Proposed text modifications for Network Announcement and selection for 802.1X-REV

1 Overview

This section outlines the suggest changes. Section 2 provides specific modifications to the text of the document. Section 3 describes an alternate encoding for specific and generic attributes.

1.1 Announcements

Announcements may be solicited or unsolicited. An announcement may contain information that is specific for a single supplicant on a port or information that is generic for all supplicants on a port.

1.1.1 Announcement sent in response to requests

An announcement may be requested in 1 on 2 ways: using an EAPOL-Announcement-Req and using the request bit in the EAPOL-Start. There should be an upper limit on the time a supplicant needs to wait for the response, an announcement should be sent within 200ms (perhaps even sooner) of receiving a request. In addition, the responses should be sent unicast to the supplicant with information that is specific for that supplicant. If the announcement is sent in response to an EAPOL-start containing a valid NID Set TLV then the response announcement shall indicate the selected NID by setting the requested bit in the information-access TLV. The announcement shall precede any EAPOL-EAP packets sent to the supplicant.

Document Change (section 2.2) – Define upper limit on time to respond to request, clarify that responses should be unicast, define order of response

1.1.2 Generic versus Specific announcements

Announcements may contain generic information that is valid for all supplicants attached to the port or the announcements may contain information that is specific to a particular supplicant. Specific announcements must be unicast to the supplicant. Generic information may be unicast or multicast by the authenticator. Currently there is no way to differentiate between generic and specific information as they are all included in one TLV and there is no indication in the advertisement.

Document Change (section 2.2, 2.3; alternate approach in section 3) – Differentiate between generic and specific information
Document change (not completed) – Include rules for compliant unicast and non-unicast frames.

1.2 Selection of a NID

A NID may support 802.1X based authentication, non-802.1X (higher layer) authentication processes or both. EAPOL-EAP and/or EAPOL-MKA messages are used to carry out 802.1X authentication. Higher layer authentication is typically carried out using IP based protocols such as HTTP. In order to perform higher layer authentication the supplicant obtains an IP address on a network that allows authentication and limits other access. In many cases, it is desirable for the supplicant to obtain upper layer addresses and parameters (through a mechanism such as DHCP) that are valid for the NID if they successfully authenticate. This eliminates the need for the supplicant to acquire new parameters because the network changes when authentication completes. To achieve this the supplicant needs to select the NID before it attempts to acquire higher layer network parameters.

Since supplicants currently do not know what is supported by the network, many will attempt to obtain an IP address in parallel with 802.1X processing. In some environments, administrators do not want to assign an address initially if the supplicant will successfully complete 802.1X, so it is also common for deployments to prevent supplicants from obtaining higher layer address parameters until 802.1X has completed, failed or timed out. In this case it is useful for the supplicant to know when it can attempt to gain higher layer parameters, since the port may be initially closed. It is also useful for the supplicant to be able to indicate that it intends to use higher layer authentication for a particular NID.

1.2.1 Selection of non-802.1X mechanisms

The current specification does not indicate how non-802.1X (higher-layer) authentication can be selected. EAPOL-Start is currently used for selection with 802.1X EAP by including a NID TLV. This NID TLV indicates the beginning of a set of parameters. If the supplicant wants to perform non-802.1X (higher-layer) authentication for the NID then it should include a TLV in the NID set indicating this. One possibility is to use an access information TLV and/or a URI TLV to indicate non-802.1X access. In the announcement NIDs offering a non-.1X authentication choice will include an Access-Information and URI TLV indicating the how to access this higher layer authentication mechanism. When the authenticator receives an EAPOL-Start with this TLV then it should not attempt to initiate EAP or MKA (although it should still respond to these messages).

Document Change (Section 2.3, 2.4, 2.6) – define URI TLV add text to describe its meaning in the EAPOL-Start NID Set. Describe the use of access information TLV in EAPOL-Start.

