

IEEE Std 802.1X™- 2004

(Revision of
IEEE Std 802.1X-2001)

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



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

13 December 2004

Print: SH95298

PDF: SS95298



Documents

Document Sharing Hub

Recognized as an
American National Standard (ANSI)

IEEE Std 802.1X™-2004
(Revision of
IEEE Std 802.1X-2001)

IEEE Standard for Local and metropolitan area networks Port-Based Network Access Control

Sponsor

LAN/MAN Standards Committee
of the
IEEE Computer Society

Approved 10 March 2005

American National Standards Institute

Approved 15 November 2004

IEEE-SA Standards Board

Abstract: Port-based network access control makes use of the physical access characteristics of IEEE 802® Local Area Networks (LAN) infrastructures in order to provide a means of authenticating and authorizing devices attached to a LAN port that has point-to-point connection characteristics, and of preventing access to that port in cases in which the authentication and authorization process fails.

Keywords: authentication, authorization, controlled port, local area networks, metropolitan area networks, port access control, uncontrolled port

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

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

RC4 is a registered trademark of RSA Security Inc. and may not be used by third parties creating implementations of the algorithm. RSA Security does not hold any patents nor does it have any pending applications on the RC4 algorithm. However, RSA Security does not represent or warrant that implementations of the algorithm will not infringe the intellectual property rights of any third party. Proprietary implementations of the RC4 encryption algorithm are available under license from RSA Security Inc. For licensing information, contact RSA Security Inc., 2955 Campus Drive, Suite 400, San Mateo, CA 94403-2507, USA, or <http://www.rsasecurity.com>.

Print: ISBN 0-7381-4528-8 SH95298
PDF: ISBN 0-7381-4529-7 SS95298

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.

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.

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. When a document is more than five years old and has not been reaffirmed, 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. 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. Comments on standards and requests for interpretations should be addressed to:

Secretary, IEEE-SA Standards Board

445 Hoes Lane

P.O. Box 1331

Piscataway, NJ 08855-1331 USA

NOTE—Attention is called to the possibility that implementation of this standard may require 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. The IEEE shall not be responsible for identifying patents for which a license may be required by an IEEE standard or for conducting inquiries into the legal validity or scope of those patents that are brought to its attention.

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.

Introduction

[This introduction is not part of IEEE Std 802.1X-2004, IEEE Standard for Local and Metropolitan Area Networks—Port-Based Network Access Control.]

This standard defines a mechanism for Port-based network access control that makes use of the physical access characteristics of IEEE 802 LAN infrastructures in order to provide a means of authenticating and authorizing devices attached to a LAN port that has point-to-point connection characteristics, and of preventing access to that port in cases in which the authentication and authorization process fails.

Notice to users

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 standard may require 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. The IEEE shall not be responsible for identifying patents or patent applications for which a license may be required to implement an IEEE standard or for conducting inquiries into the legal validity or scope of those patents that are brought to its attention.

Participants

At the time this standard was revised, the working group had the following membership:

Tony Jeffree, *Chair and Editor*

Paul Congdon, *Vice-Chair*

Dolors Sala, *Chair, Link Security Task Group*

Floyd Backes
Les Bell
Paul Bottorff
Laura Bridge
Jim Burns
Dirceu Cavendish
Hesham Elbakoury
Norm Finn
David Frattura
Gerard Goubert

Steve Haddock
Ran Ish-Shalom
Neil Jarvis
Hal Keen
Bill Lane
Roger Lapuh
Loren Larsen
Dinesh Mohan
Bob Moskowitz
Don O'Connor
Glenn Parsons

Frank Reichstein
John Roesse
Allyn Romanow
Dan Romascanu
Mick Seaman
Kazuo Takagi
Michel Thorsen
Dennis Volpano
Karl Weber
Michael D. Wright

The following members of the individual balloting committee voted on this standard. Balloters may have voted for approval, disapproval, or abstention.

Butch Anton	Atsushi Ito	Jeremy Moore
Reza Arefi	Peeya Iwagoshi	Joseph Moran
William Byrd	Raj Jain	Mike Moreton
John Barnett	David James	Robert Moskowitz
Hugh Barrass	Neil Jarvis	Narayanan Murugesan
Barbara Bickham	Tony Jeffree	Andrew Myles
Gennaro Boggia	David Johnston	Charles Ngethe
Todd Cooper	Bobby Jose	Nick S.A. Nikjoo
Edward Carley Jr.	Joe Juisai	Donald O'Connor
Clifford Chamney	Thomas M. Kurihara	Bob O'Hara
Kai Moon Chow	Joerg Kampmann	Satoshi Obara
Keith Chow	Junghong Kao	Chris Osterloh
Todor Cooklev	Kevin Karcz	Stephen Palm
Javier del Prado Pavon	Piotr Karocki	Leo Pluswick
Guru Dutt Dhingra	Ken Katano	Subbu Ponnuswamy
Wael Diab	Byoung-Jo Kim	Vikram Punj
Thomas Dineen	Cees Klik	maximilian Riegel
Lakshminath Dondeti	Pi-Cheng Law	John Roesse
Dr. Sourav Dutta	Juanluis Lazaro	Floyd Ross
Clint Early, Jr.	Armando Leite	Vaughn Sheline
Jonathan Edney	Panos Lekkas	Gil Shultz
Darwin Engwer	John Lemon	Amjad Soomro
Matthew Fischer	Randolph Little	Adrian Stephens
Will Foulds	Henry Lu	Masahiro Takagi
Ernesto Garcia	William Lumpkins	Joseph Tardo
Jean-Denis Gorin	Nikolai Malykh	Mark-Rene Uchida
Ron Greenthaler	Ben Manny	Scott Valcourt
Luigi Grieco	Jacques Mathot	Tom Wandeloski
Robert Grow	Kyle Maus	Stanley Wang
Chris Guy	Jonathon McLendon	William Ward
David Halasz	Jorge Medina	Dave Willow
Matt Holdrege	Steve Methley	Derek Woo
Stuart Holoman	David Mitton	Eric Woods
David Hunter	Apurva Mody	Oren Yuen
	Leo Monteban	

When the IEEE-SA Standards Board approved this standard on 15 November 2004, it had the following membership:

Don Wright, *Chair*
Steve M. Mills, *Vice Chair*
Judith Gorman, *Secretary*

Chuck Adams	Raymond Hapeman	Daleep C. Mohla
H. Stephen Berger	Richard J. Holleman	Paul Nikolich
Mark D. Bowman	Richard H. Hulett	T. W. Olsen
Joseph A. Bruder	Lowell G. Johnson	Ronald C. Petersen
Bob Davis	Joseph L. Koepfinger*	Gary S. Robinson
Roberto de Boisson	Hermann Koch	Frank Stone
Julian Forster*	Thomas J. McGean	Malcolm V. Thaden
Arnold M. Greenspan		Doug Topping
Mark S. Halpin		Joe D. Watson

*Member Emeritus

Also included are the following nonvoting IEEE-SA Standards Board liaisons:

Satish K. Aggarwal, *NRC Representative*
Richard DeBlasio, *DOE Representative*
Alan Cookson, *NIST Representative*

Michelle D. Turner
IEEE Standards Project Editor

Historical participants

Since the initial publication, many IEEE standards have added functionality or provided updates to material included in this standard. The following is a historical list of participants who have dedicated their valuable time, energy, and knowledge to the creation of this material:

Les Bell
Alan Chambers
Marc Cochran
Paul Congdon
Hesham El Bakoury
Norman W. Finn
Sharam Hakimi
Bob Hott
Neil Jarvis
Tony Jeffree

Toyoyuki Kato
Hal Keen
Daniel Kelley
Keith Klamm
Joe Laurence
Bill Lidinsky
Yaron Nachman
LeRoy Nash
Satoshi Obara
Luc Pariseau
Anil Rijasinghani

John J. Roese
Ted Schroeder
Benjamin Schultz
Mick Seaman
Rosemary V. Slager
Andrew Smith
Michel Soerensen
Robin Tasker
Manoj Wadekar
Robert Williams

Contents

1.	Overview	1
1.1	Scope	1
1.2	Purpose	1
2.	References	3
3.	Definitions	6
3.1	Terms defined in this standard	6
3.2	Terms defined in IEEE Std 802.1D	7
3.3	Terms defined in The Authoritative Dictionary of IEEE Standards Terms [B5]	7
4.	Acronyms and abbreviations	8
5.	Conformance	9
5.1	Requirements	9
5.2	Options	9
6.	Principles of Port Access Control operation	11
6.1	Purpose of Port Access Control operation	11
6.2	Scope of Port Access Control operation	11
6.3	Systems, Ports, and system roles	12
6.4	Controlled and uncontrolled access	12
6.5	Reception and transmission control	17
6.6	Port Access Entity (PAE)	18
6.7	Coupling two IEEE 802.1X authentications	20
6.8	Use of Port Access Control with IEEE Std 802.3	21
7.	EAP encapsulation over LANs (EAPOL)	23
7.1	Transmission and representation of octets	23
7.2	EAPOL MPDU format for use with IEEE 802.3/Ethernet	23
7.3	EAPOL MPDU format for use with IEEE 802.2 Logical Link Control (LLC)	24
7.4	Tagging EAPOL MPDUs	24
7.5	EAPOL MPDU field and parameter definitions	24
7.6	Key Descriptor format	27
7.7	EAP packet format—informative	30
7.8	EAPOL addressing	31
7.9	Use of EAPOL in shared media LANs	32
8.	Port Access Control Protocol	33
8.1	Introduction to protocol operation	33
8.2	EAPOL state machines	41
9.	Management of Port Access Control	72
9.1	Management functions	72

9.2	Managed objects	73
9.3	Data types.....	74
9.4	Authenticator PAE managed objects	74
9.5	Supplicant PAE managed objects	81
9.6	System managed objects	85
10.	Management protocol	87
10.1	Introduction.....	87
10.2	The Internet-Standard Management Framework	87
10.3	Security considerations	87
10.4	Structure of the MIB	87
10.5	Relationship to other MIBs.....	91
10.6	Definitions for Port Access Control MIB	92
Annex A	(normative) PICS Proforma.....	128
Annex B	(informative) Scenarios for the use of Port-Based Network Access Control.....	136
Annex C	(informative) Design considerations and background material for Port-Based Network Access Control	140
Annex D	(informative) IEEE 802.1X RADIUS Usage Guidelines	147
Annex E	(informative) PAE state machine interface with higher layers: EAP and AAA.....	165
Annex F	(informative) Bibliography	169

IEEE Standard for Local and metropolitan area networks Port-Based Network Access Control

1. Overview

1.1 Scope

IEEE 802[®] Local Area Networks (or LANs; see 3.4 in IEEE Std 802.1D[™]) are often deployed in environments that permit unauthorized devices to be physically attached to the LAN infrastructure, or permit unauthorized users to attempt to access the LAN through equipment already attached. Examples of such environments include corporate LANs that provide LAN connectivity in areas of a building that are accessible to the general public, and LANs that are deployed by one organization in order to offer connectivity services to other organizations (for example, as may occur in a business park or a serviced office building). In such environments, it is desirable to restrict access to the services offered by the LAN to those users and devices that are permitted to make use of those services.

Port-based network access control makes use of the physical access characteristics of IEEE 802 LAN infrastructures in order to provide a means of authenticating and authorizing devices attached to a LAN port that has point-to-point connection characteristics, and of preventing access to that port in cases in which the authentication and authorization process fails. A port in this context is a single point of attachment to the LAN infrastructure. Examples of ports in which the use of authentication can be desirable include the Ports of Media Access Control (MAC) Bridges (as specified in IEEE Std 802.1D), the ports used to attach servers or routers to the LAN infrastructure, and associations between stations and access points in IEEE 802.11[™] Wireless LANs.

1.2 Purpose

For the purpose of providing compatible authentication and authorization mechanisms for devices interconnected by IEEE 802 LANs, this standard specifies a general method for the provision of port-based network access control. To this end, it

- a) Describes the architectural framework within which the authentication, and consequent actions, take place
- b) Defines the principles of operation of the access control mechanisms
- c) Defines the different levels of access control that are supported, and the behavior of the port with respect to the transmission and reception of frames at each level of access control

- d) Establishes the requirements for a protocol between the device that requires the authentication to take place (the Authenticator; see 3.1.1) and the device that is attached to the Authenticator's port (the Supplicant; see 3.1.12)
- e) Establishes the requirements for a protocol between the Authenticator and an Authentication Server (see 3.1.4)
- f) Specifies mechanisms and procedures that support network access control through the use of authentication and authorization protocols
- g) Specifies the encoding of the Protocol Data Units (PDUs) used in authentication and authorization protocol exchanges
- h) Establishes the requirements for management of port-based access control, identifying the managed objects and defining the management operations
- i) Specifies how the management operations are made available to a remote manager using the protocol and architectural description provided by the Simple Network Management Protocol (SNMP) (IETF RFC 3411)
- j) Specifies the requirements to be satisfied by equipment claiming conformance to this standard

2. References

The following standards contain provisions which, through reference in this text, constitute provisions of the standard. At the time of publication, the editions indicated were valid. All standards are subject to revision, and parties to agreements based on this standard are encouraged to investigate the possibility of applying the most recent editions of the standards indicated below. Members of ISO and IEC maintain registers of currently valid International Standards.

ANSI X3.159-1989, American National Standards for Information Systems—Programming Language—C.¹

IEEE Std 802.1DTM-2004, IEEE Standard for Local and metropolitan area networks: Media access control (MAC) Bridges.^{2, 3}

IEEE Std 802.1QTM, 2003 Edition, IEEE Standards for Local and Metropolitan Area Networks: Virtual Bridged Local Area Networks.

IEEE Std 802.3TM-2002, 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 802.5TM, 1998 Edition (ISO/IEC 8802-5-1998), IEEE Standard for Information technology—Telecommunications and information exchange between systems—Local and metropolitan area networks—Specific requirements—Part 5: Token ring access method and physical layer specifications.⁴

IEEE Std 802.11TM, 2003 Edition (ISO/IEC 8802-11: 2003), 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.

IETF RFC 1305, Network Time Protocol (Version 3) Specification, Implementation and Analysis, Mills, D. L., March 1992.⁵

IETF RFC 1321, The MD5 Message Digest Algorithm, R. Rivest, S. Dusse, April 1992.

IETF RFC 2104, HMAC: Keyed-Hashing for Message Authentication, Krawczyk, H., Bellare, M., and Canetti, R., February 1997.

IETF RFC 2433, Microsoft PPP CHAP Extensions, G. Zorn, S. Cobb, October 1998.

