



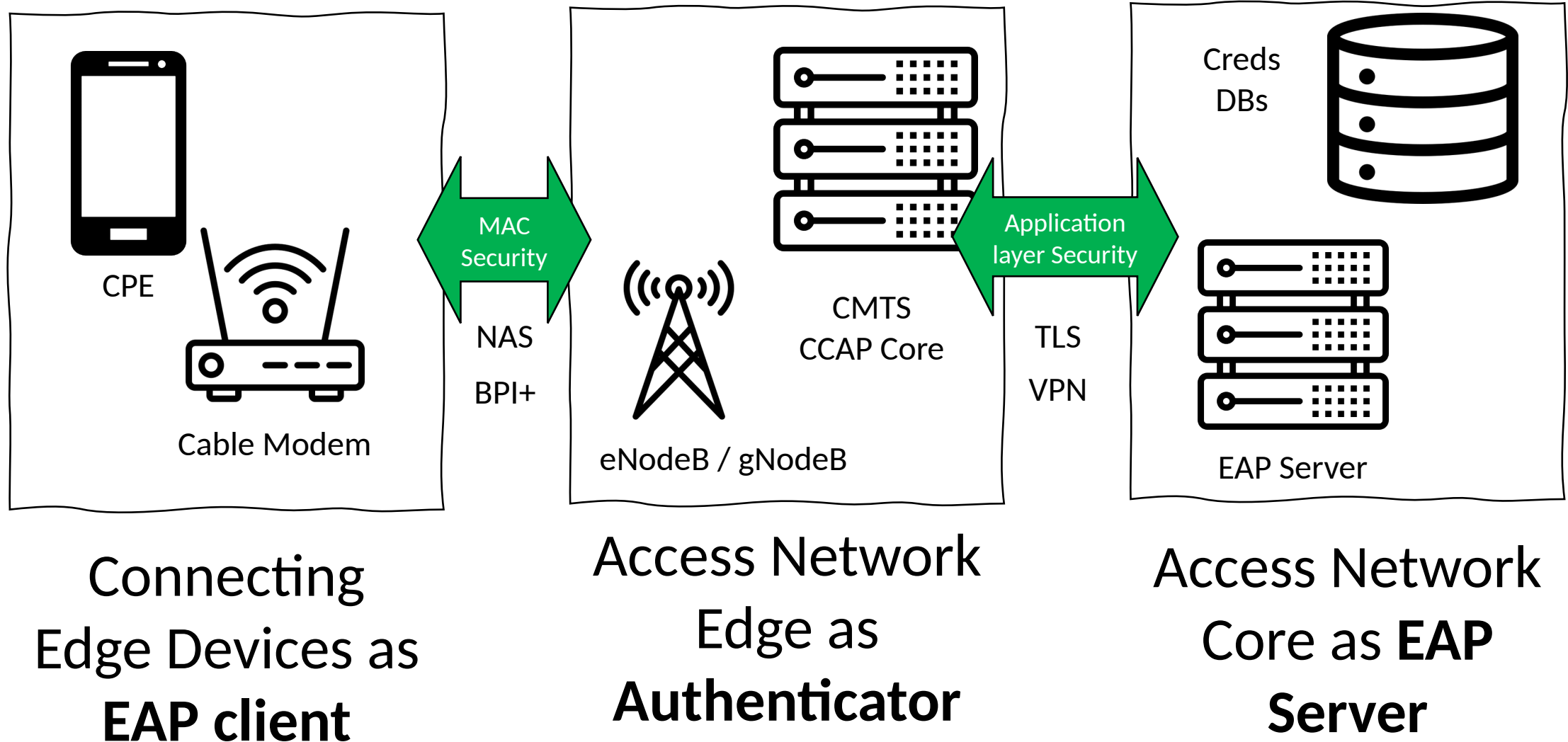
EAP-CREDS Overview

An EAP mechanism for simple and secure Access
Networks credentials management

Problem Statement

- Automated Credentials management is an important tool for managing network-layer authentications risks such as user-data privacy and theft of service.
- Differently from user-level credentials, device- and network-level credentials tend to be "forgotten" and live unmanaged for very long times.
- Today, credentials management requires active configuration of devices (such as provisioning IP addresses) and the service endpoint (e.g., the server's IP address)
- The EAP-CREDS work is aimed at automated Access Networks creds management:
 - Wired networks (i.e., DOCSIS and BPI+)
 - Wi-Fi networks (e.g., Wi-Fi and WPA2/3)
 - 3GPP networks (i.e., 4G or 5G and NAS)
- CBRS-A networks uses EAP-CREDS and SPP (TS-1003)