1.2.2 Other Selection Mechanisms

It is possible for a NID to be selected by default when the port comes up. MKA also provides selection mechanism since the CAK used for MKA is associated with a NID and therefore is a selection mechanism in itself. However, since EAPOL start is not used with MKA, the requested NID in the announcement is not set if MKA is executed by itself. Once MKA completes successfully the operation NID is indicated. This announcement information may be carried within protected MKA messages instead of announcements. The announcement is protected with MACSEC if it is available. The NID may not be changed until one of the peers stops responding to MKA packets or establishes a new MKA SA.

Document Change (section 2.3, 2.5)– Clarify different selection mechanisms (implicit default, EAPOL-Start, MKA) and how they interact.

1.3 Access Information

The Access Information TLV communicates information to the supplicant about the available authentication methods and the status of the current connectivity. The supplicant is expected to be able to make use of the information in the message.

1.3.1 Authentication Mechanisms

The following authentication mechanisms

EAP
EAP + MKA
EAP + MKA + MACSEC
MKA
MKA + MACSEC
Non-802.1X (Higher layer)
Open

The EAP and MKA combinations are executed using 802.1X packet types between the authenticator and supplicant. Non-802.1X indicates that this NID supports authentication mechanisms in addition to 802.1X mechanisms that operate at a higher layer. In order to use these mechanisms the supplicant will have to open its port to obtain addresses and other higher layer parameters. In some environments network administrators do not want provide supplicants with higher layer addresses until they succeed, fail or timeout 802.1X. This is because many supplicants will attempt to obtain an address in parallel with starting 802.1X. Delaying access to higher layer services prevents these supplicants from getting higher layer parameters and initializing the higher layer before they have a chance to do 802.1X authentication.

Open indicates that no access control is being performed and the supplicant can expect to gain access to this NID without any authentication.

Document Change(Section 2.1,2.5) – Clarify that presence of Non-802.1X does not necessarily mean that higher layers are available immediately

1.3.2 Port Status

The authenticator can indicate the status of its port. The status of the port may be indicated with the following values:

Operational – expected access – Port is connected to the NID and access is unmodified
Operational – modified access – Port is connected to the NID, but access restriction have be applied beyond what is expected
Restricted – Higher layers are available, but the port is not connected to specified NID
Closed – Port is not connected to NID, higher layers not available. .1X is possible if advertised.

It is useful for the supplicant to know if it is able to obtain higher layer parameters for the purpose of non-802.1X authentication and authorization. A network authenticator may provide non-802.1X authentication mechanisms such as web authentication locally, so its port may not be fully operational, but it may provide the ability to perform higher layer authentication.

Only one NID should be operational at a time unless two or more NIDS are aliases for the same NID.

Document change (section 2.1, 2.5) – Create 2 bit port status indicator to replace operational and access level indication

Document change (section 2.1, 2.5) – Clarify that only one NID should be operational at a time unless two or more NIDS are aliases for the same NID.

1.3.3 Supplicant Actions

In addition to indicating the status of the port the authenticator can indicate what it expects the supplicant to do in order to change its access. The authenticator also can indicate what action the supplicant should take:

Authentication needed – the authenticator expects the client to authenticate to change port status. This could be either 802.1X authentication or non-802.1X authentication if both are supported.
Non-802.1X process in progress – The authenticator is engaged in a higher layer process, access may change when process completes. The 802.1X supplicant is not expected to do anything at this point.

Document Change (section 2.1, 2.5) – two bits, one for authentication needed and one for non-802.1X process in progress.

1.3.4 Fallback

It is possible for the authenticator to provide fallback access if the authentication fails. This can be indicated by indicating limited non-802.1X communication. Fallback is a capability rather than a status. If a port initially announces closed, but also announces fallback then this indicates that it will provide restricted access in case of authentication failure.