IETF RFC 2548, Microsoft Vendor-specific RADIUS Attributes, G. Zorn, March 1999

¹ANSI publications are available from the Sales Department, American National Standards Institute, 11 West 42nd Street, 13th Floor, New York, NY 10036, USA.

²IEEE publications are available from the Institute of Electrical and Electronics Engineers, 445 Hoes Lane, P.O. Box 1331, Piscataway, NJ 08855-1331, USA. IEEE publications can be ordered on-line from the IEEE Standards Website: <http://www.standards.ieee.org>.

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

⁴IEEE [ISO] and IEEE [ISO/IEC] documents are available from ISO Central Secretariat, 1 rue de Varembe, Case Postale 56, CH-1211, Genève 20, Switzerland/Suisse; and from the Institute of Electrical and Electronics Engineers, 445 Hoes Lane, P.O. Box 1331, Piscataway, NJ 08855-1331, USA. IEEE [ISO] and IEEE [ISO/IEC] documents can be ordered on-line from the IEEE Standards Website: <http://www.standards.ieee.org>.

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

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.

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 2607, Proxy Chaining and Policy Implementation in Roaming, B. Aboba, J. Volbrecht, June 1999.

IETF RFC 2716, PPP EAP TLS Authentication Protocol, Aboba, B. and Simon, D., October 1999.

IETF RFC 2863, The Interfaces Group MIB using SMIV2, McCloghrie, K. and Kastenholz, F., June 2000.

IETF RFC 2865, Remote Authentication Dial In User Service (RADIUS), Rigney, C., Willens, S., Rubens, A., and Simpson, W., June 2000.

IETF RFC 2866, RADIUS accounting, Rigney, C., June 2000.

IETF RFC 2867, RADIUS Accounting Modifications for Tunnel Protocol Support, Zorn, G., Aboba, B., and Mitton, D., June 2000.

IETF RFC 2868, RADIUS Attributes for Tunnel Protocol Support, Zorn, G., Leifer, D., Rubens, A., Shriver, J., Holdrege, M., and Goyret, I., June 2000.

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

IETF RFC 3162, RADIUS and IPv6, B. Aboba, G. Zorn, D. Mitton, August 2001.

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

IETF RFC 3411, An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks, D. Harrington, R. Presuhn, B. Wijnen, December 2002.

IETF RFC 3412, Message Processing and Dispatching for the Simple Network Management Protocol (SNMP), J. Case, D. Harrington, R. Presuhn, B. Wijnen, December 2002.

IETF RFC 3413, Simple Network Management Protocol (SNMP) Applications, D. Levi, P. Meyer, B. Stewart, December 2002.

IETF RFC 3414, User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3), U. Blumenthal, B. Wijnen, December 2002.

IETF RFC 3415, View-based Access Control Model (VACM) for the Simple Network Management Protocol (SNMP), B. Wijnen, R. Presuhn, K. McCloghrie, December 2002.

IETF RFC 3416, Version 2 of the Protocol Operations for the Simple Network Management Protocol (SNMP), R. Presuhn, J. Case, K. McCloghrie, M. Rose, S. Waldbusser, December 2002.

IETF RFC 3417, Transport Mappings for the Simple Network Management Protocol (SNMP), R. Presuhn, J. Case, K. McCloghrie, M. Rose, S. Waldbusser, December 2002.

IETF RFC 3418, Management Information Base (MIB) for the Simple Network Management Protocol (SNMP), R. Presuhn, J. Case, K. McCloghrie, M. Rose, S. Waldbusser, December 2002.

IETF RFC 3575, IANA Considerations for RADIUS, B. Aboba, July 2003.

IETF RFC 3576, Dynamic Authorization Extensions to Remote Authentication Dial In User Service (RADIUS), M. Chiba, G. Dommety, M. Eklund, D. Mitton and B. Aboba, July 2003.

IETF RFC 3579, RADIUS Support for Extensible Authentication Protocol (EAP), B. Aboba, P. Calhoun, September 2003.

IETF RFC 3580, IEEE 802.1X Remote Authentication Dial In User Service (RADIUS) Usage Guidelines, P. Congdon, September 2003.

IETF RFC 3748, Extensible Authentication Protocol (EAP), Blunk, L., Vollbrecht, J., Aboba, B., Carlson, J., Levkowetz, H, June 2004.

ISO/IEC 8824:1990, Information technology—Open Systems Interconnection—Specification of Abstract Syntax Notation One (ASN.1) (Provisionally retained edition).⁶

ISO/IEC 8825:1990, Information technology—Open Systems Interconnection—Specification of Basic Encoding Rules for Abstract Syntax Notation One (ASN.1) (Provisionally retained edition).

⁶ISO and ISO/IEC documents are available from the ISO Central Secretariat, 1 rue de Varembé, Case Postale 56, CH-1211, Genève 20, Switzerland/Suisse; and from the Sales Department, American National Standards Institute, 11 West 42nd Street, 13th Floor, New York, NY 10036, USA.

3. Definitions

For the purposes of this standard, the following terms and definitions apply. *The Authoritative Dictionary of IEEE Standards Terms*, Seventh Edition [B5]⁷, should be referenced for terms not defined in this clause.

3.1 Terms defined in this standard

3.1.1 Authenticator: An entity at one end of a point-to-point LAN segment that facilitates authentication of the entity attached to the other end of that link.

3.1.2 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).⁸

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

3.1.4 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.

3.1.5 authentication transport: The datagram session that actively moves the authentication exchange between two systems.

NOTE—Examples include EAP Over LANs (EAPOL), Remote Authentication Dial In User Service (RADIUS), and Diameter (see IETF RFC 3588 [B4]).

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

3.1.7 Edge Port: A Bridge Port attached to a LAN that has no other Bridges attached to it.

NOTE—See 17.3 in IEEE Std 802.1D.

3.1.8 frame: MAC protocol data unit (MPDU).

3.1.9 message digest: The output produced by applying a hash function to a message.

3.1.10 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.

NOTE—The term *Port* is used in this standard as an abbreviation of network access port (see 3.3.2).

3.1.11 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.

⁷The numbers in brackets correspond to those of the bibliography in Annex F.

⁸Notes in text, tables, and figures are given for information only, and do not contain requirements needed to implement the standard.

3.1.12 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 more conventional term, *peer*, used in other access control-related specifications.

3.1.13 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.

3.2 Terms defined in IEEE Std 802.1D

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

3.2.2 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 the MAC Service defined in ISO/IEC 15802-1. IEEE 802 LANs include IEEE Std 802.3 (CSMA/CD), IEEE Std 802.5 (Token Ring), IEEE Std 802.11 (Wireless), and ISO 9314-2 (FDDI) LANs.

3.3 Terms defined in *The Authoritative Dictionary of IEEE Standards Terms* [B5]

3.3.1 nonce

3.3.2 Port

4. Acronyms and abbreviations

For the purposes of this standard, the following acronyms and abbreviations apply. *The Authoritative Dictionary of IEEE Standards Terms* [B5], should be referenced for terms not defined in this clause.

AAA	authentication, authorization, and accounting
ASF	Alerting Standards Forum
CHAP	Challenge Handshake Authentication Protocol
DHCP	Dynamic Host Configuration Protocol
EAP	extensible authentication protocol
EAP-TLS	EAP Transport Layer Security
EAPOL	EAP over LANs
FDDI	Fiber Distributed Data Interface
IP	Internet Protocol
LAN	IEEE 802 Local Area Network
LLC	Logical Link Control
MAC	media access control
MPDU	MAC protocol data unit
MSCHAP	Microsoft Challenge Handshake Authentication Protocol
PACP	Port Access Control Protocol
PAE	port access entity
PID	Protocol Identifier
Port	network access port
PDU	protocol data unit
RADIUS	remote authentication dial in user service
RIF	Routing Information Field
SASL	Simple Authentication and Security Layer
SNAP	Subnetwork Access Protocol
SNMP	Simple Network Management Protocol
VLAN	Virtual LAN

5. Conformance

5.1 Requirements

A device for which conformance to this standard is claimed shall, for all Ports for which support is claimed:

- a) Support the operation of the Port Access Entity (PAE) over the uncontrolled Port, as a Supplicant PAE, an Authenticator PAE, or both, as defined in Clause 8
- b) Support the system configuration functions as defined in 9.6.1
- c) Support operation of the controlled Port in a manner consistent with the use of AuthControlledPortControl parameter values of Force Unauthorized, Auto and Force Authorized, as defined in 6.4
- d) Support the ability to set the AuthControlledPortControl parameter to the values of Force Unauthorized, Auto and Force Authorized, as defined in 6.4, by management action
- e) Support operation of the controlled Port in a manner consistent with the use of AdminControlledDirections and OperControlledDirections parameter values of Both, as defined in 6.5
- f) Where Authenticator PAE operation is supported:
 - 1) Support the ability to configure the operation of the Authenticator as defined in 9.4.1
 - 2) Support the ability to maintain and retrieve the Authenticator statistics as described in 9.4.2
 - 3) Support regular reauthentication of the Supplicant by means of the Reauthentication Timer state machine, and support the ability to modify the reAuthTimer and reAuthEnabled parameters by management action (see 8.2.8 and 9.4.1)
- g) Where Supplicant PAE operation is supported:
 - 1) Support the ability to configure the operation of the Supplicant as defined in 9.5.1
 - 2) Support the ability to maintain and retrieve the Supplicant statistics as described in 9.5.2
- h) Where both Authenticator PAE operation and Supplicant PAE operation is supported, support a *Supplicant Access Control With Authenticator* administrative control parameter value of inactive (see 6.4, 8.2.2.2)

5.2 Options

A device for which conformance to this standard is claimed may, for any Port for which support is claimed:

- a) Support the operation of protocol entities other than the PAE over the uncontrolled Port
- b) Support operation of the controlled Port in a manner consistent with the use of AdminControlledDirections and OperControlledDirections parameter values of In, and support the ability to set the AdminControlledDirections parameter to the values In and Both by management action, as defined in 6.5
- c) Where Authenticator PAE operation is supported:
 - 1) Support the ability to maintain and retrieve the Authenticator diagnostics as described in 9.4.3
 - 2) Support the ability to maintain and retrieve the Authenticator session statistics as described in 9.4.4
 - 3) Support the ability to transmit key information to the Supplicant and support the ability to modify the KeyTransmissionEnabled parameter by management action (see 8.1.9, 8.2.5, and 9.4.1)

- d) Where Supplicant PAE operation is supported:
 - 1) Support the ability to transmit key information to the Authenticator, and support the ability to modify the KeyTransmissionEnabled parameter by management action (see 8.1.9, 8.2.6, and 9.4.1)
- e) Where both Authenticator PAE operation and Supplicant PAE operation is supported, support *Supplicant Access Control With Authenticator* administrative control parameter values of active and inactive (see 6.4, 8.2.2.2), and the ability to modify the parameter value by management action (see 9.5.1)

6. Principles of Port Access Control operation

This clause describes the architectural framework of Port-based access control and the relationship between the access control function and the operation of the device(s) within which it is deployed.

6.1 Purpose of Port Access Control operation

Port Access Control provides an optional extension to the functionality of a System (see 6.3) that offers a means of preventing unauthorized access by Supplicants (see 3.1.12) to the services offered by that System, and also preventing a Supplicant from attempting to access an unauthorized System. Port Access Control also provides a means whereby a Supplicant system may prevent an unauthorized system from connecting to it. For example, if the System concerned is a MAC Bridge, control over access to the Bridge and the LAN to which it is connected can be desirable in order to restrict access to publicly accessible Bridge Ports, or within an organization, to restrict access to a departmental LAN to members of that department. A Supplicant system can also make use of the outcome of the exchange to prevent unauthorized access.

Access control is achieved by the System enforcing authentication of Supplicants that attach to the System's controlled Ports (see 6.4); from the result of the authentication process, the System can determine whether or not the Supplicant is authorized to access its services on that controlled Port. If the Supplicant is not authorized for access, then both the Supplicant's System and the Authenticator's System set their controlled Port state to unauthorized. In the unauthorized state, the use of the controlled Port is restricted in accordance with the value of the OperControlledDirections parameter associated with that controlled Port (see 6.5), preventing unauthorized data transfer between the Supplicant System and the services offered by the Authenticator System.

The mechanisms defined can be applied to allow any System to authenticate another System that is connected to one of its controlled Ports. The Systems concerned include end stations, servers, routers, and MAC Bridges.

NOTE—Given that the Supplicant device may be a Bridge or a router that wished to connect to and thereby extend a Bridged Local Area Network, the process of authentication will determine whether it can be trusted to connect to the Bridged Local Area Network, given that by doing so, it will effectively be extending the authentication boundary to any other Ports of the Supplicant. Similarly, it may be that, in this situation, there is a need for each device to authenticate the other before either Port can become authorized; see the example shown in Figure 6-6.

6.2 Scope of Port Access Control operation

The operation of Port Access Control assumes that the Ports on which it operates offer a point-to-point connection between a single Supplicant (see 3.1.12) and a single Authenticator (see 3.1.1). It is this assumption that allows the authentication decisions to be made on a per-Port basis. The authentication of multiple Supplicant PAEs attached to a single Authenticator PAE is outside of the scope of this standard.

NOTE 1—For example, the operation of Port Access Control on a classic Token Ring LAN, or on a shared media Ethernet LAN segment, is outside of the scope of this standard.

NOTE 2—IEEE 802.11 LANs can make use of the mechanisms defined in this standard, as such, LANs create a logical port per association, and the point-to-point connection can be enforced by means of suitable encryption.

This standard provides a protocol for communicating authentication information between a Supplicant that is attached to a Port of an Authenticator System and an Authenticator Server, and for controlling the state of the Authenticator and Supplicant System Ports, depending on the outcome of the protocol exchange. This standard does not specify the nature of the authentication information that is exchanged, nor the basis upon which the Authentication Server makes its authentication decisions.

6.3 Systems, Ports, and system roles

Devices that attach to a LAN, referred to in this standard as Systems (see 3.1.13), have one or more points of attachment to the LAN, referred to in this standard as network access ports, or Ports (see 3.1.10).

NOTE 1—An end station generally has a single point of attachment in the form of a network interface card (although some end stations, such as servers, often have multiple points of attachment); a MAC Bridge generally has two or more points of attachment in the form of the Bridge Ports.

The Port(s) of a System provide the means in which it can access services offered by other Systems reachable via the LAN, and provide the means in which it can offer services to, or access the services provided by, other Systems reachable via the LAN. Port-based network access control allows the operation of a System's Port(s) to be controlled in order to ensure that access to its services, and/or access to the services of other Systems, is only permitted by Systems that are authorized to do so.

