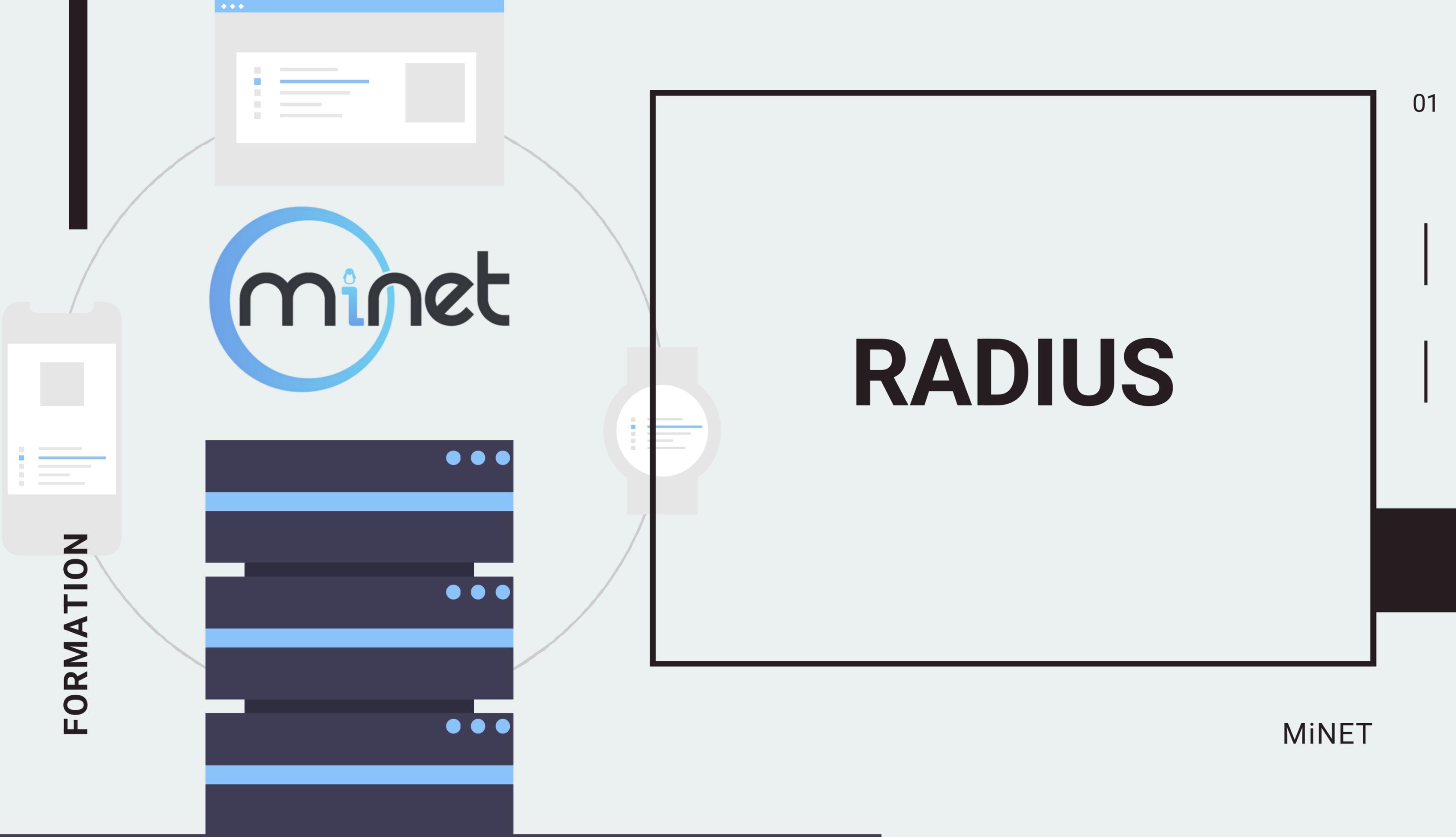




RADIUS

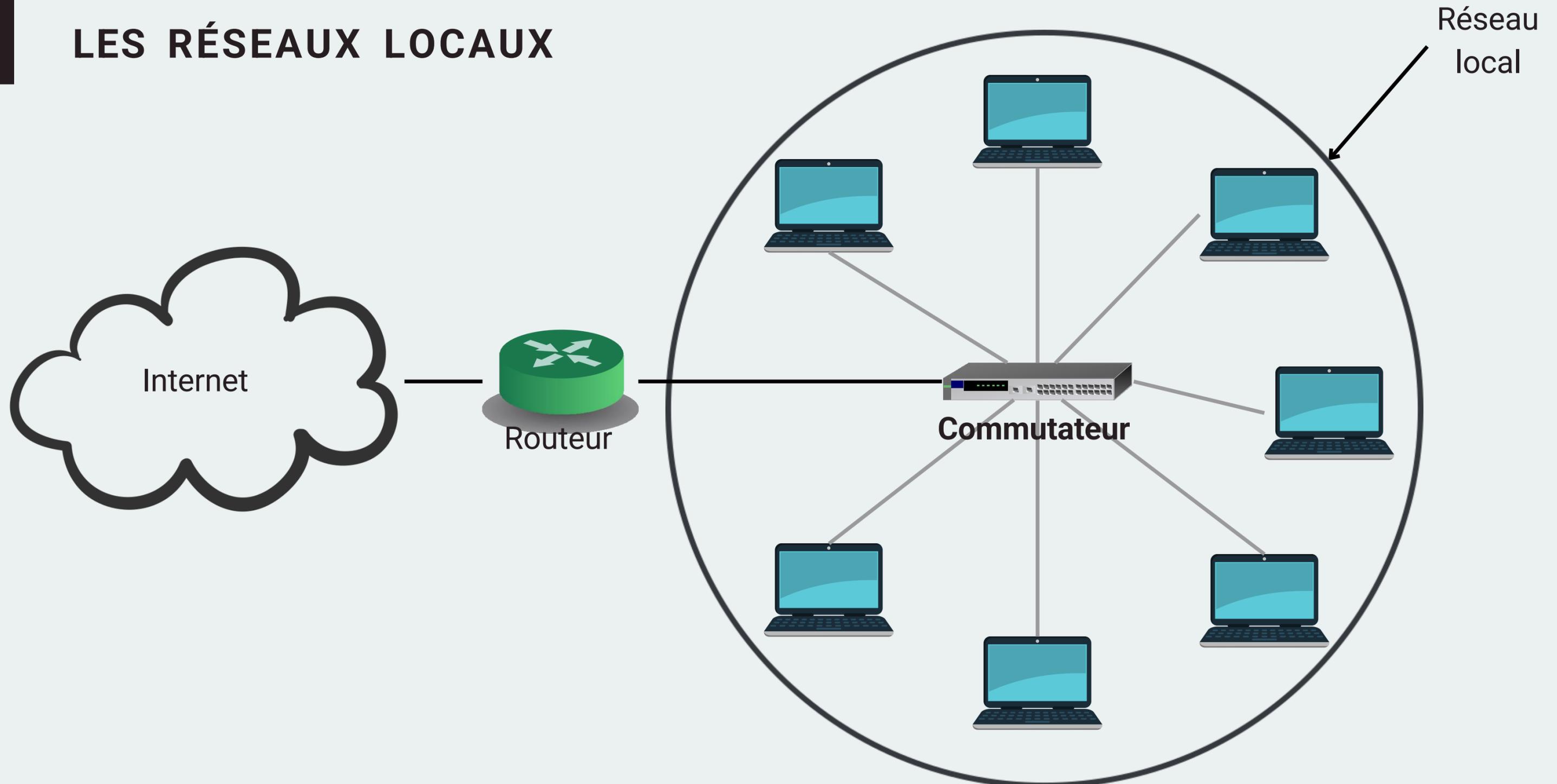
FORMATION

MiNET



PRÉLIMINAIRES

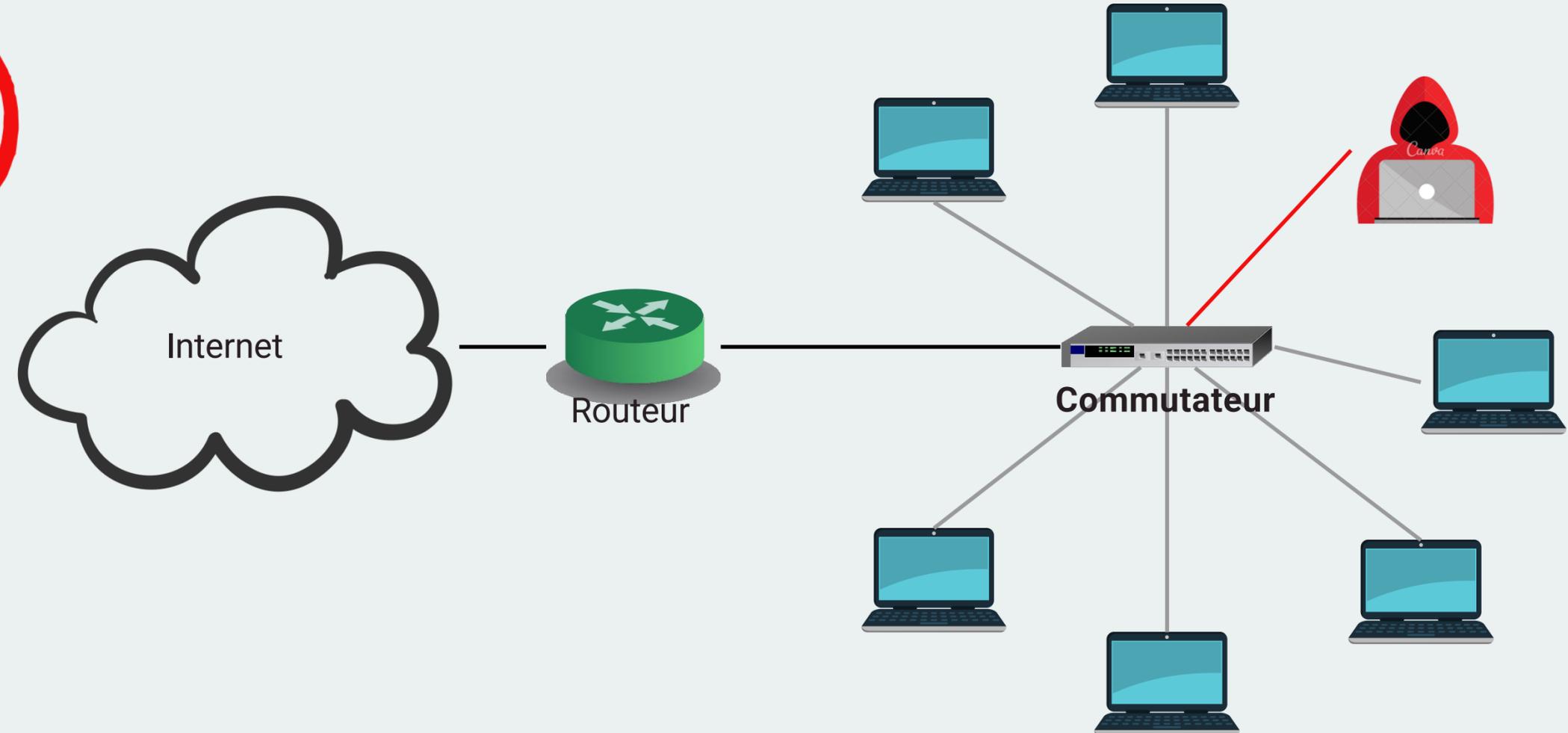
LES RÉSEAUX LOCAUX



PRÉLIMINAIRES

POURQUOI CONTRÔLER L'ACCÈS ?

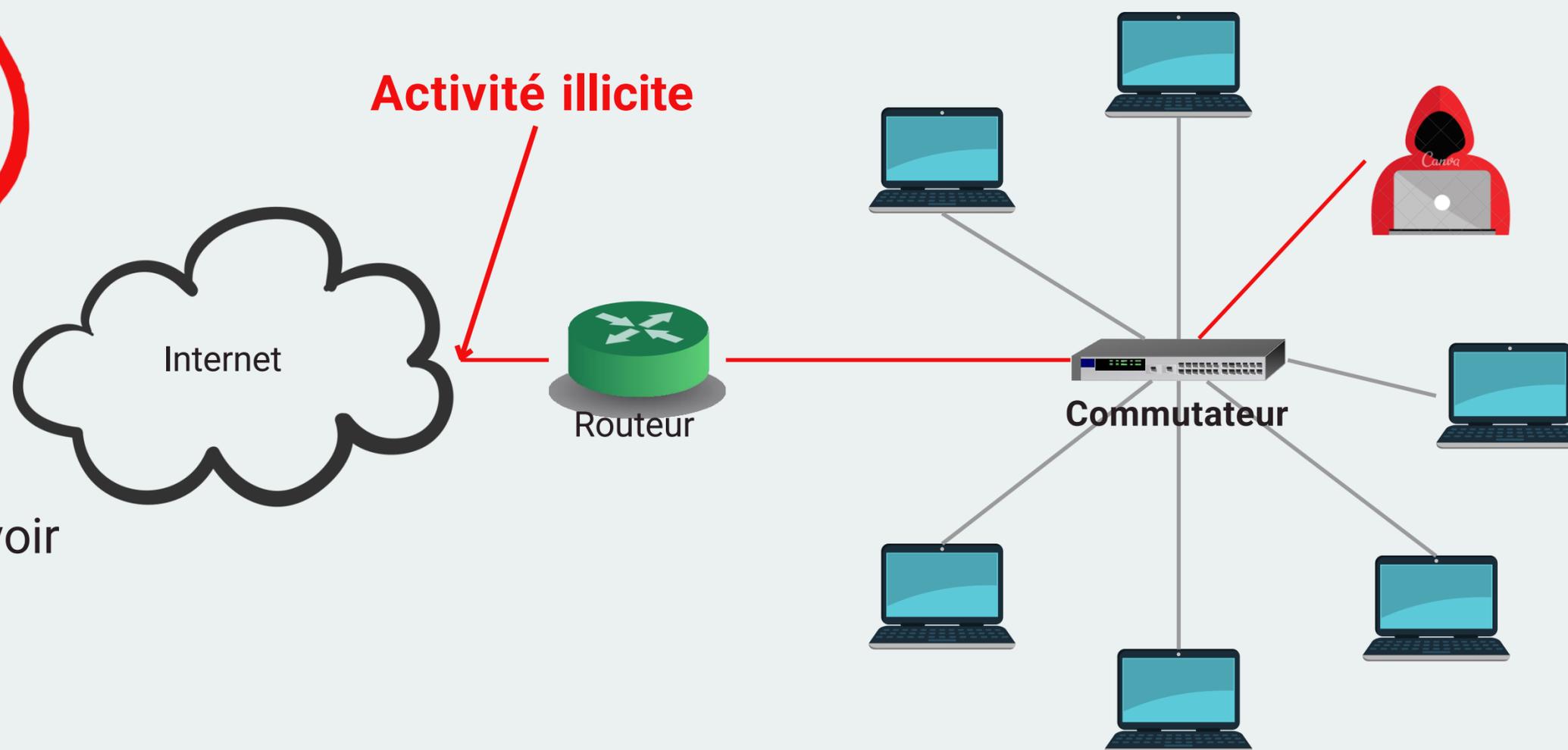