Document Change(section 2.1, 2.5) – Add indication of fallback and remove restricted from auth requirements list

1.3.5 Network change

When the network a supplicant is attached to changes it may need to reacquire high level parameters. The supplicant can detect this when the operational state of a NID changes, however it is possible that a change in NID does not require a change in address or other higher layer parameters. It may be useful to have an additional status parameter that indicates address scope. The address scope may be independent of the NID or indicated as part of the NID status. When the address scope changes it is a signal to the supplicant that new higher layer parameters are required.

Document Change (not completed) – Describe the meaning of Operational state of a NID changes.
Document Change (not completed) - Define and describe address scope attribute.

2 Proposed Changes

2.1 Announcement Information (Section 10.1)

Text following "Clause 11 specifies additional detail and encodings for the following:"

A) Supplicant specific
B) Port Status
    a. Operational Expected – the transmitters controlled port is providing access as expected for successful authentication and authorization
    b. Operational Modified – the transmitters controlled port is providing access that is less than typically expected for successful authentication and authorization

c. Restricted – the transmitter is providing access to some traffic to allow some higher layer protocols to operate, but it is not generically forwarding frames on the controlled port.

d. Closed – the transmitter is not providing access to higher layer traffic, only a minimal set of packet types are being processed including 802.1X packets if indicated.

C) Authentication Needed

D) Non-802.1X in progress

E) Access Requested

F) Fallback Access

G) Authentication Requirements—authentication mechanisms supported for the NID

a. Open—immediate access, without authentication, is available

b. EAP

c. EAP + MKA

d. EAP + MKA + MACsec

e. MKA

f. MKA +MACsec

g. Non-802.1X (Higher Layer)

h. Vendor specific authentication mechanisms

H) Supported Ciphersuites

I) Key Management Domain for the NID

More than one NID can be marked with a **port status** other than **closed** only if the NIDs are aliases for the same underlying network service. **Authentication needed** indicates that authenticator does not know the supplicants identity and needs this information to apply appropriate access controls. **Non-802.1X** in progress indicates that a non-802.1X process is in progress. The 802.1X supplicant is not expected to take any action other than to allow higher layer packets to and from its port as permitted by its policy. When the process completes it is expected that the status of the port will change. The port status change can lag successful authentication. **Fallback available** indicates that a closed port will go into **restricted** status if 802.1X authentication fails so the supplicant may be able to take some remedial action.

Access requested is an indication that the NID has been supplied in an EAPOL-Start or otherwise determined by the access point, and can be used by the accessing system as a confirmation appropriate authorization has been requested—prior to Operational becoming set for the NID.

Not all of the **Authentication Requirements** announced are necessarily equally acceptable to the recipient of the announcement, even if implemented. Some choices can be rejected by the Logon Process (12.5) controls; these controls may be configured or configurable per NID according to the sensitivity of the tasks to be performed when accessing a given network or requirements imposed by the network administration but not necessarily known to the access point.

Open indicates that immediate access, without authentication, is available. If the NID lists **open** as an authentication requirement than **fallback** should not be available.

A network path is or can be provided to a method of non-802.1X authentication (Higher Layer) if that choice is announced—if the **port status** is **closed**, that path is likely to be provided only if EAP authentication is attempted but fails.

An announcement can be marked as **supplicant specific** or **generic**. If the announcement is supplicant specific than the information has the meaning as specified as above. If the announcement is marked as generic then it is interpreted as follows:

Port Status – ignored
Authentication Needed – ignored
Non-802.1X in progress – ignored
Access Requested – set on the NID that is selected by default
Fallback – same as above
Authentication Requirements – same as above
Supported Ciphersuites – same as above
Key Management Domain – same as above

2.2 Modifications to Making and Requesting announcements (10.2)

Add the following:

The announcement should be sent within 200ms of receiving an EAPOL-Announcement-Req or an EAPOL-Start requesting an announcement. The announcement sent in response to an EAPOL-Start is sent to the unicast address of the supplicant, sets the access requested bit on the selected NID and sends the announcement before any EAPOL packets containing EAP messages for the selected NID.