NOTE 2—The services that a System can offer include the relay function of a MAC Bridge, the routing function of a network layer router, file server functionality, and so on.

For the purposes of describing the operation of Port-based access control, a Port of a System (or more correctly, a PAE associated with a Port; see 6.6) is able to adopt either or both of two distinct roles within an access control interaction:

- a) **Authenticator (see 3.1.1):** The Port that wishes to enforce authentication before allowing access to services that are accessible via that Port adopts the Authenticator role.
- b) **Supplicant (see 3.1.12):** The Port that wishes to access the services offered by the Authenticator's system adopts the Supplicant role.

A further System role is described as follows:

- c) **Authentication server (see 3.1.4):** The Authentication Server performs the authentication function necessary to check the credentials of the Supplicant on behalf of the Authenticator and indicates whether the Supplicant is authorized to access the Authenticator's services.

As can be seen from these descriptions, all three roles are necessary to complete an authentication exchange. A given System can be capable of adopting one or more of these roles; for example, an 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. Similarly, a PAE can adopt the Supplicant role in some authentication exchanges, and the Authenticator role in others. An example of the latter may be found in a Bridged Local Area Network, where a new Bridge added to the Bridged Local Area Network may need to be successfully authenticated by the PAE associated with the Port of the Bridge via which it connects to the Bridged Local Area Network before it can authenticate other systems that attach to its Ports. This type of situation is discussed further in 6.7.

NOTE 3—Although co-location of the Authentication Server with an Authenticator is possible, the most common implementation of this mechanism will likely involve the use of an Authentication Server that is external to the Systems that contain the Authenticators.

6.4 Controlled and uncontrolled access

Figure 6-1 illustrates that the operation of Port Access Control has the effect of creating two distinct points of access to the System's point of attachment to the LAN. One point of access allows the uncontrolled exchange of PDUs between the System and other Systems on the LAN, regardless of the authorization state (the uncontrolled Port); the other point of access allows the exchange of PDUs only if the current state of the Port is Authorized (the controlled Port). The uncontrolled and controlled Ports are considered to be part of

the same point of attachment to the LAN; any frame received on the physical Port is made available at both the controlled and uncontrolled Ports, subject to the authorization state associated with the controlled Port.

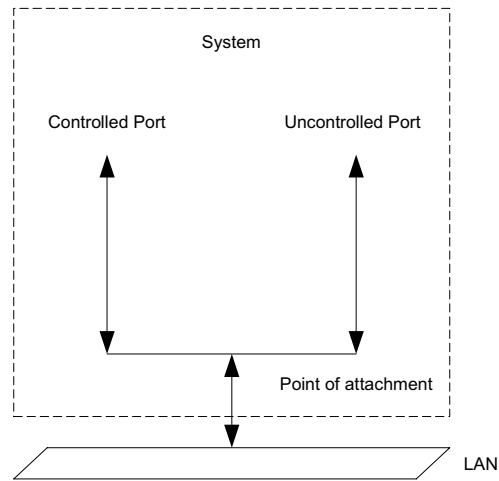


Figure 6-1—Uncontrolled and controlled Ports

NOTE 1—Although a given received frame is made available at both the controlled and uncontrolled Ports, a protocol entity can only be attached to one of the ports at a given moment in time; hence, dependent upon the authorization state of the controlled Port and which Port (if any) the relevant protocol entity is attached to, the frame can be discarded at one or both of the Ports, and is processed by (at most) one protocol entity attached to one of the Ports.

NOTE 2—Arrows are used in this and subsequent diagrams to indicate the connectivity that is available in the various configurations illustrated. For example, in Figure 6-1, the upward pointing arrows indicate that incoming frames can reach users attached to both the controlled and uncontrolled Ports; the downward pointing arrows indicate that outbound frames from either the controlled or uncontrolled Port can reach the LAN.

The point of attachment to the LAN can be provided by any physical or logical Port that can provide a one-to-one connection to another System. For example, the point of attachment could be provided by a single LAN MAC in a switched LAN infrastructure. In LAN environments where the MAC method allows the possibility of a one-to-many relationship between an Authenticator and a Supplicant (for example, in shared media environments), the creation of a distinct association between two Systems is a necessary precondition for the access control mechanisms described in this standard to function. An example of such an association would be an IEEE 802.11 association between a station and an access point.

Figure 6-2 illustrates the effect of the *AuthControlledPortStatus* associated with the controlled Port, representing that status as a switch that can be turned on or off, thus allowing or preventing the flow of PDUs via that Port. The figure shows two systems, each with a single Port; the *OperControlledDirections* parameter (see 6.5) for each Port is assumed to be set to Both. In System 1, the *AuthControlledPortStatus* associated with the controlled Port is *unauthorized* and is therefore disabled (the “switch” is turned off); in System 2, the *AuthControlledPortStatus* is *authorized* and is therefore enabled (the “switch” is turned on).

In addition to the *AuthControlledPortStatus*, an *AuthControlledPortControl* parameter associated with the Port allows administrative control over the Port’s authorization status. This parameter can take the values *ForceUnauthorized*, *Auto*, and *ForceAuthorized*; its default value is *Auto*. The relationship between the *AuthControlledPortStatus* and *AuthControlledPortControl* parameters is as follows:

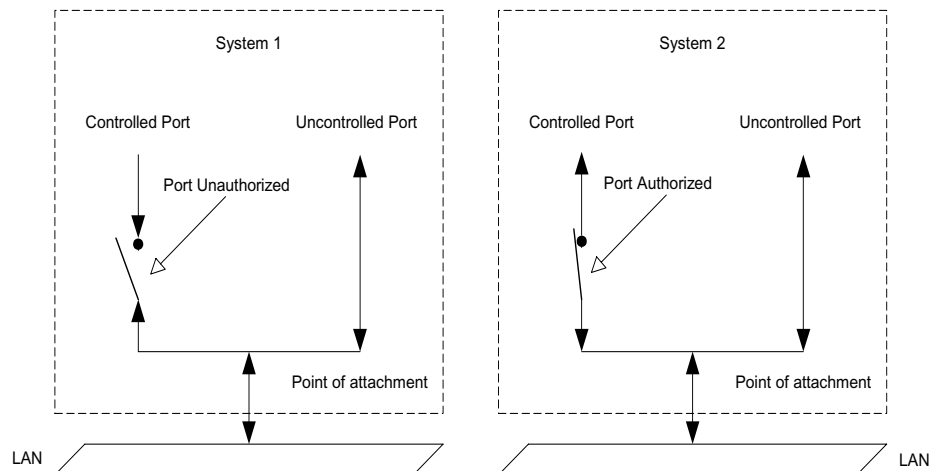


Figure 6-2—Effect of authorization state on controlled Ports

- a) An AuthControlledPortControl value of ForceUnauthorized forces the Authenticator PAE state machine (see 8.2.4) to set the value of AuthControlledPortStatus to be unauthorized; i.e., the Controlled Port is unauthorized unconditionally.
- b) An AuthControlledPortControl value of ForceAuthorized forces the Authenticator PAE state machine (see 8.2.4) to set the value of AuthControlledPortStatus to be Authorized; i.e., the Controlled Port is authorized unconditionally.
- c) An AuthControlledPortControl value of Auto allows the Authenticator PAE state machine (see 8.2.4) to control the value of AuthControlledPortStatus to reflect the outcome of the authentication exchanges between Supplicant PAE, Authenticator PAE, and Authentication Server.

In all three cases, the value of AuthControlledPortStatus directly reflects the value of the portStatus variable maintained by the Authenticator and Supplicant PAE state machines (see 8.2.2.2, 8.2.4, and 8.2.11). Three factors contribute to the value of the portStatus variable:

- d) The authorization state of the Authenticator PAE state machine (assumed to be “Authorized” if the state machine is not implemented for that Port).
- e) The authorization state of the Supplicant PAE state machine (assumed to be “Authorized” if the state machine is not implemented for that Port).
- f) The state of the *Supplicant Access Control With Authenticator* administrative control parameter. This parameter has two possible values, *active* and *inactive*. The default value of this control parameter is *inactive*; support of the *active* value is optional. The value of this parameter takes effect only if both Authenticator PAE and Supplicant PAE state machines are implemented for that Port. If the value of the parameter is *inactive*, then the portStatus parameter value is determined only by the authorization state of the Authenticator PAE state machine. If the value of the parameter is *active*, then the portStatus parameter value is determined by the authorization state of both the Authenticator PAE and Supplicant PAE state machines; if either state machine is in an unauthorized state, then the value of portStatus is unauthorized.

The value of the AuthControlledPortControl parameter for every Port of a System can be overridden by means of the SystemAuthControl parameter for the System. This parameter can take the values *Enabled* and *Disabled*; its default value is *Disabled*. If SystemAuthControl is set to *Enabled*, then authentication is enabled for the System, and each Port’s authorization status is controlled in accordance with the value of the Port’s AuthControlledPortControl parameter. If SystemAuthControl is set to *Disabled*, then all Ports behave as if their AuthControlledPortControl parameter is set to ForceAuthorized. In effect, setting the SystemAuthControl parameter to *Disabled* causes authentication to be disabled on all Ports, and it forces all controlled Ports to be Authorized.

Any access to the LAN is subject to the current administrative and operational state of the MAC (or logical MAC) associated with the Port, in addition to `AuthControlledPortStatus`. If the MAC is physically or administratively inoperable, then no protocol exchanges of any kind can take place using that MAC on either the controlled or the uncontrolled Port. This is illustrated in Figure 6-3; in system 1, both the controlled and uncontrolled Ports are able to access the LAN, as the controlled Port is authorized, and the MAC providing the point of attachment to the LAN is operable. In system 2, neither the controlled nor the uncontrolled Port can access the LAN, as the MAC providing the point of attachment to the LAN is inoperable. The inoperable state of the MAC has also caused the Authenticator PAE to transition the controlled Port to the Unauthorized state, as shown in Figure 6-3.

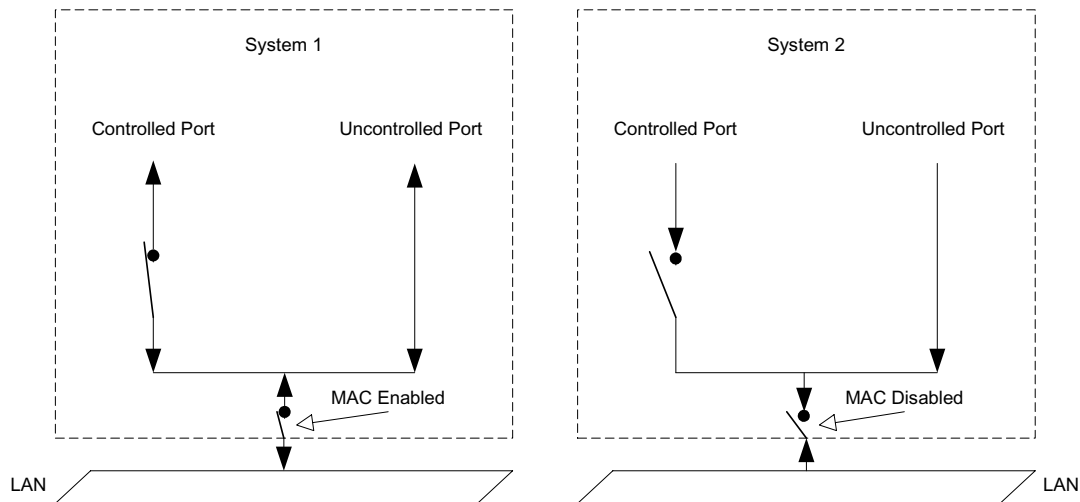


Figure 6-3—Effect of MAC enable/disable states

NOTE 3—Clause 6 of IEEE Std 802.1D describes the parameters available in a Bridge Port that indicate the administrative and operational states associated with the Port's MAC. IEEE Std 802.3 describes similar parameters that define the administrative and operational states associated with the logical MAC offered by an aggregation. The effect of the authorization state on the operability of the Controlled Port is analogous to the effect of the MAC's operational state; however, the effect of the authorization state is modified by the `OperControlledDirections` parameter associated with the Port, as illustrated in Figure 6-4.

The Authenticator and Supplicant PAEs use the uncontrolled Port for the purposes of exchanging protocol information with another Supplicant or Authenticator PAE.

Protocol exchanges between the Authenticator PAE and the Authentication Server (if the server is not colocated with the Authenticator PAE) can be conducted via one or more of the System's controlled or uncontrolled Ports.

NOTE 4—The details of communication between the Authenticator and the Authentication Server are outside of the scope of this standard. However, such communication would typically be achieved by means of an authentication protocol carried over appropriate higher layer protocols; for example, by means of 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 between the Authenticator and Authentication Server need not be subject to the authentication state of the controlled Port(s) 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.

It is expected that most protocol exchanges conducted by other functions of the System will make use of one or more of the System's controlled Ports. However, a given protocol may need to bypass the authorization function and make use of the uncontrolled Port. Figure 6-4 shows the uses of the controlled and uncontrolled Ports in an Authenticator System and a Supplicant System, and the ability of the PAEs to change the authorization state of the controlled Port depending on the outcome of an authentication exchange; the figure also gives an example of protocol entities (the PAEs) that require the use of the uncontrolled port in order to conduct their protocol exchanges.

