

IEEE Recommended Practice for Network Reference Model and Functional Description of IEEE 802® Access Network

IEEE Computer Society

Sponsored by the
LAN/MAN Standards Committee

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

IEEE Std 802.1CF™-2019

IEEE Recommended Practice for Network Reference Model and Functional Description of IEEE 802[®] Access Network

Sponsor

LAN/MAN Standards Committee
of the
IEEE Computer Society

Approved 21 March 2019

IEEE-SA Standards Board

Abstract: An access network (which connects terminals to their access routers) utilizing technologies based on the family of IEEE 802[®] standards is specified in this recommended practice. An access network reference model (NRM) that includes entities and reference points along with behavioral and functional descriptions of communications among those entities is provided in this recommended practice.

Keywords: access routers, heterogeneous networks, IEEE 802[®], IEEE 802.1CF[™], multiple network access

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

Copyright © 2019 by The Institute of Electrical and Electronics Engineers, Inc.
All rights reserved. Published 31 May 2019. Printed in the United States of America.

OpenFlow is a registered trademark of the Open Network Foundation.

WiFi CERTIFIED Passpoint is a registered trademark of the Wi-Fi Alliance.

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

PDF:	ISBN 978-1-5044-5667-8	STD23618
Print:	ISBN 978-1-5044-5668-5	STDPD23618

IEEE prohibits discrimination, harassment and bullying.

For more information, visit <https://www.ieee.org/about/corporate/governance/p9-26.html>.

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

Important Notices and Disclaimers Concerning IEEE Standards Documents

IEEE documents are made available for use subject to important notices and legal disclaimers. These notices and disclaimers, or a reference to this page, appear in all standards and may be found under the heading “Important Notices and Disclaimers Concerning IEEE Standards Documents.” They can also be obtained on request from IEEE or viewed at <https://standards.ieee.org/ipr/disclaimers.html>.

Notice and Disclaimer of Liability Concerning the Use of IEEE Standards Documents

IEEE Standards documents (standards, recommended practices, and guides), both full-use and trial-use, are developed within IEEE Societies and the Standards Coordinating Committees of the IEEE Standards Association (“IEEE-SA”) Standards Board. IEEE (“the Institute”) develops its standards through a consensus development process, approved by the American National Standards Institute (“ANSI”), which brings together volunteers representing varied viewpoints and interests to achieve the final product. IEEE Standards are documents developed through scientific, academic, and industry-based technical working groups. Volunteers in IEEE working groups are not necessarily members of the Institute and participate without compensation from IEEE. While IEEE administers the process and establishes rules to promote fairness in the consensus development process, IEEE does not independently evaluate, test, or verify the accuracy of any of the information or the soundness of any judgments contained in its standards.

IEEE Standards do not guarantee or ensure safety, security, health, or environmental protection, or ensure against interference with or from other devices or networks. Implementers and users of IEEE Standards documents are responsible for determining and complying with all appropriate safety, security, environmental, health, and interference protection practices and all applicable laws and regulations.

IEEE does not warrant or represent the accuracy or content of the material contained in its standards, and expressly disclaims all warranties (express, implied and statutory) not included in this or any other document relating to the standard, including, but not limited to, the warranties of: merchantability; fitness for a particular purpose; non-infringement; and quality, accuracy, effectiveness, currency, or completeness of material. In addition, IEEE disclaims any and all conditions relating to: results; and workmanlike effort. IEEE standards documents are supplied “AS IS” and “WITH ALL FAULTS.”

Use of an IEEE standard is wholly voluntary. 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.

In publishing and making its standards available, IEEE is not suggesting or rendering professional or other services for, or on behalf of, any person or entity nor is IEEE undertaking to perform any duty owed by any other person or entity to another. Any person utilizing any IEEE Standards document, should rely upon his or her own independent judgment in the exercise of reasonable care in any given circumstances or, as appropriate, seek the advice of a competent professional in determining the appropriateness of a given IEEE standard.

IN NO EVENT SHALL IEEE BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO: PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE PUBLICATION, USE OF, OR RELIANCE UPON ANY STANDARD, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE AND REGARDLESS OF WHETHER SUCH DAMAGE WAS FORESEEABLE.

Translations

The IEEE consensus development process involves the review of documents in English only. In the event that an IEEE standard is translated, only the English version published by IEEE should be considered the approved IEEE standard.

Official statements

A statement, written or oral, that is not processed in accordance with the IEEE-SA Standards Board Operations Manual shall not be considered or inferred to be the official position of IEEE or any of its committees and shall not be considered to be, or be relied upon as, a formal position of IEEE. At lectures, symposia, seminars, or educational courses, an individual presenting information on IEEE standards shall make it clear that his or her views should be considered the personal views of that individual rather than the formal position of IEEE.

Comments on standards

Comments for revision of IEEE Standards documents are welcome from any interested party, regardless of membership affiliation with IEEE. However, IEEE does not provide consulting information or advice pertaining to IEEE Standards documents. Suggestions for changes in documents should be in the form of a proposed change of text, together with appropriate supporting comments. Since IEEE standards represent a consensus of concerned interests, it is important that any responses to comments and questions also receive 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 comments or questions except in those cases where the matter has previously been addressed. For the same reason, IEEE does not respond to interpretation requests. Any person who would like to participate in revisions to an IEEE standard is welcome to join the relevant IEEE working group.

Comments on standards should be submitted to the following address:

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

Laws and regulations

Users of IEEE Standards documents should consult all applicable laws and regulations. Compliance with the provisions of any IEEE Standards document does not imply compliance to any applicable regulatory requirements. Implementers of the standard are responsible for observing or referring to the applicable regulatory requirements. IEEE does not, by the publication of its standards, intend to urge action that is not in compliance with applicable laws, and these documents may not be construed as doing so.

Copyrights

IEEE draft and approved standards are copyrighted by IEEE under U.S. and international copyright laws. They are made available by IEEE and are adopted for a wide variety of both public and private uses. These include both use, by reference, in laws and regulations, and use in private self-regulation, standardization, and the promotion of engineering practices and methods. By making these documents available for use and adoption by public authorities and private users, IEEE does not waive any rights in copyright to the documents.

Photocopies

Subject to payment of the appropriate fee, IEEE will grant users a limited, non-exclusive license to photocopy portions of any individual standard for company or organizational internal use or individual, non-commercial use only. To arrange for payment of licensing fees, 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.

Updating of IEEE Standards documents

Users of IEEE Standards documents should be aware that these documents may be superseded at any time by the issuance of new editions or may be amended from time to time through the issuance of amendments, corrigenda, or errata. A current IEEE document at any point in time consists of the current edition of the document together with any amendments, corrigenda, or errata then in effect.

Every IEEE standard is subjected to review at least every ten years. When a document is more than ten years old and has not undergone a revision process, 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 order to determine whether a given document is the current edition and whether it has been amended through the issuance of amendments, corrigenda, or errata, visit the IEEE-SA Website at <https://ieeexplore.ieee.org> or contact IEEE at the address listed previously. For more information about the IEEE SA or IEEE's standards development process, visit the IEEE-SA Website at <https://standards.ieee.org>.

Errata

Errata, if any, for all IEEE standards can be accessed on the IEEE-SA Website at the following URL: <https://standards.ieee.org/findstds/errata/index.html>. Users are encouraged to check this URL for errata periodically.

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 by the IEEE with respect to the existence or validity of any patent rights in connection therewith. If a patent holder or patent applicant has filed a statement of assurance via an Accepted Letter of Assurance, then the statement is listed on the IEEE-SA Website at <https://standards.ieee.org/about/sasb/patcom/patents.html>. Letters of Assurance may indicate whether the Submitter is willing or unwilling to grant licenses under patent rights without compensation or under reasonable rates, with reasonable terms and conditions that are demonstrably free of any unfair discrimination to applicants desiring to obtain such licenses.

Essential Patent Claims may exist for which a Letter of Assurance has not been received. The IEEE is not responsible for identifying Essential Patent Claims for which a license may be required, for conducting inquiries into the legal validity or scope of Patents Claims, or determining whether any licensing terms or conditions provided in connection with submission of a Letter of Assurance, if any, or in any licensing agreements are reasonable or non-discriminatory. Users of this standard are expressly advised that determination of the validity of any patent rights, and the risk of infringement of such rights, is entirely their own responsibility. Further information may be obtained from the IEEE Standards Association.

Participants

At the time this recommended practice was submitted to the IEEE-SA Standards Board for approval, the Higher Layer LAN Protocols Working Group had the following membership:

Glenn Parsons, *Chair*
John Messenger, *Vice-Chair*

Ralf Assmann
Jens Bierschenk
Christian Boiger
Paul Bottorff
Radhakrishna Canchi
David Chen
Feng Chen
Weiyang Cheng
Paul Congdon
Rodney Cummings
Hesham Elbakoury
Janos Farkas
Norman Finn
Geoffrey Garner
Eric W. Gray
Craig Gunther
Marina Gutierrez
Stephen Haddock

Mark Hantel
Marc Holness
Satoko Itaya
Michael Karl
Stephan Kehrer
Hajime Koto
Christophe Mangin
Scott Mansfield
Kenichi Maruhashi
James McIntosh
Tero Mustala
Tomoki Ohsawa
Hiroshi Ohue
Donald R. Pannell
Walter Pieniac
Michael Potts
Wei Qiu

Karen Randall
Maximilian Riegel
Jessy V. Rouyer
Atsushi Sato
Frank Schewe
Michael Seaman
Johannes Specht
Paul Unbehagen
Xinyuan Wang
Tongtong Wang
Hao Wang
Karl Weber
Brian Weis
Ludwig Winkel
Jordon Woods
Takahiro Yamaura
Xiang Yu
Nader Zein

Major contributions were received from the following individuals:

Antonio de la Oliva
Yonggang Fang

Walter Pieniac

Maximilian Riegel
Hao Wang

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

Thomas Alexander
Richard Alfvin
Johann Amsenga
Butch Anton
Stefan Aust
Joe Boyles
Nancy Bravin
Vern Brethour
Demetrio Bucaneg
William Byrd
David Chalupsky
Keith Chow
Charles Cook
Daniel Corujo
Steven Crowley
Patrick Diamond
Michael Fischer
Avraham Freedman
Yukihiro Fujimoto
Sho Furuichi
Tim Godfrey
Randall Groves
Qiang Guo
Marco Hernandez
Werner Hoelzl
Noriyuki Ikeuchi

Atsushi Ito
Raj Jain
SangKwon Jeong
Christophe Jurczak
Stuart Kerry
Evgeny Khorov
Yongbum Kim
Hyeong Ho Lee
James Lepp
Joseph Levy
Jon Lewis
Michael Lynch
Elvis Maculuba
Vinayagam Mariappan
Ignacio Marin Garcia
Roger Marks
Arthur Marriss
Michael Maytum
Jonathon McLendon
Richard Mellitz
Michael Montemurro
Nick S. A. Nikjoo
Paul Nikolich
Satoshi Obara
Robert O'Hara
Bansi Patel
Arumugam Paventhan

Brian Petry
David Piehler
Walter Pieniac
Clinton Powell
Adee Ran
Alon Regev
Duane Remein
Maximilian Riegel
Robert Robinson
Benjamin Rolfe
Jessy Rouyer
Naotaka Sato
Frank Schewe
Thomas Starai
Walter Struppler
Jun Tian
Mark-Rene Uchida
George Vlantis
Hao Wang
Lisa Ward
Stephen Webb
Karl Weber
Scott Willy
Su Yi
James Young
Oren Yuen

When the IEEE-SA Standards Board approved this recommended practice on 21 March 2019, it had the following membership:

Gary Hoffman, *Chair*
Ted Burse, *Vice Chair*
Jean-Philippe Faure, *Past Chair*
Konstantinos Karachalios, *Secretary*

Masayuki Ariyoshi
Stephen D. Dukes
J. Travis Griffith
Guido Hiertz
Christel Hunter
Joseph L. Koepfinger*
Thomas Koshy
John D. Kulick

David J. Law
Joseph Levy
Howard Li
Xiaohui Liu
Kevin Lu
Daleep Mohla
Andrew Myles

Annette D. Reilly
Dorothy Stanley
Sha Wei
Phil Wennblom
Philip Winston
Howard Wolfman
Feng Wu
Jingyi Zhou

*Member Emeritus

Introduction

This introduction is not part of IEEE Std 802.1CF-2019, IEEE Recommended Practice for Network Reference Model and Functional Description of IEEE 802[®] Access Network.

This recommended practice specifies an access network (which connects terminals to their access routers) utilizing technologies based on the family of IEEE 802 standards. An access network reference model (NRM) that includes entities and reference points along with behavioral and functional descriptions of communications among those entities is provided in this recommended practice.

Contents

1. Overview	17
1.1 Scope.....	17
1.2 Purpose.....	17
2. Normative references	18
3. Definitions	19
4. Acronyms, abbreviations, and conventions	20
4.1 Acronyms and abbreviations	20
4.2 Conventions	21
4.2.1 Occurrence of information elements	21
4.2.2 Information model notation	21
5. Access network reference model (NRM)	22
5.1 Introduction.....	22
5.2 Basic architectural concepts and terms	23
5.3 Overview of IEEE 802 NRM.....	23
5.3.1 General	23
5.3.2 Schematic overview	23
5.3.3 Reference point types	24
5.4 Basic NRM	25
5.4.1 General	25
5.4.2 Functional entities	25
5.4.2.1 Terminal (TE)	25
5.4.2.2 Access network (AN)	26
5.4.2.3 Access router (AR)	26
5.4.2.4 Subscription service (SS)	26
5.4.2.5 Network management system (NMS)	26
5.4.3 Reference points	26
5.5 NRM with coordination and information service (CIS)	27
5.5.1 General	27
5.5.2 Additional functional entities	28
5.5.2.1 Coordination and information service (CIS)	28
5.5.3 Additional reference points	28
5.6 Comprehensive NRM	28
5.6.1 General	28
5.6.2 Additional functional entities	28
5.6.2.1 Node of attachment (NA)	28
5.6.2.2 Backhaul (BH)	29
5.6.3 Additional reference points	29
5.6.4 Representation with abbreviations	29
5.7 Operational roles.....	29
5.8 Identifiers	30
5.9 Network virtualization	32
5.9.1 General	32
5.9.2 Basic assumptions	32
5.9.3 Instantiation and life cycle of virtualized access network	34
5.9.4 Multi-instance design and issues	35
5.10 Deployment scenarios.....	36

5.10.1	Introduction	36
5.10.2	Wireless local area network (WLAN) router	36
5.10.3	Home network	38
5.10.4	Enterprise network	39
5.10.5	Enterprise network with multiple bridging domains	42
5.10.6	Industrial network	43
5.10.7	Public hotspot	45
5.10.8	Virtualized WLAN access network for in-building IoT services	47
5.10.9	Fog deployment scenario	50
6.	Functional decomposition and design	53
6.1	Introduction.....	53
6.2	Access network setup.....	54
6.2.1	Introduction and overview	54
6.2.2	Roles	55
6.2.2.1	Terminal (TE)	55
6.2.2.2	Access network (AN)	55
6.2.2.3	Node of attachment (NA)	55
6.2.2.4	Backhaul (BH)	55
6.2.2.5	Access network control (ANC)	55
6.2.2.6	Network management system (NMS)	55
6.2.2.7	Coordination and information service (CIS)	55
6.2.3	Use cases	55
6.2.3.1	Access network initialization	55
6.2.3.2	Access network reconfiguration (reinitialization)	56
6.2.3.3	Radio channel adjustments	56
6.2.4	Functional requirements	56
6.2.4.1	Access network configuration	56
6.2.4.2	Access network interconnection	56
6.2.4.3	Channel selection	56
6.2.4.4	Channel reselection	56
6.2.4.5	Operation on various channels	56
6.2.4.6	Multi-mode support	57
6.2.5	Access network setup-specific attributes	57
6.2.5.1	General	57
6.2.5.2	Network management system (NMS)	57
6.2.5.3	Access network control (ANC)	57
6.2.5.4	Backhaul (BH)	57
6.2.5.5	Node of Attachment (NA)	57
6.2.5.6	Access network configuration	57
6.2.6	Access network setup-specific basic functions	57
6.2.6.1	Boot-up process of network elements	57
6.2.7	Detailed procedures	58
6.2.7.1	Access network setup procedure	58
6.2.7.2	Access network release procedure	59
6.2.8	Mapping to IEEE 802 technologies	60
6.3	Access network discovery and selection (NDS).....	60
6.3.1	Introduction	60
6.3.2	Roles	61
6.3.2.1	Terminal (TE)	61
6.3.2.2	Node of attachment (NA)	61
6.3.2.3	Access network (AN)	61
6.3.3	Use cases	62

