INTERNATIONAL STANDARD

ISO/IEC 5021-2

First edition
2023-08

Telecommunications and information exchange between systems — Wireless LAN access control —

Part 2:
Dispatching platform

Reference number
ISO/IEC 5021-2:2023(E)

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Email: copyright@iso.org
Website: www.iso.org

Published in Switzerland

Contents

Page

Foreword

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

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular, the different approval criteria needed for the different types of document should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives or www.iec.ch/members_experts/refdocs).

ISO and IEC draw attention to the possibility that the implementation of this document may involve the use of (a) patent(s). ISO and IEC take no position concerning the evidence, validity or applicability of any claimed patent rights in respect thereof. As of the date of publication of this document, ISO and IEC had not received notice of (a) patent(s) which may be required to implement this document. However, implementers are cautioned that this may not represent the latest information, which may be obtained from the patent database available at www.iso.org/patents and https://patents.iec.ch. ISO and IEC shall not be held responsible for identifying any or all such patent rights.

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation of the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT) see www.iso.org/iso/foreword.html. In the IEC, see www.iec.ch/understanding-standards.

This document was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 6, *Telecommunications and information exchange between systems*.

A list of all parts in the ISO/IEC 5021 series can be found on the ISO and IEC websites.

Any feedback or questions on this document should be directed to the user’s national standards body. A complete listing of these bodies can be found at www.iso.org/members.html and www.iec.ch/national-committees.

Telecommunications and information exchange between systems — Wireless LAN access control —

Part 2: **Dispatching platform**

1 Scope

This document defines the function, interfaces (IFs), and operating mechanism of CADP and defines the AP association, cloud AC switchover, cloud AC backup and CADP hot backup methods. This document applies to public wireless local area network (WLAN) networking scenarios.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO/IEC 5021-1, *Telecommunications and information exchange between systems - Wireless LAN Access Control - Part 1: Networking Architecture Specification*

ISO/IEC/IEEE 8802-11, *Telecommunications and information exchange between systems — Specific requirements for local and metropolitan area networks — Part 11: Wireless LAN medium access control (MAC) and physical layer (PHY) specifications*

IETF RFC 5415:2009, *Control and Provisioning of Wireless Access Points (CAPWAP) Protocol Specification*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 5021-1 and ISO/IEC/IEEE 8802-11 apply.

ISO and IEC maintain terminology databases for use in standardization at the following addresses:

- ISO Online browsing platform: available at https://www.iso.org/obp
- IEC Electropedia: available at https://www.electropedia.org/

3.1
wireless termination point
WTP
physical or network entity that contains a radio frequency (RF) antenna and wireless physical layer (PHY) to transmit and receive station traffic for wireless access networks according to IETF RFC 5415:2009, 1.4

Note 1 to entry: In this document, WTP and access point (AP) refer to the same network entity.

4 Abbreviated terms

The following abbreviated terms apply to this document.

AP	access point
AC	access controller
CADP	cloud AC dispatch platform
CAPWAP	control and provisioning of wireless access points
CPU	central processing unit
HTTP	hyper text transfer protocol
HTTPS	hyper text transfer protocol over secure socket layer
IF	interface
MAC	media access control
NMS	network management system
UDP	user datagram protocol
WLAN	wireless local area network
WTP	wireless termination point