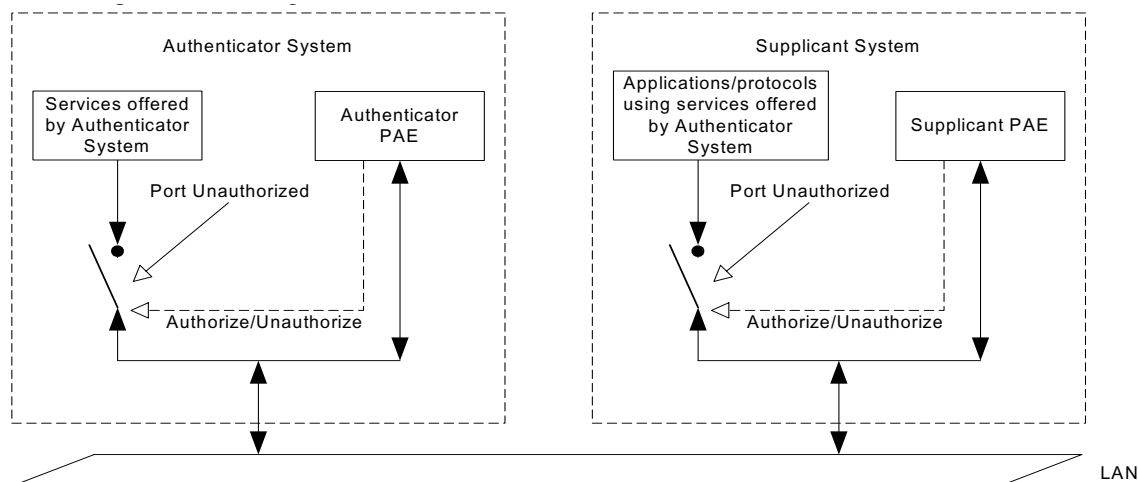


Figure 6-4—Use of the uncontrolled and controlled Ports

Figure 6-5 illustrates the relationships among the Supplicant, Authenticator, and Authentication Server, and the exchange of information among them. In this illustration, both the Authenticator's and the Supplicant's controlled Ports are in the unauthorized state and are therefore disabled from the point of view of access by the Supplicant's System to the services offered by the Authenticator's System. The two PAEs make use of their uncontrolled Ports to communicate with each other, using an authentication protocol carried at the Link Layer, and the Authenticator PAE communicates with the Authentication Server using authentication protocol carried in a higher layer protocol.

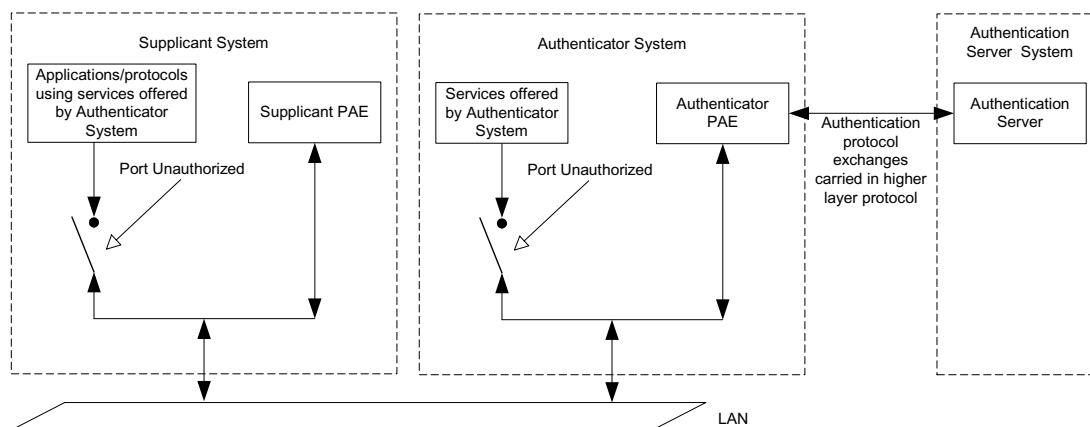


Figure 6-5—Authenticator, Supplicant, and Authentication Server roles

NOTE 5—The situation shown in Figure 6-5 could be found, for example, where the Supplicant's System was an end station and the Authenticator's System was a Bridge at the edge of a Bridged Local Area Network.

The communication between the Authenticator and the Authentication Server may make use of the services of a LAN, or it may use some other communication channel. In cases in which the Authentication Server is co-located with the Authenticator, authentication protocol exchanges between these two entities are unnecessary.

Figure 6-6 illustrates a situation in which the PAEs associated with the two systems, A and B, are able to adopt either the Supplicant or the Authenticator roles, as necessary. In order for System A to make use of

System B's services, System A's PAE must adopt the Supplicant role, and System B's PAE the Authenticator role. For System B to make use of System A's services, the roles are reversed. Note that although the Authentication Server function is shown as residing in two distinct systems in this example, this need not be the case. Note also that, since System A and System B implement both Authenticator and Supplicant PAEs, for the System's controlled Port to become Authorized, the Supplicant and the Authenticator state machines associated with that Port both have to be in the Authorized state.

NOTE 6—This can be visualized by considering the “switch” that represents the authorization state of the Port to actually consist of two individual switches in series, one controlled by the state of the Authenticator PAE for that Port, the other controlled by the state of the Supplicant PAE for that Port.

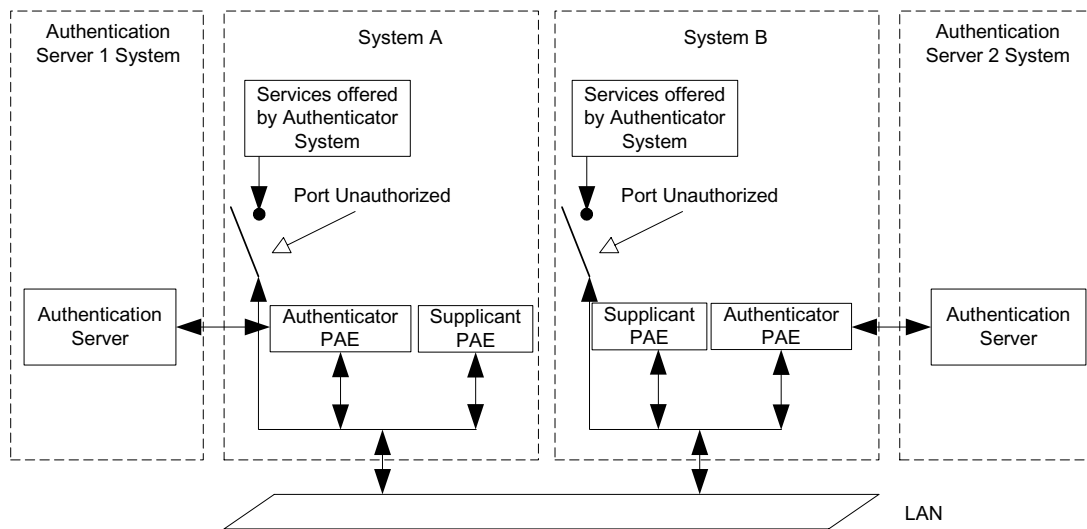


Figure 6-6—Systems adopting both Authenticator and Supplicant roles

NOTE 7—The situation shown in Figure 6-6 could be found, for example, where System A and System B are both Bridges. When they are initially connected together, each Bridge requires the other Bridge to be authenticated and authorized before it will forward frames on behalf of the other Bridge.

In general, the configuration shown in Figure 6-6 is intended for use where there is no obvious assignment of the Supplicant and Authenticator roles (for example, in peer-to-peer IEEE 802.11 networking) or where both systems desire to make use of their own Authentication Server for controlling access to their services. These concepts are further discussed in 6.7.

6.5 Reception and transmission control

The degree to which protocol exchanges that take place on the controlled Port are affected by the authorization state is determined by two *controlled directions* parameters associated with each controlled port: an *AdminControlledDirections* parameter and an *OperationalControlledDirections* parameter. These parameters determine whether a controlled Port that is unauthorized exerts control over communication in both directions (disabling both reception of incoming frames and transmission of outgoing frames), or just in the incoming direction (disabling only reception of incoming frames). The controlled directions parameters can take one of two possible values, *Both* and *In*. The relationship between these two parameters, and the meaning of their values, is as follows:

- a) **AdminControlledDirections = Both.** This indicates that control is required to be exerted over both incoming and outgoing traffic through the controlled Port. The value of OperControlledDirections is unconditionally set equal to Both if AdminControlledDirections is set equal to Both.

- b) **AdminControlledDirections = In.** This indicates that control is required to be exerted only over incoming traffic through the controlled Port. If AdminControlledDirections is set equal to In, the value of OperControlledDirections is set equal to In on initialization and when the Port's MAC becomes operable. However, the value of OperControlledDirections is set to Both if any of the following conditions is true:
- 1) The Port is a Bridge Port, and the Bridge Detection state machine (see Clause 17 of IEEE Std 802.1D) detects the presence of another Bridge connected to the Port.
 - 2) The Port is a Bridge Port, and the Edge Port parameter for the Port is FALSE.
 - 3) The Port's MAC becomes inoperable.

The value of the AdminControlledDirections parameter can only be modified by management. Implementations of Port-based access control shall support the ability to independently set the AdminControlledDirections parameter for each controlled Port to the value Both. Implementations of Port-based access control may support the ability to independently set the AdminControlledDirections parameter for each controlled Port to the value In.

NOTE—The In setting allows the security provisions of Port-based access control to be relaxed on Ports where an attached device needs to see protocol traffic from a controlled Port to support some forms of startup and initialization function (e.g., Wake-on-LAN), but where it is still desirable to prevent the attached device from transmitting into the controlled Port until authentication has taken place (see B.1). Clearly, the relaxation of the control offered by the controlled Port in this way reduces the effectiveness of Port-based access control in dealing with some types of attack.

The value of OperControlledDirections is determined by the operation of the Controlled Directions state machine (see 8.2.10).

6.6 Port Access Entity (PAE)

A Port Access Entity (PAE) operates the algorithms and protocols associated with the Port Access Control Protocol defined in Clause 8. A PAE exists for each Port of a System that supports Port Access Control functionality in the Supplicant role, the Authenticator role, or both.

In the Supplicant role, a PAE is responsible for providing information to an Authenticator that will establish its credentials. A PAE that performs the Supplicant role in an authentication exchange is known as a Supplicant PAE.

In the Authenticator role, a PAE is responsible for communication with a Supplicant, and for submitting the information received from the Supplicant to a suitable Authentication Server in order for the credentials to be checked and for the consequent authorization state to be determined. A PAE that performs the Authenticator role in an authentication exchange is known as an Authenticator PAE.

Both PAE roles control the authorized/unauthorized state of the controlled Port (see 6.4) depending on the outcome of the authentication process. If a given controlled Port has both Authenticator PAE and Supplicant PAE functionality associated with it, both PAEs must be in the Authorized state in order for the controlled Port to become Authorized.

Subclauses 6.6.1 through 6.6.4 offer an overview of the operation of a PAE in the Authenticator and Supplicant roles.

6.6.1 Authenticator role

An Authenticator PAE is responsible for enforcing the authentication of a Supplicant PAE that attaches to its controlled Port and for controlling the authorization state of the controlled Port accordingly.

In order to perform the authentication, the Authenticator PAE makes use of an Authentication Server. The Authentication Server may be co-located in the same System as the Authenticator PAE, or it may be located elsewhere, accessible via remote communication mechanisms, LAN-based or otherwise. Communication between the Supplicant PAE and the Authenticator PAE, and between the Authenticator PAE and the Authentication Server (when the Authentication Server is not co-located with the Authenticator), is achieved by means of the protocols and procedures described in Clause 8.

6.6.2 Supplicant role

A Supplicant PAE is responsible for communicating the credentials of the Supplicant to the Authenticator PAE in response to requests from the Authenticator PAE, and for controlling the authorization state of the controlled Port according to the outcome of the authentication exchange communicated to it by the Authenticator PAE. The Supplicant PAE may also initiate authentication exchanges and perform explicit logoff exchanges, as further described in 6.6.4 and Clause 8.

6.6.3 Port access restrictions

Authentication occurs primarily at System initialization time, or when a Supplicant System is connected to a Port of an Authenticator System. Until authentication has successfully completed, the Supplicant System only has access to the Authenticator System to perform authentication exchanges, or to access any services offered by the Authenticator's System that are not subject to the access control restrictions placed on either the Authenticator's controlled Port or the Supplicant's controlled Port (see 6.4 and 6.5). Once authentication has successfully completed, both Systems can allow full access by the Supplicant System to the services offered via the Authenticator System's controlled Port.

The operational state of the MAC that supports a controlled Port can be disabled or enabled. If the MAC's operational state is disabled, then the MAC is not available for use, regardless of the authorization state associated with the controlled Port.

NOTE 1—Clause 6 of IEEE Std 802.1D describes the parameters available in a Bridge Port that indicate the enable/disable states of the Port's MAC. IEEE Std 802.3 describes similar parameters that define the enable/disable states of the logical MAC offered by an aggregation.

In a System that implements a PAE, the controlled Port is placed in the unauthorized state until authentication has taken place, and it is therefore also disabled. Once authentication has succeeded, and it has been determined that the authenticated user is authorized to access the controlled Port, the controlled Port is placed in the authorized state; assuming that there is no other reason for it still to be disabled (e.g., the MAC has been disabled for administrative purposes), the controlled Port is then available for use (see 6.4).

NOTE 2—While an Authenticator System's controlled Port is in the unauthorized state, Dynamic Host Configuration Protocol (DHCP) and other initialization traffic may not be transmitted or received via the controlled Port, depending on the current value of the Port's Controlled Directions parameters (see 6.5). As a result, authentication may need to occur early in the end-station initialization sequence [prior to DHCP and Internet Protocol (IP) initialization for example].

In addition, while the Supplicant's controlled Port is in the unauthorized state, transmission or reception of DHCP and other initialization traffic is not possible. Attempts by the Supplicant to utilize its port prior to authorization may result in loss of DHCP or initialization packets, potentially resulting in an inability to obtain an IP address.

In addition to controlling the controlled Port's authorization state, the operation of the PAE may support ageing out of the authorization state of controlled Ports, and it may request that the Supplicant reauthenticate at any time. Controlled Ports remain authorized during reauthentication and transition to the unauthorized state only if reauthentication fails.

Authentication is configurable on a per-Port basis, because it will be desirable in some configurations not to perform authentication on certain Ports (e.g., on inter-Bridge links, Ports attached to servers). The management operations available for such configuration are described in Clause 9.

6.6.4 Logoff mechanisms

There are several mechanisms that can result in the controlled Port state changing to unauthorized and thereby controlling access via that Port in accordance with its OperControlledDirections parameter (see 6.5):

- a) The authentication exchanges between the Supplicant and the Authentication Server can result in failure to authorize the Port.
- b) Management controls can prevent the Port from being authorized, regardless of the credentials of the Supplicant.
- c) The MAC associated with the Port can be non-operational for any reason (including for hardware failure or administrative reasons).
- d) Connection failure between the Supplicant and the Authenticator can result in the Authenticator timing out the authorization state.
- e) Expiry of a reauthentication timer can occur without successful reauthorization.
- f) The Supplicant PAE can fail to respond to a request for authentication information by the Authenticator PAE.
- g) The Supplicant PAE can issue an explicit logoff request.

When a user logs off from an end station, it is possible in some environments for the user (or a different user) to bypass a new login request and thereby gain access to the end station and the network. Providing the explicit logoff mechanism ensures that the session is terminated, not only with respect to the user's access to the end station, but also for the end station's authorization status with the controlled Port of the Authenticator System to which it is connected. An explicit logoff therefore causes both the Supplicant and Authenticator PAEs to set their controlled Ports to the unauthorized state.