6.3.3.1	Introduction	62
6.3.3.2	Finding the most appropriate access network	62
6.3.3.3	Reconnecting to an access network	62
6.3.3.4	Handover within an access network	62
6.3.3.5	Handover to another access network	62
6.3.4	Functional requirements	63
6.3.4.1	Support for multiple access technologies	63
6.3.4.2	Support for multiple different access networks supporting same or different SSs	63
6.3.4.3	Support for multiple subscriptions on the same access technologies	63
6.3.4.4	Extensibility to support specific service requirements	63
6.3.4.5	Discovery of access network capabilities	63
6.3.5	NDS-specific attributes	63
6.3.5.1	Service selection	63
6.3.5.2	Subscription	64
6.3.5.3	Terminal (TE)	64
6.3.5.4	Node of attachment (NA)	64
6.3.6	NDS basic functions	65
6.3.6.1	NA Discovery	65
6.3.6.2	AN Detection	65
6.3.6.3	SS Detection	66
6.3.6.4	AR Detection	66
6.3.6.5	SS and AR Selection	66
6.3.7	Detailed procedures	66
6.3.7.1	First-time use of terminal without subscription	66
6.3.7.2	Initial AN access	67
6.3.7.3	NA transition	67
6.3.7.4	Access network reentry	67
6.3.7.5	Access network transition	68
6.3.8	Mapping to IEEE 802 technologies	68
6.3.8.1	Introduction	68
6.3.8.2	IEEE 802.3	68
6.3.8.3	IEEE 802.11	68
6.3.8.4	IEEE 802.16	69
6.3.8.5	IEEE 802.22	69
6.4	Association and disassociation	69
6.4.1	Introduction	69
6.4.2	Roles	70
6.4.2.1	Terminal (TE)	70
6.4.2.2	Node of attachment (NA)	70
6.4.2.3	Access network control (ANC)	70
6.4.3	Use cases	70
6.4.3.1	General	70
6.4.3.2	Connection setup as part of network entry	70
6.4.3.3	Connection relocation within the same access network	71
6.4.3.4	Connection teardown	71
6.4.4	Functional requirements	71
6.4.5	Association-specific attributes	72
6.4.5.1	Access link	72
6.4.5.2	Terminal (TE)	72
6.4.5.3	Node of attachment (NA)	72
6.4.6	Association-specific basic functions	72
6.4.6.1	Association	72
6.4.6.2	Reassociation	73

6.4.6.3	Disassociation	73
6.4.7	Detailed procedures	73
6.4.7.1	Successful connection setup with negotiation of connection parameters	73
6.4.7.2	Orderly session teardown initiated by terminal	74
6.4.7.3	Session termination enforced by NA	74
6.4.7.4	Session relocation with support of fast transition schemes	74
6.4.8	Mapping to IEEE 802 technologies	75
6.5	Authentication and trust establishment.....	75
6.5.1	Introduction	75
6.5.2	Roles	77
6.5.2.1	General	77
6.5.2.2	User	78
6.5.2.3	Service provider	78
6.5.2.4	Subscription	78
6.5.2.5	Terminal (TE)	78
6.5.2.6	Access network (AN)	78
6.5.2.7	Subscription service (SS)	78
6.5.3	Use cases	78
6.5.3.1	Introduction	78
6.5.3.2	Access network with direct relation to SS	78
6.5.3.3	Access network with relation to SS relayed over another SS	78
6.5.3.4	Access network with relation to the SS of a roaming consortia	79
6.5.4	Functional requirements	79
6.5.5	Authentication-specific attributes	79
6.5.5.1	Security association	79
6.5.5.2	Subscription	80
6.5.5.3	Terminal (TE)	80
6.5.5.4	Access network control (ANC)	80
6.5.5.5	Subscription Service (SS)	80
6.5.6	Authentication-specific basic functions	81
6.5.6.1	Identification request	81
6.5.6.2	Identification notify	81
6.5.6.3	Authentication process	81
6.5.6.4	Trust establishment	81
6.5.6.5	Trust revocation	81
6.5.7	Detailed procedures	81
6.5.7.1	Direct service access	81
6.5.7.2	Service access with relay of authentication over another SS	82
6.5.8	Mapping to IEEE 802 technologies	83
6.6	Datapath establishment, relocation, and teardown	83
6.6.1	Introduction	83
6.6.1.1	Data forwarding in access network	83
6.6.1.2	Connectivity characteristics	84
6.6.1.3	Traffic types	85
6.6.1.4	Time-sensitive networking	86
6.6.2	Roles	87
6.6.2.1	Datapath	87
6.6.2.2	Terminal interface (TEI)	88
6.6.2.3	Node of attachment (NA)	88
6.6.2.4	Backhaul (BH)	88
6.6.2.5	Access router interface (ARI)	88
6.6.2.6	Subscription service (SS)	88
6.6.2.7	Access network control (ANC)	89
6.6.2.8	Network management system (NMS)	89

6.6.3	Use cases	89
6.6.3.1	Single, plain access network	89
6.6.3.2	Industrial network for time-sensitive applications	89
6.6.3.3	Shared wireless access network	90
6.6.3.4	Multi-operator backhaul infrastructure	91
6.6.4	Functional requirements	92
6.6.5	Datapath-specific attributes	92
6.6.5.1	Datapath	92
6.6.5.2	Node of attachment (NA)	92
6.6.5.3	Backhaul (BH)	92
6.6.5.4	Access router (AR)	93
6.6.5.5	Subscription service (SS)	93
6.6.6	Datapath-specific basic functions	93
6.6.6.1	Retrieval of session-specific datapath configuration values for access network	93
6.6.6.2	Activation of datapath in the NA	93
6.6.6.3	Teardown of datapath in the NA	93
6.6.6.4	Activation of datapath in the backhaul	93
6.6.6.5	Teardown of datapath in the backhaul	94
6.6.6.6	Access router interface establishment	94
6.6.6.7	Access router interface teardown	94
6.6.7	Detailed procedures	94
6.6.7.1	Overview	94
6.6.7.2	Datapath establishment	95
6.6.7.3	Datapath relocation	96
6.6.7.4	Datapath teardown	97
6.6.8	Mapping to IEEE 802 technologies	98
6.7	Authorization, QoS, and policy control	98
6.7.1	Introduction	98
6.7.1.1	Aspects	98
6.7.1.2	QoS models supported by IEEE 802	98
6.7.1.3	Repository of QoS settings and policy parameters	99
6.7.1.4	QoS policy control architecture and mapping to the NRM	99
6.7.1.5	TSN control architecture and mapping to the NRM	100
6.7.2	Roles	102
6.7.2.1	Service flow	102
6.7.2.2	Subscription	103
6.7.2.3	Subscription service (SS)	103
6.7.2.4	Access network control (ANC)	103
6.7.2.5	Node of attachment and backhaul (NA and BH)	103
6.7.2.6	Terminal control and access router control (TEC and ARC)	103
6.7.3	Use cases	103
6.7.3.1	QoS policy provisioning to ANC	103
6.7.3.2	Default service flow creation, modification, and deletion	104
6.7.3.3	Change of authorization by SS	104
6.7.3.4	Access router-initiated service flow creation, modification, and deletion	104
6.7.3.5	Terminal-initiated service flow creation, modification, and deletion	104
6.7.4	Functional requirements	104
6.7.5	QoS policy-specific attributes	104
6.7.5.1	Service flow	104
6.7.5.2	Node of attachment (NA)	105
6.7.5.3	Backhaul (BH)	105
6.7.5.4	Subscription service (SS)	105

6.7.6	QoS policy control-specific basic functions	105
6.7.6.1	Provisioning of authorization information to policy decision point at session beginning	105
6.7.6.2	Change of authorization during session	106
6.7.6.3	Provisioning of QoS parameters to policy enforcement points	106
6.7.6.4	Request of service flow by terminal	106
6.7.6.5	Request of service flow by access router	106
6.7.7	Detailed procedures	106
6.7.7.1	Pre-provisioned service flow establishment	106
6.7.7.2	Service flow initialization by terminal	107
6.7.7.3	Service flow initialization by access router	108
6.7.7.4	Service flow modification by terminal	109
6.7.7.5	Service flow termination by terminal	110
6.7.7.6	Change of authorization by SS	110
6.7.8	Mapping to IEEE 802 technologies	111
6.8	Accounting and monitoring	111
6.8.1	Introduction	111
6.8.2	Roles	112
6.8.2.1	Terminal (TE)	112
6.8.2.2	Network management system (NMS)	112
6.8.2.3	Access network control (ANC)	112
6.8.2.4	Node of attachment and backhaul (NA and BH)	113
6.8.2.5	Subscription service (SS)	113
6.8.3	Use cases	113
6.8.3.1	General	113
6.8.3.2	Performance analysis	113
6.8.3.3	Security analysis	113
6.8.3.4	Billing	113
6.8.4	Functional requirements	114
6.8.5	Accounting and monitoring-specific attributes	114
6.8.5.1	Session statistics	114
6.8.5.2	Node of attachment (NA)	114
6.8.5.3	Backhaul (BH)	114
6.8.5.4	Access network control (ANC)	115
6.8.5.5	Subscription service (SS)	115
6.8.6	Accounting and monitoring-specific basic functions	115
6.8.6.1	Monitoring	115
6.8.6.2	Collection	116
6.8.6.3	Mediation	116
6.8.7	Detailed procedures	117
6.8.7.1	Accounting configuration	117
6.8.7.2	Accounting	118
6.8.7.3	Monitoring	120
6.8.8	Mapping to IEEE 802 technologies	120
6.9	Fault diagnostics and maintenance (FDM)	125
6.9.1	Introduction	125
6.9.2	Roles	125
6.9.2.1	General	125
6.9.2.2	Network management system (NMS)	125
6.9.2.3	Access network control (ANC)	126
6.9.3	Use cases	126
6.9.3.1	General	126
6.9.3.2	Alarm notification to NMS	126
6.9.3.3	NMS maintenance requests to ANC	126

6.9.3.4	Automatic fault recovery by ANC	127
6.9.4	Functional requirements	127
6.9.5	FDM-specific attributes	128
6.9.5.1	Alarm list	128
6.9.5.2	Link-monitoring statistics	128
6.9.5.3	Test statistics	128
6.9.5.4	SelfCheck statistics	128
6.9.5.5	FDM capabilities	129
6.9.5.6	FDM configuration	129
6.9.5.7	Access network control (ANC)	129
6.9.5.8	Network management system (NMS)	129
6.9.6	FDM-specific basic functions	130
6.9.6.1	Capability discovery	130
6.9.6.2	FDM registration	130
6.9.6.3	Fault isolation	130
6.9.6.4	Fault recovery	130
6.9.7	Detailed procedures	131
6.9.7.1	FDM configuration	131
6.9.7.2	Remote failure indication	132
6.9.7.3	Link monitoring	133
6.9.7.4	Testing	135
6.9.7.5	Management information aggregation	136
6.9.8	Mapping to IEEE 802 technologies	137
7.	Network softwarization functions	139
7.1	Introduction.....	139
7.2	Information model of IEEE 802 access network	139
7.2.1	Composition of information model	139
7.2.2	Session information model	140
7.2.2.1	General	140
7.2.2.2	Service selection information model	141
7.2.2.3	Access link information model	141
7.2.2.4	Security association information model	142
7.2.2.5	Datapath information model	143
7.2.2.6	Service flow information model	144
7.2.2.7	Session statistics information model	145
7.2.2.8	Complete session information model	145
7.2.3	Access network configuration information model	147
7.2.4	Network management information model	148
7.3	Virtualized network instantiation.....	148
7.3.1	General	148
7.3.2	Roles	150
7.3.2.1	General	150
7.3.2.2	Orchestrator	150
7.3.2.3	Access network (AN)	150
7.3.2.4	Access network control (ANC)	150
7.3.2.5	Node of attachment (NA)	150
7.3.2.6	Backhaul (BH)	150
7.3.3	Use cases	151
7.3.3.1	Instantiation of a new virtualized access network	151
7.3.3.2	Dynamically adding instances to the virtualized access network	151
7.3.3.3	Dynamically removing instances from the virtualized access network ..	151
7.3.3.4	Removal of the entire virtualized access network	151

7.3.4	Functional requirements	152
7.3.4.1	Creation of multiple virtualized networking entities	152
7.3.4.2	Virtualized access network configuration	152
7.3.4.3	Multiple service provider support	152
7.3.5	Network instantiation procedures	152
7.3.5.1	Virtualized access network instantiation procedure	152
7.3.5.2	Virtualized access network release procedure	153
7.3.5.3	Adding a new NA instance to the access network procedure	154
7.3.5.4	Removal of an NA instance from the access network procedure	155
7.3.5.5	Update virtualized access network configuration procedure	155
Annex A (normative) Functional enhancements to IEEE 802 access network		156
Annex B (informative) Information model notation		163
Annex C (informative) Software-defined networking (SDN) functional decomposition		165
Annex D (informative) Network function virtualization (NFV)		178
Annex E (informative) Bibliography		182

IEEE Recommended Practice for Network Reference Model and Functional Description of IEEE 802[®] Access Network

1. Overview

1.1 Scope

This recommended practice specifies an access network (which connects terminals to their access routers) utilizing technologies based on the family of IEEE 802 standards. An access network reference model (NRM) that includes entities and reference points along with behavioral and functional descriptions of communications among those entities is provided in this recommended practice.

1.2 Purpose

Heterogeneous networks may include multiple network interfaces, multiple network access technologies, and multiple network subscriptions. In some cases such heterogeneous functionality must be supported in a single user terminal.

This recommended practice supports the design and deployment of access networks based on IEEE 802 technologies, guides the developers of extensions to the existing standards in support of a heterogeneous access network, and enables the use of IEEE 802 standards in new network deployments by specifying the functions of the IEEE 802 technologies when deployed in access networks.

2. Normative references

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

IEEE Std 802[®], IEEE Standard for Local and Metropolitan Area Networks—Overview and Architecture.^{1, 2}

IEEE Std 802.1AC[™], IEEE Standard for Local and metropolitan area networks—Media Access Control (MAC) Service Definition.

IEEE Std 802.1Q[™], IEEE Standard for Local and Metropolitan Area Networks—Bridges and Bridged Networks.

IEEE Std 802.1X[™], IEEE Standard for Local and metropolitan area networks—Port-Based Network Access Control.

IEEE Std 802.3[™], IEEE Standard for Ethernet.

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

IEEE Std 802.16[™], IEEE Standard for Air Interface for Broadband Wireless Access Systems.

IEEE Std 802.22[™], IEEE Standard for Information technology—Local and metropolitan area networks—Specific requirements—Part 22: Cognitive Wireless RAN Medium Access Control (MAC) and Physical Layer (PHY) specifications: Policies and procedures for operation in the TV Bands.

IETF RFC 7542, “The Network Access Identifier,” DeKok, 2015.³

ITU-T Y.2070, “Next Generation Networks—Frameworks and functional architecture models: Requirements and architecture of the home energy management system and home network services.”⁴

MEF 6.2, “EVC Ethernet Services Definitions Phase 3,” [https://www.mef.net/Assets/Technical Specifications/PDF/MEF_6.2.pdf](https://www.mef.net/Assets/Technical%20Specifications/PDF/MEF_6.2.pdf).

¹ The IEEE standards or products referred to in Clause 2 are trademarks owned by The Institute of Electrical and Electronics Engineers, Incorporated.

² IEEE publications are available from The Institute of Electrical and Electronics Engineers (<http://standards.ieee.org/>).

³ IETF publications are available from the Internet Engineering Task Force (<https://www.ietf.org/>).

⁴ ITU-T publication are available from the International Telecommunications Union (<https://www.itu.int/>).

3. Definitions

For the purposes of this document, the following terms and definitions apply. The *IEEE Standards Dictionary Online* should be consulted for terms not defined in this clause.⁵

access network: An IEEE 802 local area network or metropolitan area network (LAN/MAN) between terminals and access routers connecting to provider services.

access router: A router that terminates the medium access control (MAC) service from terminals and forwards user traffic to information servers according to Internet Protocol (IP) addresses.

backhaul: The portion of the access network between nodes of attachment (NAs) and the access router.

datapath: The forwarding path of packets through a network.

node of attachment (NA): A generic term for an access point, or base station, or bridge where a terminal is attached.

operations support system/business support system (OSS/BSS): The combined functions of an operations support system (OSS) and a business support system (BSS). An OSS is a software system that enables a service provider to operate, administrate, monitor, analyze, and manage the services on its network. Together with a BSS, these functions support most customer-related activities, including ordering, billing, and support.

terminal: A computer or other device that terminates connections across a communication network and is the point at which information resources, services, and applications enter and/or leave the network.

