INTERNATIONAL STANDARD

ISO/IEC/ IEEE 8802-1X

First edition
2013-12-01

Information technology — Telecommunications and information exchange between systems — Local and metropolitan area networks —

Part 1X: Port-based network access control

Technologies de l'information — Télécommunications et échange d'information entre systèmes — Réseaux locaux et métropolitains —

Partie 1X: Contrôle d'accès au réseau basé sur le port

Reference number
ISO/IEC/IEEE 8802-1X:2013(E)

© IEEE 2010

Full document details: ISO_IEC_IEEE 8802-1X_2013

COPYRIGHT PROTECTED DOCUMENT

© IEEE 2010

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized otherwise in any form or by any means, electronic or mechanical, including photocopying, or posting on the internet or an intranet, without permission in writing from ISO, IEC or IEEE at the respective address below.

ISO copyright office
Case postale 56
CH-1211 Geneva 20
Tel. + 41 22 749 01 11
Fax + 41 22 749 09 47
E-mail copyright@iso.org
Web www.iso.org

IEC Central Office
3, rue de Varembé
CH-1211 Geneva 20
Switzerland
E-mail inmail@iec.ch
Web www.iec.ch

Institute of Electrical and Electronics Engineers, Inc.
3 Park Avenue, New York
NY 10016-5997, USA
E-mail stds.ipr@ieee.org
Web www.ieee.org

Published in Switzerland

Documents
Document Sharing Hub
© IEEE 2010 – All rights reserved

Full document details: ISO_IEC_IEEE 8802-1X_2013

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work. In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1.

IEEE Standards documents are developed within the IEEE Societies and the Standards Coordinating Committees of the IEEE Standards Association (IEEE-SA) Standards Board. The IEEE develops its standards through a consensus development process, approved by the American National Standards Institute, which brings together volunteers representing varied viewpoints and interests to achieve the final product. Volunteers are not necessarily members of the Institute and serve without compensation. While the IEEE administers the process and establishes rules to promote fairness in the consensus development process, the IEEE does not independently evaluate, test, or verify the accuracy of any of the information contained in its standards.

The main task of ISO/IEC JTC 1 is to prepare International Standards. Draft International Standards adopted by the joint technical committee are circulated to national bodies for voting. Publication as an International Standard requires approval by at least 75 % of the national bodies casting a vote.

Attention is called to the possibility that implementation of this standard may require the use of subject matter covered by patent rights. By publication of this standard, no position is taken with respect to the existence or validity of any patent rights in connection therewith. ISO/IEEE is not responsible for identifying essential patents or patent claims for which a license may be required, for conducting inquiries into the legal validity or scope of patents or patent claims or determining whether any licensing terms or conditions provided in connection with submission of a Letter of Assurance or a Patent Statement and Licensing Declaration Form, if any, or in any licensing agreements are reasonable or non-discriminatory. Users of this standard are expressly advised that determination of the validity of any patent rights, and the risk of infringement of such rights, is entirely their own responsibility. Further information may be obtained from ISO or the IEEE Standards Association.

ISO/IEC/IEEE 8802-1X was prepared by the LAN/MAN Standards Committee of the IEEE Computer Society (as IEEE Std 802.1X-2010). It was adopted by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 6, *Telecommunications and information exchange between systems*, in parallel with its approval by the ISO/IEC national bodies, under the “fast-track procedure” defined in the Partner Standards Development Organization cooperation agreement between ISO and IEEE. IEEE is responsible for the maintenance of this document with participation and input from ISO/IEC national bodies.

ISO/IEC/IEEE 8802 consists of the following parts, under the general title *Information technology — Telecommunications and information exchange between systems — Local and metropolitan area networks*:

— *Part 11: Wireless LAN medium access control (MAC) and physical layer (PHY) specifications*

— *Part 1X: Port-based network access control*

— *Part 1AE: Media access control (MAC) security*

— *Part 15-4: Wireless medium access control (MAC) and physical layer (PHY) specifications for low-rate wireless personal area networks (WPANs)*

© IEEE 2010 – All rights reserved

Documents
Document Sharing Hub
Full document details: ISO_IEC_IEEE 8802-1X_2013

(Blank page)

© IEEE 2010 – All rights reserved
Documents
Document Sharing Hub
Full document details: ISO_IEC_IEEE 8802-1X_2013

802.1X™

IEEE Standard for

Local and metropolitan area networks—

Port-Based Network Access Control

IEEE Computer Society

Sponsored by the
LAN/MAN Standards Committee

IEEE
3 Park Avenue
New York, NY 10016-5997, USA

5 February 2010

IEEE Std 802.1X™-2010
(Revision of
IEEE Std 802.1X-2004)

Copyright © 2010 IEEE. All rights reserved.

Documents
Document Sharing Hub

Full document details: ISO_IEC_IEEE 8802-1X_2013

(Blank page)

Copyright © 2010 IEEE. All rights reserved.
Documents
Document Sharing Hub
Full document details: ISO_IEC_IEEE 8802-1X_2013

IEEE Std 802.1X™-2010
(Revision of
IEEE Std 802.1X-2004)

IEEE Standard for
Local and metropolitan area networks—

Port-Based Network Access Control

Sponsor

LAN/MAN Standards Committee
of the
IEEE Computer Society

Approved 2 February 2010

IEEE-SA Standards Board

Copyright © 2010 IEEE. All rights reserved.

Documents
Document Sharing Hub
Full document details: ISO_IEC_IEEE 8802-1X_2013

Abstract: Port-based network access control allows a network administrator to restrict the use of IEEE 802® LAN service access points (ports) to secure communication between authenticated and authorized devices. This standard specifies a common architecture, functional elements, and protocols that support mutual authentication between the clients of ports attached to the same LAN and that secure communication between the ports, including the media access method independent protocols that are used to discover and establish the security associations used by IEEE 802.1AE™ MAC Security.

Keywords: access control, authentication, authorization, controlled port, key agreement, LANs, local area networks, MAC security, MAC Service, MANs, metropolitan area networks, port-based network access control, secure association, security, service access point, uncontrolled port

The Institute of Electrical and Electronics Engineers, Inc.
3 Park Avenue, New York, NY 10016-5997, USA

Copyright © 2010 by the Institute of Electrical and Electronics Engineers, Inc.
All rights reserved. Published 5 February 2010. Printed in the United States of America

IEEE and 802 are registered trademarks in the U.S. Patent & Trademark Office, owned by The Institute of Electrical and Electronics Engineers, Incorporated.

PDF: ISBN 978-0-7381-6145-7 STD96008
Print: ISBN 978-0-7381-6146-4 STDPD96008

IEEE prohibits discrimination, harassment, and bullying. For more information, visit http://www.ieee.org/web/aboutus/whatis/policies/p9-26.html.

No part of this publication may be reproduced in any form, in an electronic retrieval system or otherwise, without the prior written permission of the publisher.

Copyright © 2010 IEEE. All rights reserved.

Documents
Document Sharing Hub

Full document details: ISO_IEC_IEEE 8802-1X_2013

IEEE Standards documents are developed within the IEEE Societies and the Standards Coordinating Committees of the IEEE Standards Association (IEEE-SA) Standards Board. The IEEE develops its standards through a consensus development process, approved by the American National Standards Institute, which brings together volunteers representing varied viewpoints and interests to achieve the final product. Volunteers are not necessarily members of the Institute and serve without compensation. While the IEEE administers the process and establishes rules to promote fairness in the consensus development process, the IEEE does not independently evaluate, test, or verify the accuracy of any of the information or the soundness of any judgments contained in its standards.

Use of an IEEE Standard is wholly voluntary. The IEEE disclaims liability for any personal injury, property or other damage, of any nature whatsoever, whether special, indirect, consequential, or compensatory, directly or indirectly resulting from the publication, use of, or reliance upon this, or any other IEEE Standard document.

The IEEE does not warrant or represent the accuracy or content of the material contained herein, and expressly disclaims any express or implied warranty, including any implied warranty of merchantability or fitness for a specific purpose, or that the use of the material contained herein is free from patent infringement. IEEE Standards documents are supplied **"AS IS."**

The existence of an IEEE Standard does not imply that there are no other ways to produce, test, measure, purchase, market, or provide other goods and services related to the scope of the IEEE Standard. Furthermore, the viewpoint expressed at the time a standard is approved and issued is subject to change brought about through developments in the state of the art and comments received from users of the standard. Every IEEE Standard is subjected to review at least every five years for revision or reaffirmation, or every ten years for stabilization. When a document is more than five years old and has not been reaffirmed, or more than ten years old and has not been stabilized, it is reasonable to conclude that its contents, although still of some value, do not wholly reflect the present state of the art. Users are cautioned to check to determine that they have the latest edition of any IEEE Standard.

In publishing and making this document available, the IEEE is not suggesting or rendering professional or other services for, or on behalf of, any person or entity. Nor is the IEEE undertaking to perform any duty owed by any other person or entity to another. Any person utilizing this, and any other IEEE Standards document, should rely upon the advice of a competent professional in determining the exercise of reasonable care in any given circumstances.

Interpretations: Occasionally questions may arise regarding the meaning of portions of standards as they relate to specific applications. When the need for interpretations is brought to the attention of IEEE, the Institute will initiate action to prepare appropriate responses. Since IEEE Standards represent a consensus of concerned interests, it is important to ensure that any interpretation has also received the concurrence of a balance of interests.For this reason, IEEE and the members of its societies and Standards Coordinating Committees are not able to provide an instant response to interpretation requests except in those cases where the matter has previously received formal consideration. A statement, written or oral, that is not processed in accordance with the IEEE-SA Standards Board Operations Manual shall not be considered the official position of IEEE or any of its committees and shall not be considered to be, nor be relied upon as, a formal interpretation of the IEEE.At lectures, symposia, seminars, or educational courses, an individual presenting information on IEEE standards shall make it clear that his or her views should be considered the personal views of that individual rather than the formal position, explanation, or interpretation of the IEEE. Comments for revision of IEEE Standards are welcome from any interested party, regardless of membership affiliation with IEEE. Suggestions for changes in documents should be in the form of a proposed change of text, together with appropriate supporting comments. Recommendations to change the status of a stabilized standard should include a rationale as to why a revision or withdrawal is required.

Comments and recommendations on standards, and requests for interpretations should be addressed to:

Secretary, IEEE-SA Standards Board
445 Hoes Lane
Piscataway, NJ 08854
USA

Authorization to photocopy portions of any individual standard for internal or personal use is granted by the Institute of Electrical and Electronics Engineers, Inc., provided that the appropriate fee is paid to Copyright Clearance Center. To arrange for payment of licensing fee, please contact Copyright Clearance Center, Customer Service, 222 Rosewood Drive, Danvers, MA 01923 USA; +1 978 750 8400. Permission to photocopy portions of any individual standard for educational classroom use can also be obtained through the Copyright Clearance Center.

Documents
Document Sharing Hub

Copyright © 2010 IEEE. All rights reserved.

Full document details: ISO_IEC_IEEE 8802-1X_2013

Introduction

This introduction is not part of IEEE Std 802.1X-2010, IEEE Standard for Local and Metropolitan Area Networks—Port-Based Network Access Control.

Port-based network access control allows a network administrator to restrict the use of IEEE 802 LAN service access points (ports) to secure communication between authenticated and authorized devices. IEEE Std 802.1X specifies an architecture, functional elements, and protocols that support mutual authentication between the clients of ports attached to the same LAN and secure communication between the ports.

The first edition of IEEE Std 802.1X was published in 2001. The second edition, IEEE Std 802.1X-2004, clarified areas related to mutual authentication and the interface between IEEE 802.1X specified state machine, and those specified by the Extensible Authentication Protocol (EAP), and by IEEE Std 802.11™ in support of IEEE Std 802.1X.

Work on this edition, IEEE Std 802.1X-2010, began as IEEE P802.1af™—an amendment to specify authenticated key agreement in support of IEEE 802.1AE MAC Security. Part of that work clarified and generalized the relationship between the common architecture specified for port-based network access control, and the functional elements and protocols that support that architecture as specified in IEEE Std 802.1X, other IEEE 802 Standards, and in IETF RFCs. The extent of the changes necessary to IEEE Std 802.1X-2004 made it appropriate to revise IEEE Std 802.1X as a whole. Further changes updated the standard to reflect best current practice, insisting, for example, upon mutual authentication methods and using such methods in examples. A greater emphasis is placed on the security of systems accessing the network, as well as upon the security of the network accessed, and some prior provisions, such as the 'controlled directions' parameters, have been removed and replaced with a more comprehensive treatment of segregating and limiting connectivity to unauthenticated systems.

Every effort has been made to maintain interoperability, without prior configuration, with implementations conforming to IEEE Std 802.1X-2004 and IEEE Std 802.1X-2001. However it is anticipated that claims of conformance in respect of some existing implementations will continue to refer to IEEE Std 802.1X-2004. Changes to the functionality provided by that prior edition and its documentation include those detailed in the following paragraph.

This edition, IEEE Std 802.1X-2010, describes applications of port-based network access that use IEEE 802.1AE MAC Security (MACsec) and/or MKA (MACsec Key Agreement protocol) as well as those previously supported. The specification of the use of EAP for authentication has been updated, enforcing a stricter separation between the port access control protocol (PACP), local to the Supplicant and Authenticator, and the EAP state machines proper. Details of particular EAP methods are no longer interpreted by the PACP machines. The existing EAPOL (EAP over LANs) PDU formats have not been modified, but additional EAPOL PDUs have been added to support MKA and the specification of EAPOL improved. The bibliography, previously Annex F, has been moved to Annex B. The discussions previously in Annex B and Annex C have been updated and integrated into the main body of the standard. The state machine diagram and language conventions, now used by a number of clauses in the standard, have been moved to a new Annex C.

Notice to users

Laws and regulations

Users of these documents should consult all applicable laws and regulations. Compliance with the provisions of this standard does not imply compliance to any applicable regulatory requirements.

Copyright © 2010 IEEE. All rights reserved.
Documents
Document Sharing Hub
Full document details: ISO_IEC_IEEE 8802-1X_2013

Implementers of the standard are responsible for observing or referring to the applicable regulatory requirements. IEEE does not, by the publication of its standards, intend to urge action that is not in compliance with applicable laws, and these documents may not be construed as doing so.

Copyrights

This document is copyrighted by the IEEE. It is made available for a wide variety of both public and private uses. These include both use, by reference, in laws and regulations, and use in private self-regulation, standardization, and the promotion of engineering practices and methods. By making this document available for use and adoption by public authorities and private users, the IEEE does not waive any rights in copyright to this document.