6.7 Coupling two EAPOL authentications

This subclause discusses the ability of the Port Access Control Protocol (PACP) specified in Clause 8 to transport two simultaneous authentication dialogs in opposite directions, how implementation asymmetries affect authentication results, and how simultaneous bi-directional transport may be utilized.

In the PACP, there is a requestor role (Authenticator) and a responder role (Supplicant). The Authenticator transmits frames to the Supplicant and the Supplicant responds to those frames with frames of its own. The PACP, like the authentication protocol carried within it (EAP), is a request/response protocol, and the state machines reflect this. Such a transport is sometimes called “unidirectional” meaning the protocol exchanges always originate from one side (the requestor).

However, it is not the IEEE 802.1X transport that controls whether the authentication is mutual or one-way. Rather, the chosen EAP method controls whether the authentication is mutual or one-way, and support for a Supplicant controlled port determines whether authorization is mutual or one-way.

Despite the asymmetry of IEEE 802.1X and EAP transports, if a mutually authenticating EAP method [such as EAP-Transport Layer Security (EAP-TLS)] is carried within IEEE 802.1X frames, then the Supplicant and Authenticator can mutually authenticate. However, if an EAP method is chosen that only authenticates the Supplicant to the Authenticator (e.g., EAP MD5-CHALLENGE), then the authentication will be one-way.

In an earlier version of IEEE Std 802.1X (see IEEE Std 802.1X-2001 [B6]), only the Authenticator was specified to have a controlled port. The lack of a Supplicant controlled port prevented the Supplicant from enforcing authentication decisions, thus creating a possibility of Supplicant connecting to a rogue

Authenticator even when a mutual authentication method was used. However, this was due to the lack of a specification of the controlled port on the Supplicant, not due to the one-way nature of the PACP transport protocol. The current version of IEEE Std 802.1X remedies this by specifying how both Authenticator and Supplicant roles affect the controlled port.

In the PACP, each role has its own state machine and it is possible that a single device can implement both the Supplicant and Authenticator roles (state machines). If a device implementing both roles encounters another device implementing both roles, then two separate (and simultaneous) PACP transports will take place in opposite directions. This is sometimes referred to as a bi-directional authentication transport or two coupled one-way authentication exchanges. PACP does not support “tie breaking” wherein two hosts initiating authentication with each other will only go forward with a single authentication.

Two coupled one-way authentication exchanges are not equivalent in security to a single exchange of a mutually authenticating EAP method (such as EAP-TLS). Since the two coupled one-way authentication exchanges are not cryptographically bound together, there is no way to ascertain that the party involved in the first one-way exchange is the same party that is involved in the alternate one-way exchange.

Even though a single PACP exchange may provide mutual authentication, there may be other reasons to run two PACP exchanges in opposite directions. RFC 3748, Section 2.4 discusses some of these cases, which include:

- a) When the devices require the creation of separate key material in each direction but the keying protocol is uni-directional (as in the group handshake in IEEE 802.11 adhoc networks).
- b) When different credentials are used for different roles (one credential for the Supplicant role and one for the Authenticator).
- c) When two bridges are connected, each bridge may implement the Supplicant role, but may have authorization requirements that can only be enforced by the Authenticator (“Supplicant Access Control with Authenticator” variable set to inactive).

When a device that implements both PACP roles on a single port encounters a device that implements only a single Authenticator role, this may result in asymmetric controlled port state (the single role device authorizes its controlled port while the dual role device does not because its Authenticator role has not been satisfied). A complete table of encounters and results appears in Table 6-1.

It is suggested that applications utilizing IEEE Std 802.1X should specify which PACP roles must be implemented to avoid encounters that will result in failed network connections. See Section 2.4 of RFC 3748 for other issues that may arise in peer-to-peer usage of EAP.

6.8 Use of Port Access Control with IEEE Std 802.3

Where Port Access Control is used in conjunction with Ports that can be aggregated in accordance with Clause 43 of IEEE Std 802.3, the authentication and authorization mechanisms of the PAE shall operate on the individual Ports, and Ports shall be considered not to be aggregatable while they are in the Unauthorized state. Any Port that has become part of an aggregation, and that subsequently becomes Unauthorized, shall therefore be removed from that aggregation.

NOTE 1—The above is a requirement for interoperability in LAN environments that support both Clause 43 of IEEE Std 802.3 and Port Access Control. The background to this requirement is discussed in C.1.2.

Table 6-1 — Result of encounters between EAPOL transport roles assuming key-generating EAP methods are run and authentication result is success.

		Local		
		Supplicant	Authenticator	Both
Remote	Supplicant	<i>Fails gracefully</i> No link will be formed if media is considered unsafe without encryption (IEEE Std 802.11). Unauthenticated link will be formed if media is considered safe by default (IEEE Std 802.3).	<i>Works</i> Authenticated link. Authentication policy is set by choice of EAP method.	<i>Works</i> Authenticated link. Authentication policy set by choice of EAP method. Remote Supplicant and local Authenticator are authorized. Local Supplicant will receive no response and assume no Authenticator. Successful authentication to the local Authenticator will have made the port secure.
	Authenticator	<i>Works</i> Authenticated link. Authentication policy is set by choice of EAP method.	<i>Fails gracefully</i> No link will be formed. Each Authenticator will send initial EAP Requests but no response will arrive.	<i>Fails</i> Asymmetric link. Remote controlled port is authorized, but local controlled port remains unauthorized. Remote Authenticator and local Supplicant are authorized, local Authenticator remains unauthorized.
	Both	<i>Works</i> Authenticated link. Authentication policy set by choice of EAP method. Local Supplicant and remote Authenticator are authorized. Remote Supplicant will receive no response and assume no Authenticator. Successful authentication to the remote Authenticator will have made the port secure.	<i>Fails</i> Asymmetric link. Local controlled port is authorized, but remote controlled port remains unauthorized. Local Authenticator and remote Supplicant are authorized, remote Authenticator remains unauthorized.	<i>Works</i> Authenticated link. Authentication policy set by choice of two uncoupled EAP methods. Two keys will be formed and some mechanism must exist so that local and remote choose the same key.

In order to ensure the secure creation of an aggregation in this environment, the Ports that form a single aggregation should be authorized, either to the same entity, or to entities that are all authorized to join the aggregation. The process of determining if a Port is actually authorized to join an aggregation is beyond the scope of this standard, but could be determined by the Authentication Server and returned to the Authenticator as part of a successful authentication exchange. For example, in the case of RADIUS, an aggregation key could be generated using the attributes returned with the Access-Accept message.

NOTE 2—Link Aggregation will combine this aggregation key with other aggregation key information in order to create the final aggregation key to be used in LACP.

7. EAP encapsulation over LANs (EAPOL)

This clause defines the encapsulation techniques that shall be used to carry EAP packets between Supplicant PAEs and Authenticator PAEs in a LAN environment. The encapsulation is known as *EAP over LANs*, or *EAPOL*. At present, EAPOL encapsulations are described for IEEE 802.3/Ethernet MACs and Token Ring/FDDI MACs. The EAPOL encapsulation used with IEEE 802.3/Ethernet MACs can be applied to other LAN technologies that share the same basic frame format as Ethernet (for example, IEEE 802.12 Demand Priority operating in IEEE 802.3 compatibility mode). Similarly, the EAP encapsulation used with Token Ring/FDDI MACs can be applied to other LAN technologies that share the same basic frame format as IEEE 802.5 Token Ring (for example, FDDI or IEEE 802.12 Demand Priority operating in IEEE 802.5 compatibility mode).

NOTE—In this standard, “IEEE 802.3/Ethernet MACs” is used to refer to IEEE 802 MACs in which the native Link Layer protocol identification mechanism is based on a choice between the Type interpretation and Length interpretation of the Length/Type field. “Token Ring/FDDI MACs” is used to refer to MACs in which the native Link Layer protocol identification mechanism is based on LLC addressing.

7.1 Transmission and representation of octets

All EAPOL PDUs consist of an integral number of octets, numbered starting from 1 and increasing in the order that they are put into a MAC frame. The bits in each octet are numbered from 1 to 8, where 1 is the low-order bit.

When consecutive octets are used to represent a binary number, the lower numbered octet contains the more significant bits of the binary number.

When the encoding of (an element of) an EAPOL PDU is represented using a diagram in this clause, the following representations are used:

- Octet 1 is shown toward the top of the page, higher numbered octets being toward the bottom.
- Where more than one octet appears on a given line, octets are shown with the lowest numbered octet to the left, higher numbered octets being to the right.
- Within an octet, bits are shown with bit 8 to the left and bit 1 to the right.

7.2 EAPOL MPDU format for use with IEEE 802.3/Ethernet

A summary of the Ethernet form of an EAPOL MPDU is shown in Figure 7-1, starting with the Length/Type field of the MPDU. The fields shown in the diagram are defined in 7.5.

	Octet Number
PAE Ethernet Type (7.5.1)	1-2
Protocol Version (7.5.3)	3
Packet Type (7.5.4)	4
Packet Body Length (7.5.5)	5-6
Packet Body (7.5.6)	7-N

Figure 7-1—EAPOL MPDU format for IEEE 802.3/Ethernet

7.3 EAPOL MPDU format for use with IEEE 802.2 Logical Link Control (LLC)

A summary of the form of IEEE 802.2 LLC form of an EAPOL MPDU is shown in Figure 7-2. The fields shown in the diagram are defined in 7.5.

	Octet Number
SNAP-encoded Ethernet Type (7.5.2)	1-8
Protocol Version (7.5.3)	9
Packet Type (7.5.4)	10
Packet Body Length (7.5.5)	11-12
Packet Body (7.5.6)	13-N

Figure 7-2—EAPOL MPDU format for IEEE 802.2 LLC

7.4 Tagging EAPOL MPDUs

EAPOL MPDUs transmitted by a PAE shall not be Virtual LAN (VLAN) tagged, but may optionally be priority tagged. All PAEs shall be capable of receiving both priority tagged and untagged EAPOL MPDUs.

The structure of the tag header used for priority tagging is specified in IEEE Std 802.1Q.

7.5 EAPOL MPDU field and parameter definitions

7.5.1 PAE Ethernet type

This field is two octets in length, and it shall contain the Ethernet Type value assigned for use by the PAE, as defined in Table 7-3.

7.5.2 Subnetwork Access Protocol (SNAP)-encoded Ethernet type

This field is eight octets in length, and it shall contain the SNAP-encoded Ethernet Type, encoded in SNAP format, as follows:

- a) Octets numbered 1 through 3 carry the standard SNAP header, consisting of the hexadecimal value AA-AA-03.
- b) Octets numbered 4 through 6 carry the SNAP Protocol Identifier (PID), consisting of the hexadecimal value 00-00-00.
- c) Octets 7 and 8 carry the PAE Ethernet Type value, as defined in Table 7-3.

7.5.3 Protocol version

This field is one octet in length, taken to represent an unsigned binary number. Its value identifies the version of EAPOL protocol supported by the sender of the EAPOL frame. An implementation conforming to this specification shall use the value 0000 0002 in this field.

7.5.4 Packet type

This field is one octet in length, taken to represent an unsigned binary number. Its value determines the type of packet being transmitted. The following types are defined:

- a) **EAP-Packet.** A value of 0000 0000 indicates that the frame carries an EAP packet.
- b) **EAPOL-Start.** A value of 0000 0001 indicates that the frame is an EAPOL-Start frame.
- c) **EAPOL-Logoff.** A value of 0000 0010 indicates that the frame is an explicit EAPOL-Logoff request frame.
- d) **EAPOL-Key.** A value of 0000 0011 indicates that the frame is an EAPOL-Key frame.
- e) **EAPOL-Encapsulated-ASF-Alert.** A value of 0000 0100 indicates that the frame carries an EAPOL-Encapsulated-ASF-Alert.

All other possible values of this field shall not be used, as they are reserved for use in potential future extensions to this protocol.

NOTE—The EAPOL-Key packet type is used only where the optional ability to transmit key information between the Authenticator and the Supplicant is supported (see 8.1.9).

The EAPOL-Encapsulated-ASF-Alert packet type is provided for use by the Alerting Standards Forum (ASF) as a means of allowing alerts (e.g., specific SNMP traps; see B.1.4) to be forwarded through a Port that is in the Unauthorized state. All EAPOL frames with this packet type that are received on the uncontrolled Port are passed to the protocol entity responsible for handling ASF alerts for validation and further processing in accordance with the relevant ASF protocol specifications. This standard does not further specify either the syntax or semantics of the alert messages that can be carried in this type of packet, or the protocol actions taken on receipt of a packet of this type.

7.5.5 Packet Body length

This field is two octets in length, taken to represent an unsigned binary number. The value of this field defines the length in octets of the Packet Body field (see 7.5.6); a value of 0 indicates that there is no Packet Body field present.

7.5.6 Packet Body

The Packet Body field is present if the Packet Type contains the value EAP-Packet, EAPOL-Key, or EAPOL-Encapsulated-ASF-Alert; for all other values of Packet Type, this field is not present.

In a frame carrying a Packet Type of EAP-Packet, this field contains an EAP packet as described in 7.7. Exactly one EAP packet is encapsulated.

In a frame carrying a Packet Type of EAPOL-Key, this field contains a Key Descriptor as described in 7.6. Exactly one Key Descriptor is encapsulated.

In a frame carrying a Packet Type of EAPOL-Encapsulated-ASF-Alert, this field contains an ASF alert frame as specified by the ASF (see B.1.4). Exactly one ASF alert frame is encapsulated.

NOTE—The maximum size of EAP packet that can be carried within an EAPOL frame will depend on the maximum MAC frame size supported by the MAC method by which the frame is transmitted.

7.5.7 Validation of received EAPOL MPDUs and EAPOL protocol version handling

A PAE shall process a received EAPOL MPDU as specified in this clause if and only if the following conditions are all true:

- a) The Destination MAC address field contains the PAE group address, as specified in 7.8 (in non-shared media LANs), or the specific MAC address of the PAE (in shared media LANs).

- b) The PAE Ethernet Type field contains the value of the PAE Ethernet Type, as specified in 7.8.
- c) The Packet Type field contains one of the values EAP-Packet, EAPOL-Start, EAPOL-Logoff, or EAPOL-Key, as specified in 7.5.4.

NOTE 1—The model of operation, as described in 6.4, is such that any MPDU received by the underlying MAC is made available at both the Controlled Port and the Uncontrolled Port. The Port Access Entity is always attached to the Uncontrolled Port (and never attached to the Controller Port); hence, regardless of the state of the Controlled Port, any EAPOL MPDU that is made available at the Controlled Port is discarded.

