802.1X Related Data Models

Mick Seaman

The colloquial use of the term ‘802.1X’ is very loose. It has and is used in a number of different ways, usually often with the assumption that the context is sufficient to identify what is meant. So ‘802.1X’ has been used to mean any or all of the following: the general architectural approach of using access control at the edge of a network (rather than relying entirely on an ‘end-to-end’ approach); the use of EAP (and EAP methods) to authenticate a network clients and to provide keys for securing data transmission[1]; the use of both EAP and Radius (or Diameter) for authentication and authorization[2]; the specific frame formats (EAPOL) used to carry EAP over an access LAN, and the (rather simple) state machines[3] that are used with these to initiate and re-initiate authentication; the actual securing of the data conveyed, and/or the shim that performs that function; all the associated control protocols and the entities that operate them; and last (and possibly least) what is actually specified in IEEE Std 802.1X. Picking just one of these aspects of the overall 802.1X solution can yield an appealingly simple but impractical view of what constitutes .1X and its management— emphasizing .1X’s role in controlling access through individual ports doesn’t mean that the significant control plane aspects of .1X are best (or even can be) modeled by augmenting an interface. The simply stated requirement for ‘management of .1X’ is probably a requirement for the management of a ‘802.1X solution’, going beyond even the most extensive of the meanings of ‘802.1X’[4]. At the same time the level of detail, accuracy, and completeness required means that the only practical approach is to align management models with the underlying standards. This may well disappoint the naive who expect a YANG model for IEEE Std 802.1X to manage their ‘802.1X solution’, but developing a single YANG model for the latter would necessarily involve collating (and in a number of areas developing) and standardizing a complete management model for the solution as a first step. This is not practical, it would take too long, involve too much effort, and run the risk of reworking much that has already been decided. What is actually needed is a description of how the data models for the various components fit together (or at the present, how they are expected to fit together).

In describing the relationship of the IEEE Std 802.1X YANG Data Model to the other models that might comprise an 802.1X solution the challenge lies in the variety of systems that can use .1X. This note begins by reprising the component parts of the .1X operation as described in IEEE Std 802.1X Clause 12’s specification of PAE operation .

---

1. PAE management for an Ethernet solution

802.1X Clause 12 describes PAE operation (the ‘PAE’ is the Port Access Entity responsible for controlling a port’s use of 802.1X). While the 802.1X standard specifies a solution that is ‘media-independent’ in the sense that it can be used with all MAC types that support the MAC Service and the ISS as specified in IEEE Std 802.1AC (referenced by IEEE Std 802) the predominant wireless standards have either evolved their own distinctive architecture (as has 802.11) or are not currently capable of providing the MAC Service defined in those references or have significant other limitations (as has 802.15). For simplicity 802.1X Clause 12 can be thought of as specifying an Ethernet solution, and this will be assumed in this note. The use of parts of this solution (and its management) for other media is considered later.

Figure 12-1 provides an overview of the PAE state machines and their interfaces to the other components of the .1X solution. It shows:

[1] More precisely a key or keys that serve as the root of a key hierarchy that provides keys to secure data transmission.

[2] Configuring, for example, which VLANs an authenticated client can access. See RFC 4675, Radius Attributes for Virtual LAN and Priority Support.

[3] Formally (as specified by IEEE Std 802.1X) these are state machines for ‘PACP’, Port Access Control Protocol.

[4] For example management of 802.1X using EAP implies selection of EAP method(s), policy controls over their use (where more than one EAP method is implemented), controls over the use of credentials, and for mutual authentication (required for BCP and by IEEE Std 802.1X-2010), checking of the EAP Authenticators own credentials which will likely involve management of roots of trust and possibly of revocation lists.

—The KaY (Key Agreement Entity, operating the MACsec Key Agreement protocol, MKA)

—The Controlled Port state machine (CP)

—The ‘Logon Process’

—Authenticator and Supplicant PACP (Port Access Control Protocol) state machines

—The CAK Cache

and

—Interfaces between the ‘Logon Process’ and the KaY, CP, PACP state machines, and the CAK Cache

—Interfaces between the KaY and the CP and the IEEE Std 802.1AE SecY (if present) operating MACsec

Management of the KaY, the CP, and the PACP state machines is described in clause 12.9 together with high level control that provides context for their operation.

Some management of the Logon Process and of the CAK Cache is provided, but their operation (and particularly that of the Logon Process, specified in 12.5) is expected to be highly dependent on the type of the system being managed. For some systems, e.g. PCs, with direct user interfaces and their own way of managing the rest of their operation (be that installed applications, ‘system preferences’ screens, periodic update processes, corporate applications for assessing the devices ‘posture’) it may be that management using YANG is not expected. Certainly the complexity and requirements for their management will differ significantly from that of small unattended infrastructure devices. Clause 12.5 attempts to abstract the detail important to interfacing to the rest of the solution as shown in Figure 12-1 and provides rudimentary control that is easily understood in terms of Controlled Port connectivity.

The most significant part of PAE operation that is hidden within the Logon Process is the selection and use of credentials (whether these are requested from a human user typing at a console, or acquired from some credential store) and the use of EAP proper (selection and use of one or more EAP methods). So the additional functionality that would need to be managed by YANG data models to provide a complete solution includes:

a) Management of EAP, and in particular management of the allowed EAP methods and the ordering and possible chaining of EAP methods

b) Management of credentials or the process of obtaining credentials from an immediate human user of the device.

c) Since mutual authentication is a requirement we also need to be able to manage roots of trust and (possibly) revocation lists, at least to the extent of a manager being able to confirm that suitable constraints are being placed on the authentication of the Authentication Server.

d) Where 1X is being use for infrastructure support we will also be concerned with managing devices that act as Authentication Servers.

Of course 802.1X and EAP are not the only standards and protocols that are interested in the use of credentials. There is already concern amongst YANG model developers over the possible proliferation of ‘key chain’ models, an issue that is (probably) strongly related to (b) above. Similarly EAP is not the only protocol that has mutual authentication requirements involving trust roots. In both these case we need to be able to point to, co-opt, or at the very least not simply duplicate with minor tweaks, what is in other models.

Another strong modeling relationship is that between 802.1X and Radius, or between 802.1X, 802.1Q, and Radius. Is it possible that YANG (or rather YANG used in conjunction with a suitable protocol) might emerge as a Radius/Diameter substitute.

2. Management of 802.11 802.1X solutions

There is probably very little overlap between the management details of the Ethernet solution that are found in IEEE Std 802.1X and what needs to be done for an 802.11 mobile device, let alone what needs to be done for 802.11 infrastructure. While the ‘big idea’ has been extremely useful, organizing a management approach around a small number of EAPOL messages and related statistics would be tail wagging the dog. However other aspects of the overall solution, in particular EAP and cerdential management should be closely aligned. Beyond that, there is a lot of very specific 802.11 management, so the challenge will be to put together moddels that appropriately factor common elements.