5 CADP-based WLAN architecture

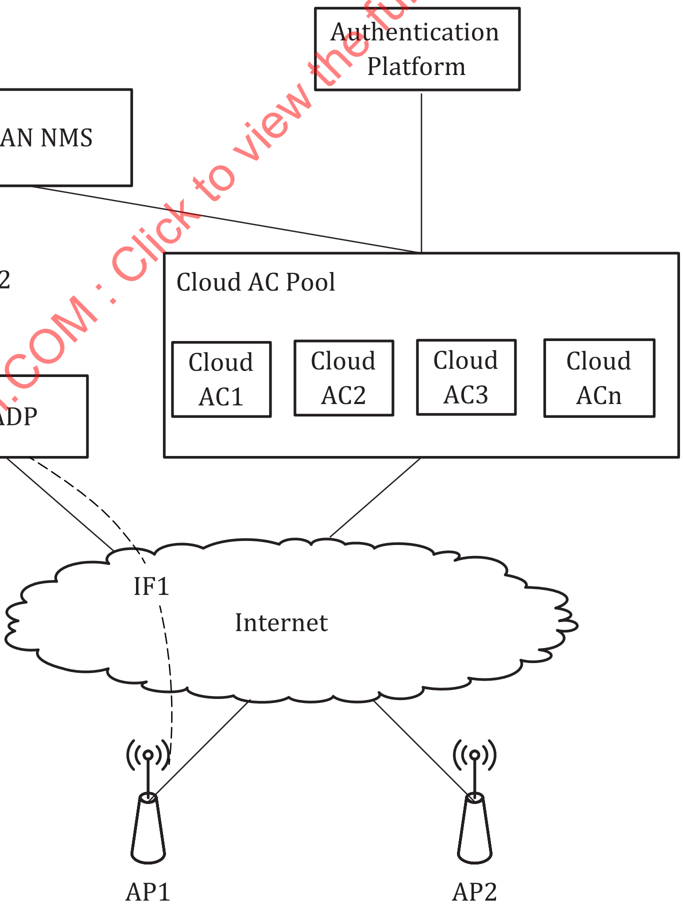

Figure 1 — CADP-based WLAN architecture

Figure 1 shows the architecture of a CADP-based WLAN, where CADP is deployed at the core layer of the network to assign the optimal cloud AC to onboarding APs and provide cloud AC switchover and redundancy for online APs. ISO/IEC 5021-1 shall be referred to for CADP based WLAN network architecture.

CADP uses the following interfaces (IFs) to communicate with the other WLAN network elements:

a) Interface one (IF1): IF connecting CADP to APs, provides CAPWAP-based information exchange. Packets transmitted over this IF include AP registration requests that carry AP information and CADP responses that carry the address of the assigned AC.

b) Interface two (IF2): IF connecting CADP to the WLAN NMS, provides HTTP/HTTPS connection for the WLAN NMS to deploy AP and AC association information to CADP.

6 Operating mechanism of CADP

6.1 CADP service functions

The WLAN NMS obtains cloud AC load information in real time, including the number of managed APs, traffic throughput, the number of clients and the CPU usage. Each cloud AC load factor is assigned with a weight for the WLAN NMS to calculate the load of cloud ACs, based on which the WLAN NMS performs cloud AC selection. For an onboarding AP, if an AP providing the same wireless service is already online, the WLAN NMS prefers to assign the same AC to both APs so that clients can roam between the APs seamlessly.

CADP obtains AP and cloud AC association information from the WLAN NMS and provides the following functions:

a) sends the IP address of the assigned cloud AC to an on boarding AP;

b) sends the IP address of the backup cloud AC to an AP based on the cloud AC backup policy in case of cloud AC failure;

c) provides hot backup to ensure system availability.