In the case of EAPOL MPDUs that carry the Packet Type values EAPOL-Start and EAPOL-Logoff, any octets that appear in the PDU following the Packet Type field shall be ignored. In the case of EAPOL MPDUs that carry the Packet Type value EAP-Packet and EAPOL-Key, any octets that appear in the PDU following the Packet Body field shall be ignored.

The following rules apply to the validation and interpretation of EAPOL MPDUs, in order to ensure that backward compatibility is maintained between versions of this protocol.

For an implementation that supports version A of the protocol, a received EAPOL MPDU of a given Packet Type that carries a protocol version number B is interpreted as follows:

- d) Where B is greater than or equal to A, the EAPOL PDU shall be interpreted as if it carried the supported version number, A. Specifically:
 - 1) All EAPOL PDU parameters that are defined in version A shall be interpreted in the manner specified for version A of the protocol for the given EAPOL PDU Packet Type.
 - 2) All EAPOL PDU parameters that are undefined in version A for the given EAPOL PDU Packet Type shall be ignored.
 - 3) All octets that appear in the EAPOL PDU beyond the largest numbered octet defined for version A for the given EAPOL PDU Packet Type shall be ignored.

NOTE 2—As a consequence of the rules stated in item d) and its sub-bullets, a version 1 implementation may ignore the Protocol Version Identifier. This set of validation rules allows the possibility of future specification of extensions to the EAPOL Protocol, identified as new versions by different values of the identifier. Subsequent versions will be required to check the Protocol Version Identifier in order to correctly interpret the received PDU.

- e) Where B is less than A, the EAPOL PDU shall be interpreted as specified for the version number, B, carried in the EAPOL PDU. Specifically:
 - 1) All EAPOL PDU parameters shall be interpreted in the manner specified for version B of the protocol for the given EAPOL PDU Packet Type.
 - 2) All EAPOL PDU parameters that are undefined in version B for the given EAPOL PDU Packet Type shall be ignored.
 - 3) All octets that appear in the EAPOL PDU beyond the largest numbered octet defined for version B for the given EAPOL PDU Packet Type shall be ignored.

7.6 Key Descriptor format

A summary of the Key Descriptor format is shown in Figure 7-3. The fields shown in the diagram are defined in the following subclauses.

	Octet Number
Descriptor Type (7.6.1)	1
Descriptor Body (7.6.2)	2-N

Figure 7-3—Key Descriptor format

7.6.1 Descriptor type

This field is one octet in length, taken to represent an unsigned binary number. The value defines the type of of the Key Descriptor, which in turn defines how the Descriptor Body is used and interpreted.

Table 7-2 lists the values of Descriptor Type that are currently assigned.

Table 7-2—Descriptor Type value assignments

Assignment	Value
RC4 Key Descriptor Type (see 7.6.3) ^a	1
IEEE 802.11 Key Descriptor Type (see 7.6.4) ^b	2

^aNOTE—Use of this descriptor type is deprecated—see D.5.7.

^bIEEE 802.11 Key Descriptor Type has been assigned for use by the IEEE 802.11 standard.

All other possible values of Descriptor Type are reserved for future standardization.

As the Descriptor Type number space is small and finite, the first two fields in the Descriptor Body (see 7.6.2) shall comprise a Subtype and a Version,⁹ thus allowing revisions of, and extensions to, existing Descriptor Types to be defined without incurring further depletion of Descriptor Type values. The format of the Subtype and Version fields is not constrained by this standard, and forms part of the definition of the descriptor Body associated with each Descriptor Type.

7.6.2 Descriptor Body

The Descriptor Body contains an integral number of octets. The format and semantics of the Descriptor Body is as defined for a particular value of Descriptor Type.

⁹The RC4 Descriptor Type is the only exception to this rule, as it was already defined at the time the rule was imposed.

7.6.3 RC4 Key Descriptor

Use of the RC4[®] Key Descriptor¹⁰ is now deprecated (see D.5.7); however, its definition is included here for consistency with earlier versions of this standard.

NOTE—Annex D contains a more detailed description of the RC4 descriptor type.

The format of the RC4 Key Descriptor is shown in Figure 7-4. The Descriptor Type takes the value 1 to indicate an RC4 Key Descriptor; the remaining fields are as defined in the subclauses that follow.

	Octet Number
Descriptor Type = 1 (7.6.1)	1
Key Length (7.6.3.1)	2-3
Replay Counter (7.6.3.2)	4-11
Key IV (7.6.3.3)	12-27
Key Index (7.6.3.4)	28
Key Message Digest (7.6.3.5)	29-44
Key (7.6.3.6)	45-Packet Body Length

Figure 7-4—RC4 Key Descriptor format

7.6.3.1 Key length

This field is two octets in length, taken to represent an unsigned binary number. The value defines the length of the key in octets. For example, a value of 5 in this field indicates a 40-bit key.

7.6.3.2 Replay counter

This field is 8 octets in length, taken to represent an unsigned binary number. It carries a counter value, used to detect and prevent replay of key messages.

7.6.3.3 Key IV

This field carries a 16-octet Initialization Vector value, consisting of 128 bits of random data.

7.6.3.4 Key index

This field is one octet in length, taken to represent a 7-bit unsigned binary number and a flag. The value is generated by the Authenticator specifying the key, and it is used as a key index number if multiple keys are supported. The index number is carried in bits 1 through 7, and it can carry an integer in the range 0–127. Bit 8 is a flag bit. If bit 8 is set to 1, the key is a unicast key; if bit 8 is set to 0, the key is a broadcast key.

¹⁰The mark RC4 is a registered trademark of RSA Security Inc. and may not be used by third parties creating implementations of the algorithm. RSA Security does not hold any patents nor does it have any pending applications on the RC4 algorithm. However, RSA Security does not represent or warrant that implementations of the algorithm will not infringe the intellectual property rights of any third party. Proprietary implementations of the RC4 encryption algorithm are available under license from RSA Security Inc. For licensing information, contact RSA Security Inc., 2955 Campus Drive, Suite 400, San Mateo, CA 94403-2507, USA, or <http://www.rsasecurity.com>.

7.6.3.5 Key message digest

This field is 16 octets in length. The Key Message Digest is a message digest of all of the fields of the EAPOL packet, from and including the EAPOL protocol version field, to and including the Encrypted Key field, with the message digest set to 0. The Key Message Digest is an HMAC-MD5 message digest over the EAPOL MPDU, as described in 7.6.3.7.

7.6.3.6 Key

This field is optional. If it is not present, the Supplicant uses the peer key generated as part of the EAP authentication process as the key material for this message. If the key is longer than the key length specified in this message, then only the first N octets are used, where N is equal to the value of key length.

When RADIUS is used as the Authentication Server, and when the MS-MPPE-Send-Key and MS-MPPE-Recv-Key (see IETF RFC 3079 and IETF RFC 2548) are used to transport cryptographic keys, then the key field is interpreted as follows:

If Packet Body Length = 44 + Key Length, then the Key Field contains the key in encrypted form, of length Key Length. If Packet Body Length = 44, then the Key field is absent, and the least significant Key Length octets from the MS-MPPE-Send-Key attribute are used as the keying material. Where the Key field is encrypted using RC4, the RC4 encryption key used to encrypt this field is formed by concatenating the 16 octet (128 bit) Key-IV field with the 32 octet MS-MPPE-Recv-Key attribute. This yields a 48 octet RC4 key (384 bits).

7.6.3.7 Construction and interpretation of an RC4 Key Descriptor

Key Descriptors carrying a Descriptor Type of RC4 Key Descriptor are constructed and interpreted as follows:

- a) The Replay Counter field carries an NTP time value (see IETF RFC 1305).
- b) The Key IV field carries a random number used to generate an RC4 encryption key.
- c) A message digest type of HMAC-MD5 is used to generate the Key Message Digest (see IETF RFC 2104). The key used for the message digest is the server key generated by the EAP authentication (e.g., as defined in IETF RFC 2716).
- d) RC4 is used to encrypt the Key field. The RC4 encryption key is generated by concatenating the Key IV and the session key generated by the EAP authentication process (e.g., as defined in IETF RFC 2716). The key material is then encrypted according to the method specified by Encrypt Type (e.g., RC4 encrypted using the RC4 key).

7.6.4 IEEE 802.11 Key Descriptor Type

A single value of Key Descriptor Type has been assigned for use by IEEE Std 802.11, as shown in Table 7-2. The format and semantics of the Descriptor Body for these Key Descriptor Types are as defined in IEEE Std 802.11.¹¹ Authenticator and Supplicant key machines utilizing the IEEE 802.11 key descriptor are also defined by IEEE Std 802.11; these state machines completely replace the machines defined in this document when IEEE Std 802.1X is used in conjunction with the IEEE 802.11 key exchange mechanism.

¹¹At the time of publication of this standard, the specification of the IEEE 802.11 Key Descriptor was “work in progress” as part of the development of P802.11i.

7.7 EAP packet format—informative

A summary of the EAP packet format is shown in Figure 7-5. The figure and the accompanying field descriptions are included for illustrative purposes only; the normative definition of the EAP packet format and its associated semantics are to be found in the specification of EAP contained in IETF RFC 3748.

Code	Octet Number 1
Identifier	2
Length	3-4
Data	5-N

Figure 7-5—EAP packet format

7.7.1 Code

The Code field is one octet in length and identifies the type of EAP packet. EAP Codes are assigned as follows:

- 1 Request
- 2 Response
- 3 Success
- 4 Failure

7.7.2 Identifier

The Identifier field is one octet in length and allows matching of responses with requests. The Code field, Identifier field, and System Port together uniquely identify an authentication exchange. The Authentication server must also maintain a separate identifier space for each session, and the System Port identifier should be used for this purpose.

The operation of EAP (see 8.1.1) in the Authenticator determines the value of Identifier used in new EAP-Request frames. The Supplicant uses the same Identifier in subsequent EAP-Response frames responding to that initial request frame. The Authenticator PAE uses the same Identifier value in any retransmissions of the same request.

7.7.3 Length

The Length field is two octets in length and indicates the length of the EAP packet, including the Code, Identifier, Length, and Data fields.

NOTE—Because in this specification EAP frames are transported directly over the link layer medium, the frame size cannot exceed the maximum permissible on that medium, as fragmentation is not supported.

7.7.4 Data

The Data field is zero or more octets. The format of the Data field is determined by the Code field.

7.8 EAPOL addressing

PAEs (see Clause 8) transmit and receive:

- a) EAPOL frames exchanged between an Authenticator and a Supplicant
- b) EAP frames exchanged between an Authenticator and an Authentication Server

NOTE 1—An Authentication Server may be co-located with an Authenticator; in which case, a communication protocol may not be required.

NOTE 2—This standard refers to EAP carried in RADIUS as a basis of these exchanges; however, the use of other protocols to achieve these exchanges is permitted.

PAEs use the DL_UNITDATA.request and DL_UNITDATA.indication primitives associated with each active Port to transmit and receive EAPOL frames. In IEEE 802.3/Ethernet MACs, frames carry the Port Access Entity Ethernet Type as the data link address; this type value is defined in Table 7-3. In Token Ring/FDDI MACs, frames carry the Port Access Entity Ethernet Type in SNAP-encoded form, using a SNAP header of AA-AA-03 and a SNAP PID of 00-00-00, followed by the Ethernet Type value.

Table 7-3—Standard Ethernet Type assignment

Assignment	Value
Port Access Entity Ethernet Type	88-8E

A group MAC address, the PAE group address (see Table 7-4), is assigned by IEEE Std 802.1D¹² for use by PAEs. In MACs where the LAN technology concerned is such that the individual MAC address of the Supplicant is known to the Authenticator, and vice versa (for example, in IEEE 802.11, where the establishment of an association between a station and an access point involves the exchange of MAC addresses), all EAPOL frames transmitted by a PAE shall carry the individual MAC address associated with the destination PAE's point of LAN attachment as the destination MAC address. Otherwise (i.e., in MACs where the LAN technology concerned is such that the individual MAC address of the Supplicant can be unknown to the Authenticator, and vice versa, for example IEEE Std 802.3), all EAPOL frames transmitted by a PAE shall carry the PAE group address as the destination MAC address even if the individual MAC address of the destination PAE is later discovered. All EAPOL frames shall carry the individual MAC address associated with the source PAE's point of LAN attachment to its counterpart (Authenticator or Supplicant PAE) as the source MAC address. In an IEEE 802.11 access point, the BSSID associated with the wireless interface would be used in place of this MAC address.

Table 7-4—PAE group address assignment

Assignment	Value
Port Access Entity group address (PAE group address)	01-80-C2-00-00-03

NOTE—The PAE group address is one of the reserved set of group MAC addresses that are not forwarded by MAC Bridges.

¹²The assignment of this address is to be found in Table 7-9 of IEEE Std 802.1D. The value is repeated here for informative purposes.

7.9 Use of EAPOL in shared media LANs

In order to make use of EAPOL in shared media LANs, it is necessary to establish a pairwise association between the Supplicant and Authenticator. The use of individual MAC addresses with EAPOL (7.8) permits such an association to be established, and in particular, this has been allowed in order to support the use of Port-based Network Access Control in IEEE 802.11 wireless LAN networks. However, it should be noted that in shared media LANs, it is necessary to take steps to ensure:

- a) Reliability of the authentication that takes place between Authenticator and Supplicant.
- b) Data confidentiality for data transmitted on the association subsequent to successful authentication.

This standard takes no steps to provide either reliable authentication or data confidentiality in a shared medium environment. The use of EAPOL in a shared medium environment renders Port-based network access control highly vulnerable to attack. In addition, use of EAPOL in an environment where reliable transmission is not supported will result in frequent timeouts; even though EAP supports retransmission, (see RFC 3748, Section 4.3) frequent timeouts will result in a degraded user experience.

8. Port Access Control Protocol

8.1 Introduction to protocol operation

8.1.1 Overview

The operation of the authentication process makes use of the Extensible Authentication Protocol (EAP, specified in IETF RFC 3748) as the means of communicating authentication information between the Supplicant and the Authentication Server. EAP is a general protocol that supports multiple authentication mechanisms. For example, through the use of EAP, support for a number of authentication schemes may be added, including smart cards, Kerberos, Public Key Encryption, One Time Passwords, and others.

The approach taken in this standard is to define an encapsulation format that allows EAP Messages to be carried directly by a LAN MAC service. The encapsulated form of EAP, known as EAP over LANs, or EAPOL, is used for all communication between the Supplicant PAE and the Authenticator PAE.