⁵ *IEEE Standards Dictionary Online* is available at <http://dictionary.ieee.org>.

4. Acronyms, abbreviations, and conventions

4.1 Acronyms and abbreviations

AAA	authentication, authorization, and accounting
ACK	acknowledgment
AN	access network
ANC	access network control
ANC-ID	access network control identifier
AN-ID	access network identifier
API	application programming interface
AR	access router
ARC	access router control
ARI	access router interface
AR-ID	access router identifier
BH	backhaul
BH-ID	backhaul identifier
BSS	basic service set
BSSID	basic service set identifier
CIS	coordination and information service
CNC	Centralized Network Configuration
CPE	customer-premises equipment
CUC	Centralized User Configuration
DL	data link
DP	datapath
DP-ID	datapath identifier
DSL	digital subscriber line
EAP	Extensible Authentication Protocol
EAPoL	Extensible Authentication Protocol over LAN
EIRP	equivalent isotropic radiated power
E-LAN	Ethernet local area network
FDM	fault diagnostics and maintenance
FQDN	fully qualified domain name
HESSID	homogeneous extended service set identifier
HO	handover
IoT	Internet of Things
IP	Internet Protocol
LAN	local area network
LLC	logical link control
LSAP	link service access point
MAC	medium access control
MIB	management information base
MSAP	MAC service access point
NA	node of attachment (e.g., access point or base station)
NAI	network access identifier
NA-ID	node of attachment identifier
NDS	network discovery and selection
NE	network element
NE-ID	network element identifier
NETCONF	Network Configuration Protocol
NFV	network function virtualization

NFVI	network function virtualization infrastructure
NFV-MANO	network function virtualization management and orchestration
NMS	network management system
NMS-ID	network management system identifier
NRM	network reference model
OAM	operations, administration, and management
OFN	Open Network Foundation
OSS/BSS	operations support system/business support system
PHY	physical layer
PSAP	presentation service access point
QoS	quality of service
RADIUS	Remote Authentication Dial-In User Service
SDN	software-defined networking
SF	service flow
SFID	service flow identifier
SNMP	Simple Network Management Protocol
SRP	Stream Reservation Protocol
SS	subscription service
SSID	service set identifier
SUB-ID	subscription identifier
SUS-ID	subscription service identifier
TCP	Transmission Control Protocol
TE	terminal
TEC	terminal control
TE-ID	terminal identifier
TEI	terminal interface
TSN	time-sensitive network
TVWS	television white space
UNI	user network interface
VLAN	virtual local area network
VNF	virtualized network function
VPN	virtual private network
WAN	wide area network
WLAN	wireless local area network
XML	Extensible Markup Language

4.2 Conventions

4.2.1 Occurrence of information elements

The following notation is used for indicating the occurrence of the information elements:

- {0+} Zero or more instances of this attribute are present.
- {0-1} Zero or one instance of this attribute is present.
- {1} Exactly one instance of this attribute is present.
- {1+} One or more instances of this attribute are present.

4.2.2 Information model notation

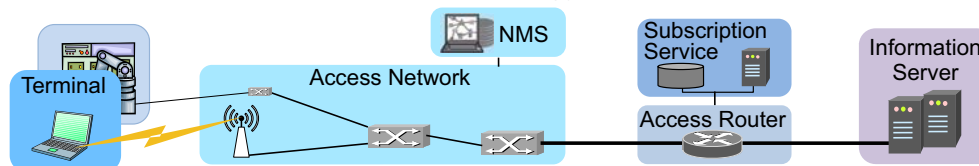
UML 2.x object model notation is used for representation of the information model in this recommended practice. A subset of the notation used in this recommended practice is presented in Annex B for information.

5. Access network reference model (NRM)

5.1 Introduction

Within the bigger picture of an end-to-end network model for providing access to provider services over an IEEE-802-based network, the NRM introduced in this clause as a generic representation of various implementations deals with the link-layer communication infrastructure between the network layer interface in the terminal and the network layer interface in the access router as depicted in Figure 1.

End-to-end communication network topology



Datapath protocol layer architecture

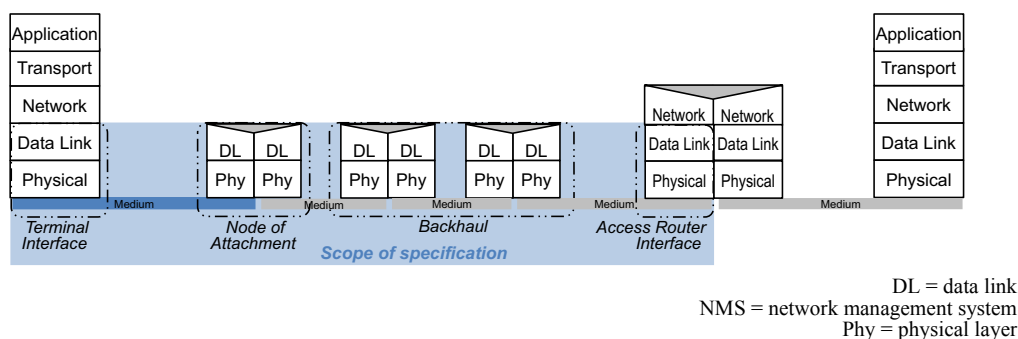


Figure 1—Scope of NRM

In a generic picture of the end-to-end communication network topology, a terminal is connected by a wired or a wireless link to a node of attachment (NA) of the network. An NA is used in this recommended practice as a generic reference to an access point, or a base station, or a bridge connecting a terminal. To concurrently serve multiple terminals across a wider coverage area, multiple NAs can be interconnected with each other within an access network. Traffic in the access network is aggregated and forwarded to the access router through the backhaul. The access router terminates the layer 2 [i.e., data link (DL) layer] connectivity from the terminal and forwards user traffic to information servers according to Internet Protocol (IP) addresses carried in the payload of the layer 2 frames. A subscription service (SS) provides authentication for the terminals requesting access to the network, and it delivers authorization to the access network to configure the appropriate kind of connectivity to enable information services to the terminals.

As shown in the protocol layer architecture in Figure 1, the IEEE 802 access networks forward user data frames according to medium access control (MAC) addresses, and MAC addresses identify the endpoints of the links in the IEEE 802 access network.

5.2 Basic architectural concepts and terms

The architectural concepts used in this and other IEEE 802.1™ standards are based on the layered protocol model introduced by the OSI Reference Model (ISO/IEC 7498-1:1994 [B25]) and used in the MAC Service definition (IEEE Std 802.1AC), in IEEE Std 802, in other IEEE 802 standards, and, with varying degrees of fidelity, in networking in general.^{6,7} IEEE 802.1 standards in particular have developed terms and distinctions useful in describing the MAC Service and its support by protocol entities within the MAC sublayer.

5.3 Overview of IEEE 802 NRM

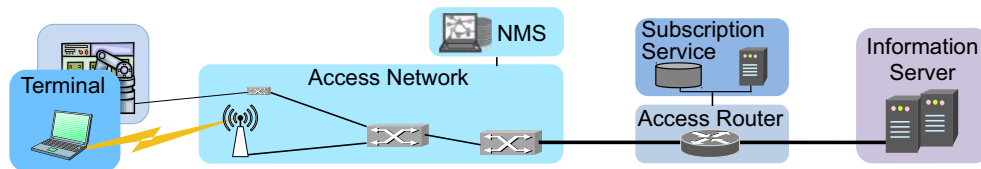
5.3.1 General

The NRM defines a generic foundation for the description of IEEE 802 access networks, which may include multiple network interfaces, multiple network access technologies, and multiple network subscriptions, aimed at unifying the support of different interface technologies, enabling shared network control and use of software-defined networking (SDN) principles.

5.3.2 Schematic overview

At first glance, the NRM of an IEEE 802 access network consists of the terminal, the access network, the network management system (NMS) of the access network, the access router, and the subscription service (SS), as shown in Figure 2. The SS provides authentication, authorization, and accounting, as well as policy functions specific for particular user accounts and terminals.

End-to-end communication network topology



Network Reference Model Schematic

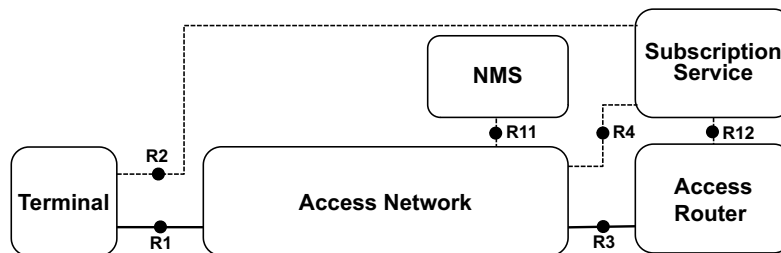


Figure 2—NRM overview

Communication interfaces between the entities are denoted by R1 for the interface between the terminal and the NA; by R2 for the authentication procedures between terminal and SS; by R3 for the interface between access network and the access router; by R4 for the authentication, authorization, accounting, and policy

⁶ Numbers in brackets correspond to the numbers in the bibliography in Annex E.

⁷ Information on normative references can be found in Clause 2.

functions between the access network and the SS; and by R11 for the network management procedures between the access network and NMS. R12 indicates the interface between SS and access router, mainly for exchange of authorization and accounting information.

On the datapath indicated by R1 and R3, the NRM covers all physical layer (PHY) and DL layer functions providing an integrated model for backhaul connectivity combined with user-specific connectivity functions as facilitated through the IEEE 802.1 bridging technologies.⁸

Beyond the scope of this recommended practice are the functions above the link layer and the infrastructure beyond the access router for providing IP-based information services to the terminals.

5.3.3 Reference point types

According to IEEE 802 basic architectural concepts and terms as described in Clause 7 of IEEE Std 802.1AC-2016, information out of an IEEE 802 communication element is exchanged with another entity either over the port through the communication medium or as management information as payload over an unspecified kind of control protocol. See Figure 3.

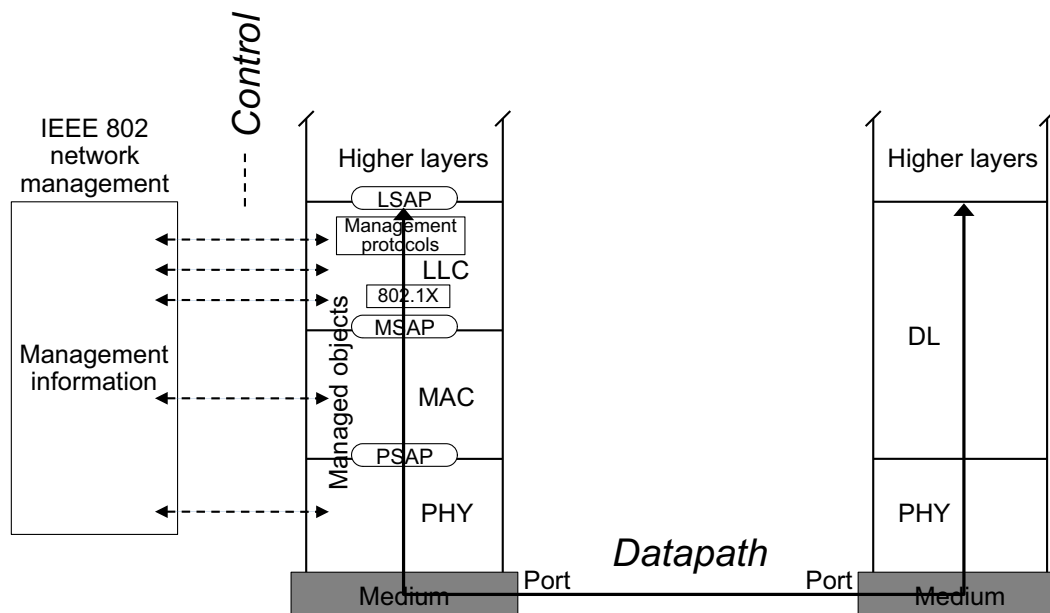


Figure 3—Reference point types

As shown in Figure 3, there are two kinds of reference points used in the NRM:

- A **control interface** conveys IEEE 802 layer management information to another entity and is represented in the NRM by a dashed line. Usually IP-based protocols [e.g., Simple Network Management Protocol (SNMP), Remote Authentication Dial-In User Service (RADIUS), or Network Configuration Protocol (NETCONF)] will be used to communicate layer management information.
- A **datapath interface** conveys user data and can also convey IEEE 802 control protocol information to the peer entity encoded in layer 2 frames. It is represented in the NRM by a solid line.

⁸ In the telecommunication domain, there is often differentiation between data plane functions and transport plane functions. The IEEE 802 access NRM integrates both planes into a common model aligned to IEEE 802.1Q™ layered networking capabilities.

5.4 Basic NRM

5.4.1 General

The NRM adopts the generic concepts of SDN by introducing dedicated control functions in the terminal, access network, and access router, with well-defined semantics for interfacing with higher layer management, orchestration, and analytics functions. Additionally the model deploys a clear separation of functional roles in the operation and management of access networks to support various deployment models including leveraging wholesale network services for backhaul, network sharing, and roaming.

Figure 4 presents the basic NRM. Solid lines represent the interfaces between the data plane and connecting ports, while dashed lines show the flow of control and management information. This NRM is the foundation for further refinements and includes the basic differentiation between functional entities and the reference points for their communication. The basic NRM is composed of five main elements: the terminal (TE), the access network (AN), the access router (AR), the subscription service (SS), and the network management system (NMS).

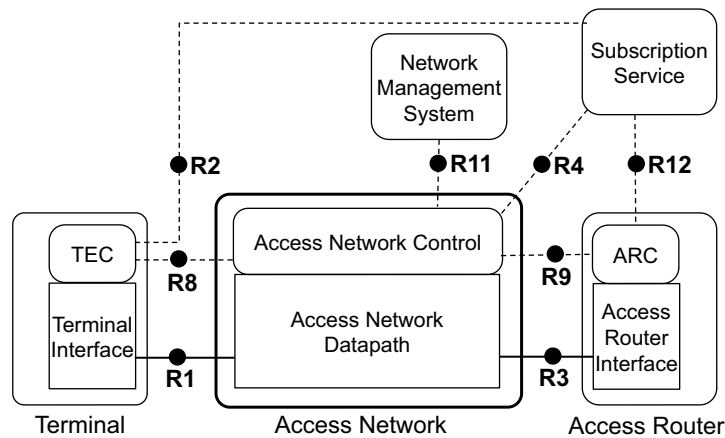


Figure 4—Basic NRM

The NMS comprises the services for operation, administration, and maintenance of the IEEE 802 access network, as well as the IEEE 802 interfaces with the terminal and access router. As depicted in Figure 4, the terminal, access network, and access router each contain a control entity, which is denoted by terminal control (TEC), access network control (ANC), and access router control (ARC), respectively. Each of the three elements has its own specific control.

NOTE—The access router is a logical functional unit with various options for implementation depending on the design and architecture of the ARC.⁹

5.4.2 Functional entities

5.4.2.1 Terminal (TE)

The terminal is a device that seeks connectivity to a communication infrastructure to get access to communication services. The terminal contains a terminal interface (TEI) providing the link for network connectivity, and eventually deploys a TEC for dealing with the parameters and configurations conveyed by the control and management interfaces to ANC and SS for establishment and maintenance of the network

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

connectivity. Some terminal configurations may be performed out-of-band through a user interface or other means.

5.4.2.2 Access network (AN)

The access network consists of the NAs providing the physical ports to the terminals and the backhaul for connecting the NAs to the access router. The access network deploys an ANC for configuration and management of the elements inside the access network as well as for exchange of control and management information with both the terminal and access router. The ANC also provides the interface to the NMS for propagating network management information on behalf of the network elements (NEs) of the access network.

5.4.2.3 Access router (AR)

The access router terminates the layer 2 connectivity to the terminal by providing network layer communication to the terminal side. The access router contains an access router interface that establishes the physical port of the connectivity to the access network, and may eventually include a dedicated ARC that handles and exchanges layer management information and configurations. With a dedicated ARC, the access router becomes a logical functional unit with various implementation options for the control and the packet forwarding engine attached to the access router interface.