Updating of IEEE documents

Users of IEEE standards should be aware that these documents may be superseded at any time by the issuance of new editions or may be amended from time to time through the issuance of amendments, corrigenda, or errata. An official IEEE document at any point in time consists of the current edition of the document together with any amendments, corrigenda, or errata then in effect. In order to determine whether a given document is the current edition and whether it has been amended through the issuance of amendments, corrigenda, or errata, visit the IEEE Standards Association website at http://ieeexplore.ieee.org/xpl/standards.jsp, or contact the IEEE at the address listed previously.

For more information about the IEEE Standards Association or the IEEE standards development process, visit the IEEE-SA website at http://standards.ieee.org.

Errata

Errata, if any, for this and all other standards can be accessed at the following URL: http://standards.ieee.org/reading/ieee/updates/errata/index.html. Users are encouraged to check this URL for errata periodically.

Interpretations

Current interpretations can be accessed at the following URL: http://standards.ieee.org/reading/ieee/interp/index.html.

Patents

Attention is called to the possibility that implementation of this amendment may require use of subject matter covered by patent rights. By publication of this amendment, no position is taken with respect to the existence or validity of any patent rights in connection therewith. The IEEE is not responsible for identifying Essential Patent Claims for which a license may be required, for conducting inquiries into the legal validity or scope of Patents Claims or determining whether any licensing terms or conditions provided in connection with submission of a Letter of Assurance, if any, or in any licensing agreements are reasonable or non-discriminatory. Users of this amendment are expressly advised that determination of the validity of any patent rights, and the risk of infringement of such rights, is entirely their own responsibility. Further information may be obtained from the IEEE Standards Association.

Copyright © 2010 IEEE. All rights reserved.

Documents
Document Sharing Hub
Full document details: ISO_IEC_IEEE 8802-1X_2013

Contents

1. Overview ... 1

1.1 Scope ... 1
1.2 Purpose ... 1
1.3 Introduction ... 2
1.4 Provisions of this standard ... 2

2. Normative references ... 4

3. Definitions ... 6

4. Acronyms and abbreviations ... 10

5. Conformance ... 12

5.1 Requirements terminology ... 12
5.2 Protocol Implementation Conformance Statement ... 12
5.3 Conformant systems and system components ... 13
5.4 PAE requirements ... 13
5.5 PAE options ... 14
5.6 Supplicant requirements ... 14
5.7 Supplicant options ... 14
5.8 Authenticator requirements ... 14
5.9 Authenticator options ... 14
5.10 MKA requirements ... 15
5.11 MKA options ... 15
5.12 Virtual port requirements ... 16
5.13 Virtual port options ... 16
5.14 Announcement transmission requirements ... 16
5.15 Announcement transmission options ... 17
5.16 Announcement reception requirements ... 17
5.17 Announcement reception options ... 17
5.18 Requirements for SNMP access to the PAE MIB ... 17
5.19 Options for SNMP access to the PAE MIB ... 17
5.20 PAC requirements ... 17
5.21 System recommendations ... 18
5.22 Prohibitions ... 18

6. Principles of port-based network access control operation ... 19

6.1 Port-based network access control architecture ... 19
6.2 Key hierarchy ... 21
6.3 Port Access Entity (PAE) ... 25
6.4 Port Access Controller (PAC) ... 29
6.5 Link aggregation ... 31
6.6 Use of this standard by IEEE Std 802.11 ... 32

7. Port-based network access control applications ... 33

7.1 Host access with physically secure LANs ... 33
7.2 Infrastructure support with physically secure LANs ... 36
7.3 Host access with MACsec and point-to-point LANs ... 38
7.4 Use with MACsec to support infrastructure LANs ... 39
7.5 Host access with MACsec and a multi-access LAN ... 41

Copyright © 2010 IEEE. All rights reserved.
Documents
Document Sharing Hub
Full document details: ISO_IEC_IEEE 8802-1X_2013

7.6 Group host access with MACsec ... 44
7.7 Use with MACsec to support virtual shared media infrastructure LANs ... 45

8. Authentication using EAP ... 48

8.1 PACP Overview ... 49
8.2 Example EAP exchanges ... 50
8.3 PAE higher layer interface ... 51
8.4 PAE Client interface ... 52
8.5 EAPOL transmit and receive ... 54
8.6 Supplicant and Authenticator PAE timers ... 54
8.7 Supplicant PACP state machine, variables, and procedures ... 55
8.8 Supplicant PAE counters ... 55
8.9 Authenticator PACP state machine, variables, and procedures ... 57
8.10 Authenticator PAE counters ... 58
8.11 EAP methods ... 58

9. MACsec Key Agreement protocol (MKA) ... 60

9.1 Protocol design requirements ... 61
9.2 Protocol support requirements ... 62
9.3 MKA key hierarchy ... 62
9.4 MKA transport ... 64
9.5 Key server election ... 67
9.6 Use of MACsec ... 68
9.7 Cipher suite selection ... 69
9.8 SAK generation, distribution, and selection ... 69
9.9 SA assignment ... 71
9.10 SAK installation and use ... 72
9.11 Connectivity change detection ... 73
9.12 CA formation and group CAK distribution ... 73
9.13 Secure announcements ... 74
9.14 MKA participant creation and deletion ... 74
9.15 MKA participant timer values ... 75
9.16 MKA management ... 76
9.17 MKA SAK distribution examples ... 78

10. Network announcements ... 80

10.1 Announcement information ... 80
10.2 Making and requesting announcements ... 83
10.3 Receiving announcements ... 85
10.4 Managing announcements ... 85

11. EAPOL PDUs ... 87

11.1 EAPOL PDU transmission, addressing, and protocol identification ... 87
11.2 Representation and encoding of octets ... 89
11.3 Common EAPOL PDU structure ... 90
11.4 Validation of received EAPOL PDUs ... 91
11.5 EAPOL protocol version handling ... 92
11.6 EAPOL-Start ... 93
11.7 EAPOL-Logoff ... 94
11.8 EAPOL-EAP ... 94
11.9 EAPOL-Key ... 94
11.10 EAPOL-Encapsulated-ASF-Alert ... 95

Documents
Document Sharing Hub

Copyright © 2010 IEEE. All rights reserved.

Full document details: ISO_IEC_IEEE 8802-1X_2013

11.11 EAPOL-MKA ... 95
11.12 EAPOL-Announcement ... 104
11.13 EAPOL-Announcement-Req ... 109

12. PAE operation ... 110

12.1 Model of operation ... 110
12.2 KaY interfaces ... 112
12.3 CP state machine interfaces ... 114
12.4 CP state machine ... 114
12.5 Logon Process ... 116
12.6 CAK cache ... 118
12.7 Virtual port creation and deletion ... 119
12.8 EAPOL Transmit and Receive Process ... 120
12.9 PAE management ... 123

13. PAE MIB ... 126

13.1 The Internet Standard Management Framework ... 126
13.2 Structure of the MIB ... 126
13.3 Relationship to other MIBs ... 126
13.4 Security considerations ... 134
13.5 Definitions for PAE MIB ... 135

Annex A (normative) PICS proforma ... 181
A.1 Introduction ... 181
A.2 Abbreviations and special symbols ... 181
A.3 Instructions for completing the PICS proforma ... 182
A.4 PICS proforma for IEEE 802.1X ... 184
A.5 Major capabilities and options ... 185
A.7 Supplicant requirements and options ... 186
A.6 PAE requirements and options ... 186
A.8 Authenticator requirements and options ... 187
A.9 MKA requirements and options ... 188
A.12 Management and remote management ... 189
A.10 Announcement transmission requirements ... 189
A.11 Announcement reception requirements ... 189
A.13 Virtual ports ... 190
A.14 PAC ... 190

Annex B (informative) Bibliography ... 191

Annex C (normative) State diagram notation ... 193

Annex D (normative) Basic architectural concepts and terms ... 195
D.1 Protocol entities, peers, layers, services, and clients ... 195
D.2 Service interface primitives, parameters, and frames ... 195
D.3 Layer management interfaces ... 196
D.4 Service access points, interface stacks, and ports ... 196
D.5 Media independent protocols and shims ... 197
D.6 MAC Service clients ... 197
D.7 Stations and systems ... 198
D.8 Connectionless connectivity and connectivity associations ... 198

Copyright © 2010 IEEE. All rights reserved.
Documents
Document Sharing Hub
Full document details: ISO_IEC_IEEE 8802-1X_2013

Annex E (informative) IEEE 802.1X EAP and RADIUS usage guidelines 199
E.1 EAP Session-Id 199
E.2 RADIUS Attributes for IEEE 802 Networks 199

Annex F (informative) Support for 'Wake-on-LAN' protocols 200

Annex G (informative) Unsecured multi-access LANs 201

Annex H (informative) Test vectors 203
H.1 KDF 203
H.2 CAK Key Derivation 203
H.3 CKN Derivation 204
H.4 KEK Derivation 204
H.5 ICK Derivation 204
H.6 SAK Derivation 205
Annex I (informative) IEEE list of participants 206

Copyright © 2010 IEEE. All rights reserved.

Documents
Document Sharing Hub
Full document details: ISO_IEC_IEEE 8802-1X_2013

Figures

Figure 6-1 Port-based network access control processes ... 20
Figure 6-2 Port-based network access control with MACsec ... 21
Figure 6-3 MKA key hierarchy ... 22
Figure 6-4 Use of pairwise CAKs to distribute group SAKs ... 22
Figure 6-5 Network access control with MACsec and a multi-access LAN ... 29
Figure 6-6 Port Access Controller ... 29
Figure 6-7 PACs and Link Aggregation in an interface stack ... 31
Figure 6-8 SecYs and Link Aggregation in an interface stack ... 31
Figure 7-1 Network access control with a physically secure point-to-point LAN ... 33
Figure 7-2 Network access control with a physically secure point-to-point LAN ... 34
Figure 7-3 Network access controlled VLAN-aware Bridge Port with PAC ... 35
Figure 7-4 Selective relay to a physically secured unauthenticated port ... 36
Figure 7-5 Network infrastructure with a physically secure point-to-point LAN ... 37
Figure 7-6 Network access control with MACsec and a point-to-point LAN ... 38
Figure 7-7 Network access control with MACsec and a point-to-point LAN ... 39
Figure 7-8 Point-to-point LAN within a secured network ... 40
Figure 7-9 Shared media LAN within a secured network ... 40
Figure 7-10 Network access control within the network infrastructure ... 41
Figure 7-11 Network access control with MACsec and a multi-access LAN ... 41
Figure 7-12 Network access control with MACsec and a multi-access LAN ... 43
Figure 7-13 Secure and unsecured connectivity on a multi-access LAN ... 43
Figure 7-14 Group host access ... 44
Figure 7-15 Multipoint connectivity across a Provider Bridged Network ... 45
Figure 7-16 Internal organization of the MAC sublayer in a Provider Bridged Network ... 46
Figure 7-17 Secure PBN transit and access with priority selection ... 47
Figure 7-18 Secure PBN transit and with priority selection ... 47
Figure 8-1 PAEs, PACP, EAP Messages, and EAPOL PDUs ... 49
Figure 8-2 Authenticator-initiated EAP-TLS (success) ... 51
Figure 8-3 Supplicant-initiated EAP exchange ... 51
Figure 8-4 PAE state machines and interfaces ... 53
Figure 8-5 PAE Timer state machines ... 55
Figure 8-6 Supplicant PACP state machine ... 56
Figure 8-7 Authenticator PACP state machine ... 57
Figure 11-1 Common EAPOL PDU structure ... 90
Figure 11-2 EAPOL Start-PDU (Protocol Version ≤ 2) ... 93
Figure 11-3 EAPOL Start-PDU (Protocol Version ≥ 3) ... 93
Figure 11-4 EAPOL-EAP Packet Body with EAP packet format ... 94
Figure 11-5 EAPOL-Key Packet Body with Key Descriptor format ... 94
Figure 11-6 EAPOL-MKA Packet Body with MKPDU format ... 96
Figure 11-7 MKPDU—Parameter set encoding ... 96
Figure 11-8 Basic Parameter Set ... 99
Figure 11-10 MACsec SAK Use parameter set ... 100
Figure 11-9 Live Peer List and Potential Peer List parameter sets ... 100
Figure 11-11 Distributed SAK parameter set (GCM-AES-128) ... 101
Figure 11-12 Distributed SAK parameter set (other MACsec Cipher Suites) ... 101
Figure 11-13 Distributed CAK parameter set ... 101
Figure 11-14 KMD parameter set ... 102
Figure 11-15 Announcement parameter set ... 102
Figure 11-16 ICV Indicator ... 102
Figure 11-17 EAPOL-Announcement ... 104
Figure 11-18 EAPOL-Announcement TLV format ... 104
Figure 11-19 NID Set TLV format ... 105

Copyright © 2010 IEEE. All rights reserved.
Documents
Document Sharing Hub
Full document details: ISO_IEC_IEEE 8802-1X_2013

Figure 11-20 Access Information TLV format 106
Figure 11-21 MACsec Cipher Suites TLV format 107
Figure 11-22 Key Management Domain TLV format 107
Figure 11-23 Organizationally Specific TLV format 107
Figure 11-24 Organizationally Specific Set TLV format 107
Figure 11-25 EAPOL-Announcement-Req (Protocol Version = 3) 109
Figure 12-1 PAE state machines—overview and interfaces 111
Figure 12-2 CP state machine 115
Figure 12-3 PAE management information 125
Figure 13-1 Use of the ifStackTable 127
Figure D-1 MAC entities, the MAC Service, and MAC Service users (clients) 195
Figure D-2 An interface stack 197

Copyright © 2010 IEEE. All rights reserved.

Documents
Document Sharing Hub
Full document details: ISO_IEC_IEEE 8802-1X_2013

Tables

Table 5-1 System recommendations 18
Table 9-1 MKA Algorithm Agility parameter values 64
Table 9-2 Key Server Priority values 67
Table 9-3 MKA Participant timer values 75
Table 10-4 Announcement performance parameters 84
Table 11-1 EAPOL group address assignments 88
Table 11-2 EAPOL Ethernet Type assignment 89
Table 11-3 EAPOL Packet Types 90
Table 11-4 EAPOL Packet Type Destination Addressing 92
Table 11-5 Descriptor Type value assignments 95
Table 11-6 MKA parameters—fixed width encoding 97
Table 11-7 MKPDU parameter sets 98
Table 11-8 EAPOL-Announcement TLVs 104
Table 11-9 Access Information 106
Table 13-1 Use of ifGeneralInformationGroup objects 127
Table 13-4 PAE managed object cross-reference table 128
Table 13-2 Use of ifCounterDiscontinuityGroup Object 128
Table 13-3 Use of ifStackGroup2 Objects 128
Table 13-5 PAC managed object cross-reference table 134
Table C-1 State machine symbols 194

Copyright © 2010 IEEE. All rights reserved.
Documents
Document Sharing Hub
Full document details: ISO_IEC_IEEE 8802-1X_2013

IEEE Standard for
Local and metropolitan area networks—

Port-Based Network Access Control

IMPORTANT NOTICE: This standard is not intended to ensure safety, security, health, or environmental protection in all circumstances. Implementers of the standard are responsible for determining appropriate safety, security, environmental, and health practices or regulatory requirements.