Pour la sécurité



PRÉLIMINAIRES

POURQUOI CONTRÔLER L'ACCÈS ?

Pour la législation

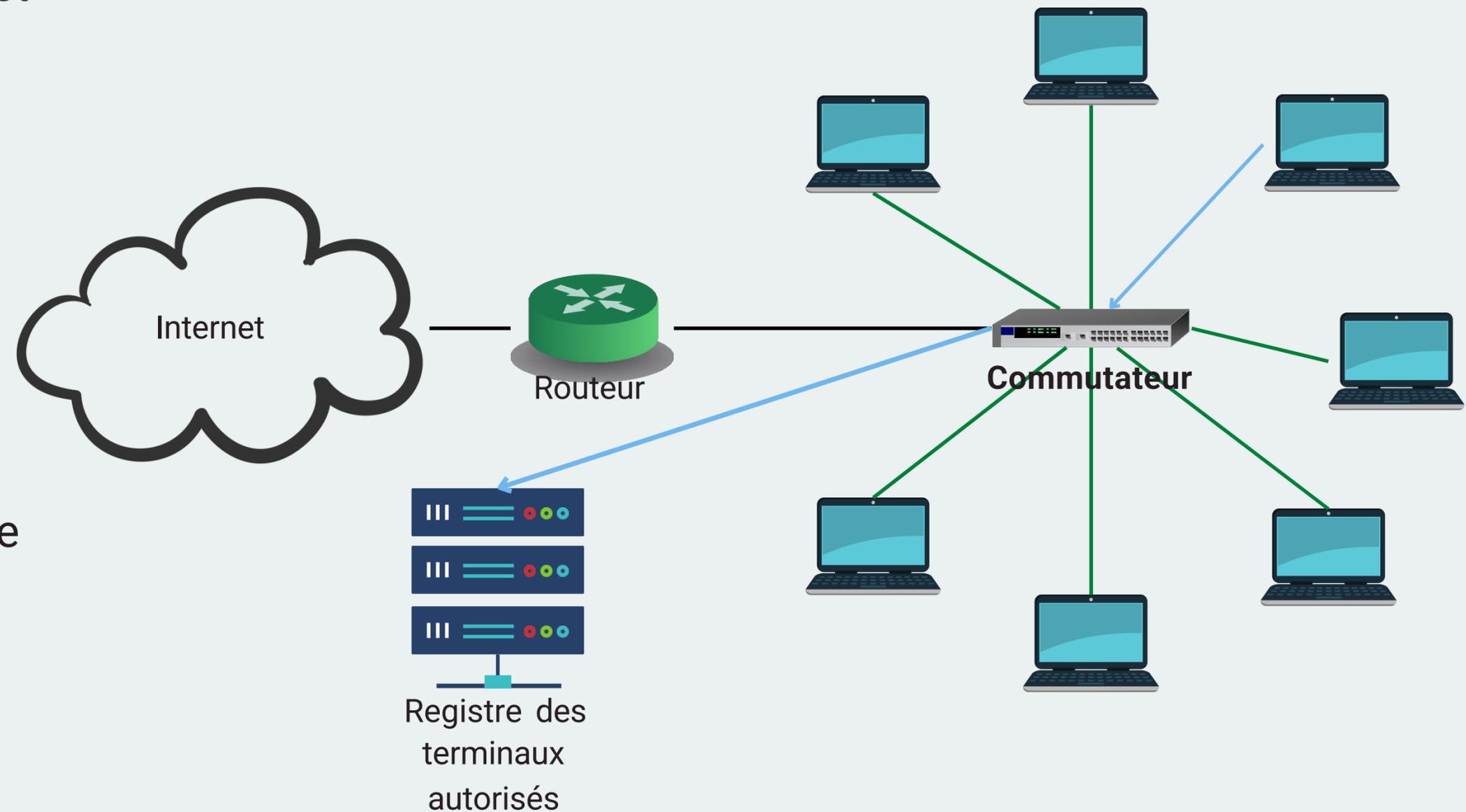


On doit être en mesure de savoir qui (**adresse + appareil**) s'est connecté et **quand** sous demande de la justice.