5.4.2.4 Subscription service (SS)

The SS provides authentication, authorization, and accounting services; user-specific policies to the terminal, the access network, and the access router; and potentially a means to provision terminals to enable successful authentication. The SS usually contains a database containing all the subscription-specific information. Multiple SSs may be interlinked with each other for roaming users who use resources of networks not having direct relation to their service providers.

5.4.2.5 Network management system (NMS)

The NMS consists of the functions that allow the operator of an access network to configure the access network infrastructure; to manage functions related to the interaction among multiple network elements and between the access network and terminal and access router; to monitor the usage and correct operation of the access network; and to perform tests for detection, determination, and correction of faults. Network elements are the entities in the NRM that forward user data. A NMS exists in every access network; however, the kind of implementation and sophistication widely varies and depends on the size of the network and particular operational requirements.

5.4.3 Reference points

R1 represents the reference point for the PHY and MAC sublayer functions establishing the link, as specified in numerous IEEE 802 standards, between terminal and access network.

R2 represents a logical control interface between terminal and the SS, e.g., for authentication. Information elements of the logical interface are tunneled over R1 and R4 between terminal and SS.

R3 represents the link for the communication between the access network and the access router as specified by IEEE 802 standards.

R4 represents a control interface communicating subscription-specific information elements between the ANC and the SS.

R8 represents a logical control and management interface between the access network and the terminal, which terminates in ANC and TEC, respectively. The functionalities of this reference point are related to the management of the terminal and the control of the datapaths into the terminal. In addition, the reference point may include some additional configuration parameters to influence the behavior and configuration of the terminal. Information elements of the logical interface are conveyed over R1 between terminal and access network.

R9 represents a logical control and management interface between the access network and the access router, which terminates in ANC and ARC. The functionalities of this reference point are related to the management of the access router and the control of the datapath into the access router. In addition, the reference point may include some additional configuration parameters to influence the behavior and configuration of the access router. Information elements of the logical interface are conveyed over R3 between access network and access router.

R11 represents a control and management interface for conveying network management information between the NMS and network element management functions located in the ANC. It includes information elements for the management of the network elements, such as planning, organization, supervision, control, protection, and security of communications resources.

R12 represents a control interface communicating subscription-specific information between the SS and the ARC.

5.5 NRM with coordination and information service (CIS)

5.5.1 General

Some deployments include a CIS, integrated into Figure 5, to provide advanced services such as spectrum management, coexistence, and information services for mobility. The reference model includes the option for CIS by providing a reference point to communicate the information between CIS and the ANC, possibly propagated further by the ANC to the TEC and ARC over the R8 and R9 interfaces, respectively. All reference points are covered by IEEE 802 standards. For control interfaces, only information elements are defined within IEEE 802 standards.

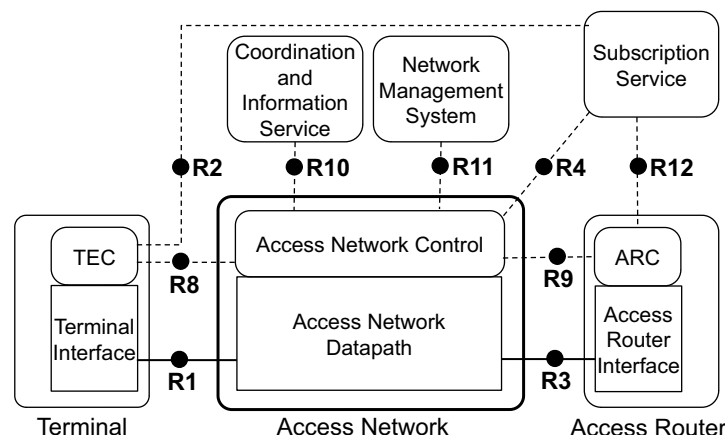


Figure 5—NRM with CIS

5.5.2 Additional functional entities

5.5.2.1 Coordination and information service (CIS)

The CIS is an entity that coordinates the use of common resources and exchange of operational parameters among multiple access networks. A CIS is usually present only when an external entity dynamically provides resources for the operation of the access network, or when multiple access networks coordinate their operations with the help of a third-party entity.

5.5.3 Additional reference points

R10 represents a control and management interface between the ANC and the CIS. R10 may be present between the ANCs of different access networks, when no third-party entity is involved, for the coordination of the operation between multiple access networks. In this case, the CIS is provided in a distributed manner. Centralized and distributed CIS may coexist for different purposes in the same access network arrangement.

5.6 Comprehensive NRM

5.6.1 General

The comprehensive NRM provides further details of functional entities and their interfaces inside the access network. In Figure 6, the model decomposes the access network into the NA and backhaul in addition to the ANC. The NA represents the entity providing the link to the terminal, the interface to the backhaul, and the data forwarding function between these two. The connections between NA, backhaul, and ANC are described by reference points R5, R6, and R7.

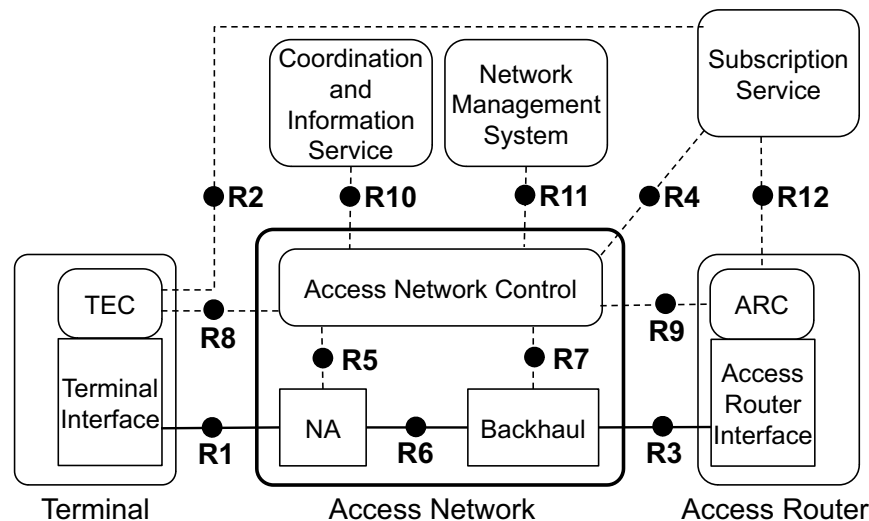


Figure 6—NRM exposing access network details

5.6.2 Additional functional entities

5.6.2.1 Node of attachment (NA)

The NA represents the access network element that provides the physical link to the terminal. It forwards user data to a network side port inside the access network and is connected with the ANC for configuration and management.

5.6.2.2 Backhaul (BH)

The backhaul represents the aggregation and forwarding infrastructure inside the access network providing the link between the network side port of the NA and the access router interface.

5.6.3 Additional reference points

R5 represents a control-only interface for the configuration and operation of the NA. It includes information elements for the configuration of the R6 port to the backhaul, the R1 port to the terminal, and the data-forwarding functions inside the NA.

R6 represents a reference point for the physical ports between the NA and the backhaul.

R7 represents an interface used to control and configure the datauser plane within the backhaul. The backhaul interconnects the NAs with the access router.

5.6.4 Representation with abbreviations

For schematic use cases and when less space is available for reproducing the NRM with all terms spelled out, a representation of the NRM with abbreviations can be used. This approach is illustrated in Figure 7.

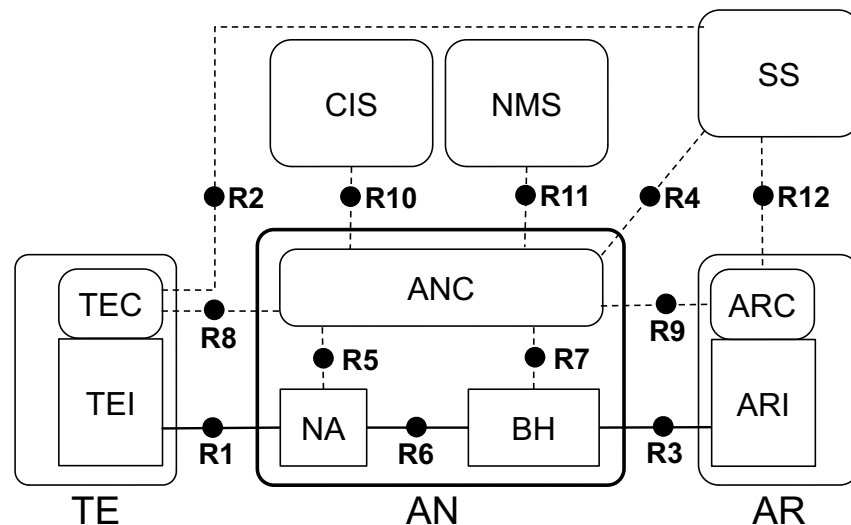


Figure 7—NRM with abbreviations

5.7 Operational roles

The NRM defines functional entities and their relationships without any assumptions about the ownership or operational domains of various portions of the NRM. To achieve highest flexibility in the deployment of the IEEE 802 access network, no assumptions are made regarding the integration of the IEEE 802 access network with interconnected network functions.

In its most generic realization, the operation of the IEEE 802 access network involves the following operational roles or operational domains, which are also shown in Figure 8:

- **User** represents the organization or individual in charge of the terminal.
- **Access Network Operator** represents the organization operating the access network together with the related NMS and the CIS, as well as further operations support system/business support system (OSS/BSS) functions dedicated to the access network.
- **Service Provider** represents the organization owning and operating the SS and related OSS/BSS functions.
- **IP Provider** represents the organization owning and operating the access router, related OSS/BSS functions, and further networking functions for the realization of IP services.

NOTE—Some deployment scenarios may not expose such fine-grain operational separation but may combine several operational roles into a single operation with partial or full integration of the OSS/BSS. Access network, SS, and access router may belong to the same operator or may be distributed among distinct operators. A frequent scenario is, for example, the integration of a service provider with an IP provider, commonly called ISP, providing access to the Internet. Such integration is considered as a particular implementation model of the NRM and is not further detailed in this recommended practice.

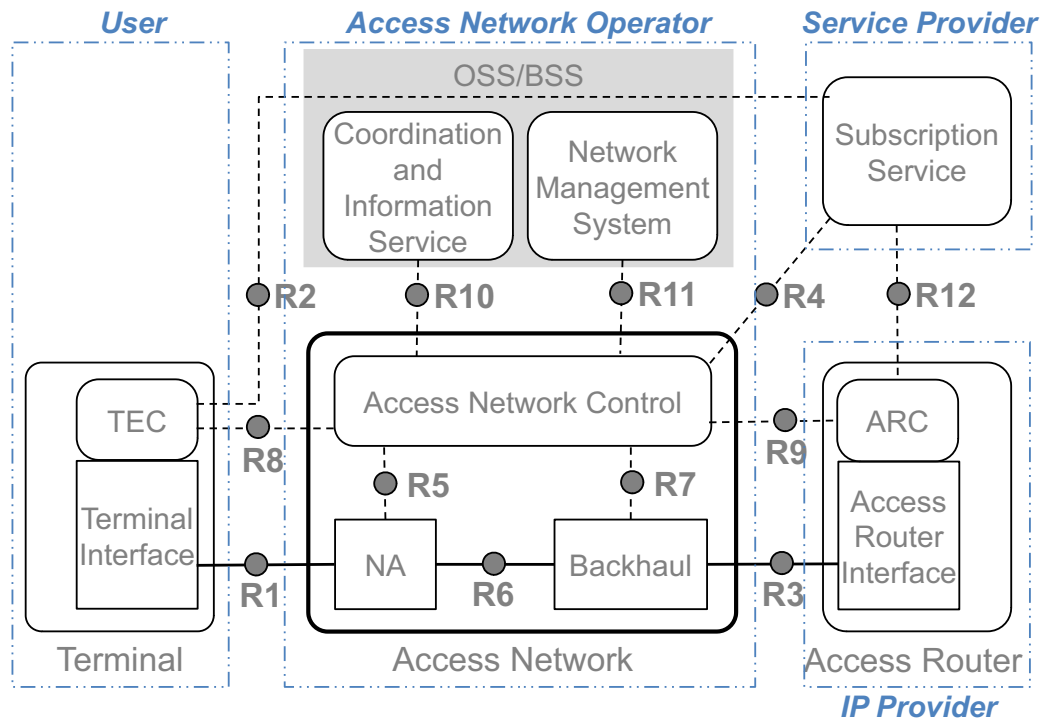


Figure 8—Operational roles of IEEE 802 access network

5.8 Identifiers

This subclause details the kind and format of identifiers used in IEEE 802 access networks. Table 1 lists identifiers of access technology-dependent entities, Table 2 lists identifiers of access technology independent network entities, and Table 3 lists identifiers of operational roles within the IEEE 802 access network. The formats shown in Table 2 and Table 3 are provided as examples.

Table 1—Identifiers of access technology-dependent entities

Entity	Identifier	Format			
		IEEE 802.3™	IEEE 802.11™	IEEE 802.16™	IEEE 802.22™
Terminal	TE-ID	48-bit ^{a,b}	48-bit ^{c,b}	EUI-48 ^{d,b}	EUI-48 ^e
Node of Attachment	NA-ID	48-bit ^{a,b}	BSSID ^d	BSID ^d	EUI-48 ^e
Access Network	AN-ID	CHAR[511] ^f	SSID, HESSID ^c	Operator ID ^d	EUI-48 ^e

^a IEEE Std 802.3-2018, Clause 3.

^b IEEE Std 802-2014.

^c IEEE Std 802.11-2016, 9.2.4.3 and 11.23.2.

^d IEEE Std 802.16-2017, Clause 6.

^e IEEE Std 802.22-2011, Clause 7.

^f IEEE Std 802.1X-2010, Clause 10.

Table 2—Identifiers of access technology independent entities

Entity	Identifier	Format
Network management system	NMS-ID	FQDN
Access network control	ANC-ID	FQDN
Access router	AR-ID	48-bit ^a
Backhaul	BH-ID	FQDN
Subscription service	SUS-ID	FQDN
Coordination and information service	CIS-ID	FQDN

^a IEEE Std 802-2014.

Table 3—Identifiers of operational roles

Role	Identifier	Format
User	User-ID	String
Service Provider	SP-ID	CID ^a or Domain Name
Subscription	SUB-ID	NAI ^b
Access Network Operator	ANO-ID	CID or Domain Name
IP Provider	IP-ID	CID or Domain Name
Infrastructure Provider	INF-ID	CID or FQDN

^a IEEE-SA Registration Authority, “Guidelines for Use of Extended Unique Identifier (EUI), Organizationally Unique Identifier (OUI), and Company ID (CID).”

^b Network access identifier (IETF RFC 7542).

5.9 Network virtualization

5.9.1 General

Network virtualization allows for cost-effective installations of multiple dedicated access networks for different applications, for particular security requirements, or for isolated operational domains at the same area. To enable virtualization, access network elements are designed in a way that a single hardware element can realize multiple logical instances of the network element. However, due to common usage of a single hardware resource, some limitations regarding the configuration of the hardware-dependent parameters may exist; e.g., the operation channel of a radio interface must be the same for all the virtual interfaces operating on the same device, or the PHY speed of a wired Ethernet interface will be the same for all connections going over a common local area network (LAN) cable.

IEEE 802 technologies provide the capabilities to realize multiple virtualized instances of network elements under the potential restrictions mentioned above, and support two variants of virtual networking:

- Virtual networks define multiple instances of multipoint networks, i.e., layer 2 forwarding domains within an access network.

For example, IEEE Std 802.1Q defines the methods to share a common Ethernet infrastructure for the establishment of multiple virtual LANs (VLANs), each identified through a VLAN ID; and IEEE Std 802.11 describes the implementation of multiple virtual access points, each exposing its own service set identifier (SSID) and defining its own security environment on a single radio interface.

- Virtualized access networks define instances of access network, each with its own ANC and NMS serving a number of network functions. Network functions in the access network are all elements relaying data frames, i.e., NAs and backhauls.

The model of a virtualized access network is defined by a template representing an abstract description of a particular design, which can be instantiated multiple times.

The CIS is the only network entity shared among multiple virtualized access networks to allow access to, and adaptation of, operational parameters for shared processing and transmission resources.

A virtualized access network may consist of multiple virtual networks; however, virtual networks can exist without network virtualization. Network virtualization leads to multiple administrative domains.