Example Access Network Architecture

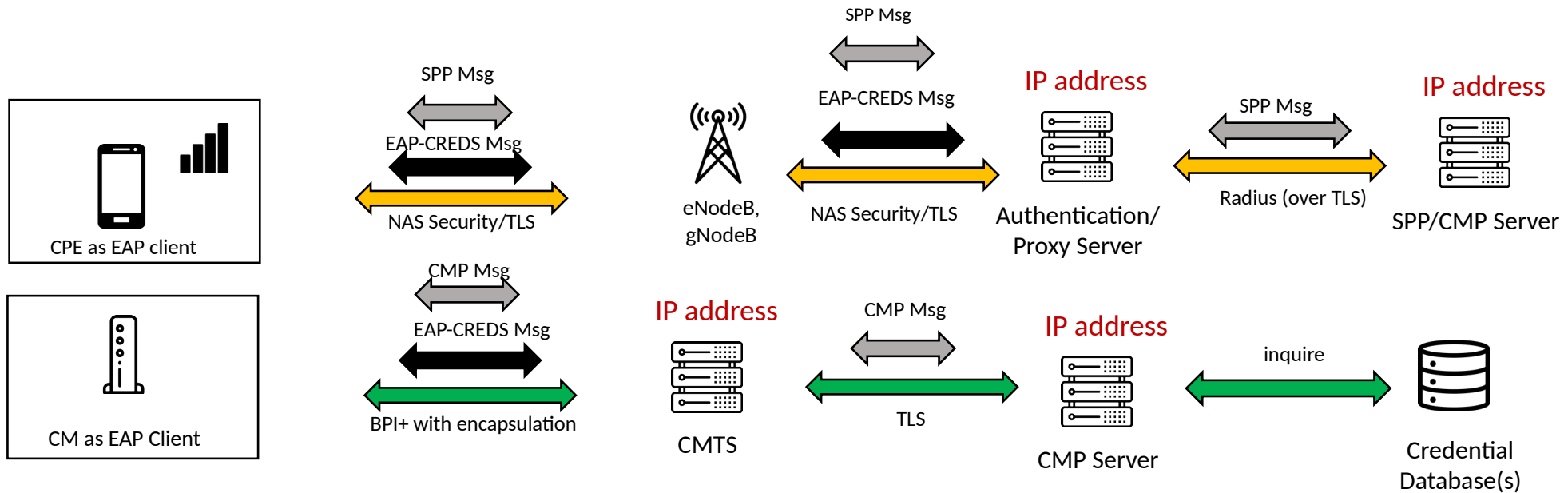


EAP-CREDS in a Nutshell

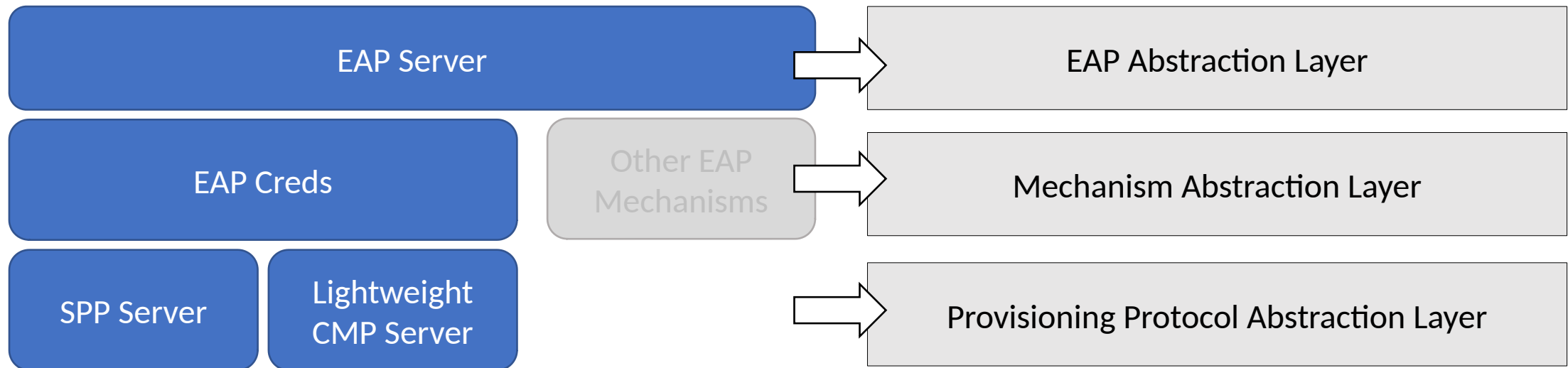


- EAP-CREDS provides a non-IP based mechanism to support **multi-protocols credentials management** to actively manage device or network layer credentials
- EAP-CREDS has simple message flow and relies on the security of the communication channel for confidentiality (see next slide).
- EAP-CREDS workflow is divided in **three phases**
 - **Initialization Phase:** The entities exchange the list of credentials available to be managed, device capability and supported protocols.
 - **Provisioning Phase** (optional): the Server and the Client execute the encapsulated protocol
 - **Validation Phase** (optional): Validates the ability for the client to correctly use the managed credentials

Example Message Encapsulation Flow



EAP-CREDS Logical Architecture



- Implementation can use the abstraction layer concept to ***separate the EAP-CREDS server/mechanism implementation from the provisioning protocol's endpoint*** implementation
- Components at different levels of abstraction can be ***implemented in separate processes and connected via IPC*** (e.g., HTTPS, etc.)

Other info

- We are currently working on two separate I-Ds
 - **EAP-CREDS** current draft is available at: <https://datatracker.ietf.org/doc/draft-pala-eap-creds/>
 - **EAP-CREDS-SPP** will be split from the Core document. This new I-D will describe the SPP separately from the Core document and can be used as a template for other protocols' encapsulation with EAP-CREDS (e.g., CMP).
- After the initial new drafts are ready, we plan to resume the activities within the WG and hopefully arrive at the next meeting with an indication about the appetite to work on such item.
- We are always looking for collaborations and contributions. If you are interested and/or would like to get more details, please contact us:
 - Dr. Massimiliano Pala m.pala@cablelabs.com
 - Yuan Tian y.tian@cablelabs.com