This IEEE document is made available for use subject to important notices and legal disclaimers. These notices and disclaimers appear in all publications containing this document and may be found under the heading "Important Notice" or "Important Notices and Disclaimers Concerning IEEE Documents." They can also be obtained on request from IEEE or viewed at http://standards.ieee.org/IPR/disclaimers.html.

1. Overview

1.1 Scope

For the purpose of providing compatible authentication, authorization, and cryptographic key agreement mechanisms to support secure communication between devices connected by IEEE 802® Local Area Networks (LANs), this standard

a) Specifies a general method for provision of port-based network access control.

b) Specifies protocols that establish secure associations for IEEE Std 802.1AE™ MAC Security.

c) Facilitates the use of industry standard authentication and authorization protocols.

1.2 Purpose

IEEE 802 LANs are deployed in networks that convey or provide access to critical data, that support mission critical applications, or that charge for service. Protocols that configure, manage, and regulate access to these networks and network-based services and applications typically run over the networks themselves. Port-based network access control regulates access to the network, guarding against transmission and reception by unidentified or unauthorized parties, and consequent network disruption, theft of service, or data loss.

Copyright © 2010 IEEE. All rights reserved.

Documents
Document Sharing Hub

Full document details: ISO_IEC_IEEE 8802-1X_2013

1.3 Introduction

The stations attached to an IEEE 802 LAN transmit and receive data frames using the service provided by the IEEE 802 LAN MAC at a service access point, often referred to as a port, within each end station or bridge. Port-based network access control specifies a common architecture comprising cooperative functional elements and protocols that

a) Use the service provided by the LAN MAC, at a common service access point, to support a Controlled Port that provides secure access-controlled communication and an Uncontrolled Port that supports protocols that initiate the secure communication or do not require protection.
b) Support mutual authentication between a Port Access Entity (PAE) associated with a Controlled Port, and a peer PAE associated with a peer port in a LAN attached station that desires to communicate through the Controlled Port.
c) Secure the communication between the Controlled Port and the authenticated peer port, excluding other devices attached to or eavesdropping on the LAN.
d) Provide the Controlled Port with attributes that specify access controls appropriate to the authorization accorded to the peer station or its user.

This standard specifies the use of EAP, the Extensible Authentication Protocol (IETF RFC 3748 [B14][1]), to support authentication using a centrally administered Authentication Server and defines EAP encapsulation over LANs (EAPOL, Clause 11) to convey the necessary exchanges between peer PAEs attached to a LAN.

Where communication over the LAN connecting a Controlled Port to its peer(s) is physically secure, no additional protocol is required to protect their communication. This mode of operation is supported by this standard. More commonly intrusion into the LAN communication is a principal security threat, and the result of mutual authentication is not simply Controlled Port authorization to transmit and receive data, but secure distribution of master keys and associated data to the communicating peers. Proof of possession of master keys subsequently serves as proof of mutual authentication in key agreement protocols. These protocols generate keys that are used to cryptographically protect data frames transmitted and received by the Controlled Port. IEEE Std 802.11™ Wireless LANs specifies protocols that associate wireless stations with access points and initiate mutual authentication using the procedures specified in this standard, the subsequent generation of keys to protect data transfer, and the cryptographic methods that protect data frames using those keys. IEEE Std 802.1AE MAC Security (MACsec) specifies cryptographic support of the Controlled Port for other media access methods. Authenticated key agreement for MAC Security, as specified in this standard, specifies the generation of the Secure Association Keys (SAKs) used by MACsec.

Use of the Controlled Port can be restricted by access controls bound to the results of authentication and distributed via AAA protocols such as Diameter (IETF RFC 3588 [B13]) or RADIUS (IETF RFC 2865 [B8]). Attributes supporting certain port-based network access control scenarios are described in IETF RFC 3580, IETF RFC 4675, and IETF RFC 4849.

Clause 7 illustrates use of the above components and protocols in typical network access control scenarios.

1.4 Provisions of this standard

The scope (1.1) of this standard is addressed by detailed specification of the following:

a) The principles of port-based network access control operation, identifying the protocol components that compose a port-based network access control implementation (Clause 6).

[1]The numbers in brackets correspond to those of the bibliography in Annex B.

Copyright © 2010 IEEE. All rights reserved.

Documents
Document Sharing Hub

Full document details: ISO_IEC_IEEE 8802-1X_2013

b) A PAE component, that supports authentication, authorization, and the key agreement functionality required by IEEE Std 802.1AE to allow a MAC Security Entity (SecY) to protect communication through a port (6.3, Clause 12).

c) A Port Access Controller (PAC) component, that controls communication where the attached LAN is deemed to be physically secure and provides point-to-point connectivity (6.4).

d) The key hierarchy used by the PAE and SecY (6.2).

e) The use of EAP by PAEs to support authentication and authorization using a centrally administered Authentication or AAA Server (Clause 8).

f) An encapsulation format, EAPOL, that allows EAP Messages and other protocol exchanges to support authentication and key agreement to be carried directly by a LAN MAC service (Clause 11).

g) A MAC Security Key Agreement protocol (MKA) that the PAE uses to discover associations and agree the keys used by a SecY (Clause 9).

h) An EAPOL Announcement protocol that allows a PAE to indicate the availability of network services, helping other PAEs to choose appropriate credentials and parameters for authentication and network access (Clause 10).

i) Requirements for management of port-based access control, identifying the managed objects and defining the management operations for PAEs (12.9).

j) SMIv2 MIB objects that can be used with SNMPv3 to manage PAEs (Clause 13).

The use of port-based network access control in a number of applications is described (Clause 7) to illustrate the use of these components and the requirements taken into account in their specification. To facilitate migration to this standard, Annex G (informative) uses the same concepts to describe the architectural modeling of unsecured multi-access LANs, a widely deployed form of authenticated port-based network access control that does not meet the security requirements of this standard. Administrative connectivity to unauthenticated devices, as required for use of industry standard ‘Wake-on-LAN’ (WoL) protocols, is described for the scenarios of Clause 7; Annex F (informative) provides background information on WoL.

This standard defines conformance requirements (Clause 5) for the implementation of the following:

k) Port Access Entities (PAEs)

l) Port Access Controllers (PACs)

Annex A provides PICS (Protocol Implementation Conformance Statement) Proformas for completion by suppliers of implementations that are claimed to conform to this standard.

The basic architectural concepts, such as ‘port’, that this standard relies on are reviewed in Annex D.

This standard uses and selects options provided by EAP and AAA protocol specifications, but does not modify those specifications (see Clause 2 for references). Annex E (informative) provides EAP and RADIUS usage guidelines.

The specification and conformance requirements for association discovery and key agreement for IEEE 802.11 Wireless LANs are outside the scope of this standard (see IEEE Std 802.11). That standard makes use of the PAE specified by this standard.

Copyright © 2010 IEEE. All rights reserved.

Documents
Document Sharing Hub

Full document details: ISO_IEC_IEEE 8802-1X_2013

2. Normative references

The following referenced documents are indispensable for the application of this document (i.e., they must be understood and used, so each referenced document is cited in text and its relationship to this document is explained). For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments or corrigenda) applies.

IEEE Std 802.1D™, IEEE Standard for Local and Metropolitan Area Networks: Media access control (MAC) Bridges.[2, 3]

IEEE Std 802.1Q™, IEEE Standard for Local and Metropolitan Area Networks: Virtual Bridged Local Area Networks.

IEEE Std 802.1AB™, IEEE Standard for Local and Metropolitan Area Networks: Station and Media Access Control Connectivity and Discovery.

IEEE Std 802.1ad™-2005, IEEE Standard for Local and Metropolitan Area Networks: Virtual Bridged Local Area Networks—Amendment 4: Provider Bridges.

IEEE Std 802.1AE™-2006, IEEE Standard for Local and Metropolitan Area Networks: Media Access Control (MAC) Security.

IEEE Std 802.1AX™, IEEE Standard for Local and Metropolitan Area Networks: Link Aggregation.

IEEE Std 802.2™, 1998 Edition [ISO/IEC 8802-2: 1998], Information technology—Telecommunications and information exchange between systems—Local and metropolitan area networks—Specific requirements—Part 2: Logical link control.[4]

IEEE Std 802.3™, IEEE Standard for Information technology—Local and metropolitan area networks—Part 3: Carrier sense multiple access with collision detection (CSMA/CD) access method and physical layer specifications.

IEEE Std 802.11™, IEEE Standard for Information technology—Telecommunications and information exchange between systems—Local and metropolitan area networks—Specific requirements—Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications.

IEEE Std 802.17™-2004 IEEE Standard for Information Technology—Telecommunications and information exchange between systems—Local and metropolitan area networks—Specific requirements—Part 17: Resilient packet ring (RPR) access method and physical layer specifications.

IEEE Std 802.1AR™, IEEE Standard for Local and Metropolitan Area Networks: Secure Device Identifier.

IETF RFC 2578, STD 58, Structure of Management Information for Version 2 of the Simple Network Management Protocol (SNMPv2), McCloghrie, K., Perkins, D., Schoenwaelder, J., Case, J., Rose, M., Waldbusser, S., April 1999.[5]

---

[2]IEEE publications are available from the Institute of Electrical and Electronics Engineers, 445 Hoes Lane, Piscataway, NJ 08854, USA. IEEE publications can be ordered on-line from the IEEE Standards Website: http://www.standards.ieee.org.

[3]The IEEE standards or products referred to in this clause are trademarks of the Institute of Electrical and Electronics Engineers, Inc.

[4]ISO [IEEE] and ISO/IEC [IEEE] documents are available from ISO Central Secretariat, 1 rue de Varembé, Case Postale 56, CH-1211, Genève 20, Switzerland/Suisse; and from the Institute of Electrical and Electronics Engineers, 445 Hoes Lane, Piscataway, NJ 08854, USA. ISO [IEEE] and ISO/IEC [IEEE] documents can be ordered on-line from the IEEE Standards Website: http://www.standards.ieee.org.

[5]IETF RFCs are available from the Internet Engineering Task Force website at http://www.ietf.org/rfc.html.

Copyright © 2010 IEEE. All rights reserved.

Documents Document Sharing Hub

Full document details: ISO_IEC_IEEE 8802-1X_2013

IETF RFC 2579, STD 58, Textual Conventions for Version 2 of the Simple Network Management Protocol (SNMPv2), McCloghrie, K., Perkins, D., Schoenwaelder, J., Case, J., Rose, M., Waldbusser, S., April 1999.

IETF RFC 2580, STD 58, Conformance Statements for SMIv2, McCloghrie, K., Perkins, D., Schoenwaelder, J., Case, J., Rose, M., Waldbusser, S., April 1999.

IETF RFC 2863, The Interfaces Group MIB using SMIv2, McCloghrie, K. and Kastenholz, F., June 2000.

IETF RFC 2869, RADIUS Extensions, Rigney, C., Willats, W., and Calhoun, P., June 2000.

IETF RFC 3394, Advanced Encryption Standard (AES) Key Wrap Algorithm, J. Schaad, R. Housley, September 2002.

IETF RFC 3410, Introduction and Applicability Statements for Internet Standard Management Framework, J. Case, R. Mundy, D. Partain, B. Stewart, December 2002.

IETF RFC 3579, RADIUS (Remote Authentication Dial In User Service) Support For Extensible Authentication Protocol (EAP), Aboba, B., Calhoun, P., September 2003.

IETF RFC 3580, IEEE 802.1X Remote Authentication Dial In User Service (RADIUS) Guidelines, Congdon, P., Aboba, B., Smith, A., Zorn, G., Roese, J., September 2003.

IETF RFC 3629, STD 63, UTF-8, a transformation format of ISO 10646, Yergeau, F., November 2003.

IETF RFC 4017, Extensible Authentication Protocol (EAP) Method Requirements for Wireless LANs, Stanley, D., Walker, J., Aboba, B., March 2005.

IETF RFC 4346, The Transport Layer Security (TLS) Protocol Version 1.1, Diercks, T., Rescorla, E., April 2006.

IETF RFC 4675, RADIUS Attributes for Virtual LAN and Priority Support, Congdon, P., Sanchez, M., Aboba, B., September 2006.

IETF RFC 5216, The EAP-TLS Authentication Protocol, Simon, D., Aboba, B., Hurst, R., March 2008.

IETF RFC 5247, Extensible Authentication Protocol (EAP) Key Management Framework, Aboba, B., Simon, D., Eronen, P., October 2007.

FIPS Publication 197, The Advanced Encryption Standard (AES), U.S. DoC/NIST, November 26, 2001.

NIST Federal Information Processing Standard 140-2, Security Requirements for Cryptographic Modules[6], 3 December 2002.NIST Special Publication 800-38B, Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication, Morris Dworkin, May 2005.[7]

NIST Special Publication 800-90, Recommendation for Random Number Generation Using Deterministic Random Bit Generators, E. Barker, J. Kelsey, revised March 2007.

NIST Special Publication 800-108, Recommendation for Key Derivation Using Pseudorandom Functions, Lily Chen, November 2008.

[6]National Institute of Standards and Technology, FIPS 140-2 is available at http://www.nist.gov/cmvp.
[7]NIST Special Publications (800 Series) are available at http://csrc.nist.gov/publications/PubsSPs.html.

Copyright © 2010 IEEE. All rights reserved.

Documents
Document Sharing Hub

Full document details: ISO_IEC_IEEE 8802-1X_2013

3. Definitions

For the purposes of this document, the following terms and definitions apply. *The IEEE Standards Dictionary: Glossary of Terms & Definitions* should be referenced for terms not defined in this clause.[8]

Association Number (AN): A number that is concatenated with a MACsec Secure Channel Identifier to identify a Secure Association.

authentication exchange: The two-party conversation between systems performing an authentication process.

NOTE—For example, Extensible Authentication Protocol (EAP) and Simple Authentication and Security Layer (SASL).[9]

authentication process: The cryptographic operations and supporting data frames that perform the actual authentication.

Authentication Server: An entity that provides an authentication service to an Authenticator. This service determines, from the credentials provided by the Supplicant, whether the Supplicant is authorized to access the services provided by the system in which the Authenticator resides.

NOTE—The Authentication Server function can be co-located with an Authenticator, or it can be accessed remotely via a network to which the Authenticator has access.

Authenticator: An entity that facilitates authentication of other entities attached to the same LAN.

bounded receive delay: A guarantee that a frame will not be delivered after a known bounded time, in the case of protocols designed to use the MAC Service this is typically assumed to be less than two seconds.

Bridged Local Area Network: A concatenation of individual IEEE 802 LANs interconnected by MAC Bridges.