5.9.2 Basic assumptions

The NRM, as illustrated in Figure 9, includes a single instance of a virtualized IEEE 802 access network. The virtualized access network, highlighted with shading in the figure, follows all the functional descriptions and exposes the same functional behavior at the reference points. The terminal has no need to be aware of a virtualized access network. The interface to the terminal does not change through virtualization.

In the case of a single instance of a virtualized access network, the NRM completely covers the functional behavior. It does not, however, show the internal structure and operation of a virtualized infrastructure. Virtualization of the access network leads to a separation of the physical infrastructure from the functional behavior.

As shown in Figure 10, the PHY components of the NA requiring dedicated hardware, as well as the PHY of the backhaul realized through hardware, become part of the access infrastructure layer, which consists of all the hardware components and computing resources that provide all the necessary resources of the virtualized access network.

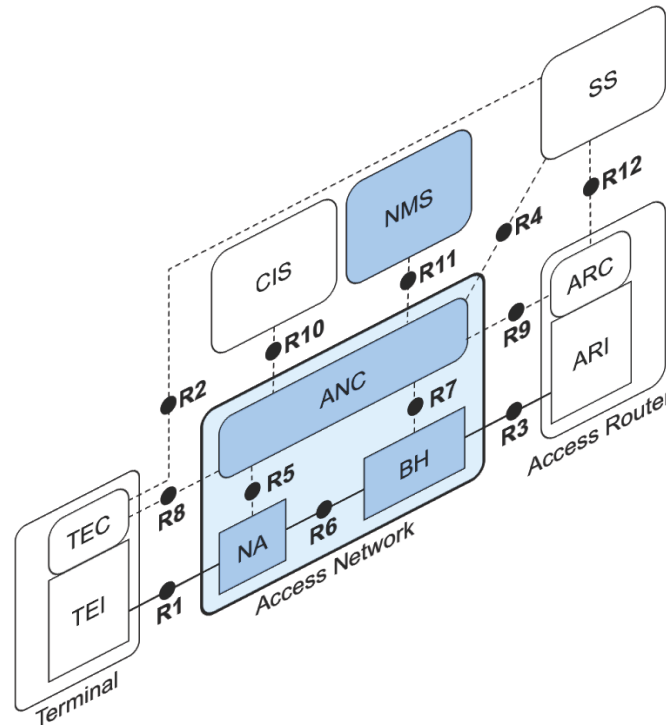


Figure 9—Single instance of virtualized IEEE 802 access network

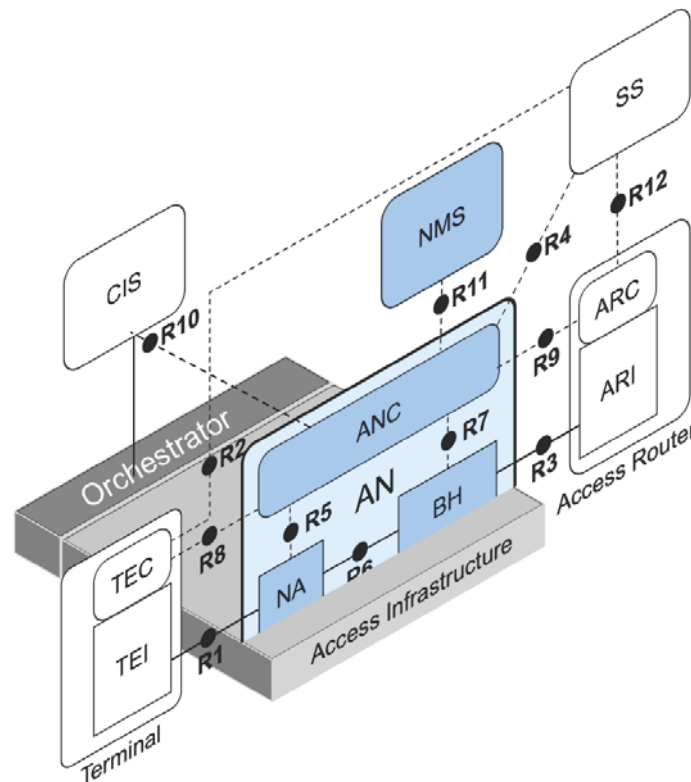


Figure 10—Virtualized access network residing on access infrastructure

Each of the virtualized access networks owns an instance of the NMS, which itself may be virtualized. However, as a virtualized access network provides exactly the same kind of interfaces as a physical implementation, the related NMS does not need to be virtualized.

An orchestrator is attached to the access infrastructure and provides the automated arrangement, coordination, and management of the hardware and computing resources for the instantiation of the virtualized access network, and potentially also for the virtualized NMS instance. The orchestrator provides configuration information about the assigned resources to the access networks through the CIS, and allows for dynamic adjustments of resources as long as other access networks on the same access infrastructure are not impacted.

The ANC still knows about every detail of the lower PHY configurations of NA as well as the details of the backhaul; however, the information is provided through CIS, as the configuration of the access infrastructure predefines the configuration parameters of the lower PHY.

5.9.3 Instantiation and life cycle of virtualized access network

A virtualized infrastructure allows for dynamic creation, modification, and teardown of access network instances. A new instance of access network is initiated by the access network operator by sending a instantiation request with a template to the infrastructure provider, which creates the instance and reserves and assigns infrastructure resources to that instance through the orchestrator. Part of the instantiation is the establishment of the transport links to CIS, NMS, SSs, and access routers. The virtualized IEEE 802 access network instantiation is shown in Figure 11.

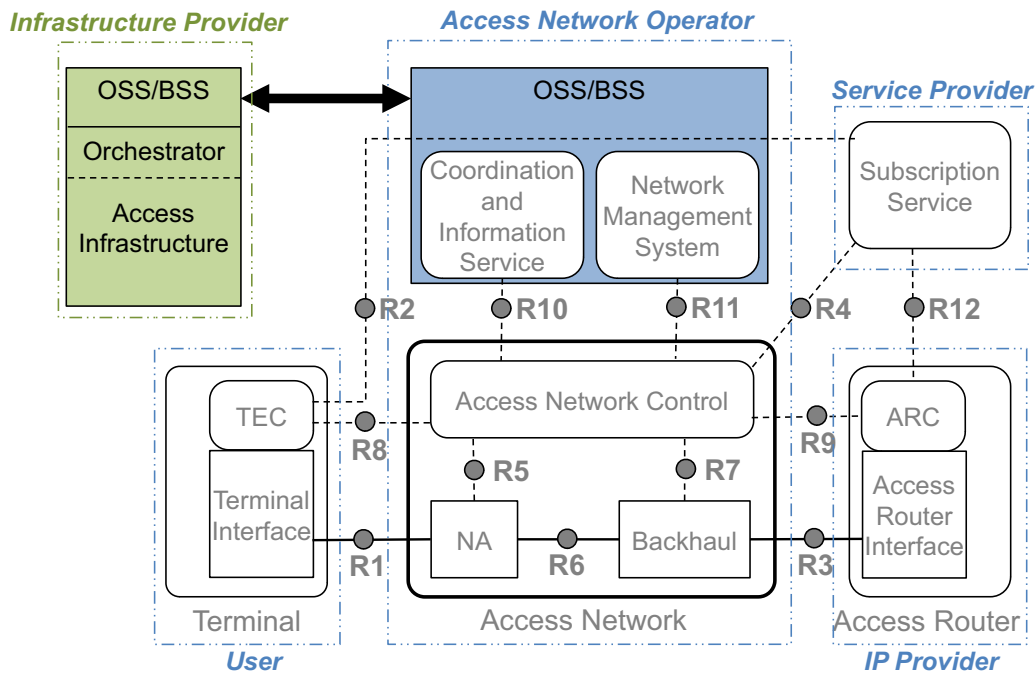


Figure 11—Virtualized access network instantiation

After instantiation by the infrastructure provider, the access network initializes its operation, establishes the control connections to SSs and access routers, and gets ready for serving terminals.

During operation, the access network is able to adjust its resources by sending requests through the CIS to the orchestrator of the infrastructure provider within the bounds given by the contracts and policies between access network operator and infrastructure provider. It should be kept in mind that not all resource requests may be successfully fulfilled in the virtualized environment.

Allocated resources can be released during the runtime of the access network. It is possible to completely remove an access network by first terminating service to terminals; then tearing down the control connections to NMSs, SSs, and access routers; and finally releasing all resources by instructing the orchestrator of the infrastructure provider to dissolve the access network instance.

5.9.4 Multi-instance design and issues

The full capabilities of network virtualization become visible in Figure 12, which depicts three different access network instances on a common access infrastructure. All three access networks have an R10 reference point to the common CIS; therefore, each of the virtualized access networks can get access to the lower PHY parameters—which are common for all three networks—and request from the orchestrator modifications to the networking and computing resource parameters. If the requests do not collide with requests of the other virtualized access networks, the orchestrator can dynamically adjust the assignment of resources according to requests. For clarity of the visualization, the R2 reference point and signal flow are not shown in Figure 12.

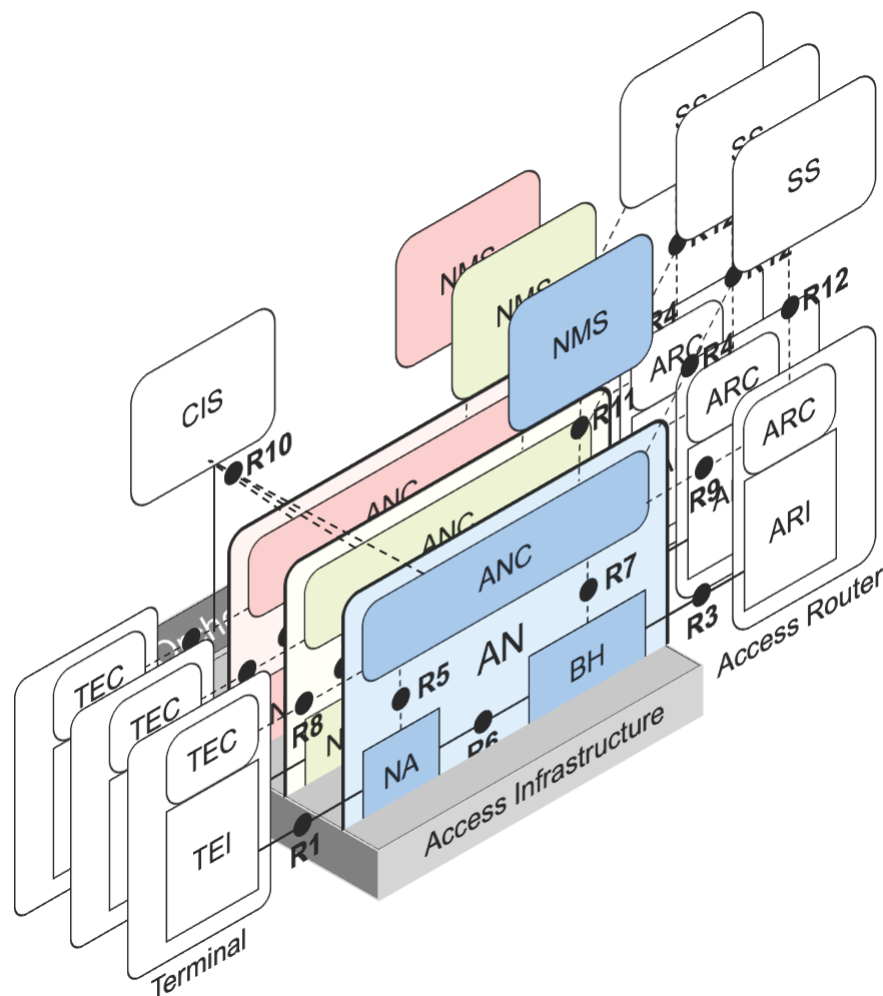


Figure 12—Multi-instance virtualization

Each of the three virtualized networks fully realize the complete NRM, including NMS and its own relations with SSs as well as access routers. Each of the instances can have its completely separate arrangements, and the virtualized networks are completely independent of each other, except in the use of the access infrastructure resources, which are shared among the access networks and imply some limitations, as the sum of used resources cannot exceed the total available resources. All virtualized access networks are connected through R10 to the CIS, which provides access to the infrastructure parameters and allows for request of dynamic allocation of resources. As the access infrastructure is shared among multiple access network instances, an access network can request to the orchestrator modifications to the lower PHY parameters through the CIS, and it becomes possible that the resources are dynamically allocated by the ANC depending on load conditions and service requirements.

5.10 Deployment scenarios

5.10.1 Introduction

Subclauses 5.10.2 through 5.10.9 present a variety of deployment scenarios of the IEEE 802 NRM to show its applicability to many different kinds of IEEE-802-based networks. The presented use cases are examples and are not exhaustive. There are further use cases possible beyond the presented examples.

5.10.2 Wireless local area network (WLAN) router

The term *WLAN router* denotes a single device commonly used in residential networks to provide Internet access to a number of terminals over either a wireless or a wired connection. Usually a WLAN router consists of the following functional elements:

- An Ethernet port for the network connection to a digital subscriber line (DSL) or cable modem.
- A router with a Dynamic Host Configuration Protocol (DHCP) server, network address translation (NAT), and a firewall to allow multiple terminals to communicate concurrently into the Internet through a secured gateway.
- An Ethernet bridge providing multiple Ethernet ports to establish a small residential LAN for wired connections of terminals and local services.
- One or more IEEE 802.11 radio interfaces, which provide connectivity for WLAN terminals.

In addition, the WLAN router contains a local network management function, often realized through a web-based portal running on a microcontroller. The microcontroller also performs the routing functions, as well as the higher layer control and data frame processing functions of IEEE 802.11.

Figure 13 shows the circuit diagram of a common implementation of a WLAN router. Chip technology allows integration of all WLAN router circuitry—likely without the random-access memory (RAM) and the field-programmable read-only memory (FPRM)—onto a single chip.

Figure 14 depicts the functions and interfaces of a WLAN router mapped to the functional decomposition of the NRM. It is clearly visible that a WLAN router comprises all the functional entities of the NRM and also implements a LAN-WAN gateway function. It acts as access router to the LAN side and as terminal to the wide area network (WAN) side to provide IP connectivity from a local access network to a remote access network.

Through the high integration of all the functions of an IEEE 802 access network into a single device, only a few reference points of the NRM become exposed. All the internal interfaces of the access network—as well as the interfaces of the access network to the access router, SS, and NMS—exist only as functional interfaces within the firmware of the WLAN router. Implementations may favor the adoption of the reference points as defined in this recommended practice, but could also follow other decomposition and interfacing approaches.

