined for inclusion in the AD-REP:

Key Management Domain TLV (Authenticator Information)
Network Identity TLV (NID TLV)

3.2.1 Key Management Domain TLV

The key management domain TLV is authenticator information TLV that provides information about the transmitting authenticator's key management domain. This is useful in identifying which cached keys are usable in a particular location.

Key Management domain TLV (7 bits)	TLV information string length (9 bits)	TLV information String (0 <= n <= 255)

The key management domain TLV information string contains a string of UTF-8 characters up to 255 bytes in length. Ports the share the same Key Management Domain TLV can be assumed to share the same key cache.

3.2.2 Network Identity TLV (NID TLV)

The network Identity TLV contains basic information about a network such as its name and its authentication capabilities.

NID TLV (7 bits)	TLV Information String length (9 bits)	NID properties (4 bytes)	NID Name (0 <=n <=255)

The NID name is a UTF-8 encoded string used to identify a network profile supported by this authenticator. The maximum length for a NID name is 255 bytes. The bit vector is a list of properties supported by the NID. The currently defined bits are listed below:

Bit	Property
0	Default Network
1	Fallback network available
2	802.1X
3	802.1af
4	Higher Layer Authentication Available
5-31	reserved

Additional properties that are vendor or site specific can be included as optional TLVs in the Network Identity entry following the network identity TLV. The default network is the network an entity should attempt to use if it does not recognize any of the network identities. The fallback network available flag indicates that the supplicant may have some limited level of network access even if authentication fails.
Note: should we include an indication of key management capabilities in the NID property bit vector?

The Network Identity TLV defines the start of a Network Identity entry. Additional TLVs may be included after a NID TLV and before the next NID TLV to describe additional attributes of the TLV.

3.3 SEL-REQ Format

The network selection request message is used to select a particular network. If the supplicant is selecting a default network then it may skip network selection and start the authentication process. The NASP-PDU of the SEL-REQ looks as follows:

SEL-REQ Message
NID TLV
Optional TLVs for NID

The SEL-REQ contains the single NID TLV that is being selected. Optional TLVs may be included that provide additional information about the selection. An authenticator can ignore these TLVs if it does not understand them.

3.4 SEL-REP Format

The network selection response message is used by an authenticator to indicate the status of the selection. The NASP-PDU of the SEL-REQ looks as follows:

SEL-REP Message
Status TLV
NID TLV
Optional TLVs for NID

The NID TLV indicates the network profile that was selected along with any optional TLVs describing the type of profile. The Status TLV indicates whether the selection succeeded or not.

3.4.1 Status TLV

Status TLV (7 bits)	TLV information string length (9 bits)	Status (1 byte)

The status TLV communicates a one byte status code. The status codes are allocated as follows:

Code	Status
0	Successful
1	Busy
2	Invalid or unsupported NID property
3	Invalid or unavailable NID name
4	Conflicting selection
5-255	reserved