LE CONTRÔLE D'ACCÈS

DANS LES GRANDES LIGNES

On contrôle quel terminal est autorisé à se connecter au réseau.

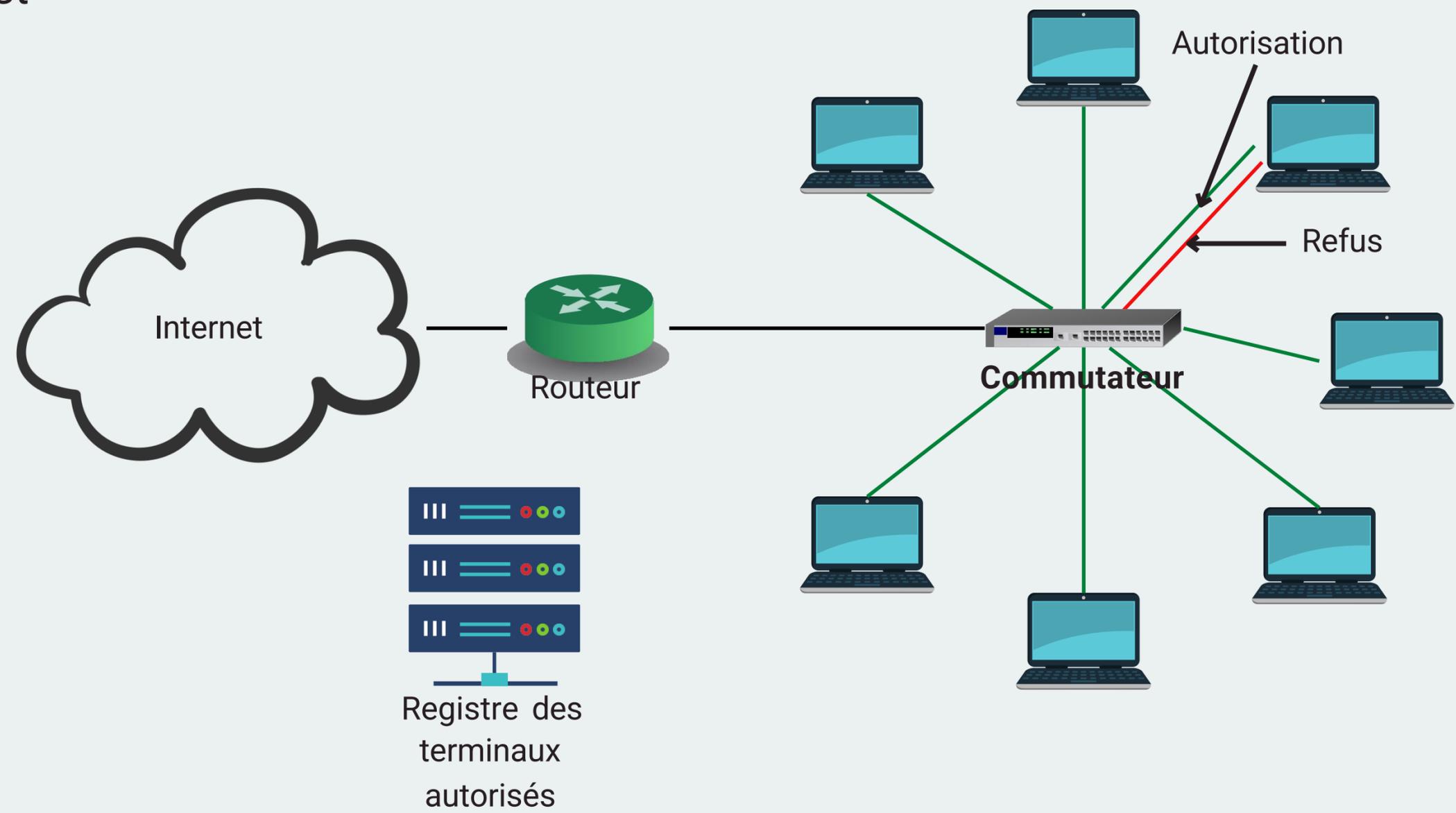


1ère étape : On regarde si le terminal est autorisé à se connecter

LE CONTRÔLE D'ACCÈS

DANS LES GRANDES LIGNES

On contrôle quel terminal est autorisé à se connecter au réseau.



2ème étape : On autorise / refuse la connexion

AUTHENTIFICATION

PROTOCOLE AAA

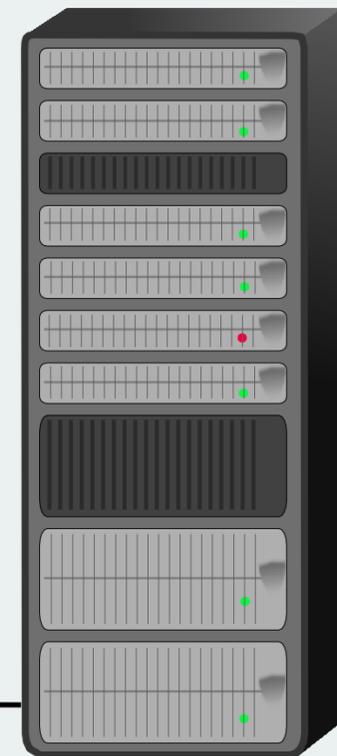
En général :

AAA = *Authentication, Authorization, Accounting* (Authentification, Autorisation et Traçabilité)

AAA désigne ainsi un type de protocole, qui remplit dans un réseau 802.1X ces trois fonctions.



Client



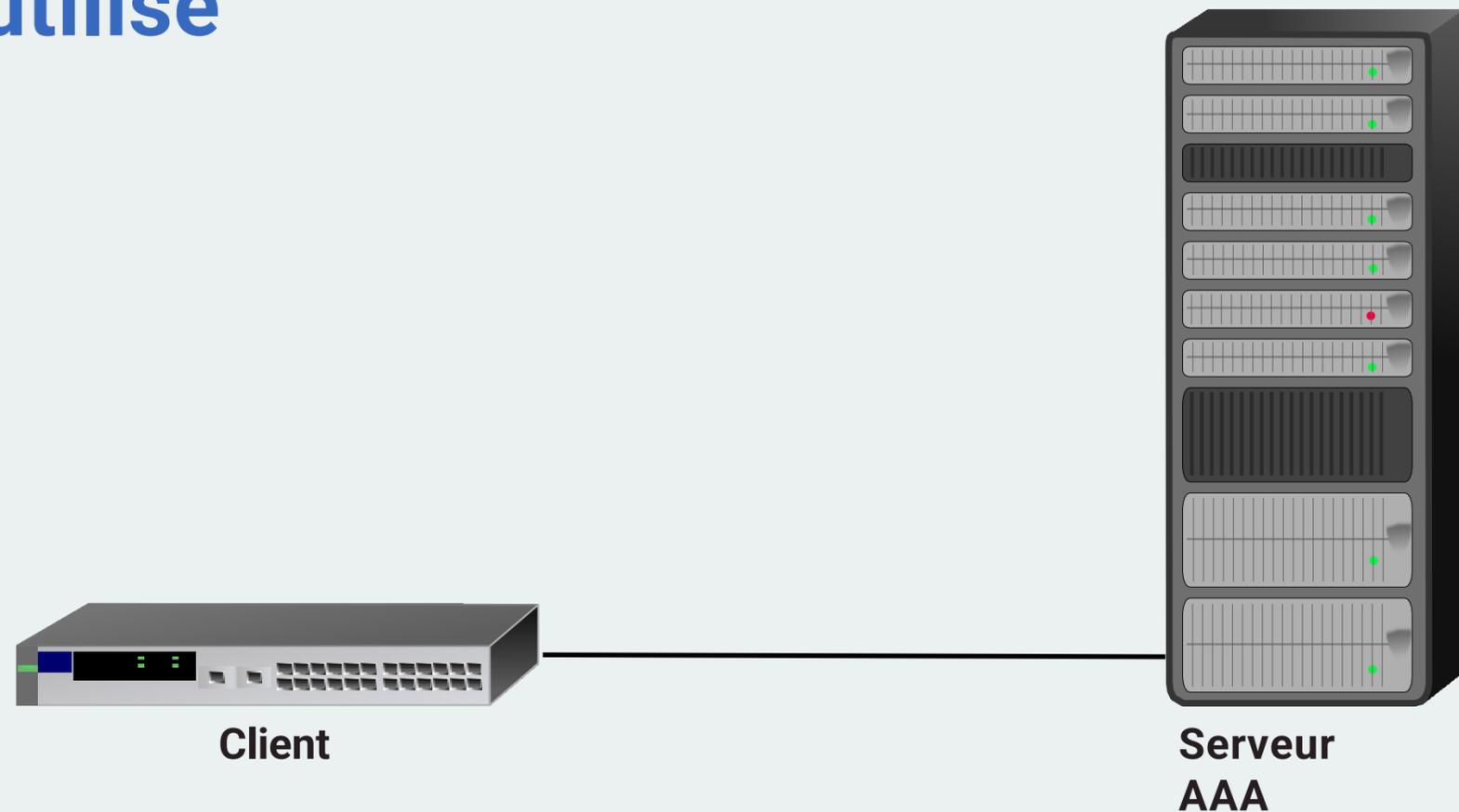
Serveur
AAA

AUTHENTIFICATION

PROTOCOLE RADIUS

**Radius = un protocole AAA
particulier, le plus utilisé**

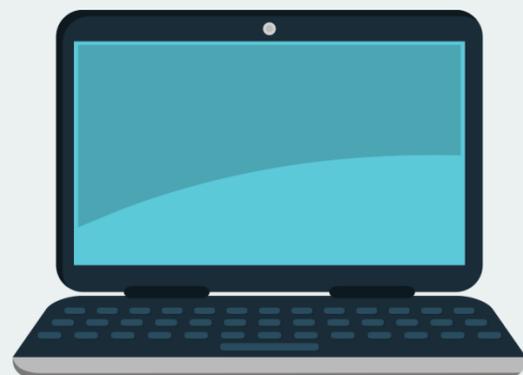
(il en existe 3 autres : Diameter, TACACS et TACACS+)