6.2 CADP-based AP association

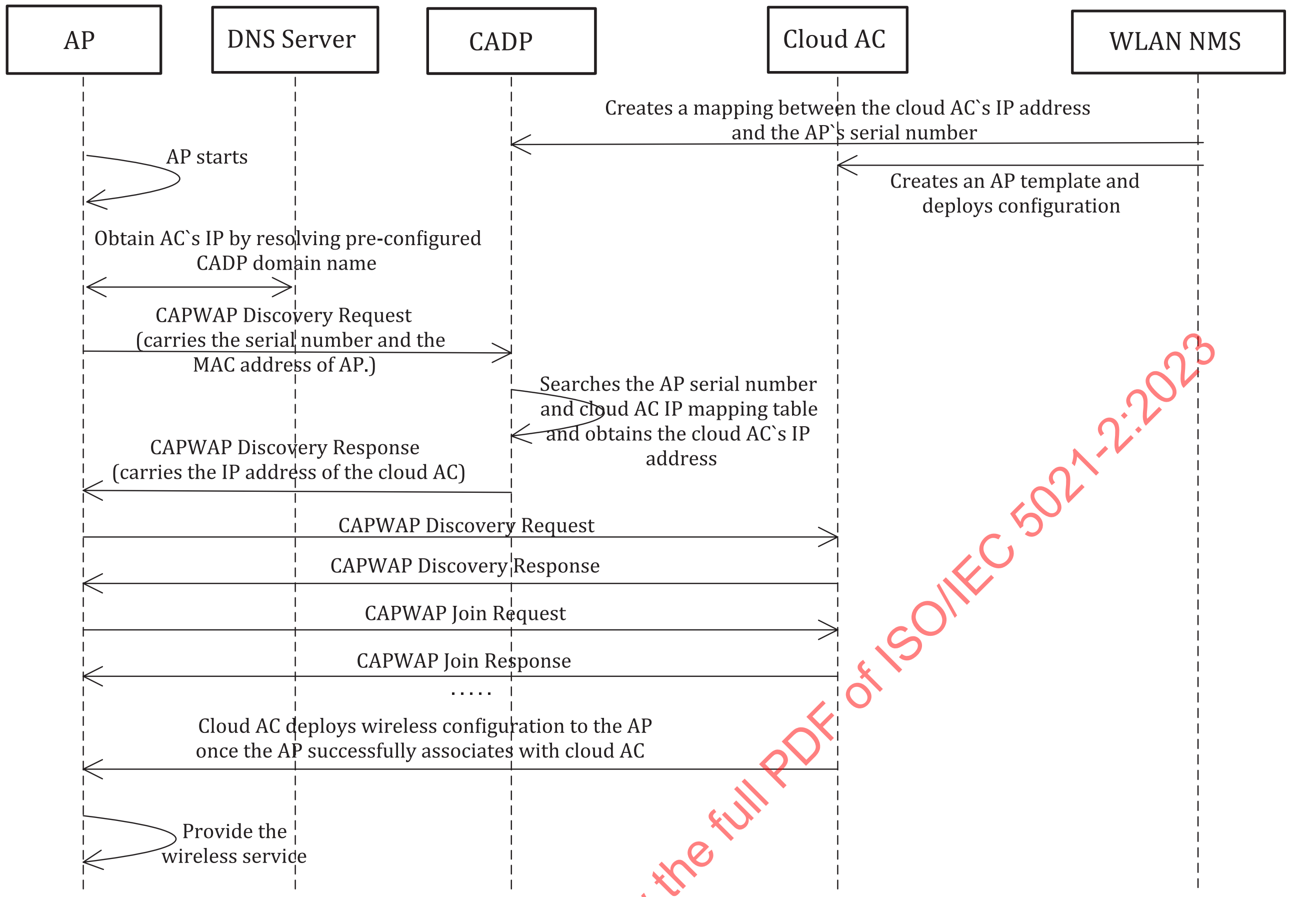
AP
DNS Server
CADP
Cloud AC
WLAN NMS
Creates a mapping between the cloud AC`s IP address and the AP`s serial number
AP starts
Creates an AP template and deploys configuration
Obtain AC`s IP by resolving pre-configured CADP domain name
CAPWAP Discovery Request (carries the serial number and the MAC address of AP.)
Searches the AP serial number and cloud AC IP mapping table and obtains the cloud AC`s IP address
CAPWAP Discovery Response (carries the IP address of the cloud AC)
CAPWAP Discovery Request
CAPWAP Discovery Response
CAPWAP Join Request
CAPWAP Join Response
.....
Cloud AC deploys wireless configuration to the AP once the AP successfully associates with cloud AC
Provide the wireless service

Figure 2 — CADP-based AP association

APs communicate with CADP by using CAPWAP discovery requests and discovery responses through IF1. As shown in Figure 2, an AP comes online and associates with a cloud AC as follows:

a) AP pre-configuration:

- A CADP domain name is pre-configured to APs.
- WLAN NMS informs CADP (IF2) of AP association, associated cloud AC change and other events.

b) After an AP starts, the local gateway assigns an IP address to AP through DHCP and the AP obtains the CADP IP address by resolving the pre-configured domain name.

c) The AP sends a Discovery Request to CADP. This message carries AP information, including AP model number, serial number and the MAC address, etc. This information encapsulated into a field called "WTP Board Data" shall be in accordance with IETF RFC 5415:2009, 4.6.40.

d) Upon receiving the request, CADP obtains the AP's information and searches its local database. If a match is found, which indicates that the AP is licensed, CADP sends a response to the AP. If no match is found, CADP does not respond.

e) If a match is found, CADP sends a Discovery Response message to AP. This message carries the IP address of the cloud AC assigned to the AP by the WLAN NMS.

f) After receiving the response, the AP extracts the IP address of the cloud AC in the CAPWAP Control IP Address field from the message and re-initiates the Discovery and Join requests process to the cloud AC. The cloud AC then completes the subsequent process.