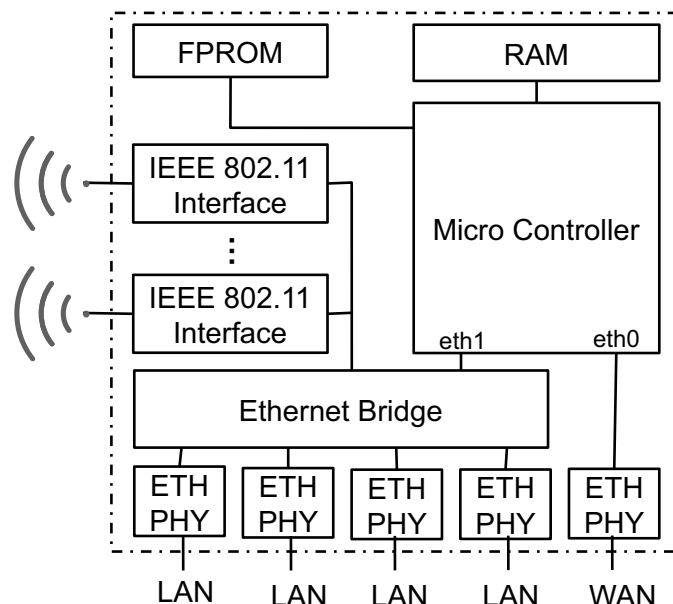


Figure 13—Example schematic of WLAN router circuitry

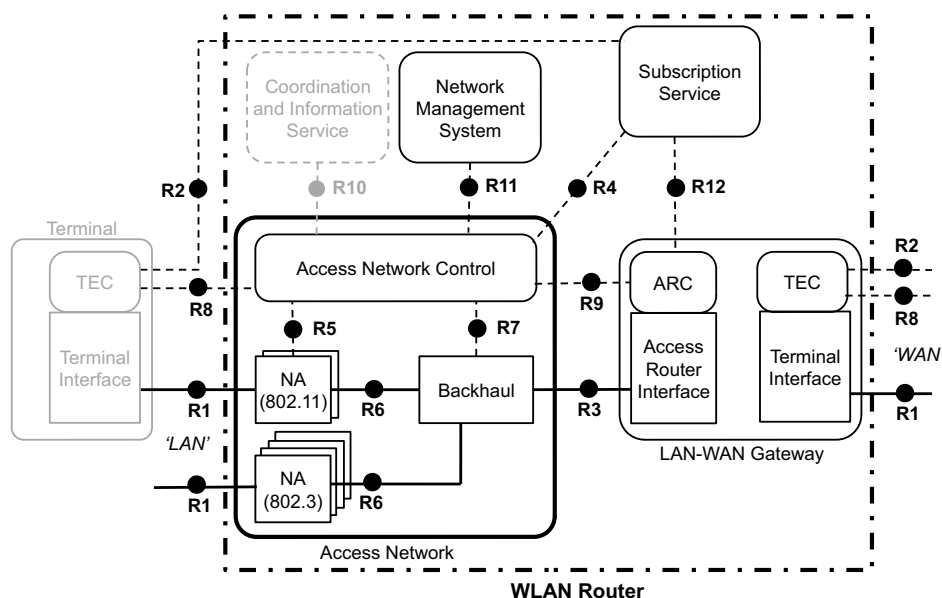


Figure 14—NRM mapping of the WLAN router functions

The WLAN router physically exposes only reference points belonging to the interfaces to the terminal (LAN side) and to the wide area access network (WAN side). The reference point R8 on the LAN side represents, for example, the key management protocol and potentially the fast basic service set (BSS) transition protocol of IEEE Std 802.11; and R2 represents, for example, the Extensible Authentication Protocol (EAP) method when IEEE 802.1X authentication is applied. On the WAN side, R8 represents the remote configuration of the WAN interface (e.g., the assignment of VLAN parameters through BBF TR-069 [B3]), and R2 could be present when the WAN operator deploys authentication based on user credentials.

As WLAN routers usually realize an isolated independent entity of an access network, the CIS might be missing in most of the implementations. Nevertheless, in special cases, also a CIS may exist when, for example, radio interfaces operating in television white space (TVWS) are implemented and an interface to a central spectrum database is present as an over-the-top service over the WAN interface.

5.10.3 Home network

As a result of the spread of the broadband network, it has become common to interconnect devices in the home by building a home network. This is illustrated in Figure 15, which shows the functional architecture for the home network as defined in ITU-T Y.2070 and TTC TR-1053 [B31], and in Figure 16, which adds its mapping to NRM. A home network is made up of home gateways and a mix of devices that are different in the way they are installed, maintained, and connected to the network and in the level of quality they require, such as home appliances, audio-video and other consumer electronics products, set-top boxes, sensors, smart meters, computers, smartphones, tablets, and game consoles.

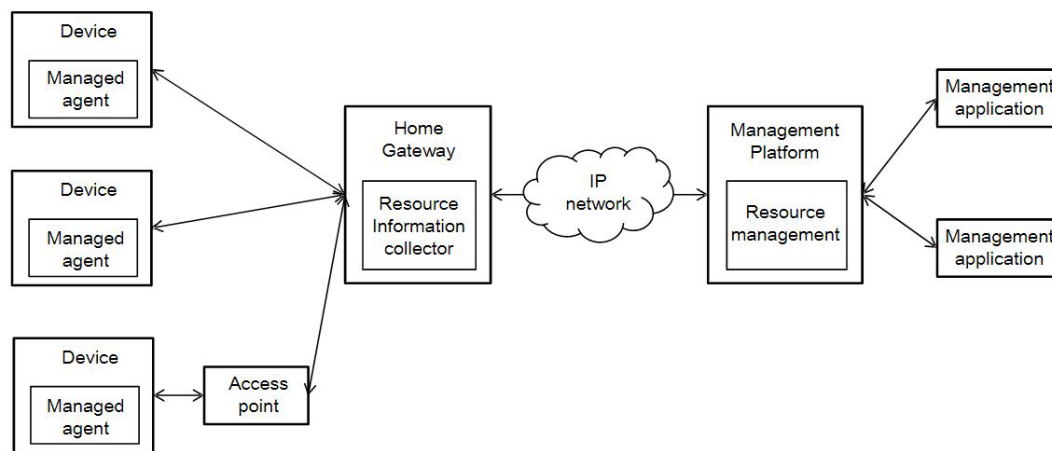


Figure 15—Functional architecture for home network defined in ITU-T Y.2070 (flipped)

Home gateway is an always-on, always-connected device that acts as the central point connecting the devices on the home network to the applications on the WAN, and monitors and provides data transport service within the home network as well as between the home network and the WAN. The home network is IP-based, and the home gateway interconnects the WAN and the home network. Hence, home gateway integrates the functions of access router and access network. The terminal can be mapped to the end devices inside the home.

- A device with wired connection is usually connected to the home gateway directly. In this case, home gateway provides the full function of an access network.
- A wireless device is connected to the home gateway though an access point. Therefore, the access point is NA, and the home gateway resembles the functions of backhaul plus ANC in the comprehensive NRM.

In either case, the home gateway provides the control functions of ANC, such as device provisioning, application execution, and resource information collection. For example, to meet the management requirement from NMS, the resource information collector in a home gateway should be able to discover the newly connected devices, identify each of them and set their configurations, collect the internal status of each device and other home network resources, and monitor the traffic status of the home network.

Figure 16 also shows the internal components of a home gateway and the reference points between entities when mapped to the NRM. The dashed box (home gateway) represents the usual integration of access router, backhaul, and NA in the deployment of, for example, a DSL network. Note that the wireless device

has a logical reference point R8 with ANC function in the home gateway, but the flow of control or management information may go through R1 and R5 interfaces.

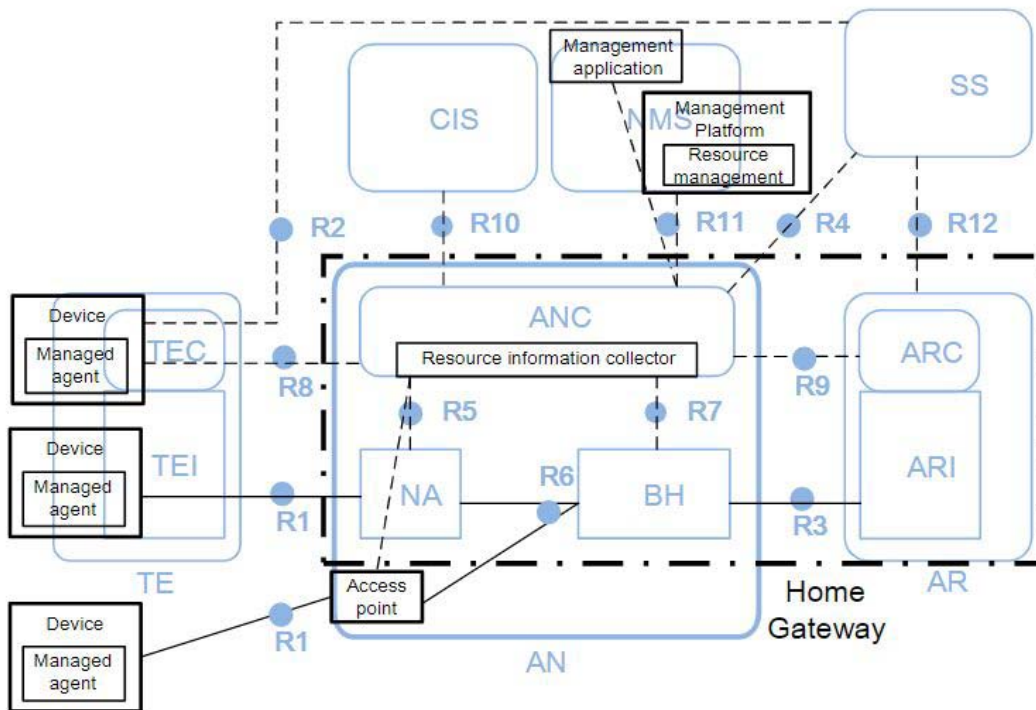


Figure 16—Functional architecture for home network mapping to NRM

In the distributed type of architecture shown in Figure 16, the management functions are separately distributed to the home gateway inside the home and the management platform on the Internet. This architecture enables the applications to access the devices from the Internet. For example, some management applications, such as energy management system monitor and control devices, are connected to the home network from outside the home through this architecture.

The management application is used by network operators or service providers such as call centers and customer support centers. It provides a function to display the entire resource information for faults diagnosis and to set the specified properties for recovery operation from such faults.

Management platform is the NMS, which has common functions providing the interface and the management for the home network applications, and the device management and the resource management for the home gateway and the devices.

5.10.4 Enterprise network

Enterprise networks are privately operated network infrastructures within enterprises, organizations, or corporations. They encompass a huge variety of implementations and sizes. Enterprise networks can vary in complexity, from a completely isolated network with a few PCs connected through a single Ethernet bridge, up to a global network of many privately interconnected sites each having its comprehensive LAN with wired and wireless IEEE 802 connectivity of hundreds to thousands of terminals, devices, and servers. The commonality of all such enterprise networks is the deployment of IEEE 802 bridging among all connected terminals in the LAN. The Internet Protocol is used for delivering services within enterprise networks. It implies that at least one access router exists, which is often embedded in the WAN router with the firewall to the Internet and the virtual private network (VPN) gateway to the other remote sites of the same enterprise network.

Figure 17 shows a typical enterprise network scenario providing wireless access to portable devices through a number of access points connected to an aggregation bridge. Often, the aggregation bridge is complemented by a WLAN controller to accomplish a more seamless wireless network by facilitating central coordination of higher layer IEEE 802.11 functions. Another aggregation bridge provides wired IEEE 802.3 connectivity to a number of workstations or PCs, and potentially also to special devices, e.g., printers. The bridges build the backhaul of the wireless access points and the wired TEIs to the access router. The access router forwards the IP-based protocols inside the enterprise and provides outside connectivity to the Internet and other sites of the enterprise.

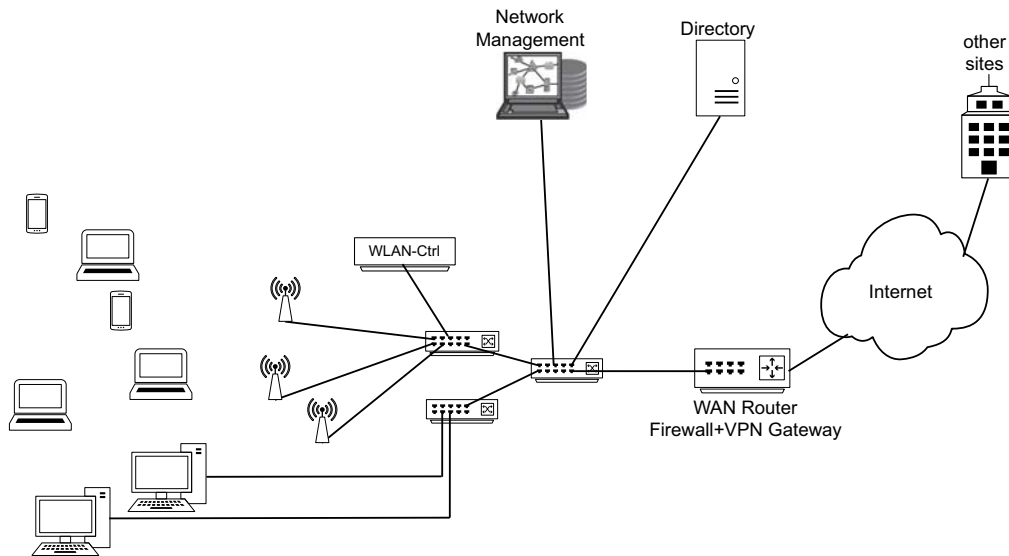


Figure 17—Enterprise network scenario

A directory service enables the central storage and maintenance of user-specific subscription information. It allows user-specific access rights to the network and services to be centrally configured.

Due to the distributed nature of the network with its devices spread over the whole campus, enterprise networks usually have a dedicated network management station for configuration, administration, monitoring, and maintenance of the whole network.

The components of an enterprise network can be easily mapped to the NRM. The bridging infrastructure builds the backhaul of the network, with terminal Ethernet ports and WLAN access points resembling the NAs. The functions of the WLAN controller fit well to the role of the ANC, and network management station and directory are typical realizations of the NMS and SS, respectively.

The implementation of a real enterprise network may not exactly resemble the functional decomposition of the NRM, but it is clearly visible in Figure 18 that the components of an enterprise network are well matched with the functional entities of the NRM. All reference points to terminals are supported. Many of the reference points of the access network directly exist as interfaces in the enterprise networks. R6 is exposed on the interface between the bridge and the access point, and R3 maps to the LAN cable between the core bridge and the WAN router. Even control interfaces of the access network may be exposed in enterprise networks. R5 could be mapped to the communication between the WLAN controller and the WLAN access points, and R4 and R11 denote the protocol connections between the WLAN controller and the directory server and network management station, respectively. The information exchange between WAN router and directory server can be mapped to R12. However, not all reference points are so clearly exposed in enterprise networks. R7 and R9 may exist, but the related ANC functions may be distributed across the Ethernet bridges in the backhaul.

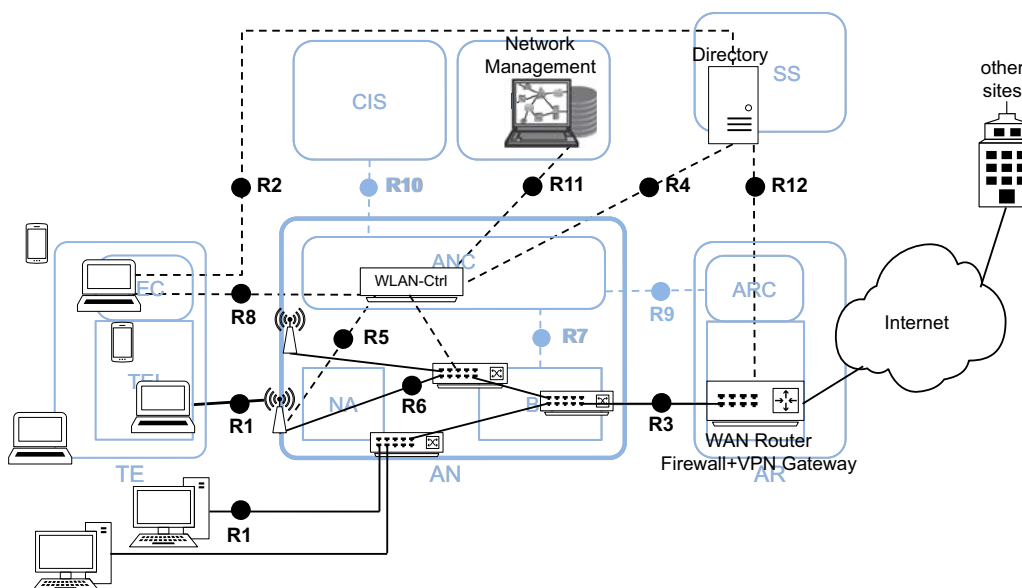


Figure 18—Mapping of enterprise network to the NRM

Even when a typical implementation of an enterprise network widely follows the decomposition of functions represented by the NRM, equipment exists that integrates and combines functions into a single device for functional or economic reasons. For example, many WLAN controllers do not act only as controller for the WLAN access points but also as Ethernet bridge for the aggregation of the user data. Enterprise networks may deploy virtualized instances of WLAN controllers, NMSs, and directories, hosted either in the Cloud or in local data centers, when higher security requirements exist.

Figure 19 illustrates that Cloud-managed network realizations also fit well to the NRM. As the NRM defines only the information carried over control interfaces and not the protocol or physical transport, all or part of the ANC, NMS, SS, and CIS may be realized as virtual instances and be operated in the Cloud or a local data center.