AUTHENTIFICATION

CONNEXION À UN RÉSEAU 802.1X

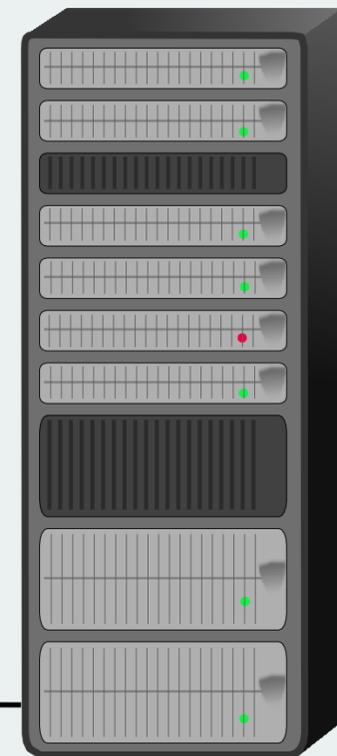
Au plus simple : un supplicant (utilisateur), un client (commutateur ou WLC) et un serveur AAA



Supplicant



Client



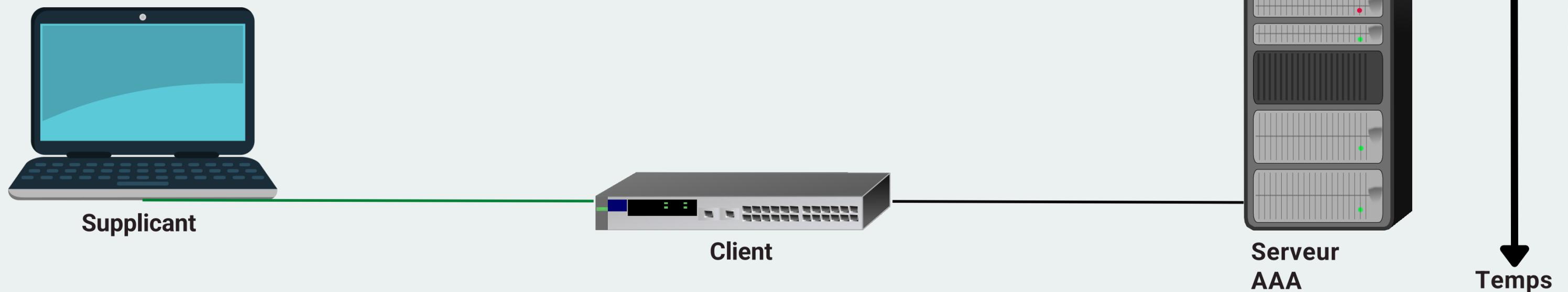
Serveur
AAA

AUTHENTIFICATION

CONNEXION À UN RÉSEAU 802.1X

Au plus simple : un supplicant (utilisateur), un client (commutateur ou WLC) et un serveur AAA

On branche le client au supplicant sur un port ayant un accès contrôlé

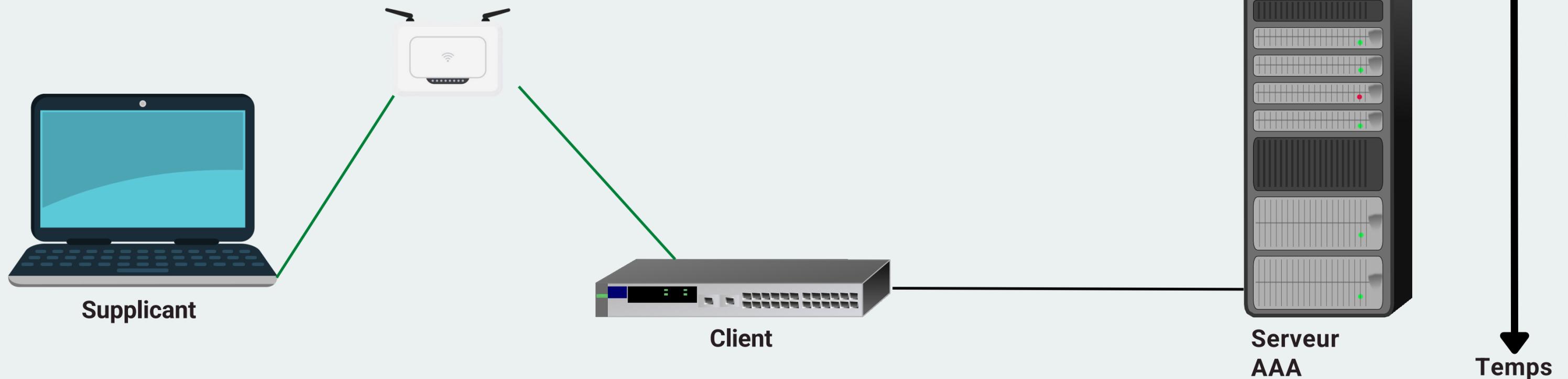


AUTHENTIFICATION

CONNEXION À UN RÉSEAU 802.1X

Au plus simple : un supplicant (utilisateur), un client (commutateur ou WLC) et un serveur AAA

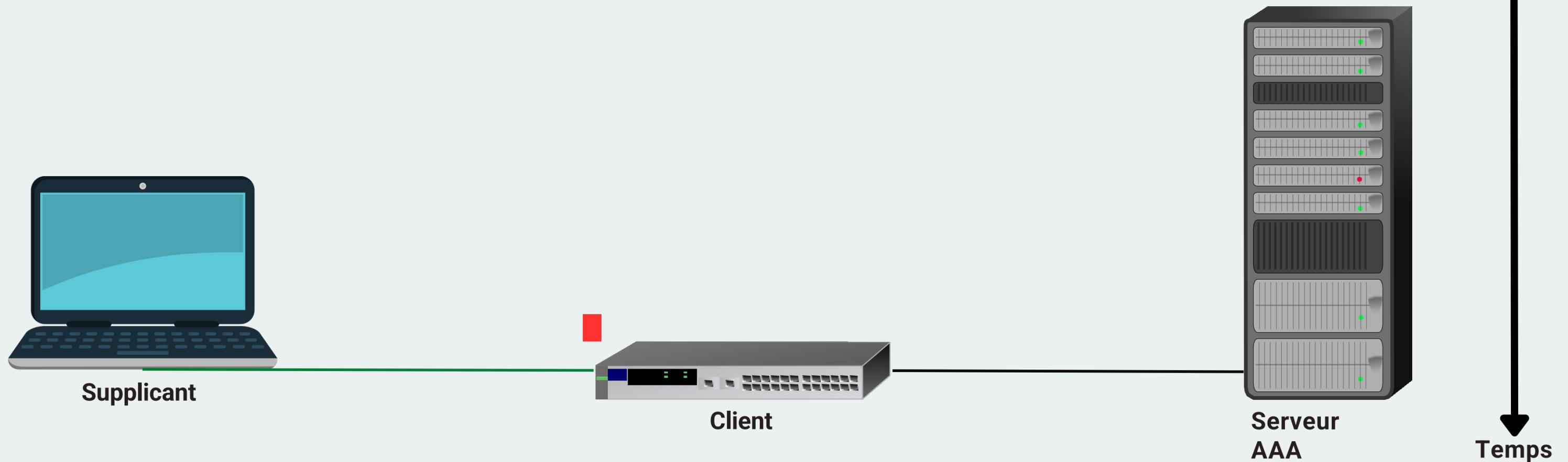
On branche le client au supplicant sur un port ayant un accès contrôlé