NOTE—Unless explicitly specified the use of the word *network* in this Standard refers to a Bridged Local Area Network. The term Bridged Local Area Network is not otherwise abbreviated. The term Local Area Network and the abbreviation LAN are used exclusively to refer to an individual LAN specified by a MAC technology without the inclusion of Bridges. This precise use of terminology within this specification allows a Bridged Local Area Network to be distinguished from an individual LAN that has been bridged to other LANs in the network. In more general usage such precise terminology is not required.

Bridge Port: A Port of an IEEE 802.1D or IEEE 802.1Q Bridge.

Cipher Suite: A set of one or more algorithms, designed to provide any number of the following: data confidentiality, data authenticity, data integrity, replay protection.

clear: When applied to a Boolean variable, **clear** means to make the value of the variable false. *See also:* **set**.

client: The protocol entity that makes use of a service.

Common Port: an instance of the MAC Internal Sublayer Service used by the SecY to provide transmission and reception of frames for both the controlled and uncontrolled ports.

[8] *The IEEE Standards Dictionary: Glossary of Terms & Definitions* is available at http://shop.ieee.org/.

[9] Notes in text, tables, and figures are given for information only, and do not contain requirements needed to implement the standard.

Copyright © 2010 IEEE. All rights reserved.

Documents Document Sharing Hub

Full document details: ISO_IEC_IEEE 8802-1X_2013

Controlled Port: The access point used to provide the secure MAC Service to a client of a SecY.

cryptographic key: A parameter that determines the operation of a cryptographic function such as the following:

a) The transformation from plain text to cipher text and vice versa
b) Synchronized generation of keying material
c) Digital signature computation or validation[10]

cryptographic mode of operation: Also referred to as mode. An algorithm for the cryptographic transformation of data that features a symmetric key block cipher algorithm.[11]

data integrity: A property whereby data has not been altered in an unauthorized manner since it was created, transmitted or stored.[12]

entity authentication: The process of identifying and verifying the identity of an entity, using credentials issued to entities (e.g., username/password, token card, public-key-certificates).

frame: MAC protocol data unit (MPDU).

IEEE 802 Local Area Network (LAN): IEEE 802 LANs (also referred to in the text simply as LANs) are LAN technologies that provide a MAC Service equivalent to that defined in ISO/IEC 15802-1. IEEE 802 LANs include IEEE Std 802.3 (CSMA/CD), IEEE Std 802.11 (Wireless), and IEEE Std 802.17 (Resilient Packet Ring).

ifIndex: A unique identifying number associated with a logical or physical interface. The term ifIndex is defined and used by SNMP standards.

initialization vector (IV): A vector used in defining the starting point of an encryption process within a cryptographic algorithm.[13]

integrity: *See:* **data integrity**.

Integrity Check Value (ICV): A value that is derived by performing an algorithmic transformation on the data unit for which data integrity services are provided. The ICV is sent with the protected data unit and is recalculated and compared by the receiver to detect data modification.

key: *See:* **cryptographic key**.

Key Agreement Entity (KaY): A PAE entity responsible for MKA.

key management: The generation, storage, distribution, deletion, archiving, and application of keys in accordance with a security policy.

Key Management Domain (KMD): A string that identifies systems that share cached CAKs.

[10]This and other definitions in this clause have been drawn from ASC X9 TR1, Technical Report for ABA ASC/X9 Standards Definitions, Acronyms, and Symbols, 2002.

[11]This and other definitions in this clause have been drawn from Federal Information Processing Standard (FIPS) 300-38A, Recommendation for Block Cipher Modes of Operation: Methods and Techniques, 2001.

[12]This and other definitions in this clause have been drawn from Federal Information Processing Standard (FIPS) 800-57, Recommendation for Key Management, 2005.

[13]This and other definitions in this clause have been drawn from Federal Information Processing Standard (FIPS) 140-2, Security Requirements for Cryptographic Modules, 2001.

Copyright © 2010 IEEE. All rights reserved.

Documents
Document Sharing Hub

Full document details: ISO_IEC_IEEE 8802-1X_2013

Layer Management Interface (LMI): the interface between a protocol entity in a system and the system management, providing for the exchange of parameters with other system entities that are not attached to the service access points used and provided by the protocol entity.

MAC Security Entity (SecY): The entity that operates the MAC Security protocol within a system.

MAC Security TAG (SecTAG): A protocol header, comprising a number of octets and beginning with an EtherType, that is prepended to the service data unit supplied by the client of the protocol, and is used to provide security guarantees.

MAC service data unit (MSDU): A sequence of zero or more octets that compose the data to be communicated with a single MAC Service request or indication.

master key: A secret key that is used to derive one or more cryptographic keys that are used directly to protect data transfer.

message authentication: If the message arrives authenticated, the cryptographic guarantee is that the message was not modified in transit and that the message originated from an entity with the proper cryptographic credentials.

mode: *See:* **cryptographic mode of operation.**

multipoint: Involving or potentially involving more than one participant in the role of receiver, or in the role of transmitter, in a single data transfer or set of related data transfers.

network access point: A system, typically incorporating bridging or routing functionality, that comprises one or more network access ports that provides controlled access to a network for one or more systems, usually hosts.

network access port: A point of attachment of a system to a LAN. It can be a physical port, for example, a single LAN MAC attached to a physical LAN segment, or a logical port, for example, an IEEE 802.11 association between a station and an access point.

Network Identity (NID): A UTF-8 (IETF RFC 3629) string identifying an network or network service.

nonce: A non-repeating value, such as a counter, used in key management protocols to thwart replay and other types of attack.

packet number (PN): A monotonically increasing value used to uniquely identify a MACsec frame in the sequence of frames transmitted using an SA.

Port: A service access point for the MAC Service or MAC Internal Sublayer Service.

port access entity (PAE): The protocol entity associated with a Port. It can support the protocol functionality associated with the Authenticator, the Supplicant, or both.

Port Identifier: A 16-bit number that is unique within the scope of the address of the port.

protocol data unit (PDU): A unit of data specified in a protocol and consisting of protocol information and, possibly, user data.

real port: A port that is not created on demand by the mechanisms specified in this standard, but that can transmit and receive frames for one or more virtual ports.

Copyright © 2010 IEEE. All rights reserved.

Documents
Document Sharing Hub

Full document details: ISO_IEC_IEEE 8802-1X_2013

secret key: A cryptographic key used with a secret key cryptographic algorithm that is uniquely associated with one or more entities and should not be made public.[14]

Secure Association (SA): A security relationship that provides security guarantees for frames transmitted from one member of a CA to the others. Each SA is supported by a single secret key, or a single set of keys where the cryptographic operations used to protect one frame require more than one key.

Secure Association Identifier (SAI): An identifier for an SA, comprising the SCI concatenated with the Association Number (AN).

Secure Association Key (SAK): The secret key used by an SA.

Secure Channel (SC): A security relationship used to provide security guarantees for frames transmitted from one member of a CA to the others. An SC is supported by a sequence of SAs thus allowing the periodic use of fresh keys without terminating the relationship.

Secure Channel Identifier (SCI): A globally unique identifier for a secure channel, comprising a globally unique MAC Address and a Port Identifier, unique within the system that has been allocated that address.

secure Connectivity Association (CA): A security relationship, established and maintained by key agreement protocols, that comprises a fully connected subset of the service access points in stations attached to a single LAN that are to be supported by MACsec.

secure Connectivity Association Key (CAK): A secret key possessed by members of a given CA.

secure Connectivity Association Key Name (CKN): A text that identifies a CAK.

secured connectivity: Data transfer between two or more Controlled Ports that is protected by MACsec.

NOTE—MACsec requires mutual authentication between communicating peers, so secured connectivity is always authenticated. Connectivity that is not secured could have been preceded by mutual authentication, but is not proof against intrusion.

set: When applied to a Boolean variable, **set** means to make the value of the variable true. *See also:* **clear**.

Supplicant: An entity at one end of a point-to-point LAN segment that seeks to be authenticated by an Authenticator attached to the other end of that link.

NOTE—The term *Supplicant* is used in this standard in place of the term *peer*, used in other access control-related specifications, as peer is used throughout IEEE 802.1 standards and elsewhere to denote a protocol entity of equal status in a layered protocol model.

system: A device that is attached to a LAN by one or more Ports. Examples of systems include end stations, servers, MAC Bridges, and routers.

unauthenticated connectivity: Data transfer between peers that are not mutually authenticated (such data transfer cannot be secured by MACsec).

Uncontrolled Port: the access point used to provide the insecure MAC Service to a client of a SecY.

unsecured connectivity: Data transfer that is not protected by MACsec, but has been preceded by mutual authentication between the (supposedly) communicating peers.

virtual port: A MAC Service or Internal Sublayer service access point (D.4) that is created on demand. Virtual ports can be used to provide separate secure connectivity associations over the same LAN.

[14]FIPS 140-2.

Copyright © 2010 IEEE. All rights reserved.

Documents
Document Sharing Hub

Full document details: ISO_IEC_IEEE 8802-1X_2013

4. Acronyms and abbreviations

For the purposes of this standard, the following acronyms and abbreviations apply. *The IEEE Standards Dictionary: Glossary of Terms & Definitions* should be referenced for acronyms not defined in this clause.[15]

AAA	authentication, authorization, and accounting
AES	Advanced Encryption Standard
AN	Association Number
ASF	Alerting Standards Forum
CA	Secure Connectivity Association
CAK	Secure Connectivity Association Key
CKN	Secure Connectivity Association Key Name
CMAC	Cipher-based Message Authentication Code
CP	PAE Controlled Port state machine
DA	Destination Address
DHCP	Dynamic Host Configuration Protocol
EAP	Extensible Authentication Protocol
EAP-TLS	EAP Transport Layer Security
EAPOL	EAP over LANs
EPON	Ethernet Passive Optical Network
ES	End station
FDDI	Fiber Distributed Data Interface
FIPS	Federal Information Processing Standard
ICK	ICV Key
ICV	Integrity Check Value
IP	Internet Protocol
ISS	Internal Sublayer Service
IV	Initialization Vector
KaY	MAC Security Key Agreement Entity
KDF	Key Derivation Function
KEK	Key Encrypting Key
KI	Key Identifier
KMD	Key Management Domain
LAN	IEEE 802 Local Area Network
LLC	Logical Link Control
LLDP	Link Layer Discovery Protocol
LLPN	Lowest acceptable PN for the Latest Key
LMI	Layer Management Interface
LPN	Lowest acceptable PN
MAC	Media Access Control
MI	Member Identifier
MIB	Management Information Base
MKA	MACsec Key Agreement protocol
MKPDU	MACsec Key Agreement Protocol Data Unit
MN	Message Number
MPDU	MAC Protocol Data Unit
MSAP	MAC Service Access Point
MSDU	MAC Service Data Unit
MSK	Master Session Key
NID	Network Identity
NIST	National Institute of Standards and Technology

[15] *The IEEE Standards Dictionary: Glossary of Terms & Definitions* is available at http://shop.ieee.org/.

Copyright © 2010 IEEE. All rights reserved.

Documents Document Sharing Hub

Full document details: ISO_IEC_IEEE 8802-1X_2013

OLPN	Lowest acceptable PN for the Old Key
OUI	Organizationally Unique Identifier
PAC	Port Access Controller
PACP	Port Access Control Protocol
PAE	Port Access Entity
PBBN	Provider Backbone Bridged Network
PBN	Provider Bridged Network
PDU	Protocol data unit
PN	Packet Number
PSK	pre-shared key
PVID	Port VID
RADIUS	Remote Authentication Dial in User Service
RNG	Random number generator
SA	Secure Association
SAI	Secure Association Identifier
SAK	Secure Association Key
SASL	Simple Authentication and Security Layer
SC	Secure Channel
SCB	Single Copy Broadcast
SCI	Secure Channel Identifier
SecTAG	MAC Security TAG
SecY	MAC Security Entity
SMIv2	Structure of Management Information version 2
SNAP	Subnetwork Access Protocol
SNMP	Simple Network Management Protocol
TLV	Type Length Value (a form of encoding, or an item encoded using that encoding)
VID	VLAN Identifier
VLAN	Virtual LAN
WoL	Wake-on-LAN

Copyright © 2010 IEEE. All rights reserved.

Documents
Document Sharing Hub
Full document details: ISO_IEC_IEEE 8802-1X_2013

5. Conformance

A claim of conformance to this standard is a claim that the behavior of a system meets requirements of this standard for the operation of protocols, management of protocol operation, and provision of service to other systems, as revealed through externally observable behavior of the system.

This clause specifies requirements and options for implementation of system components (5.3) that support port-based network access control, and requirements and options for each of those components (5.4–5.13). Conformance to this standard does not ensure that a system is secure, or that other protocols supported by the system do not provide a way for an attacker to breach that security.

5.1 Requirements terminology

For consistency with existing IEEE and IEEE 802.1 standards, requirements placed upon conformant implementations of this standard are expressed using the following terminology:

a) ***shall*** is used for mandatory requirements
b) ***may*** is used to describe implementation or administrative choices (*may* means is permitted to, hence *may* and *may not* mean precisely the same thing)
c) ***should*** is used for recommended choices (the behaviors described by *should* and *should not* are both permissible but not equally desirable choices).

The PICS proforma (Annex A) reflects occurrences of the words shall, may, and should within the standard.

The standard avoids needless repetition and apparent duplication of its formal requirements by using ***is***, ***is not***, ***are***, and ***are not*** for definitions and the logical consequences of conformant behavior. Behavior that is permitted but is neither always required nor directly controlled by an implementor or administrator, or whose conformance requirement is detailed elsewhere, is described by ***can***. Behavior that never occurs in a conformant implementation or system of conformant implementations is described by ***cannot***. The word ***allow*** means that the mechanisms specified by this standard are intended to support the indicated use or capabilities, and the word ***capable*** means “is configurable such that ...”.

5.2 Protocol Implementation Conformance Statement

The supplier of an implementation that is claimed to conform to this standard shall complete a copy of the PICS proforma provided in Annex A and shall provide the information necessary to identify both the supplier and the implementation.

Where this conformance clause (Clause 5) requires additional information concerning the capabilities of an implementation that information shall also be specified as part of the PICS.

Port-based network access control can be implemented for each of a number of ports of a given system. The ports, and any restrictions placed on individual ports or their total number, shall be specified. If the components or options implemented for different classes of ports differ, a separate PICS shall be completed for each class of port.

The provisions of this standard can require the implementation of one or more MAC Security Entities for each port, as specified by IEEE Std 802.1AE. One or more PICS, as specified by IEEE Std 802.1AE, shall be completed for those ports.

Copyright © 2010 IEEE. All rights reserved.