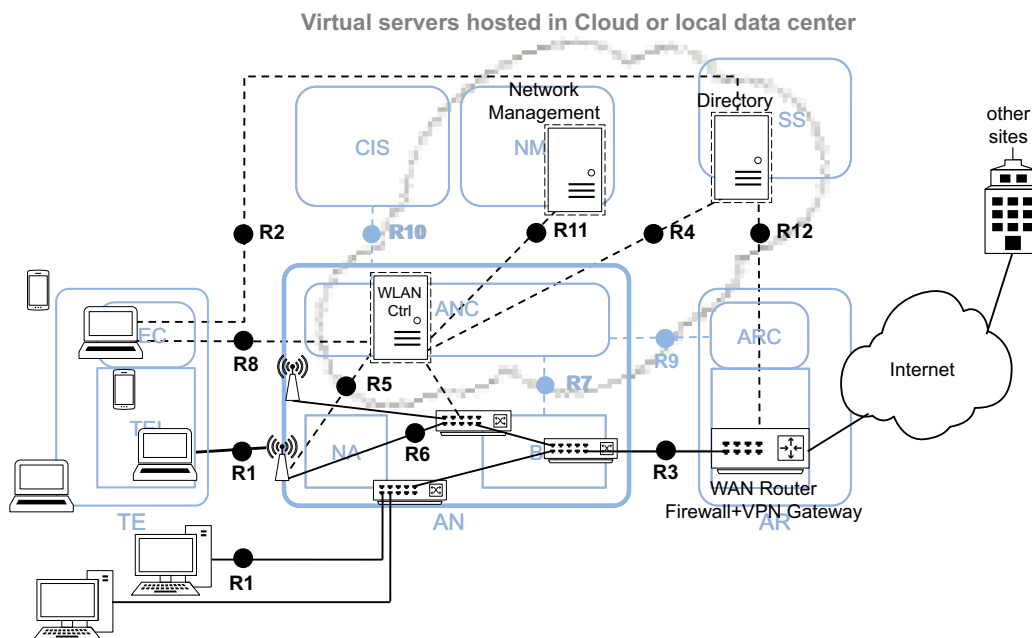


Figure 19—Cloud-managed enterprise network

5.10.5 Enterprise network with multiple bridging domains

Many enterprise networks are not operated as a single flat bridging domain, but are segmented into multiple separate bridging domains to differentiate various traffic classes and to introduce borders for the uncontrolled transfer of information to facilitate more fine-grained security concepts.

Such segmentation can be achieved in a common infrastructure through the deployment of VLAN technology as defined in IEEE Std 802.1Q. It allows bridges to handle multiple different broadcast domains in a single bridge, with broadcast domains establishing a VLAN identified either as an exclusive assignment of bridge ports to a VLAN or through VLAN tags added to the MAC frames, when multiple different VLANs are forwarded on a bridge port.

Figure 20 depicts the enterprise network scenario introduced in 5.10.4 with the addition of VLAN technology leading to multiple virtual LANs within the same infrastructure.

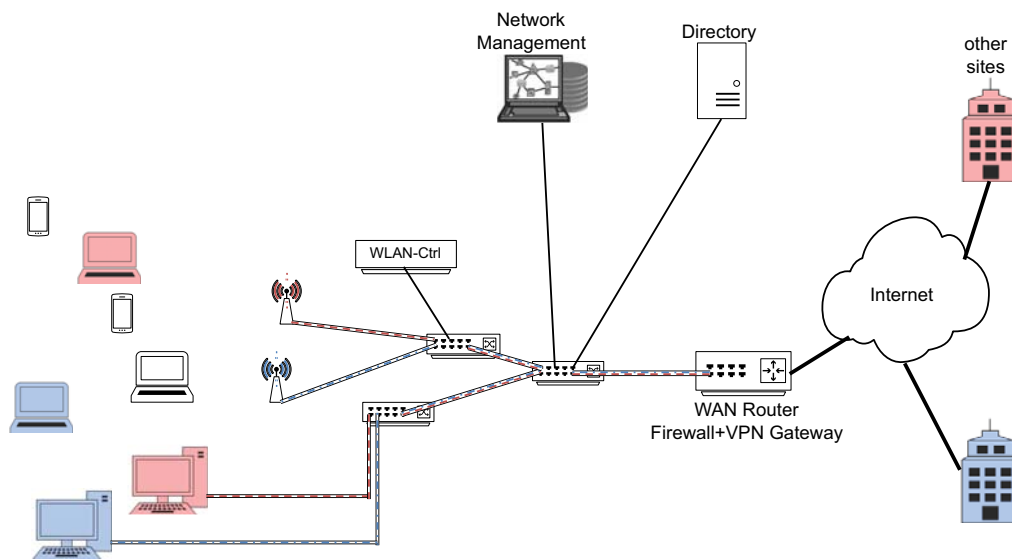


Figure 20—VLAN-enabled enterprise network scenario

Three different VLANs are shown in Figure 20, two of them connected through VPNs over the Internet with other sites of the same enterprise, and a third one (black, solid lines) aimed for providing “Bring Your Own Device” access to the Internet. To realize the multiple LANs, VLAN support has to be enabled in the bridges. All the VLANs belong to a single network under the control of a single entity. Therefore, single instances of the control entities (Network Management, Directory, WLAN-Control) are sufficient to operate the multiple VLANs belonging to the same operational domain (enterprise).

The mapping to the NRM follows the single LAN enterprise scenario in 5.10.4. The bridging infrastructure builds the backhaul of the network, with terminal Ethernet ports and WLAN access points resembling the NAs. The functions of the WLAN controller fit well to the role of the ANC, and network management station and directory are typical realizations of the NMS and SS, respectively. VLAN capability is enabled on the datapath between access router and backhaul, inside the backhaul, and on the interfaces between backhaul and NAs. The interface between the terminal and NA does not change through enabling VLAN support in the network. Each terminal is assigned to a single VLAN at the NA according to configuration information provided by the ANC.

As shown in Figure 21, the NRM is able to cover VLAN support without adding new interfaces or functional entities. Only the datapath and the bridges located within the NA and backhaul require additional functionalities, which are visible on the control interfaces through additional attributes. Support of multiple bridging domains in the NRM closely follows the procedures for adding VLAN capabilities to physical IEEE 802 networks and shows that the NRM is well suited to model the wide variety of physical networks.

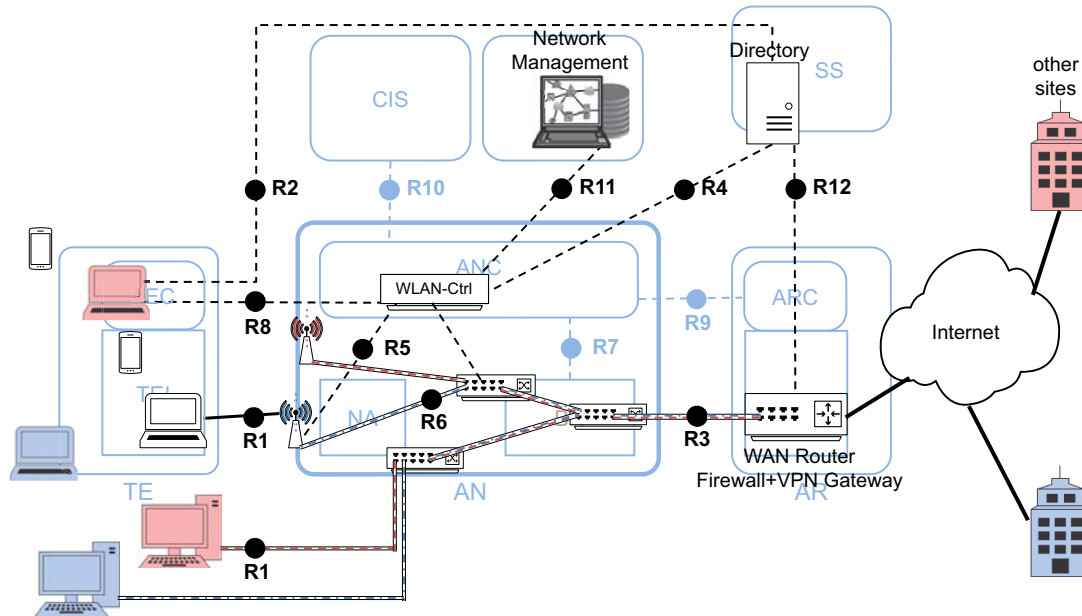


Figure 21—Mapping of VLAN-enabled enterprise network to the NRM

5.10.6 Industrial network

Industrial networks connect Internet of Things (IoT) devices, control processes of machineries and robots, surveillance equipment and building control gear among themselves or to central control processes. Often industrial networks in factory floors and power plants provide connectivity to virtual servers residing in a local data center or in the Cloud. It is quite common that the local area part of industrial networks are based on Ethernet, in particular due to its multiplexing capability of multiple networks and services within a single infrastructure, and its support for guaranteed frame delivery through time-sensitive networking features. Industrial networks are used as well to allow mobile terminals to connect through IEEE 802 wireless technologies to gateways, local servers, or even to the Internet.

Figure 22 shows a schematic network of a factory floor with three robots at an assembly line, supervised through surveillance cameras forwarding live video to a central control room not depicted here. A WLAN network throughout the factory floor allows the operators to remotely access the control processes of the robots, live video streams, and other information while walking along the assembly line. Virtual servers in the Cloud are used for controlling the environment, running the applications accessed by the mobile terminals, and processing various measurements delivered to the central control room.

Control processes of robots require highest reliability and immediate response to their messaging. Video streaming is not as critical as robot control, but sufficient bandwidth has to be reserved on the network to ensure that the control center has the latest insights into the factory hall. The applications running on smartphones, tablets, and notebook computers that allow operators to access control information while walking around in the factory hall may be able to deal with packet losses and delays associated with accessing services over the Internet. However, the network has to ensure through scheduling and prioritization that bulk data transferred to wireless devices does not impact the transmission of the low-latency real-time messaging and streaming data.

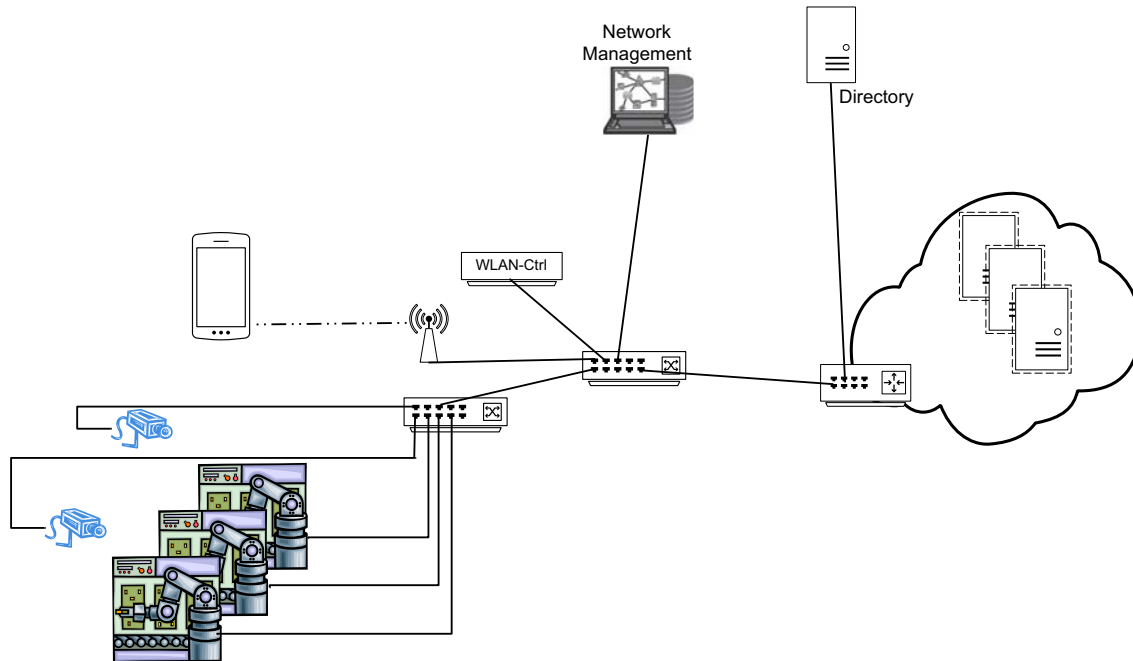


Figure 22—Industrial (access) network

The industrial network scenario can be mapped to the NRM as depicted in Figure 23.

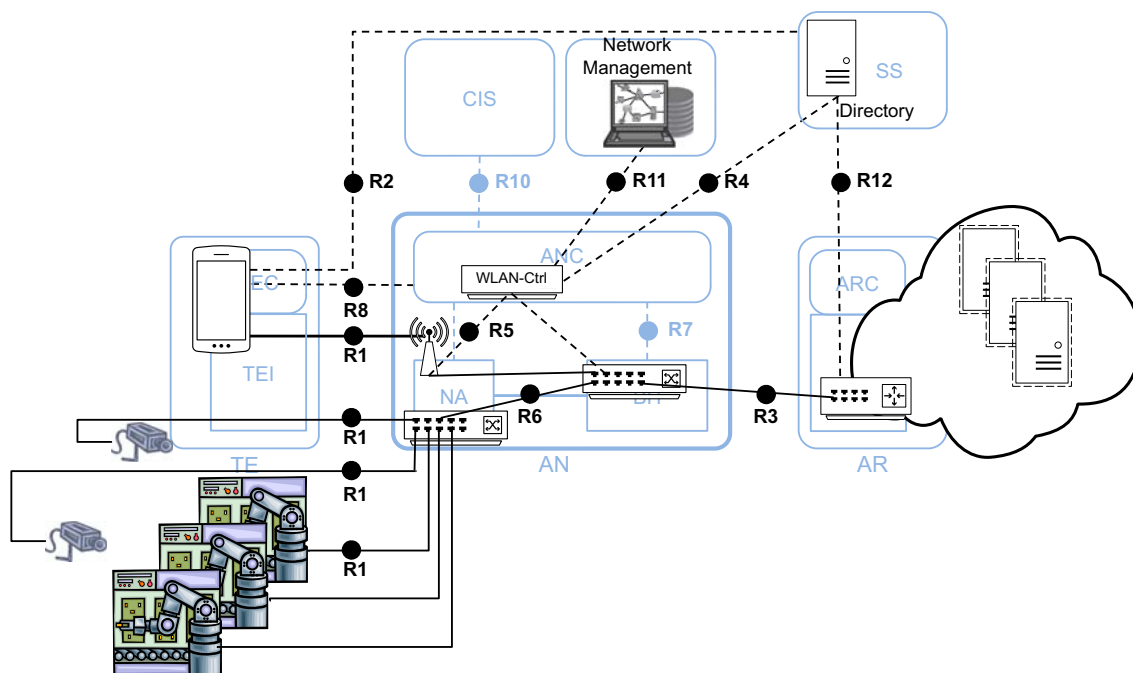


Figure 23—Mapping of industrial network to NRM

The access bridge connecting the robots and surveillance cameras to the Ethernet backbone represents the NA for the wired connections of terminals, while the access point represents the NA for wireless terminals. The backhaul is mapped to the second-level aggregation bridge, with the uplink to the gateway to the local data center fitting to the interface between access network and the access router. The router functionality is located in the gateway to the local data center, where multiple virtual servers collect information over the industrial network and control mechanical processes on the factory floor. To ensure high availability and security of the industrial network, a network management station provides configuration information to the network elements and monitors their operation. The network management station also provides the tools to analyze faults and initiate countermeasures. A directory server provides account information of users of the network. The information is processed by the WLAN controller to enable authorized personal to use the WLAN at the factory floor.

The small example of an industrial network shows the mapping of the elements and the reference points of the NRM to networks not primarily aimed at serving mobile terminals. Nevertheless, industrial networks can gain increased reliability and security through deployment of a SS, NMSs, and even a CIS, when applicable.

5.10.7 Public hotspot

Public hotspots deploy IEEE 802 access networks similar to enterprise networks, and usually provide access to the Internet only over a WLAN. Public hotspots can widely vary in size and capabilities; however, they have a defined set of commonalities to ensure that customers find access regardless of the particular implementation.

They all provide at least an open WLAN, and they block access to the Internet until the user has opened a captive-portal page and confirmed the terms and conditions, a step that is often combined with the entry of credentials that the hotspot operator can use for identification of the user and for charging for the service. More capable hotspots provide in addition possibilities for fully automatic login, sometimes through proprietary solutions based either on detecting the MAC addresses of the terminals or on establishing temporary credentials in the web browser used for accessing the captive portal page. Aside from proprietary solutions for automatic access to open WLANs, standardized solutions exist for access to secured WLANs based on IEEE 802.1X authentication and provisioning of credentials. The credentials can be made available at the terminal, either through prior establishment of a permanent subscription with the hotspot operator or one of its roaming partners, or through an online signup process at the hotspot according to the WI-FI CERTIFIED Passpoint® procedures.¹⁰

VLAN capabilities in IEEE 802 technologies allow both kinds of public hotspots to be configured within the same network infrastructure. A hotspot usually consists of a number of WLAN access points connected through an Ethernet bridge to an access gateway, which contains the mechanisms of the captive portal and provides the access router with network address translation and firewall for the IP connectivity of the terminals to the Internet.