2.3 Modifications to EAPOL-Start (11.6)

Text following table 11-3:

The first, and possibly only, TLV in an EAPOL-Start Packet Body is likely to be a NID Set TLV. If the supplicant is intending to use a Vendor Specific or Non-802.1X authentication mechanism then it should include an Access-Information TLV with a single authentication requirement set. Any additional TLVs specific to the indicated mechanism should also be included in the NID set. For non-802.1X mechanism, if the URI TLV is sent in the announcement, it should be included in the NID set.

If the EAPOL-Start solicits an announcement, the NID Set TLV should be included in that announcement with an Access Information TLV with the Access Requested bit set. If the authenticator is going to initiate EAP it shall send the announcement with the Access Requested bit set before any EAPOL packets containing EAP packets. If the NID set contains a valid access information TLV indicating non-EAP authentication requirement that is supported by the NID then the authenticator should not initiate EAP. The rest of the access information TLV is ignored. Note that it is not necessary to send an EAPOL start if the supplicant intending to authenticate with MKA since MKA explicitly selects the NID associated with the CAK.

2.4 Modifications to EAPOL-Announcement (11.12)

Add Supplicant specific indicator to Figure 11-17

Protocol Version	
Packet Type = EAPOL-Announcement	
Packet Body Length	
Packet Body	Supplicant Specific
	TLVs

If bit 1 (the least significant bit) of the first octet of the Packet Body of is set, the PDU is specific to the receiver. The other bits in this initial octet, shall be transmitted as 0 and ignored on receipt. The remaining octets (if any of) the Packet Body encode TLVs

Add URI TLV to the list of TLVs

110	URI-TLV	No	Announcement: NID-set, EAPOL-Start	O	11.12.5
111	Access-Informaiton TLV	No	Announcement: NID-set, global EAPOL-Start	M	11.12.5

2.5 Modifications to access information TLV (11.12.2)

Modified text after figure 11-19:

Port Status indicates the status of the port. The operational states (expected and modified) indicate the transmitter's Controlled Port is providing access to a network (service) associated with the NID (or, if the TLV is global, simply has MAC_Operational TRUE).

-- Operation – Expected: indicate that the port is forwarding frames onto the selected NID with the access control as expected.
-- Operational – Modified: indicates that restrictions beyond what is expected have been placed on the port.
-- Restricted: indicates that some higher layer services are available, but the port is not yet forwarding frames to the selected NID.

-- Closed: indicates that the port is not forwarding any traffic and only 802.1X authentication mechanisms may be used at this point.

In most cases only one NID is operational. The exception to this is the case where more than one NID is an alias for the same underlying NID. Port status is supplicant specific information and should be ignored in a generic announcement.

NOTE—The Announcement can contain additional TLVs that refine or override Access Level. The use of (extended) RADIUS attributes to communicate information to the authenticator for announcement is one possibility.

Access requested is set if the last authentication or reauthentication attempt indicated access to the network (service) associated with the NID (either explicitly or implicitly), and results from that attempt are being used or still being acquired. This is supplicant specific information. If it is set in a generic advertisement it indicates which NID, if any, is the default selected NID. Only one NID may be set access-requested in an announcement. Access-requested may be implicitly set when the port first comes up to a default value. MKA requests do not have an affect on this parameter.

Information	Field	Indicates
Requested	Octet 1: bits 1	Is NID currently requested for access
Port Status	Octet 1: bits 2-3	Operational Expected (1) Operational Modified (3) Restricted (2) Closed (0)
Authentication needed	Octet 1: bit 4	Is supplicant expected to perform 802.1X or non-802.1X authentication?
Non-802.1X process in progress	Octet 1 : bit 5	Is 802.1X authentication ongoing?
Reserved	Octet 1 : bit 6-7	Reserved for future standardization. Encoded as (0)
Fallback Available	Octet 1: bit 8	
Authentication Requirements	Octet 2	Vendor Specific
		Open
		EAP
		EAP + MKA
		EAP + MKA + MACSEC
		MKA
		MKA + MACSEC
		Non-802.1X authentication

Authentication Needed indicates that the supplicant is expected to try to authenticate to obtain the access expected for this NID. If this bit is cleared then the supplicant is authenticated or authentication is not required. This is supplicant specific information and should be ignored in a generic announcement.