AUTHENTIFICATION

CONNEXION À UN RÉSEAU 802.1X

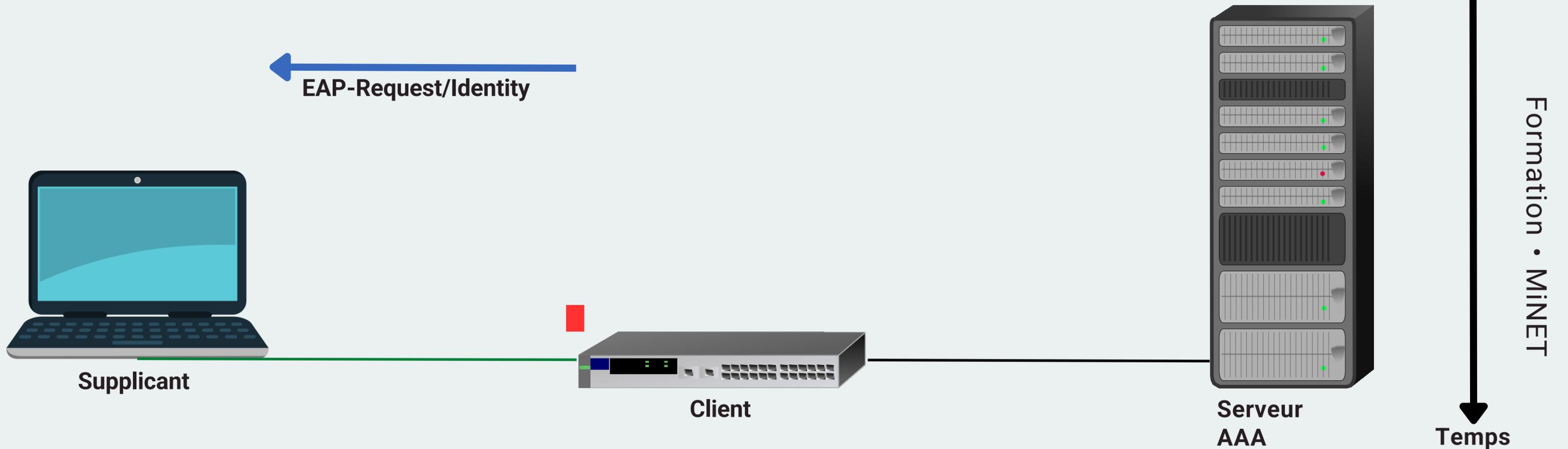
1 - Initialisation



AUTHENTIFICATION

CONNEXION À UN RÉSEAU 802.1X

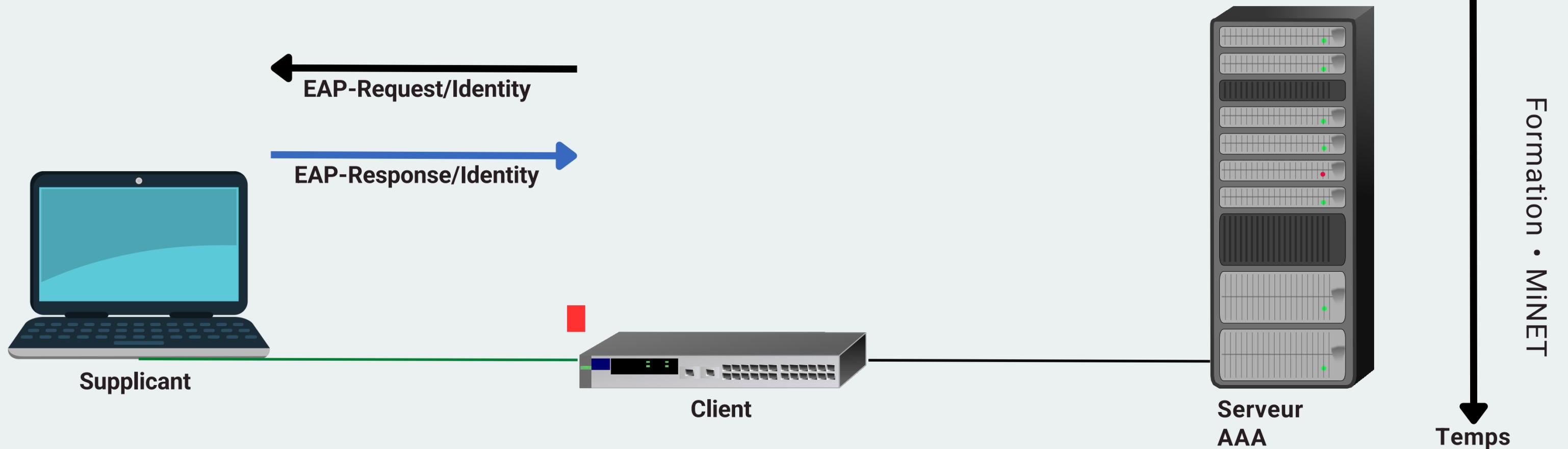
- 1 - Initialisation
- 2 - Identification



AUTHENTIFICATION

CONNEXION À UN RÉSEAU 802.1X

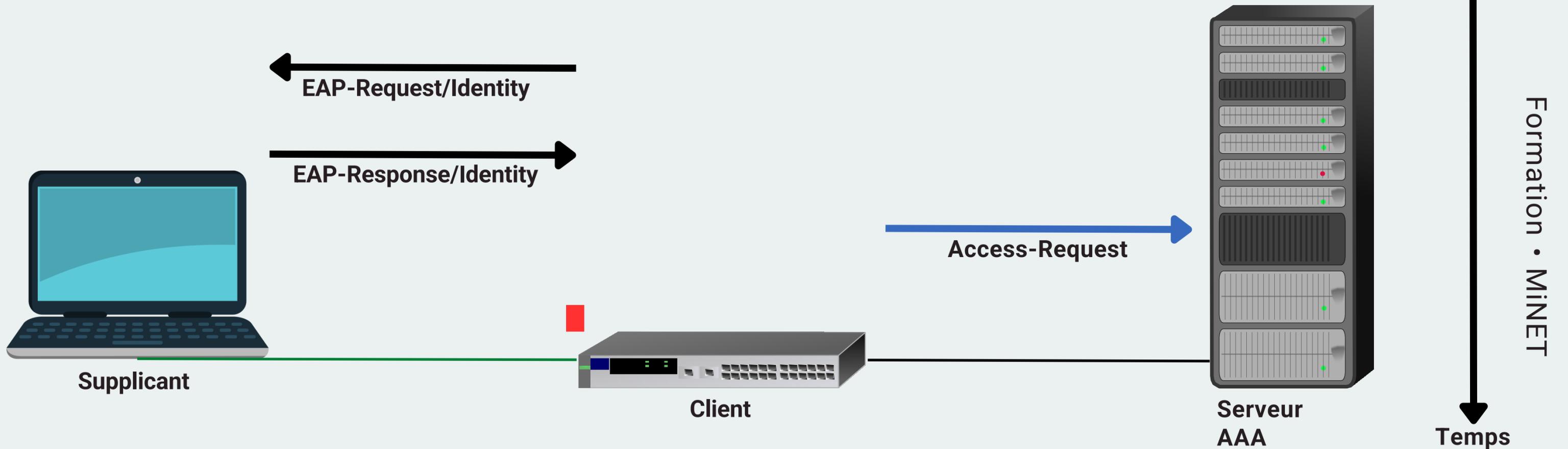
- 1 - Initialisation
- 2 - Identification



AUTHENTIFICATION

CONNEXION À UN RÉSEAU 802.1X

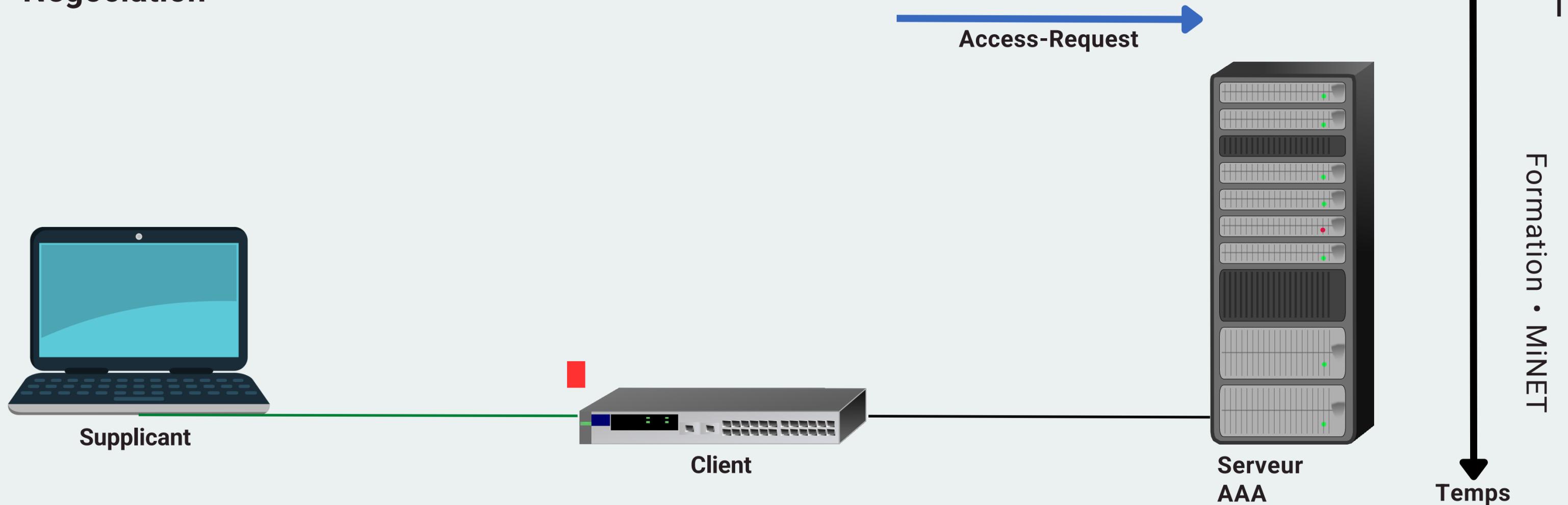
- 1 - Initialisation
- 2 - Identification