Documents
Document Sharing Hub

Full document details: ISO_IEC_IEEE 8802-1X_2013

5.3 Conformant systems and system components

This clause (5) specifies requirements and options for implementation of the following components:

a) Port Access Entity (PAE, see 6.3, Clause 12) (5.4, 5.5, 5.6–5.15, 5.18, 5.19)
b) Port Access Controller (PAC, see 6.4) (5.20)

A port for which conformance to this standard is claimed shall implement the mandatory functions of the PAE (5.4) and the mandatory functionality for at least one of the following PAE functions:

— Supplicant (5.6, 5.7)
— Authenticator (5.8, 5.9)
— MACsec Key Agreement (MKA) (5.10, 5.11)

That port may also implement the mandatory functionality for all or any of the following PAE functions:

— Announcement transmission (5.14, 5.15)
— Announcement reception (5.16, 5.17)
— SNMP access to the PAE MIB (5.18, 5.19)

A port that implements Authenticator or MKA functionality may also implement the mandatory functionality for the following PAE function:

— Virtual ports (5.12)

A port may implement the optional functionality for any function for which the mandatory functionality has been implemented.

The operation of one or more MAC Security Entities (as specified by IEEE Std 802.1AE) can be required to secure communication for each port. A port that does not implement a SecY shall implement the PAC (5.20).

Any implementation that is claimed to conform to this standard shall not violate the provisions of 5.22 (Prohibitions).

5.4 PAE requirements

A PAE shall

a) Encode, decode, address, and validate EAPOL PDUs as specified in Clause 11.
b) Transmit group addressed EAPOL PDUs using one, and only one, of the destination addresses specified in Table 11-1.
c) Implement the Logon Process functionality specified in 12.5.
d) Implement the CP state machine as specified in 12.4.
e) Maintain and allow retrieval of the EAPOL frame reception statistics specified in 12.8.1.
f) Maintain and allow retrieval of the EAPOL frame reception diagnostics specified in 12.8.2.
g) Maintain and allow retrieval of the EAPOL frame transmission statistics specified in 12.8.3.
h) Support the system configuration functions specified in 12.9.

A PAE that supports both EAP (Supplicant or Authenticator) and MKA functionality shall

i) Derive a CAK from each EAP MSK, and a corresponding CKN for the corresponding EAP session ID as specified in 6.2.2.

Copyright © 2010 IEEE. All rights reserved.

Documents
Document Sharing Hub

Full document details: ISO_IEC_IEEE 8802-1X_2013

A claim that an implementation conforms to this standard shall specify

j) The group address used to transmit group addressed PDUs. If the implementation can be configured in a way that changes the address used, that configuration shall be specified.

A PAE shall not

k) Use a MACsec protected Controlled Port to transmit EAPOL Packet Types other than EAPOL-Announcement (10.2).

5.5 PAE options

This standard does not specify any options for PAE conformance other than those detailed in 5.6 through 5.15.

5.6 Supplicant requirements

A Supplicant shall

a) Use EAP as an authentication protocol, exhibiting external behavior consistent with an implementation of the Supplicant PACP state machine, state machine variables, procedures, and interfaces specified in Clause 8.
b) Not use any EAP method that fails to meet the requirements specified in 8.11.

5.7 Supplicant options

5.7.1 Integration with IEEE Std 802.1AR

An implementation that is claimed to conform to the provisions of this standard for integration with IEEE Std 802.1AR shall

a) Implement the EAP method EAP-TLS as specified in 8.11.2.

5.8 Authenticator requirements

An Authenticator shall

a) Use EAP as an authentication protocol, exhibiting external behavior consistent with an implementation of the Authenticator PACP state machine, state machine variables, procedures, and interfaces specified in Clause 8.
b) Not use any EAP method that fails to meet the requirements specified in 8.11.
c) Allow remote configuration of the reAuthEnabled and reAuthPeriod parameters specified in 8.6 and 8.9.

5.9 Authenticator options

An Authenticator may

a) Maintain and allow retrieval of the Authenticator PAE diagnostic counters specified in 8.10.

Copyright © 2010 IEEE. All rights reserved.

Documents
Document Sharing Hub

Full document details: ISO_IEC_IEEE 8802-1X_2013

5.9.1 Integration with IEEE Std 802.1AR

An implementation that is claimed to conform to the provisions of this standard for integration with IEEE Std 802.1AR shall

a) Implement the EAP method EAP-TLS as specified in 8.11.2.

5.10 MKA requirements

A PAE that supports MKA shall

a) Be capable of maintaining 2 or more simultaneous MKA instances as specified in Clause 9.
b) Specify the maximum number of simultaneous MKA instances it supports.
c) Create, delete, and activate MKA participants as specified in 9.13 and 9.16.
d) Be capable of receiving and using Group CAKs distributed by a Key Server.
e) Meet the requirements for MKA parameter encoding and for MKPDU validation, encoding, and decoding, specified in 11.11.
f) Be capable of using 128 bit CAKs and derived keys as specified in 6.2 and 9.3.
g) Observe the restrictions on the use and disclosure of each CAK and derived keys specified in 6.2 and 9.16.
h) Protect each distributed CAK and SAK by AES Key Wrap, as specified in 9.8.2 and 9.12.1.
i) Include the parameters of EAPOL-Announcements in MKPDUs, as specified in 9.13.

5.11 MKA options

A PAE that supports MKA may

a) Be capable of using a 256 bit CAK and derived keys as specified in 6.2 and 9.3.

5.11.1 Support for PSKs

A PAE that supports Pre-Shared Keys (PSKs) shall

a) Support the configuration of PSKs in the CAK Cache as specified in 6.3.3 and 12.6.

5.11.2 Key Server support for Group CAs

A PAE that supports Group CAs as an MKA Key Server

a) Shall be capable of operating as an MKA Key Server (9.5).
b) If support for EAP Authenticator functionality is claimed, shall be capable of:
   1) Distributing a group CAK using MKA with EAP derived pairwise CAKs (6.2, 9.12).
c) If support for PSKs is claimed, shall be capable of:
   1) Distributing a group CAK using an MKA instance with a PSK (6.2, 6.3.3, 9.12).

5.11.3 CAK Cache

A PAE that implements a CAK Cache shall

a) Associate a lifetime with each cached CAK, deleting the CAK when that lifetime has expired as specified in 12.6.
b) Associate a CKN, KMD, NID, and other relevant authorization information with each cached CAK, as specified in 12.6.

Copyright © 2010 IEEE. All rights reserved.

Documents
Document Sharing Hub
Full document details: ISO_IEC_IEEE 8802-1X_2013

c) Cache group CAKs distributed by an MKA Key Server, as specified in 12.6.
d) If support for EAP Authenticator or EAP Supplicant functionality is claimed, shall be capable of:
   1) Caching pairwise CAKs derived from EAP exchanges.

A PAE shall not

e) Cache a CAK derived from an EAP exchange if that is prohibited by 12.6.
f) Distribute a KMD for a Group CAK unless the PAE distributed the CAK when acting as a Key Server as specified in 12.6.

5.12 Virtual port requirements

A PAE that supports the use of virtual ports shall

a) Specify the number of virtual ports that can be supported for each real port, or for the system as a whole.
b) Implement MKA functionality, and be capable of operating 2 or more simultaneous MKA instances for each of the specified number of virtual ports.
c) Support each virtual port with a SecY.
d) Create and manage virtual ports as specified in 6.3.6, 9.14, and 12.7.
e) Shall not create or maintain virtual ports if Supplicant functionality is enabled for the real port.

A PAE that supports both virtual ports and Authenticator functionality shall

f) Be capable of supporting at least the same number of simultaneous EAP Exchanges as the number of virtual ports supported.

A PAE implementation that creates virtual ports in a system that bridges frames to and from those ports as specified by IEEE Std 802.1D or IEEE Std 802.1Q shall

g) Support each of those virtual ports as specified by that standard (IEEE 802.1D or IEEE 802.1Q, as applicable) for each Bridge Port, including support for Spanning Tree Protocol (see 7.6).

5.13 Virtual port options

No options are specified for virtual port creation and deletion.

5.14 Announcement transmission requirements

A PAE that transmits EAPOL-Announcements shall

a) Support the use of the null NID and zero or more additional NIDs as specified in Clause 10.
b) Be capable of using the Uncontrolled Port to transmit generic EAPOL-Announcements containing the information for each supported NID, as specified in 10.1 and 10.2.
c) Encode EAPOL-Announcements as specified in 11.12
d) Rate limit the transmission of announcements as specified in 10.2.

A PAE that transmits EAPOL-Announcements shall not

e) Transmit EAPOL-Announcements through an unsecured Controlled Port (10.2).

Copyright © 2010 IEEE. All rights reserved.

Documents
Document Sharing Hub

Full document details: ISO_IEC_IEEE 8802-1X_2013

5.15 Announcement transmission options

No options are specified for conformance to Announcement transmission functionality.

5.16 Announcement reception requirements

A PAE that listens to EAPOL-Announcements shall

a) Interpret each received EAPOL-Announcement as specified in Clause 11 and Clause 10.
b) Be capable of using a received EAPOL-Announcement to select one or more NIDs, each representing a network or network service, and using the authentication procedure or procedures advertised for that NID subject to the applicable Logon Process controls as specified in Clause 10 and 12.5.
c) Be capable of soliciting an EAPOL-Announcement by transmitting an EAPOL-Announcement-Req as specified in 11.13.
d) Be capable of encoding a Packet Body in an EAPOL-Announcement-Req, including TLVs to select a NID, as specified in 11.13.
e) Be capable of selecting an appropriate credential, for authentication for access to a desired NID, for use by the PAE's Supplicant (if implemented).
f) Be capable of being configured so as to ignore a received EAPOL-Announcement for all NIDs.

A Supplicant that listens to EAPOL-Announcements shall

g) Be capable of encoding a Packet Body in an EAPOL-Start, including TLVs to select a NID, as specified in 11.6.

5.17 Announcement reception options

No options are specified for conformance to Announcement reception functionality.

5.18 Requirements for SNMP access to the PAE MIB

An implementation that is claimed to conform to the provisions of this standard for access to the PAE MIB using SNMP shall

a) Support access to the MIB module specified in Clause 13 using SNMP version v3 or higher.

5.19 Options for SNMP access to the PAE MIB

No options are specified for SNMP access to the PAE MIB.

5.20 PAC requirements

A PAC shall

a) Provide an Uncontrolled Port, for use by the PAE, and a Controlled Port as specified in 6.4.

Copyright © 2010 IEEE. All rights reserved.

Documents
Document Sharing Hub
Full document details: ISO_IEC_IEEE 8802-1X_2013

5.21 System recommendations

Whether the use of a given system or port is appropriate in a given network access control scenario involves considerations that go beyond the scope of this standard, and include details of the port's interface stack, higher layer EAP functionality, and the mechanisms chosen to support unauthenticated connectivity. Clause 7 illustrates use of the components and protocols specified in this standard in typical scenarios. Table 5-1 makes recommendations for the use of this standard, for each of the system roles in each scenario.

5.22 Prohibitions

An implementation that is claimed to conform to this standard shall not

a) Support access to the MIB specified in Clause 13 or any other MIB that provides access to the functionality provided by the implementation using any version of SNMP prior to version 3.

Table 5-1—System recommendations

Clause 7 scenario and system role	System role	Minimum functionality	Recommended functionality
7.1 Host access with physically secure LANs	Host	Supplicant, PAC	Supplicant, MKA, Listener,[a] PAC, or SecY
	Network access point	Authenticator, PAC	Authenticator, Announcer, MKA, PAC, or SecY
7.2 Infrastructure support with physically secure LANs	Intermediate System	Supplicant or Authenticator or MKA with PSKs, PAC	Supplicant, Authenticator, Announcer[b], Listener, MKA with PSKs, PAC, or SecY
7.3 Host access with MACsec and point-to-point LANs	Host	Supplicant, MKA, SecY	Supplicant, Listener, MKA with CAK cache, SecY
	Network access point	Authenticator, MKA, SecY	Authenticator, Announcer, MKA with CAK cache, SecY
7.4 Use with MACsec to support infrastructure LANs	Intermediate System	MKA with PSKs, SecY	Supplicant, Authenticator, Announcer, MKA with PSKs and CAK cache, SecY
7.5 Host access with MACsec and a multi-access LAN	Host	Supplicant, MKA, SecY	Supplicant, Listener, MKA with CAK cache, SecY
	Network access point	Authenticator, MKA, Virtual ports, SecY	Authenticator, Announcer, MKA with CAK cache, SecY
7.6 Group host access with MACsec	Host	Supplicant, MKA, SecY	Supplicant, Listener, MKA with CAK cache, SecY
	Network access point	Authenticator, MKA with Key Server support for Group CA, SecY	Authenticator, Announcer, MKA with Key Server support for Group CA and CAK cache, SecY
7.7 Use with MACsec to support virtual shared media infrastructure LANs	Intermediate System	MKA with PSKs, Key Server support for Group CA, CAK cache, SecY	Supplicant, Authenticator, Announcer[b], Listener, MKA with PSKs, Key Server support for Group CA, CAK cache, SecY

[a]Listener: PAE option of listening to EAPOL announcements.
[b]Announcer and Listener functionality are recommended for 7.2 and 7.7 to facilitate deployment and error detection. Deployed infrastructure devices typically have a single policy preconfigured.

Copyright © 2010 IEEE. All rights reserved.

Documents Document Sharing Hub

Full document details: ISO_IEC_IEEE 8802-1X_2013

6. Principles of port-based network access control operation

Port-based network access control allows network administrators to restrict the use of IEEE 802 LAN service access points (ports) to secure communication with authenticated and authorized systems. This clause specifies the following:

a) Functions performed by cooperating systems that support port-based network access control (6.1).
b) The cryptographic key hierarchy used to secure communication (6.2).
c) A Port Access Entity (PAE, 6.3, Clause 12) that can
   1) Use EAP to provide mutual authentication;
   2) Support the configuration of pre-shared keys (PSKs) to support mutual authentication;
   3) Support the use of an IEEE Std 802.1AR device identity to support mutual authentication;
   4) Identify a network and key management domain to allow selection of parameters for network use and to support roaming;
   5) Meet the requirements specified in IEEE Std 802.1AE for support of the SecY, including agreeing the cryptographic keys to be used to protect data.
d) A Port Access Controller (PAC), a protocol shim that may be used to enforce access when the SecY or a media specific method for cryptographically securing communication is not used (6.4).

This clause and the other provisions of this standard also specify how the following may be used in conjunction with this standard:

e) The MAC Security Entity (SecY) specified in IEEE Std 802.1AE
f) Link Aggregation as specified in IEEE Std 802.1AX (6.5)
g) IEEE Std 802.11 (6.6)
h) IEEE Std 802.1AR (5.7, 8.11.2)

The system entities and options implemented for a given port can depend on the port-based network access control applications that the system is designed to support. For example, when cryptographic protection of data by a SecY is not required, a PAC can be used. The design of the PAE maximizes interoperability between all combinations, so far as the security requirements of each communicating system and the possibility of physical communication permit.