The above standard process compliant with the CAPWAP protocol shall be in accordance with IETF RFC 5415:2009, 2.2, but the AP software shall be upgraded to meet the interpretation and processing requirements of protocol on CAPWAP message data.

6.3 CADP-based cloud AC switchover

If an AP is moved to another cloud AC, CADP removes the association between the AP and the original AC and adds information about the new cloud AC. The WLAN NMS informs CADP (IF2) and the new cloud AC.

After the AP restarts, it initiates an association request to CADP and the CADP informs the AP of the new cloud AC's IP address.

6.4 CAD-based cloud AC backup

If a cloud AC fails, the WLAN NMS assigns a new cloud AC for the APs and notifies CADP of information about the new cloud AC. CADP deploys the IP address of the new cloud AC for AP association and switches back to the original cloud AC when the failed cloud AC recovers.

This mechanism enables N active ACs and M backup ACs (N+M backup) of cloud ACs.

NOTE It is a type of backup mechanism which includes more than one backup ACs. These ACs can backup more than one working ACs. The backup relationship is N ACs to M ACs and the role of an AC can be transformed.

During the switchover process, the AP shall disassociate from the original cloud AC and reassociate with the new cloud AC.

The AC backup mechanism in the traditional network architecture can still be retained.

6.5 CADP hot backup

Two CADPs are deployed for CADP reliability (see Figure 3).

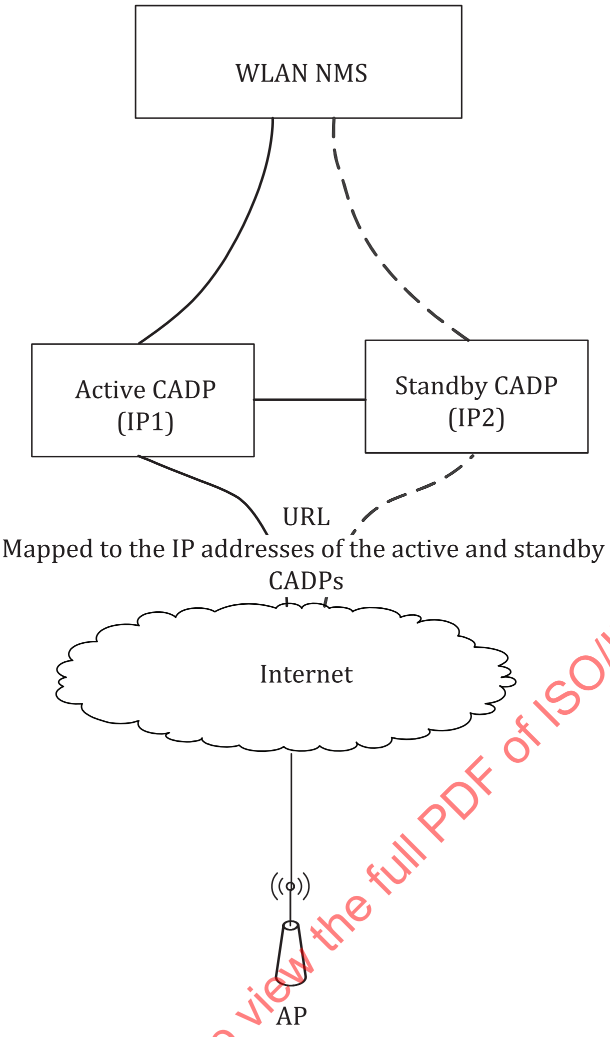

Figure 3 — CADP hot backup

When the association between the AP and cloud AC changes, the WLAN NMS synchronizes the information to the active and standby CADPs in real time.