AUTHENTIFICATION

CONNEXION À UN RÉSEAU 802.1X

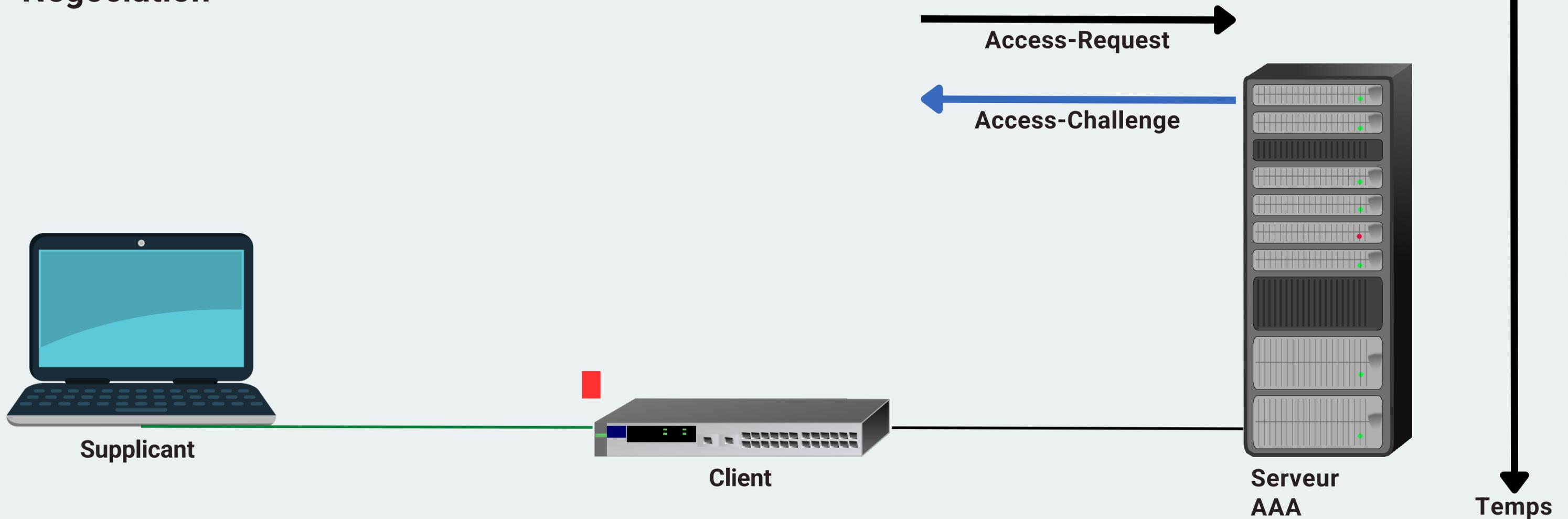
- 1 - Initialisation
- 2 - Identification
- 3 - **Négociation**



AUTHENTIFICATION

CONNEXION À UN RÉSEAU 802.1X

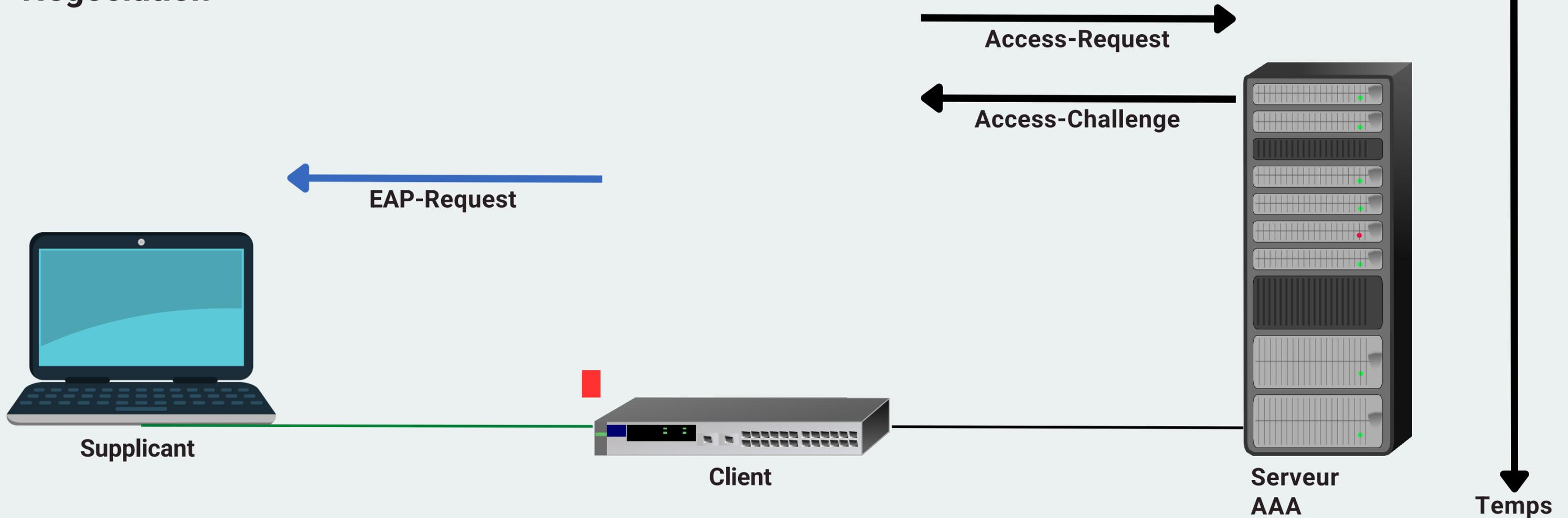
- 1 - Initialisation
- 2 - Identification
- 3 - **Négociation**



AUTHENTIFICATION

CONNEXION À UN RÉSEAU 802.1X

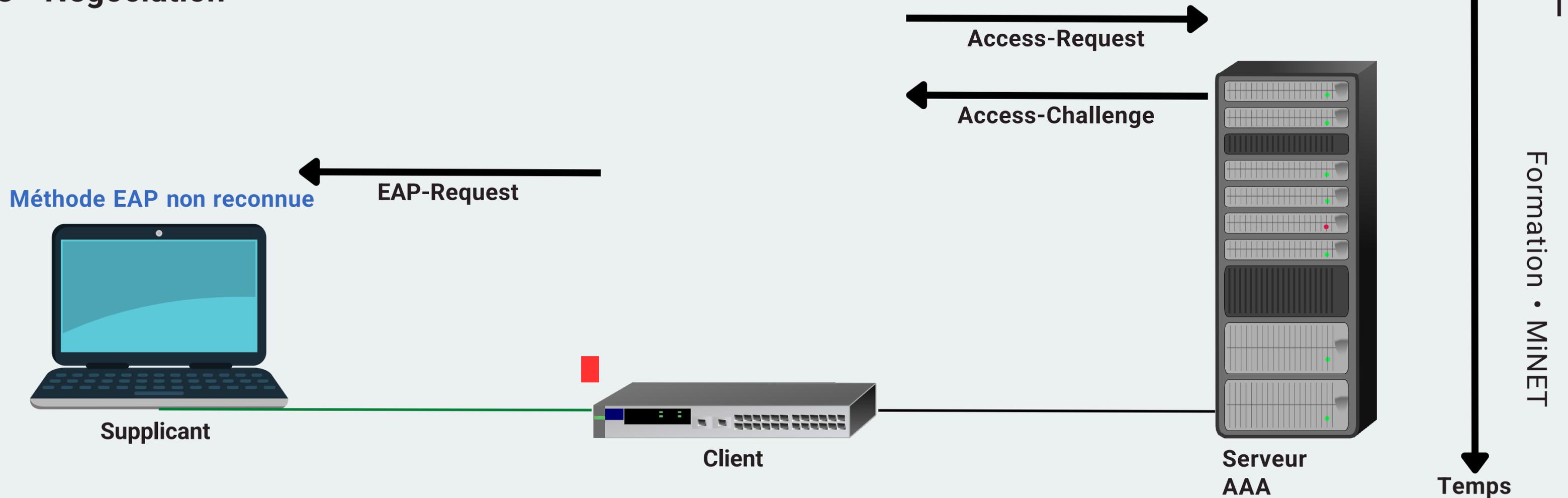
- 1 - Initialisation
- 2 - Identification
- 3 - **Négociation**



AUTHENTIFICATION

CONNEXION À UN RÉSEAU 802.1X

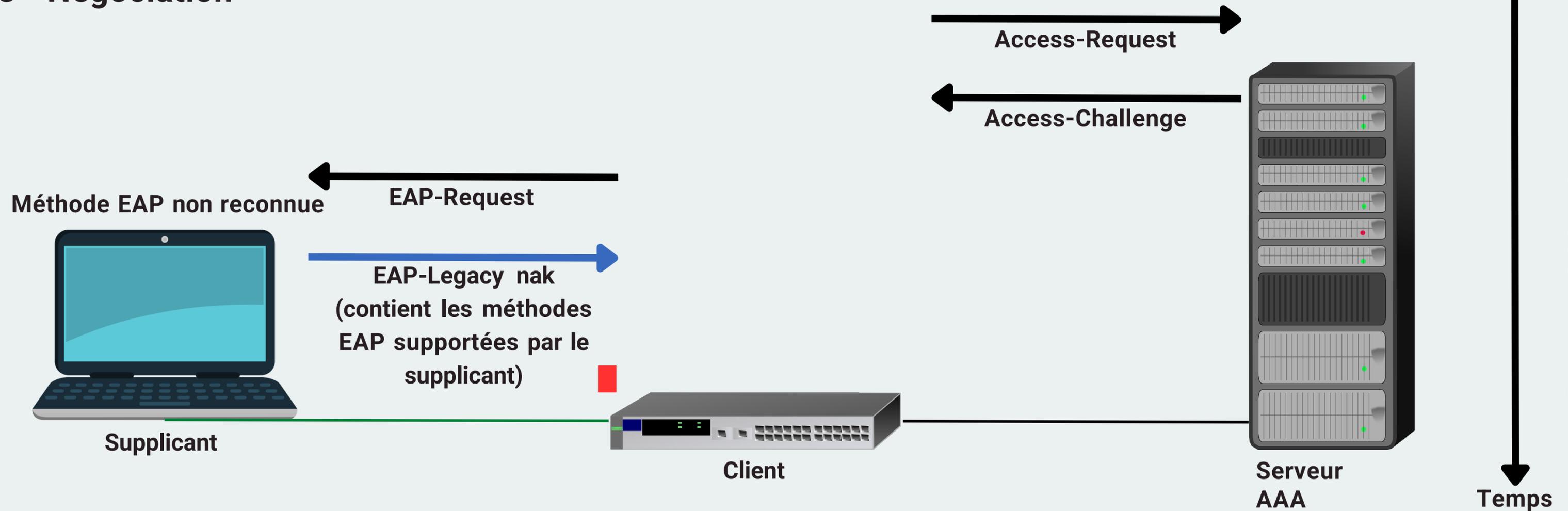
- 1 - Initialisation
- 2 - Identification
- 3 - **Négociation**