The mechanisms specified in this standard allow any type of system, including bridges and routers, to authenticate, authorize, and secure communications through one of its ports to any other system attached to the same LAN. Since that other system can also be a bridge or router, authentication and authorization can be required to determine whether each system can trust the other to extend the network and the authentication boundary to its own ports, prior to permitting traffic through controlled ports.

An understanding of architectural concepts common to this and other IEEE 802.1 standards is essential to understanding this standard's specification of port-based network access control. The reader is encouraged to review Annex D prior to reading the rest of this standard, and needs to be familiar with IEEE Std 802.1AE's description of secure LAN communication architecture including the fundamental concept of a Secure Connectivity Association (CA).

6.1 Port-based network access control architecture

The system architecture that supports port-based network access control includes the following:

a) The port, i.e., entities that compose an interface stack supporting a MAC Service access point, through which communication is controlled and secured.
b) The attached LAN, providing the MAC service to the port's client (D.6) and its peers.
c) Mechanisms that define a connectivity association between the port and a peer port or ports.

Copyright © 2010 IEEE. All rights reserved.

Documents
Document Sharing Hub

Full document details: ISO_IEC_IEEE 8802-1X_2013

and, for each port that is a potential peer in secure access controlled communication, a protocol entity or entities that

d) Possess an authentication credential, is within or attached to the same system as the port, and has a secure relationship with the port and its clients (D.6).
e) Mutually authenticate peer ports, and whose operation results in
   1) Success or failure of the authentication.
   2) A token, comprising cryptographic keys and associated data, that can serve as a proof of mutual authentication in subsequent protocols.
   3) A binding to authorization data or to a secure channel that can be used to communicate authorization data to the access controlled port and its clients.
f) Communicate authorization data to the port's clients (D.6), so that each can permit or deny the use of manageable protocol capabilities appropriately.
g) Use the results of authentication to agree on keys to cryptographically protect communication, creating a secure connectivity association between peer ports.
h) Protect the data transferred within the secure connectivity association.
i) Enforce access control based on the success or failure of the authentication.

Figure 6-1 illustrates the relationships between each of these processes, in an application scenario that uses a AAA server to centralize administration of authentication and authorization.

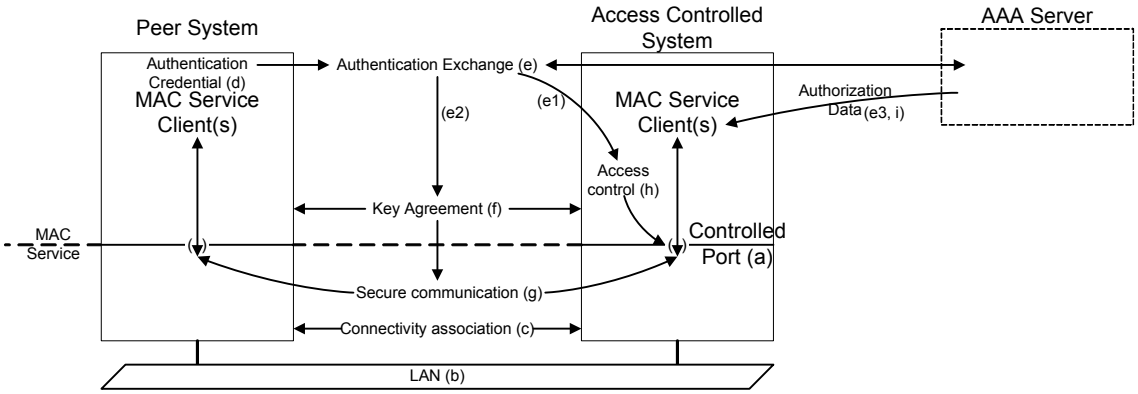

Figure 6-1—Port-based network access control processes

While the protocol entities and options used to implement port-based network access control can vary, most application scenarios (Clause 7) require the majority of functions shown in Figure 6-1 to be present and performed by entities that have the same relationship to each other and to other system components. Figure 6-2 illustrates these with reference to the use of MACsec with authentication and authorization provided by a AAA server, using EAP: the Access Controlled and Peer Systems shown in Figure 6-1 act as the EAP Authenticator and the EAP Supplicant respectively.

In Figure 6-2, authentication exchanges are supported by the Port Access Entity (PAE, 6.3, Clause 12) using EAP and EAPOL (Clause 11) as specified in this standard (Clause 8). In order to provide a specific example Figure 6-2 references the use of EAP in RADIUS to support authentication exchanges with a AAA Server; this standard does not mandate or constrain the use of methods of transporting EAP other than on a LAN that supports the Controlled Port. Similarly the figure references the communication of authorization data as RADIUS attributes; this standard does not constrain the data supplied or the protocols that convey it. Annex E (informative) provides guidelines for the use of RADIUS with this standard.

The two PAEs use the results of their mutual authentication (see 6.2), and the MACsec Key Agreement protocol (MKA, Clause 12) that in turn uses certain EAPOL PDUs (Clause 11), to communicate securely with each other. The PAEs agree the cryptographic keys to be used by their respective MAC Security Entities (SecY's) that secure communication to and from their Controlled Ports.

Copyright © 2010 IEEE. All rights reserved.

Documents Document Sharing Hub

Full document details: ISO_IEC_IEEE 8802-1X_2013

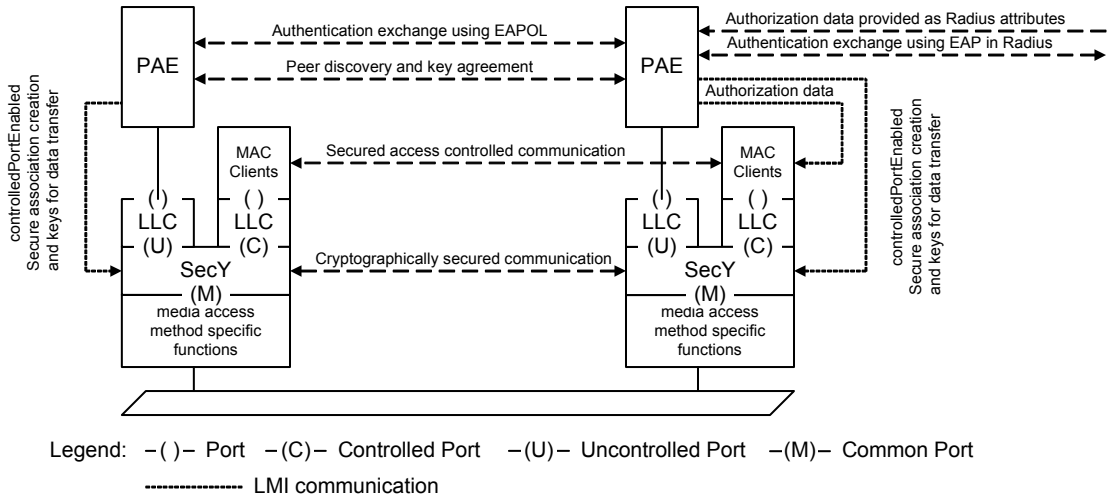

Figure 6-2—Port-based network access control with MACsec

For simplicity Figure 6-2 can be taken as depicting a single point-to-point LAN, and the resulting point-to-point CA. A PAE and a SecY can also support multipoint LANs and group CAs. Additionally, a PAE in a network access point supporting a multi-access LAN (7.5, 12.7) can reduce multipoint LAN connectivity to one or more subsets independently secured by SecYs: each SecY supporting a separate virtual port.

NOTE—This standard specifies a Key Agreement Entity (KaY) as part of the PAE, although IEEE Std 802.1AE showed it coupled with the SecY shim. The descriptions are equivalent, as the KaY controls the SecY's Controlled Port through its LMI. IEEE Std 802.1AE-2006 Figure 10-2 allowed for the possibility of using the Controlled Port to communicate authorization data prior to making it available to other MAC Clients, an approach not pursued in this standard.

A given system can be attached to one of many LANs, with potential peers providing access to many different networks or network services. A PAE for a system that provides network access can announce the identity or identities of those network(s). A given system can also be moved (roam) from one network to another before being reconnected (roaming) to the first. In that case communication can be re-established quickly if both communicating PAEs have cached the results of a prior mutual authentication—peer discovery and key agreement can be used to confirm the authentication and use it to agree fresh keys to protect data transfer, while a fresh authentication exchange with the AAA server is in progress.

6.2 Key hierarchy

The root key in the MACsec Key Agreement key hierarchy is the Connectivity Association Key (CAK), and is identified by a CAK Name (CKN). MKA (Clause 9) does not use the CAK directly but derives two further keys from the CAK using the AES cipher (FIPS Publication 197) in CMAC mode (9.3). These are the ICV Key (ICK) used to verify the integrity of MPDUs and to prove that the transmitter of the MKPDU possesses the CAK, and the Key Encrypting Key (KEK) used by Key Server, elected by MKA, to transport a succession of SAKs, for use by MACsec, to the other member(s) of a CA. See Figure 6-3.

A CAK can be obtained in several ways. It can be a pre-shared key (PSK) configured as specified in 6.3.3, 12.1, and 12.5. The PSK is identified as being a pairwise CAK or as a group CAK. Alternatively key management can be automated. This standard specifies the use of EAP for automatic CAK management through mutual authentication and key derivation of a pairwise CAK.

The ICK and KEK derived from a CAK can be used to distribute SAKs to systems that possess that CAK. A number of pairwise CAKs, each possessed only by the Key Server and one other system, can also be used by the Key Server to derive ICK, KEK tuples to distribute a further, different, group CAK. See Figure 6-4. Each

Copyright © 2010 IEEE. All rights reserved.

Documents
Document Sharing Hub
Full document details: ISO_IEC_IEEE 8802-1X_2013

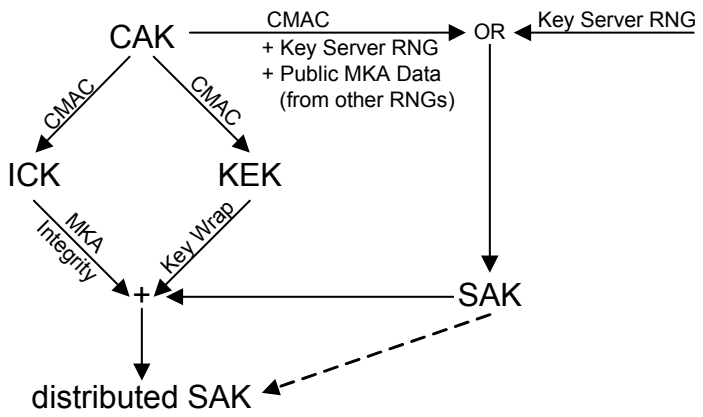

Figure 6-3—MKA key hierarchy

of the communicating systems use this group CAK to derive a further ICK and KEK, that are then used by the Key Server to transport a succession of SAKs to the group. A group CAK can be used to distribute a further group CAK, but systems can be configured only to accept CAK distributed using a pairwise CAK. The ICK and KEK derived from a CAK shall not be used to distribute that CAK, and in particular a pairwise CAK derived using EAP shall not be distributed for use as a group CAK.

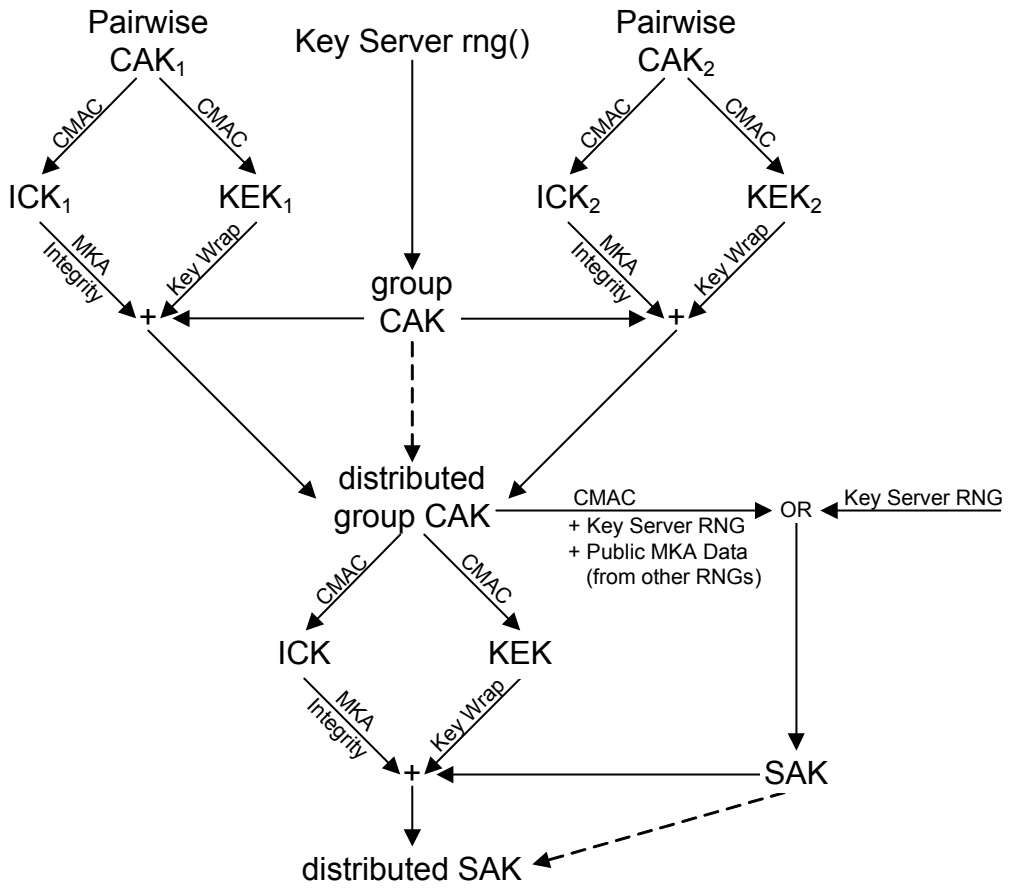

Figure 6-4—Use of pairwise CAKs to distribute group SAKs

Copyright © 2010 IEEE. All rights reserved.

Documents Document Sharing Hub

Full document details: ISO_IEC_IEEE 8802-1X_2013

SAKs should be generated by MKA using the CAK with a random number generated specifically for that SAK and contributions from each of the participants in the CAK (9.8.1). These contributions guard against weakness in the Key Server's RNG but do not relax the RNG conformance requirement. Alternatively, SAKs may be generated directly by the Key Server's strong random number generator (RNG, 9.2.1).

6.2.1 Key derivation function (KDF)

This standard uses a KDF that is compatible with the counter mode KDF described in the NIST Special Publication 800-108. The KDF uses a pseudorandom function (PRF) which shall be AES-CMAC-128 when the derivation key is 128 bits, and AES-CMAC-256 when the derivation key is 256 bits.