Each PAE has two separate components, a set of PACP state machines, and a higher layer with which these machines communicate. In the case of the Supplicant PAE, the higher layer consists of EAP functionality, while in the case of the Authenticator PAE, the higher layer is a combination of EAP and authentication, authorization, and accounting (AAA) functionality. This standard defines the PACP state machines and the interface between the PACP state machines and the higher-layer functionality.

The operation of the higher-layer functions with which the PAE state machines communicate is outside the scope of this standard. EAP protocol exchanges are defined by IETF EAP standards, IETF RFC 3748, and successor standards. One example of a AAA protocol, RADIUS, is defined by IETF RADIUS standards, IETF RFC 2865, IETF RFC 2866, IETF RFC 3579, and successor standards. Annex F defines the interface that the PACP PAE state machines assume from the higher layers.

Figure 8-1 shows the interface between the PACP state machines and the higher layer for the Supplicant PAE and Authenticator PAE. As shown, the portEnabled signal from the system indicates to both the higher layer and the PACP that a port is active. The PACP passes EAP messages between the physical port and the higher layer. Message flow on the Supplicant is controlled using eapResp/eapNoResp from EAP to indicate it is ready for another message and eapReq from the PACP to indicate a message is available for EAP to process. Message flow on the Authenticator side is controlled with a similar process, with the higher layer using eapReq/eapNoReq, to indicate when it is ready to receive a new message, and eapResp to indicate that a message is available to be processed by the higher layer.

Within the higher layer, EAP and associated EAP methods drive the authentication dialog, but on completion the higher layer will take its cue from AAA to signal success or failure to the PACP, using eapSuccess and eapFail signals. The separation between the higher layer and the PACP is such that all EAP messages exchanged between Supplicant and Authenticator are created by the EAP component.

The EAP method on the Authenticator acts as a “passthrough,” forwarding EAP messages back and forth to an Authentication Server using a AAA protocol as a transport. The higher layer coordinates the EAP and AAA components. RADIUS is one such transport protocol that can be used as a lower layer for this forwarding mechanism. The use of RADIUS for pass-through forwarding is described in IETF RFC 3579.

Rather than only permitting a predetermined authentication method, EAP allows the Authenticator PAE to request more information before determining the specific authentication mechanism. In EAP, the Authenticator PAE sends one or more Requests to authenticate the Supplicant PAE. The Request has a type field to indicate what is being requested. Examples of Request types include Identity, MD5-challenge, One-Time Passwords, and Generic Token Card. The MD5-challenge type corresponds closely to the Challenge Handshake Authentication Protocol (CHAP). Typically, the Authenticator will send an initial Identity Request

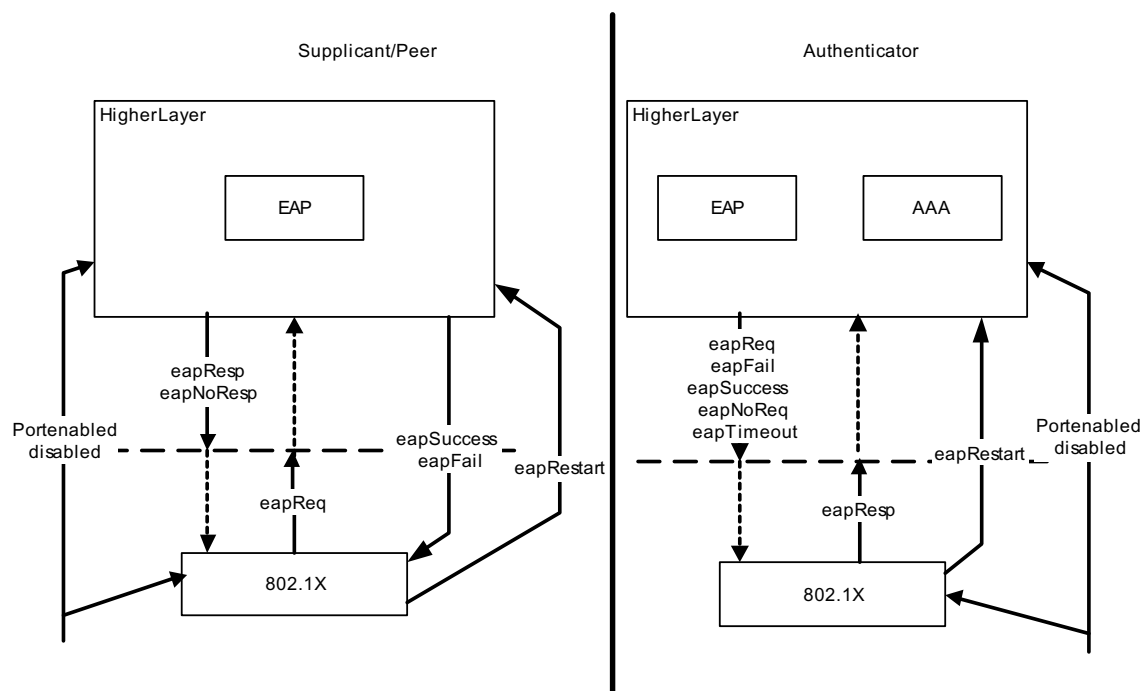


Figure 8-1 — Higher layer interface diagram

followed by one or more Requests for authentication information. However, an initial Identity Request is not required, and it may be bypassed in cases in which the identity is presumed or can be determined by other means (such as a method-specific identity exchange). The Supplicant PAE sends a Response packet in reply to each Request. As with the request packet, the Response packet contains a type field that corresponds to the type field of the Request.

The authentication exchange ends with an Accept or Reject indication from the Authentication Server. The Authenticator forwards the EAP packet included within the Accept or Reject indication, while the AAA client operating as a lower layer beneath EAP interprets the indication and indicates success or failure to the Authenticator, which will set the controlled Port to authorized or unauthorized appropriately.

8.1.2 Authentication initiation

Authentication can be initiated either by the Supplicant PAE or by the Authenticator PAE. If authentication is enabled on a given Port (i.e., if the Port supports an Authenticator PAE and the AuthControlledPortControl parameter for the Port is set to Auto and SystemAuthControl is set to Enabled; see 6.4), authentication is initiated by the Authenticator PAE on sensing that the operational state of the MAC associated with the Port has transitioned from disabled to enabled. As noted below, if the Authenticator PAE does not receive a response, EAP will retransmit the authentication request.

A Supplicant PAE may initiate the authentication sequence by sending an EAPOL-Start frame (see 7.5.4).

NOTE 1—On initialization, a Supplicant PAE may not be listening for an authentication initiation during the early portions of the initialization sequence, and consequently, the Supplicant PAE may miss the initiation frame(s) sent by the Authenticator PAE. As a result, if the Supplicant PAE did not initiate authentication itself, an authentication failure could occur purely due to timing issues. A Supplicant PAE that does not receive an authentication initiation frame from the Authenticator PAE on reinitialization may initiate authentication by sending an EAPOL-Start frame.

NOTE 2—A previously authenticated Supplicant PAE's System may be reinitialized. In this circumstance, an Authenticator PAE might not initiate authentication, because it may not sense a transition in the MAC's operational state. In this case, it could be argued that authentication is not necessary because the Supplicant PAE has already been authenticated.

However, it is possible in some environments to reinitialize a machine, bypass the normal login, and access the Authenticator System's services. To prevent an unauthorized user from accessing the Authenticator by reinitializing an authenticated machine, a Supplicant initiation of authentication is necessary upon reinitialization.

8.1.2.1 Authenticator initiation

The Authenticator PAE will typically initiate the conversation when it receives an indication that the Port has become operable. Before authentication commences, the Port state is forced to the unauthorized state.

The Authenticator PAE initiates the authentication sequence by signaling the higher layer and then sending the EAP-Request frame given to it by EAP. Typically, EAP will begin the authentication exchange with an EAP-Request frame; however, any EAP-Request can be used to initiate the exchange. A Supplicant PAE receiving an EAP-Request frame from the Authenticator PAE responds with an EAP-Response frame provided by EAP.

Authenticator PAEs may support periodic reauthentication, and they may request that a Port reauthenticate at any time. For example, if the Authenticator System reinitializes, the authentication state can be recovered by issuing EAP-Request frames on all Ports. If a controlled Port is in the authorized state prior to reauthentication, then it will remain in that state during reauthentication. If the authentication fails for a controlled Port that was in the authorized state during reauthentication, then the controlled Port's authorization state is transitioned to unauthorized in order to control external access to that Port in accordance with the current value of the OperControlledDirections parameter (see 6.5).

8.1.2.2 Supplicant initiation

In order to request that the Authenticator PAE initiate authentication, the Supplicant PAE sends an EAPOL-Start packet (see 7.5.4). The Authenticator PAE receiving an EAPOL-Start packet responds by sending an EAP-Request packet that is chosen by EAP.

8.1.3 EAPOL-Logoff

When a Supplicant wishes the Authenticator PAE to perform a logoff (i.e., to set the controlled Port state to unauthorized), the Supplicant PAE originates an EAPOL-Logoff message (see 7.5.4) to the Authenticator PAE. As a result, the Authenticator PAE immediately places the controlled Port in the unauthorized state.

NOTE—In general, it is advisable for the Supplicant PAE to originate an EAPOL-Logoff in any circumstances in which the authentication credentials are user-based, and the user of the Supplicant System has logged off (in the case of an end station), or in which the operation of the Supplicant System has been reconfigured in a manner that would invalidate any previous authentication results (for example, a management change that affects the Supplicant System's identity, or its authorization to use the services of the Authenticator's System).

8.1.4 Timing out authorization state information

Authenticator PAEs can time out the authorization state information on a periodic basis by means of the Reauthentication Timer State Machine (see 8.2.8). The time period for such timeouts is reAuthPeriod seconds since the last time that the authorization state was confirmed. The state variable reAuthEnabled controls whether periodic reauthentication takes place.

Reauthentication can be enabled and disabled, and the reAuthPeriod modified, by management. The default settings are for the reAuthPeriod to be 3600 s (one hour) and for reauthentication to be disabled.

NOTE—As with Authenticator and Supplicant initiated reauthentication, the implications of setting this to a lower value should be carefully thought out before proceeding. The value chosen will be affected by the reliability with which the MAC associated with the Port can detect and indicate MAC enabled/disabled conditions. If the Port's detection of MAC state is reliable, then longer timeout values may be appropriate.

8.1.5 Retransmission

As noted in the specification of EAP, the Authenticator PAE is responsible for retransmission of messages between the Supplicant PAE and the Authenticator PAE. In particular, EAP is the Authenticator PAE component that handles retransmission, not the IEEE 802.1X state machines. Thus, if an EAP-Packet is lost in transit between the Supplicant PAE and the Authenticator PAE (or vice versa), the Authenticator PAE will retransmit. The exceptions are EAPOL-Start messages, which are retransmitted, if necessary by the Supplicant PAE, and any EAP messages delivered during the FAIL and SUCCESS states. Because the messages delivered from the Authenticator FAIL and SUCCESS states (typically EAP-Failure and EAP-Success) are not acknowledged by the Supplicant PAE, they are not retransmitted by the Authenticator PAE. If an EAP-request is lost, the Supplicant PAE state machine transitions to the CONNECTING state on authWhile timer expiration.

In implementations in which the authentication function is performed by a remote Authentication Server, retransmissions may be necessary between the Authenticator PAE and the Authentication Server. In this instance, it may be necessary for the higher layer to adopt a retransmission strategy that is more appropriate to the transmission characteristics of the communication path involved.

NOTE—DHCP clients incorporate a randomized exponential backoff algorithm to determine the delay between retransmissions, allowing a retransmission delay of up to 64 s. Assuming that the Authenticator is in blocking mode prior to authentication and initiates authentication on receiving an initial DHCP frame from the end station, the initial DHCP frame will be dropped and will trigger authentication initiation by the Authenticator. Assuming that the authentication can complete in time to avoid a DHCP timeout, the DHCP conversation will complete successfully.

It may be necessary to adjust retransmission strategies and authentication timeouts in certain cases. For example, when a token card is used, additional time may be required to allow the user to find the card and enter the token. If the user takes a particularly long time to find the card, then a DHCP timeout can occur. This problem cannot be ameliorated by enqueueing the initial DHCP frames because DHCP client timers are started when the packets are enqueued, not when they are sent.

8.1.6 Migration considerations

It is desirable that the transition between a non-authenticated and an authenticated environment be as smooth as possible. For example, when an authentication-capable Supplicant connects to a non-authentication-capable Bridge, the Supplicant will not receive an EAP-Request packet. As a result, the Supplicant PAE will initiate an EAPOL-Start frame to the PAE group MAC address. As this address is one of the addresses that are not forwarded by MAC Bridges, the Supplicant PAE will not receive a response. Hence, after a suitable timeout period in which the EAPOL-Start has been retransmitted and no response has been received, the Supplicant can assume that it is authorized to access the Bridged Local Area Network.

As the concept of the controlled and uncontrolled Ports applies to systems that support either Authenticator or Supplicant functionality, a system that only supports Supplicant functionality cannot transmit data frames prior to completion of the authentication process. Hence, in the example above, the Supplicant system must wait for the end of the authentication timeout period before initiating data exchanges via the Bridge Port. In order to allow applications such as DHCP to run immediately on connection, it may be desirable to administratively force the Supplicant Port to the Authorized state in such situations.

NOTE—If the Supplicant finds that the authentication process times out, the choice as to whether the Supplicant enables the controlled Port or not is determined by the security policy in force in the Supplicant system.

When a non-authentication-aware Supplicant connects to an authentication enabled Bridge, the Supplicant, having no PAE, will ignore EAP-Request frames. Consequently, the Port will remain in the unauthorized state. The Supplicant will be able to access the Bridged Local Area Network via the Bridge's controlled Port only in accordance with the value of the OperControlledDirections parameter (see 6.5); access to any services that are made available via the Bridge's uncontrolled Port are unrestricted.

8.1.7 Relaying EAP frames

The Authenticator PAE is responsible for relaying EAP frames between the Supplicant and the Authentication Server via the higher layer. It must also perform any repackaging of EAP frames that is necessary in order to convert EAP frames carried as EAPOL between Supplicant PAE and Authenticator PAE. It is the responsibility of the higher layer to perform any repackaging of EAP frames required between the Authenticator and Authentication Server. In performing its relay function, the information contained in the EAP frames relayed is not modified other than as required to convert the frame format to/from the EAPOL format.