AUTHENTIFICATION

CONNEXION À UN RÉSEAU 802.1X

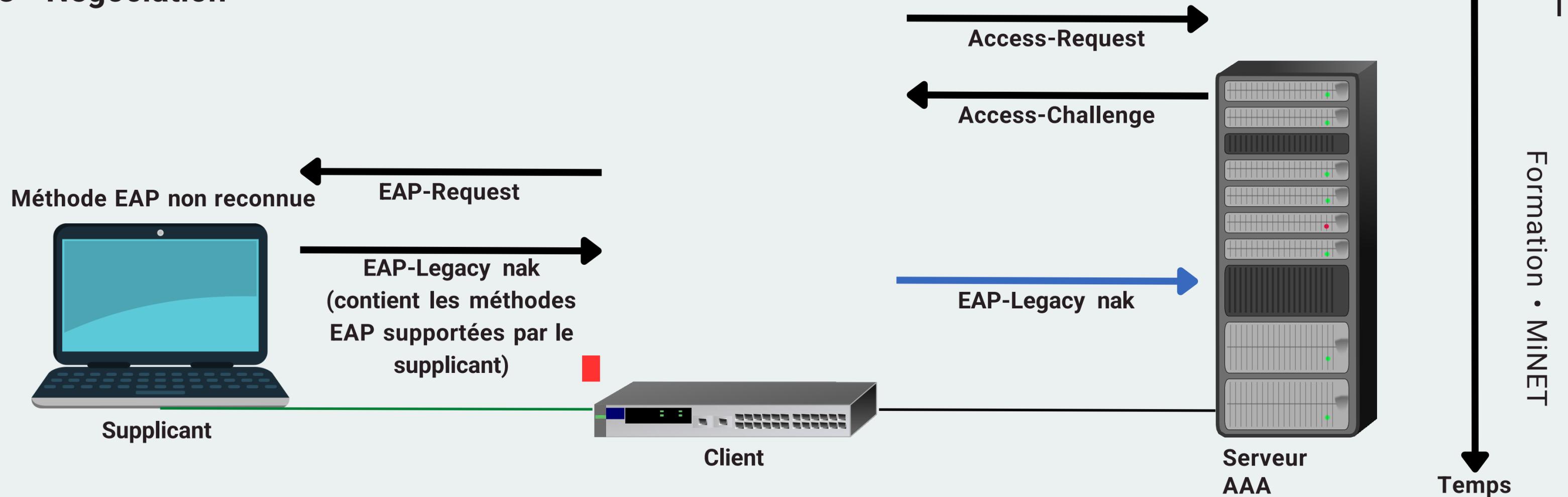
- 1 - Initialisation
- 2 - Identification
- 3 - **Négociation**



AUTHENTIFICATION

CONNEXION À UN RÉSEAU 802.1X

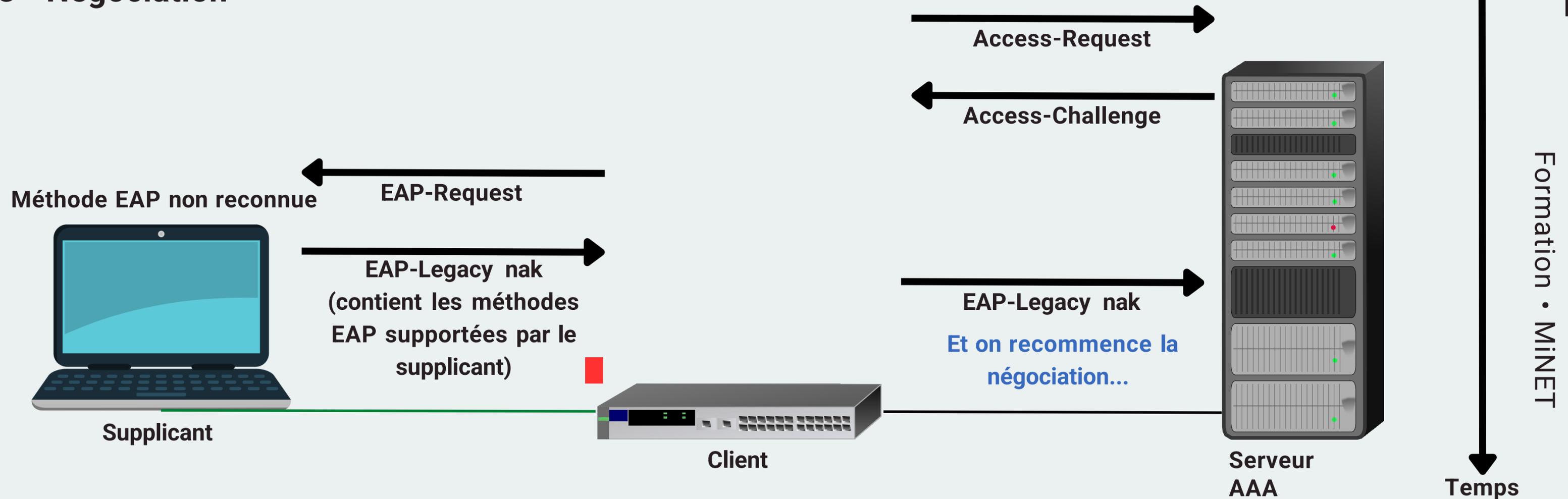
- 1 - Initialisation
- 2 - Identification
- 3 - **Négociation**



AUTHENTIFICATION

CONNEXION À UN RÉSEAU 802.1X

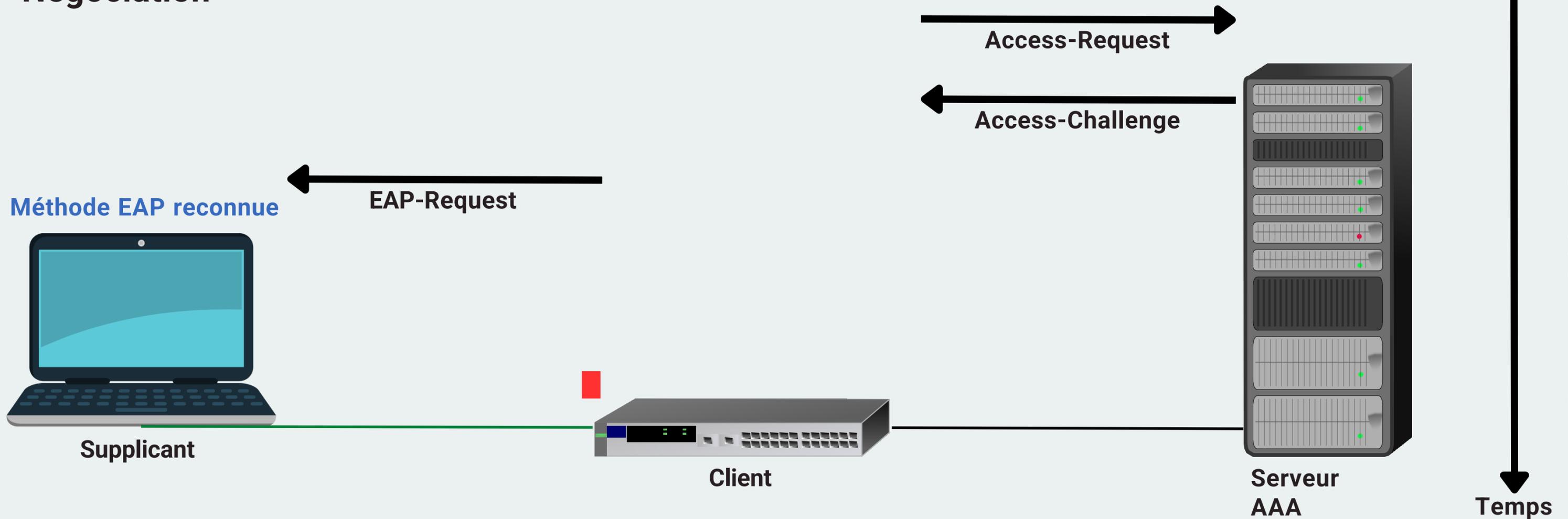
- 1 - Initialisation
- 2 - Identification
- 3 - **Négociation**