The KDF is described as follows:

```
Output← KDF (Key, Label, Context, Length) where
Input:    Key, a key derivation key of 128 or 256 bits
          Label, a string identifying the purpose of the keys derived using this KDF
          Context, a bit string that provides context to identify the derived key
          Length, the length of the output in bits encoded in two octets with the
          most significant octet first
Output:   a Length-bit derived value
Fixed values:
          h, the length of the output of the PRF in bits
          r, denoting the length of the binary representation of the counter i

iterations ← (Length + (h-1))/h

if iterations > 2^r-1, then indicate an error and stop.
result ← ""

do        i = 1 to iterations
          result ← result | PRF(Key, i | Label | 0x00 | Context | Length)
od
return first Length bits of result, and securely delete all unused bits
```

NOTE —'|', denotes concatenation of the octet strings; i and 0x00 each comprise a single octet; and Label, Context, and Length each comprise an integral number of octets. The hexadecimal representations of each of the Labels specified by this standard for use with this KDF are specified in Annex H Test vectors.

6.2.2 Using EAP for CAK key derivation

A pairwise CAK is derived directly from the EAP MSK using the following transform:

CAK = KDF(Key, Label, mac1 | mac2, CAKlength)

where

```
Key       = MSK[0-15] for a 128 bit CAK, MSK[0-31] for a 256 bit CAK
Label     = "IEEE8021 EAP CAK"
mac1      = the lesser of the two source MAC addresses used in the EAPOL-EAP exchange (11.1.2)
mac2      = the greater of the two source MAC addresses used in the EAPOL-EAP exchange
CAKlength = two octets representing an integer value (128 for a 128 bit CAK, 256 for a 256 bit
            CAK) with the most significant octet first
```

Copyright © 2010 IEEE. All rights reserved.

Documents
Document Sharing Hub

Full document details: ISO_IEC_IEEE 8802-1X_2013

NOTE 1—MSK[0-15] refers to the first 16 octets of the MSK, MSK[0-31] to the first 32. IETF RFC 3748 [B14] requires EAP methods that produce an MSK to create an MSK of 64 bytes, so there will be sufficient keying material for the KDF.

NOTE 2—The source MAC addresses, mac1 and mac2, are those that supported the EAPOL-EAP exchange. While including these addresses in the derivation ensures that the CAK and CKN differ if the MSK[0-15] chance to be the same for authentication instances using different ports, they do not define or restrict the scope of the CAK and CKN, and do not identify the PAEs that anticipated in the authentication exchange. The scope of the CAK and CKN is identified by the KMD (see 6.2.3, 6.3.5).

A 16 octet CKN is derived from the EAP session ID using the following transform:

CKN = KDF(Key, Label, ID | mac1| mac2, CKNlength)

where

Key = MSK[0-15] for a CKN naming a 128 bit CAK, MSK[0-31] for naming a 256 bit CAK
ID = EAP-Session-ID
Label = "IEEE8021 EAP CKN"
mac1 = the lesser of the two source MAC addresses used in the EAPOL-EAP exchange (11.1.2)
mac2 = the greater of the two source MAC addresses used in the EAPOL-EAP exchange
CKNlength = two octets representing an integer value (128) with the most significant octet first

NOTE 3—EAP-Session-IDs are defined by IETF RFC 5247. Each Session-ID comprises a number of concatenated fields: octets corresponding to fields earlier in the concatenation (shown to the left in text) are encoded earlier in PDUs and multi-octet fields that represent numbers or can be numerically compared are encoded as specified by this standard (in network byte order).

In each case the Label is a UTF-8 string, without a null or other termination, exactly 16 bytes in length (the quotes shown above are not part of the string) and exactly one space (a single octet with the value 0x20) separates ‘8021’ and ‘EAP ‘, and one space separates ‘EAP’ and ‘CAK’, and ‘EAP’ and ‘CKN’. The Label’s length is chosen to make the concatenated inputs to the PRF within the KDF for the CAK exactly 32 octets.

For historical reasons MAC addresses, and the 24-bit OUIs assigned so that the assignee could derive a number of MAC addresses, were defined as bit-strings. mac1 and mac2 above are sequences of 6 octets, with the value of first octet derived from the first 8 bits of the 48-bit MAC address string, the second octet from second set of eight bits and so on, each set of 8 bits being taken to represent a binary number with its first bit being the least significant. The value of each octet in the sequence corresponds to that naturally associated with the Hexadecimal Representation of the LAN MAC Address defined in ISO/IEC 10039 (LAN MAC Service Definition) and referenced by IEEE Registration Authority tutorials, and the order of the octets corresponds to the left to right order in that representation. The first bit of the address string is the Individual/Group address, and the bit order of the address is that originally used for transmission on IEEE 802.3 media. The octet sequence defined to represent the MAC address is used in a number of other IEEE 802.1 standards, including IEEE Std 802.1D and IEEE Std 802.1Q and the value and representation for an address is commonly known as the ‘canonical format’. Users of this specification are warned that the long running ‘endian’ disputes about bit ordering and bit significance mean that some seemingly authoritative and generally available tutorials do reverse the bits of the 48-bit address string in eight bit groups, in order to show the most significant bit to the left (first according to some familiar conventions), though most now retain the bit significance necessary to this specification.

When two MAC addresses are compared, each is treated as an unsigned binary number, following the convention (used throughout IEEE 802.1 standards) that binary numbers are encoded in octet strings with the most significant octets first. The greater of two addresses is that with the greater numeric value.

Copyright © 2010 IEEE. All rights reserved.

Documents
Document Sharing Hub

Full document details: ISO_IEC_IEEE 8802-1X_2013

6.2.3 CAK caching and scope

A CAK and its associated CKN may be cached for later use. The scope of use of a CAK is identified as a Key Management Domain (KMD). While the initial derivation of the CAK and the CKN include values particular to the PAEs that participate in an instance of authentication protocol (e.g. the MAC addresses of the associated ports) and to that protocol instance (e.g. the EAP-MSK), the CAK can be used as a proof of authentication with any port controlled by a PAE that participates in the same KMD (see 6.3.5). Neither the CAK or the CKN is recalculated following their initial derivation.

The cached CAK is associated with its CKN and any other contextual parameters associated with its use, such as the NID and authorization data. It can be inappropriate to cache a CAK since authorizations or other important contextual information may be dynamic in nature.

6.2.4 Algorithm agility

To accommodate future developments in cryptography, MKA provides an explicit Algorithm Agility parameter (9.3.3, 11.11.2, Figure 11-8). The Algorithm Agility parameter identifies the following:

a) How the ICV is derived from the CAK and the data of a given MKPDU; and
b) How a CAK is derived from the parameters available to the participants in an EAP exchange.

In other words, MKA instances that transmit MKPDUs with different values of the Algorithm Agility parameter could use a different KDF (see 6.2.1) to derive the ICK (9.3.3), could specify the computation of the ICV in a different way, and could specify a different way for the participants in an EAP exchange to agree on a CAK (6.2.2). The flexibility provided allows a wide range of future challenges to be addressed, but the need for substantial analysis of any proposed alternate to the provisions of this standard in these areas means that no claim of conformance is facilitated currently for any such alternate. A future revision of this standard could provide such a claim, if needed to address cryptographic developments.

MKA's Algorithm Agility parameter does not identify the KDF used to derive the KEK, or the Key Wrap (see 6.2). That identification is provided by the MKA parameter set type used to encode the Key Wrap (Figure 11-11, Figure 11-12, Figure 11-13). A different Key Wrap, or a Key Wrap using a differently derived KEK, could be introduced while still allowing MKA participants to communicate by using MKPDUs with a familiar Algorithm Agility parameter value—thus allowing negotiation or fallback to known parameter set types.

6.3 Port Access Entity (PAE)

The operation of the PAE is specified in detail in Clause 12. This clause (6.3) provides an introduction to allow the principles of port-based network access control as a whole to be understood, providing the context for operation of the protocols that the PAE uses (as specified in detail in Clause 8, Clause 9, Clause 10, and Clause 11).

6.3.1 Authentication exchanges

Each PAE may operate EAP (IETF RFC 3748 [B14]). The Uncontrolled Port provided by the SecY or PAC (6.4) is used to transmit EAP frames over the LAN (EAPOL) encoded as specified in Clause 11, as part of the Port Access Control Protocol (PACP) specified in Clause 8. PACP initiates authentication attempts, retries initial authentication (if necessary) to guard against frame loss when the two communicating Ports are enabled at different times, provides periodic reauthentication, and terminates authentication on request, in addition to transparently conveying EAP frames between the EAP PAEs.

In any given authentication exchange, each PAE adopts one of two distinct EAP specified roles:

Copyright © 2010 IEEE. All rights reserved.

Documents
Document Sharing Hub

Full document details: ISO_IEC_IEEE 8802-1X_2013

a) Authenticator ()
b) Supplicant ()

NOTE—A given PAE can participate in one authentication exchange as a Supplicant, and in another as an Authenticator. See Figure 7-10.

EAP specifies a further system role:

c) Authentication Server ()

All three roles are necessary to an EAP authentication exchange. The Authenticator and an Authentication Server can be co-located within the same system, allowing that system to perform the authentication function without the need for communication with an external server. However most port-based network access control applications use a separate Authentication Server, to allow centralized administration of authorized parties and their credentials for Authenticators throughout a network. Protocol exchanges between the Authenticator PAE and the Authentication Server (if the server is not co-located with the Authenticator PAE) can be conducted via one or more of the system's Controlled or Uncontrolled Ports.

NOTE 1—Communication between Authenticator and Authentication Server is outside the scope of this standard, but typically uses an authentication protocol carried over appropriate higher layer protocols; e.g, EAP in RADIUS. Hence, the Authentication Server can be located outside of the confines of the LAN that supports the protocol exchanges between Supplicant and Authenticator, and the communication to the server need not be subject to the authentication state of the systems concerned. If a Controlled Port is used to achieve communication with the Authentication Server, protocol exchanges can only take place if the Controlled Port is in the authorized state.

The asymmetry in some port-based network access control applications defines appropriate system roles, for example a mobile personal computer that attaches to a network is a Supplicant and the port that supports its attachment an Authenticator. Other applications, e.g. securing the connection between two bridges in the core of a network, lack this natural asymmetry. A system may implement and enable both Authenticator and Supplicant state machines to support such applications, with the attendant possibility that two separate authentication exchanges will complete. The PAE uses MKA (see 6.3.2) to ensure that communicating peers agree on the use of authentication results: each of the cryptographic keys that it uses (and the authorization data bound to that key) is derived from the result of a single exchange. By itself EAP (supported by PACP) lacks the capability to agree that the results of a particular exchange are to be used, or indeed to confirm that the communicating peers both believe the same exchange has completed, and should not be used without MKA in applications where a single port requires simultaneous Authenticator and Supplicant functionality. However if MACsec is not used further keys are not required, so communication can and should proceed if either the Supplicant or the Authenticator authenticates successfully and MKA is not available.

NOTE 2—IEEE Std 802.1X-2004 Edition provided explicit control over the combination of authentication results by management of Supplicant Access Control With Authenticator. The use of this variable is deprecated, but not prohibited.

6.3.2 Key agreement

Each PAE may operate the MACsec Key Agreement (MKA) protocol (Clause 9). The Uncontrolled Port provided by the SecY or PAC is used to transmit and receive MKPDUs (11.11) that are conveyed by EAPOL PDUs, distinguished from those used by PACP by their EAPOL Packet Type (11.3.2, Table 11-3).

A PAE can operate multiple instances of MKA. Each instance is protected by a distinct Secure Connectivity Association Key (CAK) that allows each PAE to ensure that information for a given MKA instance is only accepted from other PAEs that also possess that CAK, thus identifying themselves as members or potential members of the same CA. Each CAK is a result of an EAP authentication exchange (6.2), or is configured in two or more PAEs as a pre-shared key (PSK, 6.3.3), or is distributed by a separate MKA instance that uses the results of an authentication exchange. The last of these methods allows a key server's PAE to use a

Copyright © 2010 IEEE. All rights reserved.

Documents
Document Sharing Hub

Full document details: ISO_IEC_IEEE 8802-1X_2013

number of authentication exchanges, each with one other PAE, to create a group CA (with a group CAK) that can continue to secure communication in the absence of any of its members (including the key server).

MKPDUs are transmitted using a group MAC destination address, allowing the members of a CA to find each other without prior configuration. MKA can confirm an immediately prior or past authentication, and can be used in conjunction with a PAC (which does not use cryptographic keys itself) to verify connectivity. When used with a SecY, the PAE also uses MKA to distribute SAKs and to assign these to SAs.

6.3.3 Pre-shared keys

A PAE may support the use of one or more pre-shared CAKs (PSKs). An instance of MKA (see Clause 9) operates for each pre-shared CAK that is administratively configured as active, just as if that CAK had been provided (see 6.3.2) by a PAE using EAP (see Clause 8). A PSK can be a pairwise or group CAK.

A pre-shared CAK may be created by a management request with the following parameters:

a) enabled, True or False.
b) CKN, a name for the CAK with the format specified in 9.3.1.
c) The CAK value.

The CAK Name is required to be different from that for existing keys, and can be used to identify the key in subsequent management operations.

If provision of a pre-shared CAK is permitted, use of the pre-shared key can also be enabled or disabled by management request, the CAK name read, or the parameters for the key deleted entirely. The CAK value shall never be returned in response to a management request.

6.3.4 Interoperability and connectivity

Systems incorporating a given port-based network access control implementation can be used in a number of different application scenarios (Clause 7 provides examples) without individual pre-configuration, including attaching to LANs where the other systems do not implement PACP or MKA. A given system can be moved from LAN to LAN, and its current or potential peers added, removed, or reconfigured.

The PAE's use of EAP, PACP, and MKA can be managed. Authenticated and secured connectivity is usually preferred, but the PAE can be configured to permit unauthenticated or unsecured connectivity if required. To minimize any delay that could occur while PACP and MKA conclude that there are no port-based network access control capable peers attached to the LAN, unauthenticated connectivity can be provided until authenticated and secured connectivity is available.

Once secured connectivity is established the PAE manages reauthentication using EAP (if required) and concurrent MKA instances, so that the CAKs that result from successive authentication exchanges provide an uninterrupted supply of SAKs for the SecY's use.

Higher layer protocols that transport EAP can supply policy controls that are outside the scope of this standard but are required by management for the authorization associated with the port. Such policy controls can also be associated with a PSK. The PAE sets controlledPortEnabled for the PAC or SecY if and only if any policy controls, required by management for the authorization associated with the port but outside the scope of this standard, have been applied by the Controlled Port's clients.

NOTE—Where EAP in RADIUS is used for authentication, the RADIUS protocol can supply authorization data including, for example, VLAN configuration of the port (see 7.1.3, IEEE Std 802.1Q, RFC 4675).