Non-802.1X in Progress indicates that a non-802.1X authentication or authorization mechanism is currently in progress. The 802.1X supplicant is not expected to do anything except to allow higher layer packets to and prom its port if its policy allows. When the process completes it is expected that the status of the port will change. This is supplicant specific information and should be ignored in a generic announcement.

Fallback available indicates that a closed port will go into **restricted** status if 802.1X authentication fails so the supplicant may be able to take some remedial action. This is generic information. If the NID lists **open** as an authentication requirement than fallback should not be available.

Authentication Requirements express the combination of mechanisms whose successful use can result in access to the service. Not all choices are necessarily equally acceptable to the recipient of the announcement, who can require authentication or secured connectivity—and hence reject some options—while not implementing others. Not all choices necessarily result in an equal level of access, those that authenticate or secure access can provide a greater service. Authentication requirements are generic information.

Open indicates that immediate access, without authentication, is available.

Non-802.1X authentication indicates that higher layer authentication is supported by this NID. It may not be immediately available and require an attempt to authenticate using an 802.1X mechanism. If the **port status** is **closed** then it is not available. If the **port status** is **restricted** then access to non-802.1X authentication mechanisms is possible.

If **vendor specific** authentication and authorization procedures are indicated then TLVs for the NID Set should include an Organizationally Specific TLV to identify those procedures.

2.6 URI TLV (sub section of section 11.12)

The URI TLV contains a string of up to 253 UTF-8 characters that indicates the resource identifier for the service providing non-802.1X authentication. <Some thought needs to be put into security considerations here. Could this provide an mechanism to lure a client into contacting a URI of this attacker's choosing? Is this a problem? >

URI TLV-type = 110	TLV Information String Length	URI for accessing the non-802.1X authentication service

3 Alternate encoding of generic and specific attributes

This section outlines an alternate encoding of generic and alternate attributes in an announcement. The previous section took the approach that an announcement may be marked as specific or generic. This seems somewhat awkward so this section takes a approach where the generic and specific information is separated out into distinct TLVs.

3.1 *Modifications to EAPOL-Start (11.6)*

Text following table 11-3:

The first, and possibly only, TLV in an EAPOL-Start Packet Body is likely to be a NID Set TLV. If the supplicant is intending to use a Vendor Specific or Non-802.1X authentication mechanism then it should include an Access-requirement TLV with a single authentication requirement set. Any additional TLVs specific for the indicated mechanism should also be included in the NID set. For non-802.1X mechanism, if the URI TLV is sent in the announcement, it should be included in the NID set.

If the EAPOL-Start solicits an announcement, the NID Set TLV should be included in that announcement with an Access Status TLV with the Access Requested bit set. If the authenticator is going to initiate EAP it shall send the announcement with the Access Requested bit set before any EAPOL packets containing EAP packets. If the NID set contains a valid access requirements TLV indicating non-EAP authentication requirement that is supported by the NID then the authenticator should not initiate EAP. Note that it is not necessary to send an EAPOL start if the supplicant intending to authenticate with MKA since MKA explicitly selects the NID associated with the CAK.