NOTE—EAP in RADIUS (see IETF RFC 2865, IETF RFC 2866, IETF RFC 3579, and Annex D) offers a suitable option for the AAA protocol used between Authenticator and Authentication Server; however, use of RADIUS is not mandated by this standard.

EAPOL-Start and EAPOL-Logoff frames are transmitted by the Supplicant PAE to the Authenticator PAE; EAPOL-Key frames are transmitted by the Authenticator PAE to the Supplicant PAE and by the Supplicant PAE to the Authenticator PAE. These frames are not relayed onward by the Authenticator PAE to the Authentication Server.

The initial EAP-Request frame is typically transmitted by the Authenticator PAE to the Supplicant PAE and may not appear in the communication path between the Authentication Server and the Authenticator PAE.

All EAP frames received from the Supplicant PAE are decapsulated by the Authenticator PAE from their EAPOL format for transfer as EAP frames to EAP. It is the higher layer's responsibility to format the EAP frame for onward transmission to the Authentication Server in accordance with the AAA protocol in use between the Authentication Server and the Authenticator PAE.

All AAA protocol frames received by the Authenticator PAE from the Authentication Server are converted to EAP frames by the higher layer and then passed to the Authenticator PAE. The Authenticator PAE then converts these EAP frames to EAPOL format, as appropriate for the Port concerned, for onward transmission to the Supplicant PAE.

8.1.8 Example EAP exchanges

In these example exchanges, the exchange of EAPOL frames is shown as a solid line; the exchange of EAP frames carried in a higher-layer protocol such as RADIUS is shown by a broken line. The diagrams therefore show which PDU exchanges involve the Authenticator PAE in repackaging EAP frames in order to perform protocol translation.

NOTE 1—For the purposes of these examples, Figure 8-2 through Figure 8-7 show the Authenticator PAE and higher layer as a single entity under the heading “AUTHENTICATOR PAE”. In the diagrams, the communications shown between the headings “SUPPLICANT PAE” and “AUTHENTICATOR PAE” are managed by the Authenticator PAE and the communications shown between the headings “AUTHENTICATOR PAE” and the “AUTHENTICATION SERVER” are managed by the higher layer.

NOTE 2—For the purposes of these examples, it has been assumed that the AAA client indicates success to the Authenticator when an Accept message is received from the Authentication Server, and that the AAA client indicates failure to the Authenticator when a Reject message is received from the Authentication Server. However, it is possible for EAP to indicate success or failure to the Supplicant based on whatever criteria the EAP specification allows and would typically provide EAP-Success or EAP-Failure frames to be delivered to the Supplicant (although this is not required). Because the Backend Authentication state machine is influenced only by the success or failure indication from the AAA client, rather than the encapsulated EAP packet, this does not present a problem.

The example in Figure 8-2 shows an Authenticator-initiated conversation for the case of a One Time Password (OTP) authentication. OTP is used only for illustrative purposes; other authentication protocols could also have been used, although they may show somewhat different behavior.

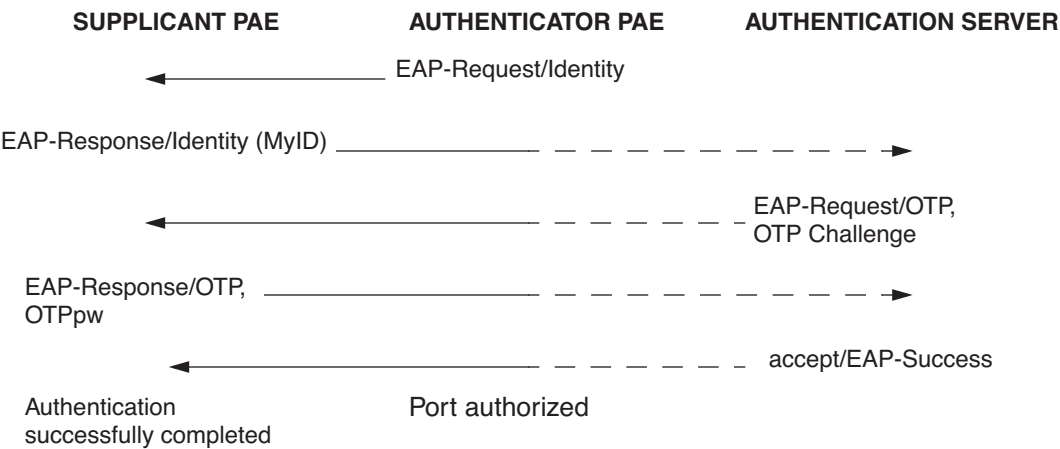


Figure 8-2— Authenticator-initiated, one-time password exchange (success)

In the case in which the Supplicant fails EAP authentication, the conversation would appear as illustrated in Figure 8-3.

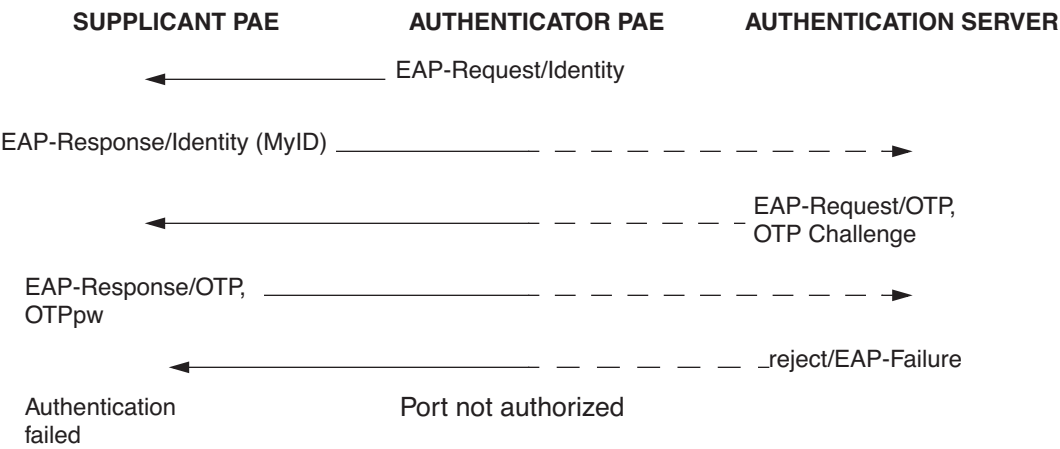


Figure 8-3— Authenticator-initiated, one-time password exchange (failure)

Figure 8-4 illustrates a successful authentication exchange, followed by an explicit logoff requested by the Supplicant.

A Supplicant-initiated authentication conversation will appear as illustrated in Figure 8-5.

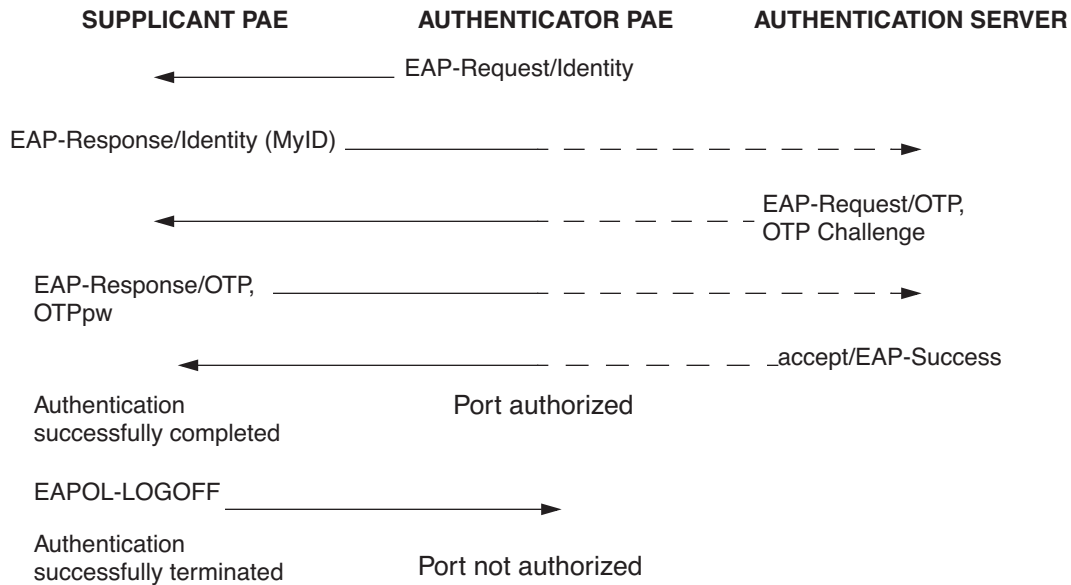


Figure 8-4—Successful authentication followed by Supplicant-initiated logoff

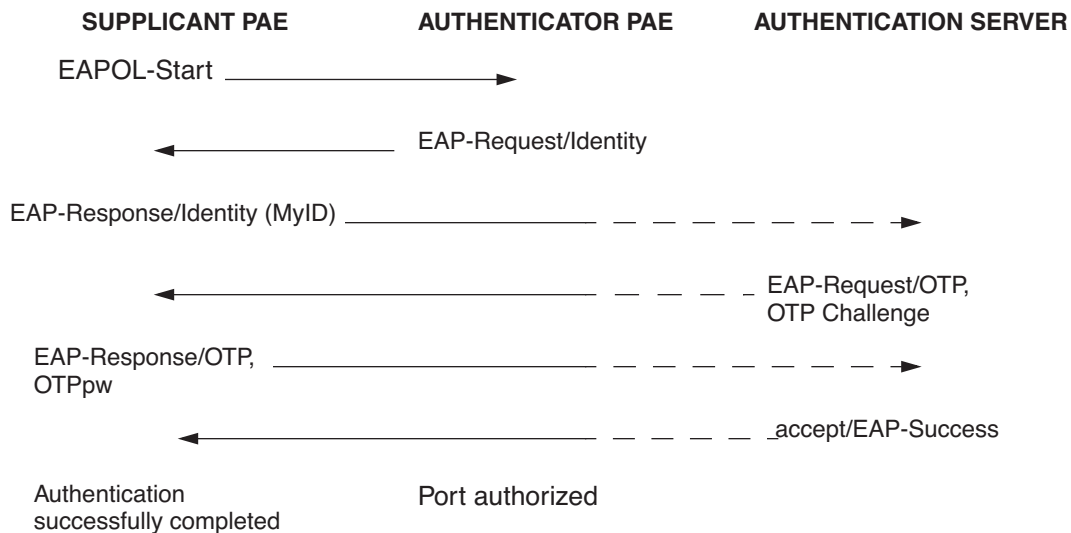


Figure 8-5—Supplicant-initiated, one-time password exchange (success)

In the case in which the Supplicant does not support authentication, but authentication is enabled on that Authenticator, the conversation would appear as illustrated in Figure 8-6.

In the case in which the Authenticator does not support authentication, but authentication is enabled on that Supplicant, the conversation would appear as illustrated in Figure 8-7.

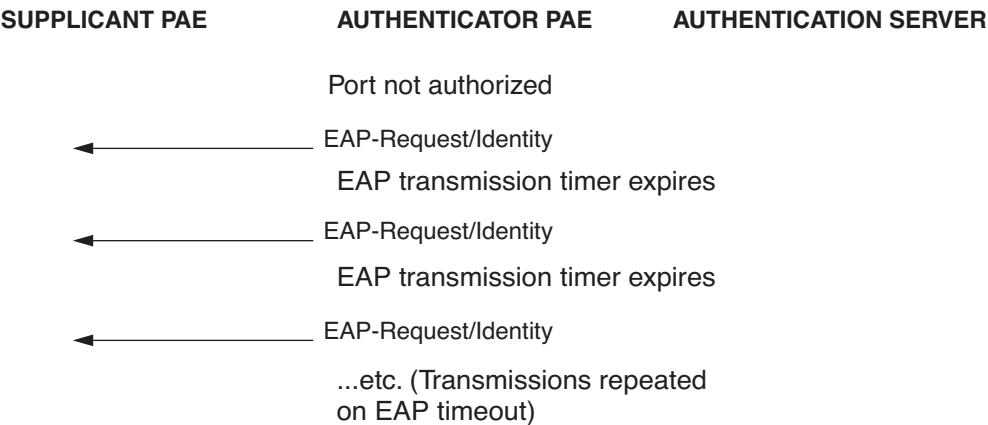


Figure 8-6—Supplicant does not support authentication

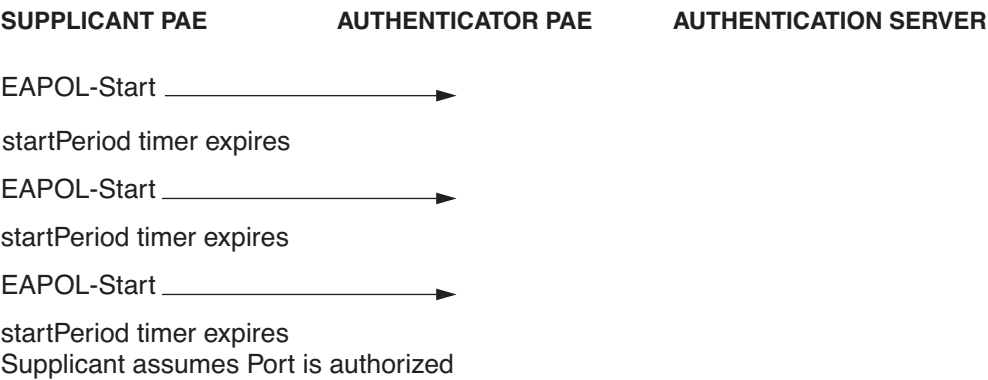


Figure 8-7—Authenticator does not support authentication

8.1.9 Transmission of key information

The EAPOL protocol optionally supports the transmission of key information from the Authenticator to the Supplicant, or from the Supplicant to the Authenticator, following a successful authentication exchange, in circumstances in which encryption is available between the Supplicant and Authenticator systems (e.g., where encryption is used on an IEEE 802.11 association between a station and an access point).

The use of this facility is controlled by the keyTxEnabled parameter, which may be modified by management. A value of TRUE allows key information to be transmitted once keyAvailable and keyRun are set TRUE.

keyAvailable may be set TRUE administratively, or may be set by the higher layer during authentication. Figure 8-8 shows the interface between the higher layer and the IEEE 802.1X Key layer that supports transmitting key material and signaling keyAvailable. Note that if keyTxEnabled is TRUE then EAP authentication dialog must result in keys being available at both Authenticator and Supplicant for this to be successful, so only EAP methods that support this can be used in environments where EAP is expected to provide the keys. The PACP also supports a variable portValid that is available to the higher layer (this is not used by