To ensure that the CADPs and the WLAN NMS have the same AP-AC association information, the active and standby CADPs synchronize the information with the WLAN NMS at specific intervals. An interval of 24 h is recommended. If the information is inconsistent, the information on the WLAN NMS is applied.

The active and standby CADPs each have a public IP address configured and they provide one URL address for access from the Internet. The AP initiates an association request to the two IP addresses in sequence. If the first IP address does not respond within a specific interval, the AP will send a request to the second IP address. The two CADPs can be deployed in one equipment room or at different locations for reliability.

7 CADP interface

7.1 Interface between CADP and AP (IF1)

7.1.1 CAPWAP protocol basic format

The CAPWAP protocol is based on the Client-Server structure and uses UDP for transmission.

The CAPWAP protocol includes the control tunnel and the data tunnel. The control tunnel, whose port number is 5246, is used to transport the control messages, and the data tunnel, whose port number is 5247, is used to transport the data messages.

This document only defines specifications for the control tunnel.

7.1.2 CAPWAP protocol preamble

The CAPWAP protocol preamble shall be in accordance with IETF RFC 5415:2009, 4.1. The preamble can be used to quickly identify the protocol version and the packet type.

The value of each field in the CAPWAP protocol preamble used in this document are defined as follows:

- Version: This value should be 0.
- Type: This value should be 0.

7.1.3 CAPWAP protocol header

The CAPWAP protocol header shall be in accordance with IETF RFC 5415:2009, 4.3.

The values of each field in the CAPWAP protocol header used in this document are defined as follows:

- Preamble: The CAPWAP preamble is defined in 7.1.2.
- HLEN: The value should be 2.
- RID: The value should be 0.
- WBID: The value should be 1 which means ISO/IEC/IEEE 8802-11.
- T: This value should be 0.
- F: This value should be 0.
- L: This value should be 0.
- W: This value should be 0.
- M: This value should be 0.
- K: This value should be 0.
- Flags: This value should be 0.
- Fragment ID: This value should be 0.
- Fragment Offset: This value shall be 0.
- Reserved: This value shall be 0.
- Radio MAC Address: The field will not be included.
- Wireless Specific Information: The field will not be included.
- Payload: Only the control message will be included.

7.1.4 CAPWAP message type

The CAPWAP protocol uses two types of messages: control message and data message. This document only defines the control message. The definition of CAPWAP control packet payload is given in IETF RFC 5415:2009, 4.1.

The CAPWAP protocol message type shall be in accordance with IETF RFC 5415:2009, 4.5.1.1:

- The value for discovery request should be 1.
- The value for discovery response should be 2.

The values of each field in the CAPWAP control message used in this document are defined as follows:

- Seq Num: When an AP wants to join the network, this value increases consecutively from 1.
- Msg Element Length: This file indicates the number of bytes following the Seq Num field.

7.1.5 Control message sending and receiving

7.1.5.1 General

Subclause 7.1.5 describes elements carried in a control message and the message sending (see 7.1.5.4) and receiving (see 7.1.5.5) processes. The control message elements that are not in the list are not illustrated. This document only covers the verification of the required message elements.

7.1.5.2 Control IPv4 Address

The CAPWAP control IPv4 Address message element is sent by a CADP to an AP during the Discovery process and is used by the CADP to provide the addresses of available cloud AC IFs and the number of APs connected to each IF.

The CAPWAP control IPv4 Address message element shall be in accordance with IETF RFC 5415:2009, 4.6.9.

The values of each field in CAPWAP control IPv4 Address message element used in this document are defined as follows:

- Type: This value should be 10.
- Length: This value should be 6.
- IP Address: The IP address of an IF.
- WTP Count: This value should be 0 in CADP responses.

7.1.5.3 Control IPv6 Address

The CAPWAP control IPv6 Address message element is sent by a CADP to an AP during the Discovery process and is used by the CADP to provide the addresses of available cloud AC IFs and the number of APs connected to each IF.

The CAPWAP control IPv6 Address message element shall be in accordance with IETF RFC 5415:2009, 4.6.10.

The values of each field in CAPWAP control IPv6 Address message element used in this document are defined as following.

- Type: This value should be 11.
- Length: This value should be 18.
- IP Address: The IP address of an IF.
- WTP Count: This value should be 0 in CADP responses.