3.2 *Modifications to EAPOL-Announcement (11.12)*

Add Supplicant specific indicator to Figure 11-17

Protocol Version	
Packet Type = EAPOL-Announcement	
Packet Body Length	
Packet Body	Supplicant Specific
	TLVs

If bit 1 (the least significant bit) of the first octet of the Packet Body of is set, the PDU is specific to the receiver. The other bits in this initial octet, shall be transmitted as 0 and ignored on receipt. The remaining octets (if any of) the Packet Body encode TLVs

Add URI TLV to the list of TLVs

109	URI-TLV	No	Announcement: NID-set, EAPOL-Start	O	11.12.5

110	Access Requirements TLV	No	Announcement: NID-set, global EAPOL-Start	M	11.12.5
111	Access-Status TLV	No	Announcement: NID-set, global	M	11.12.5

3.3 Modifications to access information TLV (11.12.2)

Define Access-Status TLV:

Access-Status TLV-type = 111	TLV Information String Length	Access Status Information

Port Status indicates the status of the port. The operational states (expected and modified) indicate the transmitter's Controlled Port is providing access to a network (service) associated with the NID (or, if the TLV is global, simply has MAC_Operational TRUE).

-- Operation – Expected: indicate that the port is forwarding frames onto the selected NID with the access control as expected.
-- Operational – Modified: indicates that restrictions beyond what is expected have been placed on the port.
-- Restricted: indicates that some higher layer services are available, but the port is not yet forwarding frames to the selected NID.
-- Closed: indicates that the port is not forwarding any traffic and only 802.1X authentication mechanisms may be used at this point.

In most cases only one NID is operational. The exception to this is the case where more than one NID is an alias for the same underlying NID.

NOTE—The Announcement can contain additional TLVs that refine or override Access Level. The use of (extended) RADIUS attributes to communicate information to the authenticator for announcement is one possibility.

Access requested is set if the last authentication or reauthentication attempt indicated access to the network (service) associated with the NID (either explicitly or implicitly), and results from that attempt are being used or still being acquired. Only one NID may be set access-requested in an announcement. Access-requested may be implicitly set when the port first comes up to a default value. MKA requests do not have an affect on this parameter.

Information	Field	Indicates

Requested	Octet 1: bits 1	Is NID currently requested for access
Port Status	Octet 1: bits 2-3	Operational Expected (1) Operational Modified (3) Restricted (2) Closed (0)
Authentication needed	Octet 1: bit 4	Is supplicant expected to perform 802.1X or non-802.1X authentication?
Non-802.1X process in progress	Octet 1 : bit 5	Is 802.1X authentication ongoing?
Reserved	Octet 1 : bit 6-7	Reserved for future standardization. Encoded as (0)

Authentication Needed indicates that the supplicant is expected to try to authenticate to obtain the access expected for this NID. If this bit is cleared then the supplicant is authenticated or authentication is not required.

Non-802.1X in Progress indicates that a non-802.1X authentication or authorization mechanism is currently in progress. The 802.1X supplicant is not expected to do anything except to allow higher layer packets to and prom its port if its policy allows. When the process completes it is expected that the status of the port will change.

Define Access-Requirements TLV

Access-Reqs TLV-type = 111	TLV Information String Length	Access requirements

Fallback available indicates that a closed port will go into **restricted** status if 802.1X authentication fails so the supplicant may be able to take some remedial action. If the NID lists **open** as an authentication requirement than fallback should not be available.

Authentication Requirements express the combination of mechanisms whose successful use can result in access to the service. Not all choices are necessarily equally acceptable to the recipient of the announcement, who can require authentication or secured connectivity—and hence reject some options—while not implementing others. Not all choices necessarily result in an equal level of access, those that authenticate or secure access can provide a greater service

Open indicates that immediate access, without authentication, is available.

Information	Field	Indicates
Fallback Available		Fallback available after

		authentication attempt if port is closed
Authentication Requirements		Vendor Specific
		Open
		EAP
		EAP + MKA
		EAP + MKA + MACSEC
		MKA
		MKA + MACSEC
		Non-802.1X authentication

Non-802.1X authentication indicates that higher layer authentication is supported by this NID. It may not be immediately available and require an attempt to authenticate using an 802.1X mechanism. If the **port status** is **closed** then it is not available. If the **port status** is **restricted** then access to non-802.1X authentication mechanisms is possible.

If **vendor specific** authentication and authorization procedures are indicated then TLVs for the NID Set should include an Organizationally Specific TLV to identify those procedures.