¹⁰ <https://www.wi-fi.org/discover-wi-fi/passpoint>.

As depicted in Figure 24, commercial hotspots usually deploy a WLAN controller to establish a more consistent and seamless service across the whole coverage area. They have a network management station in place to facilitate efficient configuration and management of the infrastructure, and they deploy an evolved authentication center, which can establish and maintain a bigger number of temporary user accounts. The authentication center is also responsible for the communication with roaming partners, which is usually performed through a RADIUS proxy for forwarding authentication requests to the home service provider.

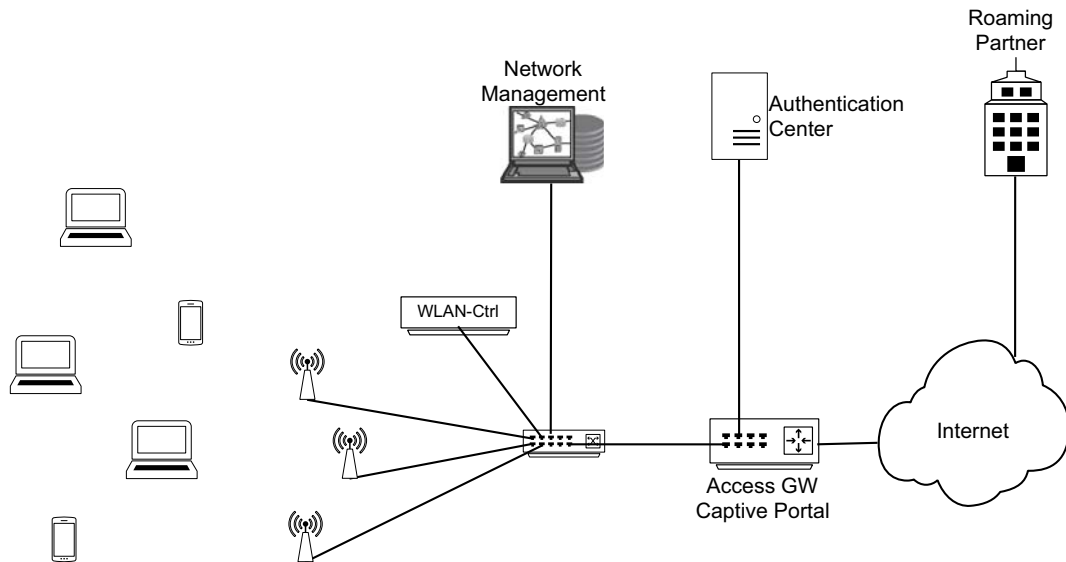


Figure 24—Public hotspot network scenario

Like the enterprise network, the public hotspot network can be well mapped to the NRM. The backhaul is represented by the Ethernet bridge; WLAN access points are building the NAs. The functions of the WLAN controller fit well to the role of the ANC, and network management station and the authentication center map well to NMS and SS, respectively.

Many of the reference points of the NRM map to interfaces of the public hotspot network, shown in Figure 25. All reference points to terminals are supported. R6 is exposed on the interface between the bridge and the access point, and R3 maps to the LAN cable between the bridge and the router in the access gateway. Also, the majority of the control interfaces of the access network are present in the public hotspot network. R5 can be mapped to the communication between the WLAN controller and the WLAN access points, and R4 and R11 denote the protocol connections between the WLAN controller and the authentication center and network management station, respectively. The information exchanges between the authentication center and the access gateway to temporarily open access to the Internet for users can be mapped to the R12 reference point.

However, not all reference points are clearly exposed in public hotspot networks. R7 and R9 may exist, but related ANC functions may be implemented in the Ethernet bridge in the backhaul. Aside from solutions that closely follow the functional decomposition represented by the NRM, there exists equipment for public hotspots that integrates and combines functions of a public hotspot into a single device to make installation and operation easier. For example, a favorable solution for a smaller public hotspot may be a device that integrates the WLAN controller, the Ethernet bridge, and the access gateway with a captive portal into a single box.

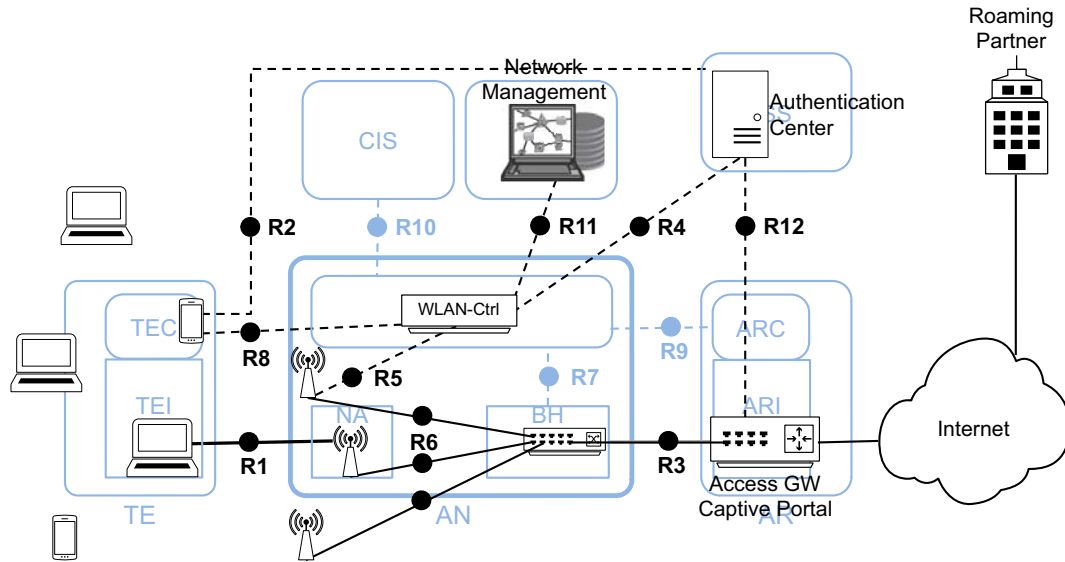


Figure 25—Mapping of the hotspot network to the NRM

5.10.8 Virtualized WLAN access network for in-building IoT services

In-building IoT services provided by utilities and other companies benefit from virtualized WLAN access infrastructures dedicated to IoT services. These IoT services are built around a client-server architecture consisting of a high number of small, inexpensive client devices connected to a central server interacting with the distributed devices and operating the higher layer control and data-processing functions of IoT services. Due to its ubiquitous availability and the availability of a vast number of low-cost chipset solutions, WLAN has become the network interface of choice for that kind of IoT service deployments.

Putting IoT devices on a WLAN network aimed for office or residential use, however, imposes a number of risks and drawbacks. IoT devices are usually kept in operation for much longer periods than smartphones, tablets, and notebook computers, and often completely miss the regular software updates that are usual for the much more powerful and complex handheld communication devices. It is quite common that IoT devices are intended to run for more than a decade, completely without maintenance, serving their very specialized purpose. Due to limited configuration and management capabilities, it is quite likely that vulnerabilities in the communication software and operating system detected during the lifetime of an IoT device will not be fixed through a firmware update. Missing agents in the legacy devices make it difficult for network administrators to remotely manage these devices. Keeping such devices in a LAN together with other systems and arbitrary access to the Internet allows not only malicious attacks to the IoT devices by leveraging unpatched vulnerabilities, but also the misuse of the IoT devices to attack other devices in the same access network as well as perform distributed denial of service attacks to any location in the Internet.

In addition to the security risks, there are also performance impacts introduced by operating potentially aged, simple, low-cost IoT devices together with the most recent smartphones, tablets, and other computing devices on a single WLAN access network. Even when the most recent WLAN is still backward compatible with the legacy IEEE Std 802.11b, attaching legacy WLAN equipment to a modern WLAN access network requires the activation of backward-compatibility modes, which lowers the efficiency of the complete WLAN access network.

Both the security and the efficiency challenges can be mitigated by setting up a dedicated WLAN access network for IoT devices. Keeping lower performance IoT devices in a separate network allows for optimizations of the network configurations to their native purpose (e.g., enabling legacy backward-compatibility modes in the radio interfaces only when there is real need for them). Specific filtering rules could be applied to IoT devices that limit broadcasting inside the access network to prevent vulnerable devices from attacking other devices in the network or connecting to any host in the Internet. The IoT devices still use Internet protocols for communication, but their communications are restricted within a VPN to mitigate the risks of the public Internet.

Network virtualization allows for establishment of multiple independent access networks on a common infrastructure and is well supported by IEEE 802 technologies through inherent support of virtualization.

Figure 26 shows how a virtualized WLAN access network for in-building IoT could be realized by leveraging the fixed broadband access infrastructure over cable, DSL, or fiber to provide broadband Internet access to homes. Core functionality of the solution is the establishment of the virtualized NA in the homes by setting up a second access point instance on the WLAN interface of the residential customer-premises equipment (CPE). To establish the desired isolation of the WLAN access network for IoT devices, the second access point instances in the CPEs have to be attached to a separate control plane to allow for the desired security and access control by the IoT service provider. A separate datapath for the second WLAN forwards all the traffic going over the IoT WLAN to the IoT service provider and prevents IoT devices from establishing uncontrolled connections to the Internet with the inherent risk of getting compromised through those connections. Remote CPE management (e.g., supported by the BBF TR-069 [B3] CPE WAN management protocol and BBF TR-181 [B4] device information model) can be used by the Internet service provider to remotely configure the second access point instance, second datapath, and second control entities within the CPE. It also allows remote reapplication of the same configurations when the CPE is replaced through newer hardware; such replacements can happen during the long lifetime of IoT applications.

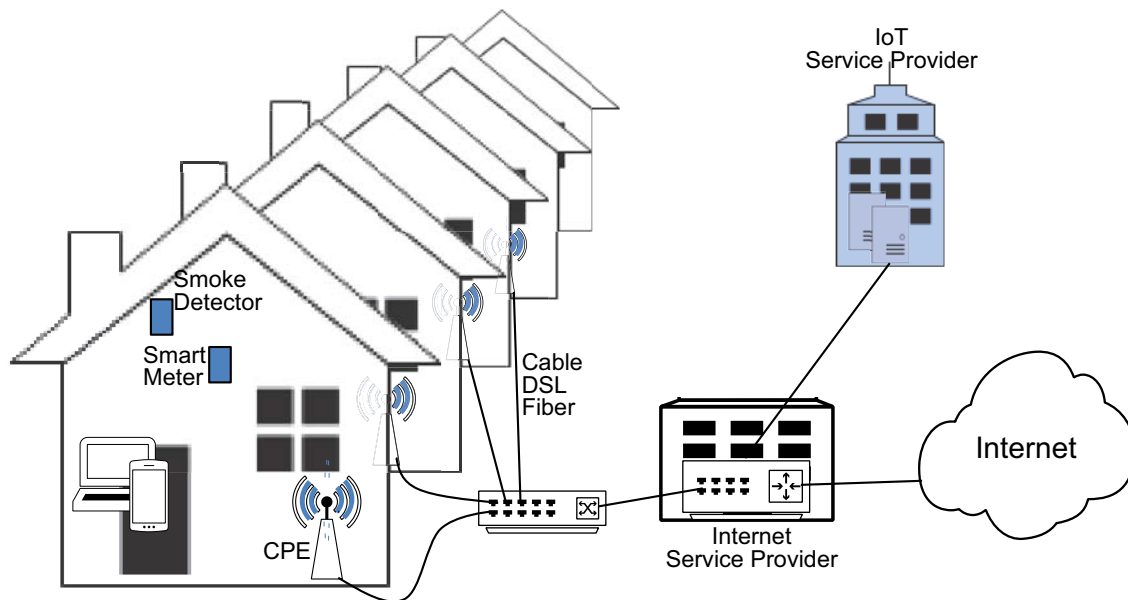


Figure 26—Virtualized WLAN access for IoT

Figure 27 shows in a schematic diagram the additional configuration elements needed to establish the IoT WLAN and the second datapath for in-building IoT services within a remotely managed CPE.

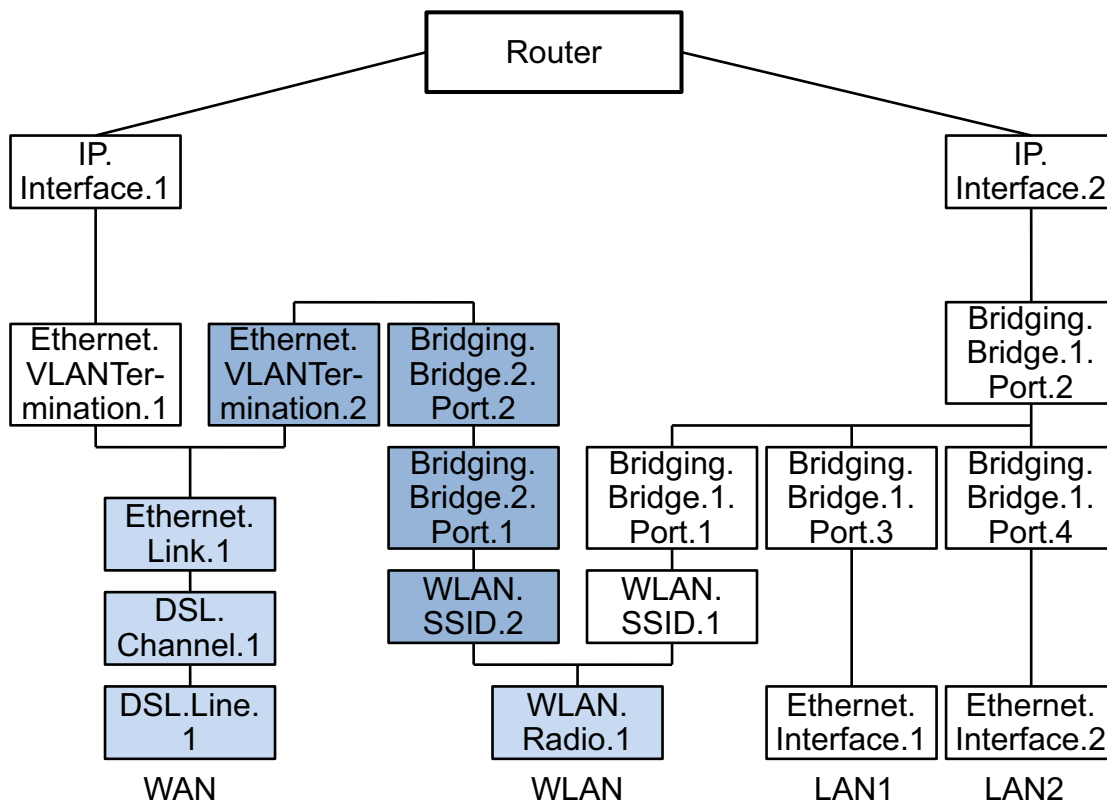


Figure 27—Schematic datapath and WLAN configuration model of CPE with IoT WLAN

In the broadband access infrastructure, the second datapath and control plane for the IoT WLAN access point instances are established by the Internet service provider and provided to the IoT service provider as a kind of “WLAN as a Service.” After instantiation of the second WLAN access network, the IoT service provider can control and operate the virtualized WLAN access network for IoT devices as if it were a dedicated network, as shown in Figure 28. It has its own operation, administration, and maintenance through a separate NMS, enabling independent access to all management data belonging to the virtualized WLAN access network. Only a few PHY-related configurations, e.g., radio channel assignments of the WLAN access points, cannot be independently configured by the IoT service provider but are preset by the owner of the infrastructure.

While the description in the previous paragraphs shows the realization of a virtualized WLAN access network in the residential broadband access network, the same kind of virtualized WLAN access for IoT devices could also be realized in enterprise WLAN access networks. The example of the enterprise network with multiple independent bridging domains and multiple SSIDs enabled on the WLAN access points introduced in 5.10.5 shows the establishment of separate datapaths for separating traffic and connectivity with a common control plane and a common NMS. Applying virtualization to the control entities and to the NMS of enterprise networks would facilitate the establishment of a dedicated WLAN for IoT devices under the control of a different entity.