Documents
Document Sharing Hub

Copyright © 2010 IEEE. All rights reserved.

Full document details: ISO_IEC_IEEE 8802-1X_2013

Changes in the nature of the Controlled Port's connectivity (from one of unauthenticated, unsecured, or secured, to another) and changes in secured connectivity (changes in the CA), are accompanied by controlPortEnabled transitions, and are seen by clients of the Controlled Port as interruptions in connectivity. These interruptions (signaled by changes in MAC_Operational for the port) should be used to restart client protocol state machines that take exceptional or accelerated action when connectivity is first available. For example, a network access point that provides unauthenticated connectivity to a host can provide that host access to a different IP subnet once it has been authenticated, and it is appropriate to reinitialize DHCP so the host can obtain a fresh IP address.

6.3.5 Network announcements, identity, authentication requirements, and status

A PAE may announce the Network Identity (NID), a string identifying a network, of the network(s) for which it controls access, and can solicit announcements from the PAEs of other systems attached to the same LAN. A Supplicant PAE can associate a NID with a configuration profile containing the parameters (e.g. selected credentials for use with EAP) necessary to access that network successfully, and can present NID information during the authentication information exchange to influence authorization processes.

An announcement can state whether the sending PAE supports open or restricted unauthenticated access to that network, PACP and or MKA for authenticated access, and MACsec for secured access, and whether authentication is supported by a higher layer protocol (such as WebAuth). The announcement can also provide the MAC_Operational status of the Controlled Port and the status of the selected NID, to allow a Supplicant to distinguish between the immediate availability of restricted access (or higher layer authentication) and its potential use after failure of an authentication attempt.

Announcements can be conveyed in EAPOL PDUs. EAPOL-Announcements can be solicited by other EAPOL PDUs. Announcements can also be conveyed securely by MKA, so that the recipient can confirm that the actions taken on the unsecured EAPOL-Announcement were appropriate.

PAEs that announce and act on announced information can shorten the time taken for a Supplicant to gain network access. A PAE can also announce its Key Management Domain (KMD), a string that identifies one or more systems that share cached CAKs. This announcement allows a peer PAE to select from amongst its cached CAKs, and re-establish authenticated connectivity before or in the absence of authentication using EAP. Such a PAE can move (roam) from one LAN to another, minimizing the time taken to connect to each.

NOTE—While a Key Management Domain can comprise more than one system, how a number of systems hold a CAK in common or convey it to the particular system that requires it to support roaming is outside the scope of this standard.

6.3.6 Multi-access LANs

A network access point may instantiate multiple virtual ports, each including a SecY, to support individually secured point-to-point connections to each of a number of other stations attached to the same shared-media individual LAN. See Figure 6-5. A network access point providing such virtual ports can support multiple distinct and simultaneous EAP exchanges with PACP, distinguishing between frames to and from each of the other stations by using the station's individual MAC address in the destination address field (on transmission) and from the source address field (on receipt).

NOTE—The addressing (individual or group) for each EAPOL Packet Type is specified in Table 11-1 and Table 11-4. For compatibility with prior revisions of this standard Supplicants attached to 802.3 networks use only group addresses in the destination address field of EAPOL frames supporting PACP.

A PAE that supports virtual ports shall also be capable of operating individual MKA instances for each virtual port. MKA frames include the CKN, which is sufficient for each station to associate each with the virtual port of potential interest, or to discard it. Other group addressed EAPOL frames, i.e. those with the individual MAC address of a network access point as their source address, apply equally to all stations.

Copyright © 2010 IEEE. All rights reserved.

Documents
Document Sharing Hub

Full document details: ISO_IEC_IEEE 8802-1X_2013

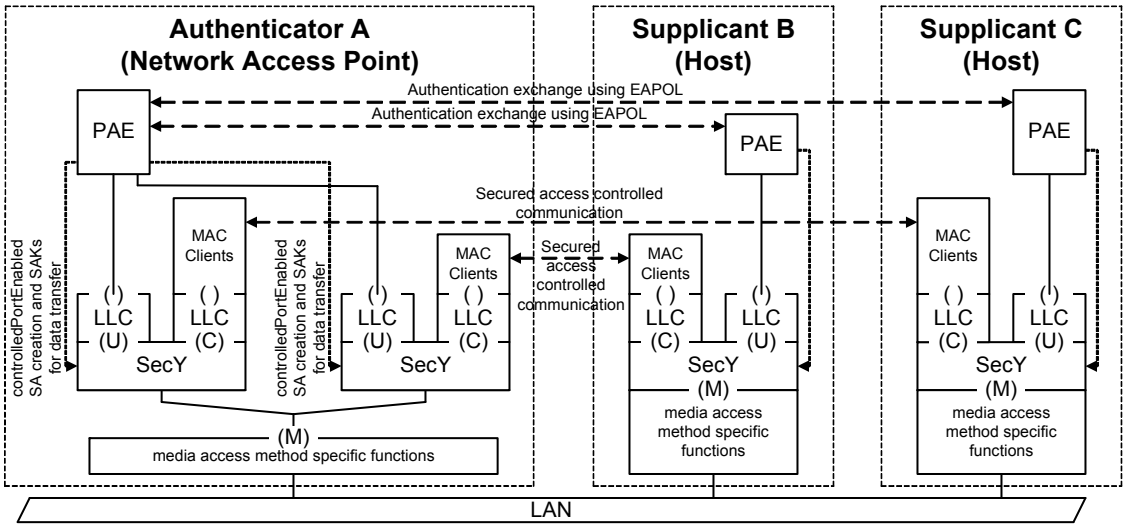

Figure 6-5—Network access control with MACsec and a multi-access LAN

6.4 Port Access Controller (PAC)

The PAC is a protocol-less shim (D.5) that provides control over frame transmission and reception by clients attached to its Controlled Port, and uses the MAC Service provided by a Common Port. The access control decision is made by the PAE, typically taking into account the success or failure of mutual authentication and authorization of the PAE's peer(s), and is communicated by the PAE using the LMI to set the PAC's controlledPortEnabled variable. The PAE itself attaches to an Uncontrolled Port, provided by the PAC to support the authentication exchange prior to authorizing use of the Controlled Port. See Figure 6-6. Either or both of the SecY's in Figure 6-2 could be replaced with a PAC if cryptographically secured communication between the two systems were not required. A SecY can be configured, using the management controls specified in IEEE Std 802.1AE, to behave exactly like a PAC—thus facilitating interoperability when only one of the communicating systems implements MACsec.

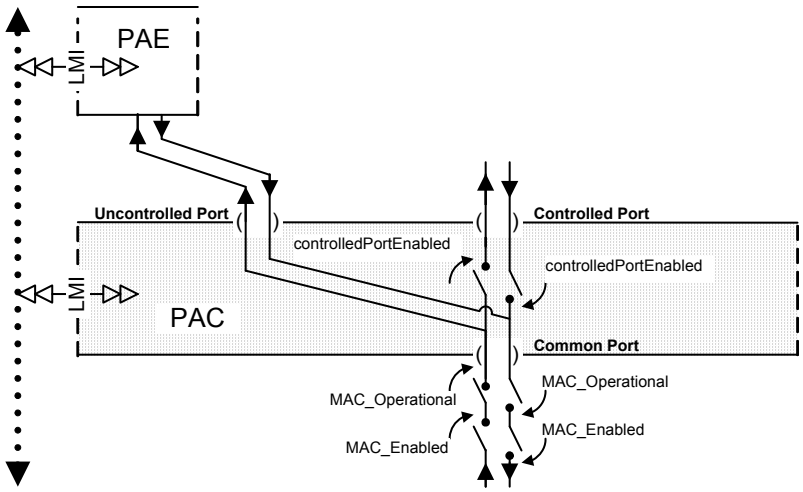

Figure 6-6—Port Access Controller

NOTE—IEEE Std 802.1X-2004 and earlier editions of this standard specified use of the Controlled Port without instantiating an entity that could realize the necessary functionality within an interface stack. The PAC formalizes that description, allows it to be applied to complex interface stacks, and clarifies the relationship with MACsec.

Copyright © 2010 IEEE. All rights reserved.

Documents
Document Sharing Hub

Full document details: ISO_IEC_IEEE 8802-1X_2013

6.4.1 Uncontrolled Port transmission and reception

Each transmit request from the Uncontrolled Port results in a single and identical transmit request at the Common Port. Each receive indication from the Common Port results in a single and identical receive indication at the Uncontrolled Port in addition to any receive indication at the Controlled Port permitted by authorization and administrative controls (6.4.2).

NOTE 1—This specification most clearly sets out the resulting behavior of a conforming implementation. Real implementations can implement the behavior in any way that yields the same externally visible behavior. There need be no implementation burden corresponding to duplication of a received frame if either of the clients of the Uncontrolled or Controlled Port will discard the frame, e.g. following examination of its destination address or Ethertype.

MAC_Operational for the Uncontrolled Port is set *True* if and only if it is *True* for the Common Port.

NOTE 2—If MAC_Operational is *False*, transmit requests are not accepted and receive indications do not occur. The MAC_Enabled status parameter reflects the result of administrative controls applied to the components that compose a port interface stack, in general if MAC_Enabled is *False*, MAC_Operational will also be *False*.

6.4.2 Controlled Port transmission and reception

Each transmit request from the client of the PAC's Controlled Port results in a corresponding transmit request at the Common Port, and each receive indication from the Common Port results in a corresponding receive indication at the Controlled Port, without omission or duplication, and with identical parameters in each case, if and only if controlledPortEnabled is set.

MAC_Operational (D.4) for the Controlled Port is set *True* if and only if MAC_Operational for the Common Port is *True* and controlledPortEnabled is set.

NOTE—Previous revisions of this standard specified an AdminControlledDirections parameter. This parameter is no longer supported — it did not satisfy its stated goals fully and is not applicable where access is cryptographically protected. The desired functionality was for unauthenticated systems to be able to see startup and initialization traffic (e.g., Wake-on-LAN) functions. This revision of this standard provides explicit support for such functions —see the application specific discussions of connectivity to unauthenticated systems in 7.5.3, 7.4.3 and elsewhere in Clause 7.

6.4.3 PAC management

The PAC management process controls, monitors, and reports on the operation of the PAC, providing access to operational controls and statistics for network management and the PAE through the LMI.

The following status parameters (D.4) for the Uncontrolled Port and the Controlled Port are provided (separately) to the user(s) of those ports, and can be read by management:

— MAC_Enabled
— MAC_Operational
— operPointToPointMAC
— adminPointToPointMAC

The value of MAC_Enabled for the Uncontrolled Port is always True, the value of MAC_Enabled for the Controlled Port is the same as that of the controlledPortEnabled parameter set by the PAE.

The following statistics are provided for the Controlled Port and (separately) for the Uncontrolled Port to support RFC2863 interface MIB Counters:

— ifInOctets
— ifInUcastPkts, ifInMulticastPkts, and ifInBroadcastPkts
— ifInDiscards

Copyright © 2010 IEEE. All rights reserved.

Documents Document Sharing Hub

Full document details: ISO_IEC_IEEE 8802-1X_2013

— ifInErrors
— ifOutOctets
— ifOutUcastPkts, ifOutMulticastPkts, ifOutBroadcastPkts
— ifOutErrors

The ifInDiscards, ifInErrors, and ifOutErrors counts are zero, as the operation of the Controlled Port and the Uncontrolled Port provides no error checking or occasion to discard packets, beyond that provided by its users or by the entity supporting the Common Port. Discards while the controlledPortEnabled is false are not considered as error (if necessary the Common Port and Controlled Port statistics can be compared).

The values of ifInOctets, ifInUcastPkts, ifInMulticastPkts, and ifInBroadcastPkts for the Uncontrolled Port are identical to those for Common Port, and are not separately recorded, but can be made available to management for consistency of presentation. The values of ifOutOctets, ifOutUcastPkts, ifOutMulticastPkts, and ifOutBroadcastPkts for the Uncontrolled Port can be obtained by subtracting the Controlled Port values of those statistics from those recorded for the Common Port.

6.5 Link aggregation

Whenever access controlled ports can be aggregated (see IEEE Std 802.1AX), a PAE associated with each port authenticates each individually, so that authentication and authorization are not compromised by an aggregation that includes unauthenticated connectivity. Authorized ports are aggregated only with others providing connectivity to the same authenticated system.

NOTE 1—Conformance to this standard requires the use of protocols that provide mutual authentication, so two link aggregation capable devices that communicate securely will both be aware of the authentication status of aggregatable ports. The requirement for connectivity to the same authenticated system supplements the system identities advertised in aggregation control protocols.

Figure 6-7 and Figure 6-8 illustrates the interface stack when access control for each port is provided by the PAC and by the SecY.

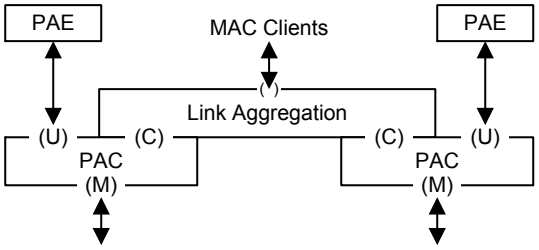

Figure 6-7—PACs and Link Aggregation in an interface stack

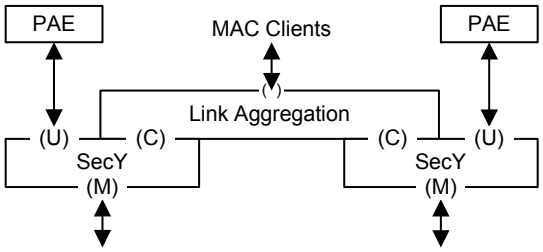

Figure 6-8—SecYs and Link Aggregation in an interface stack

Documents
Document Sharing Hub

Copyright © 2010 IEEE. All rights reserved.

Full document details: ISO_IEC_IEEE 8802-1X_2013

6.6 Use of this standard by IEEE Std 802.11

IEEE Std 802.11 specifies media-dependent cryptographic methods to protect data transmitted using the 802.11 MAC over wireless networks. Conceptually these cryptographic methods can be considered as playing the same role within systems and interface stacks as a MAC Security Entity. In addition IEEE Std 802.11 specifies media dependent key agreement, key distribution, network discovery, network selection, and roaming protocols. It is not the purpose of this standard to provide alternatives for the IEEE Std 802.11 specified functionality in 802.11 wireless networks.

IEEE Std 802.11 specifies the use of PACP and EAPOL, as defined in this standard, to authenticate using EAP (see Clause 8, Clause 11) and PAEs that support 802.11 ports implement PACP, though not the other optional functionality of the PAE.

Copyright © 2010 IEEE. All rights reserved.

Documents
Document Sharing Hub

Full document details: ISO_IEC_IEEE 8802-1X_2013