AUTHENTIFICATION

CONNEXION À UN RÉSEAU 802.1X

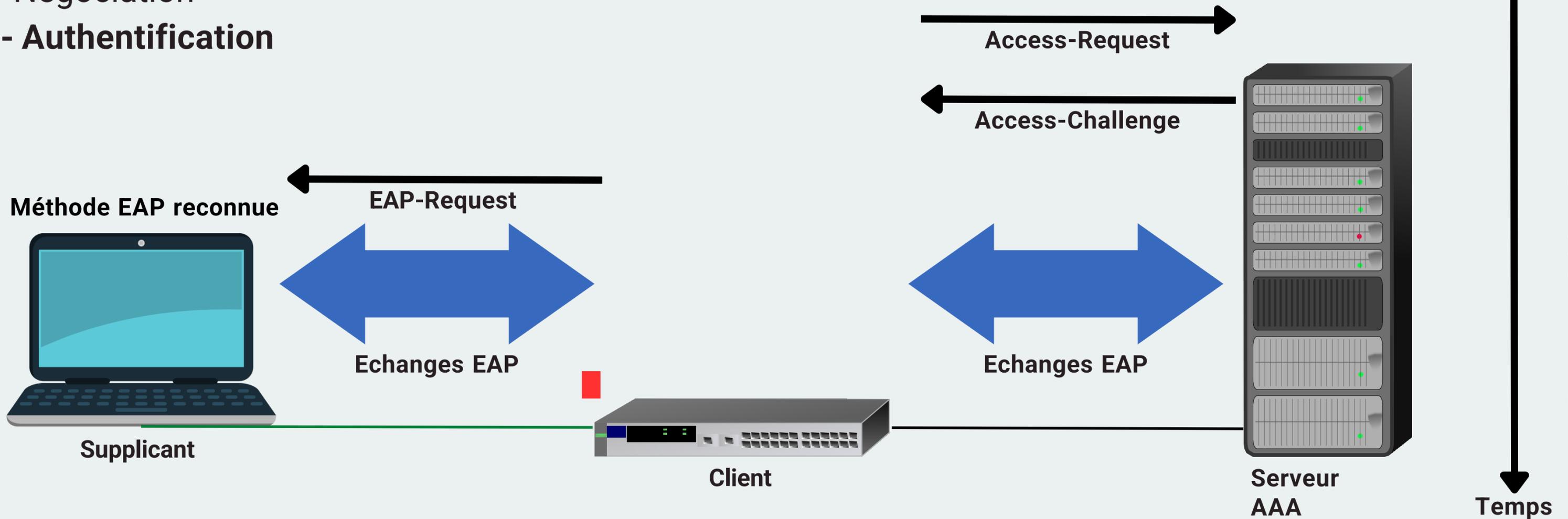
- 1 - Initialisation
- 2 - Identification
- 3 - **Négociation**



AUTHENTIFICATION

CONNEXION À UN RÉSEAU 802.1X

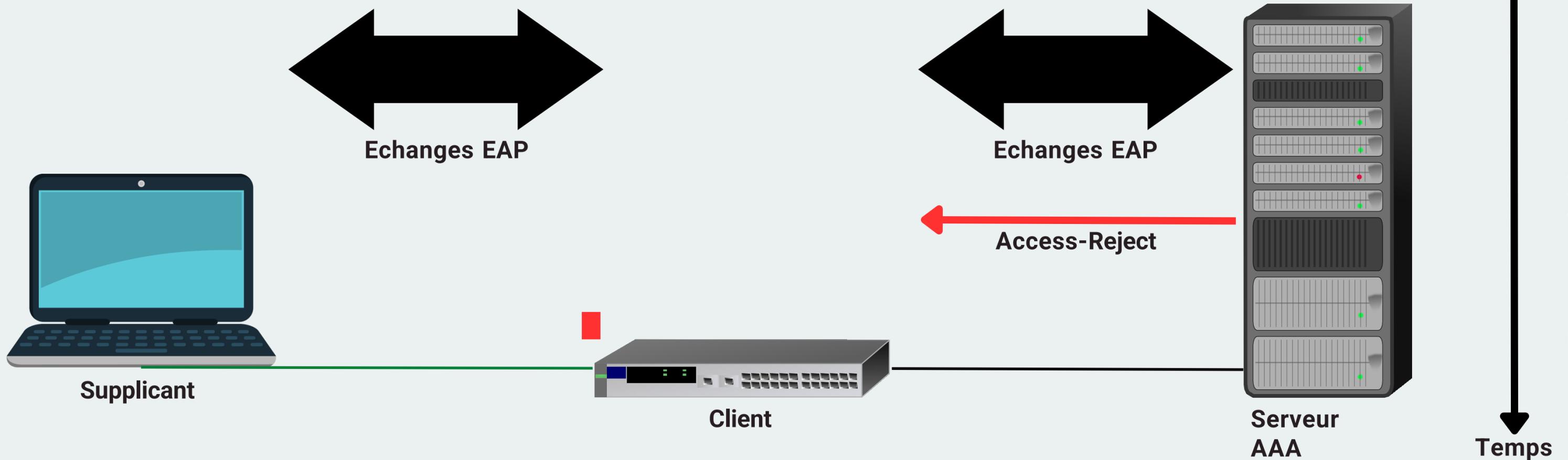
- 1 - Initialisation
- 2 - Identification
- 3 - Négociation
- 4 - **Authentification**



AUTHENTIFICATION

CONNEXION À UN RÉSEAU 802.1X

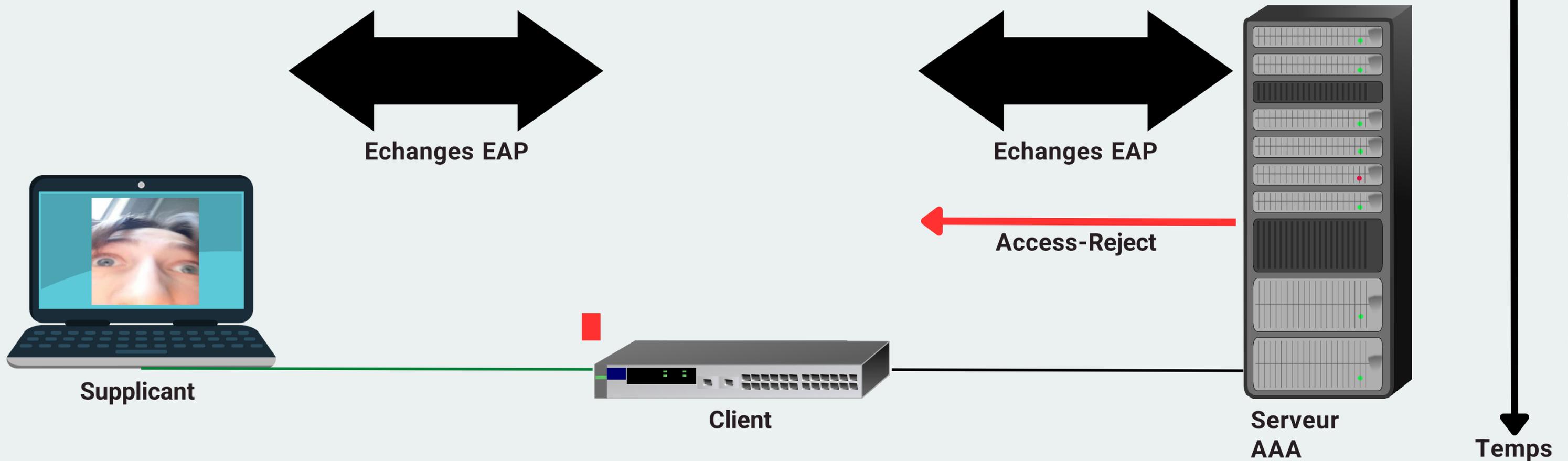
- 1 - Initialisation
- 2 - Identification
- 3 - Négociation
- 4 - Authentification**



AUTHENTIFICATION

CONNEXION À UN RÉSEAU 802.1X

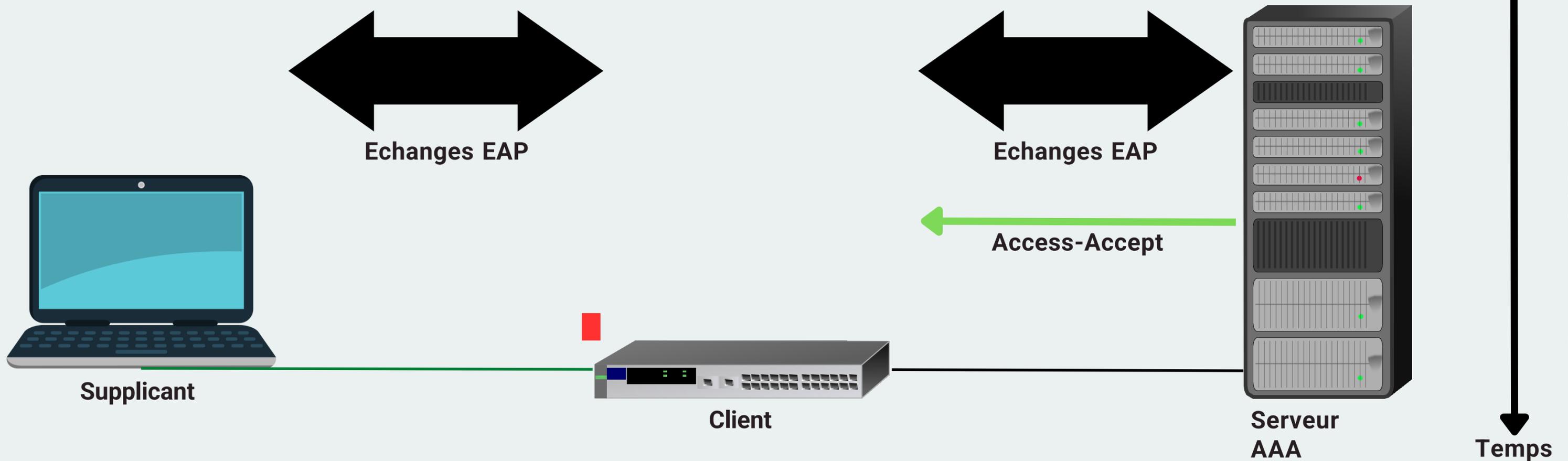
- 1 - Initialisation
- 2 - Identification
- 3 - Négociation
- 4 - **Authentification**



AUTHENTIFICATION

CONNEXION À UN RÉSEAU 802.1X

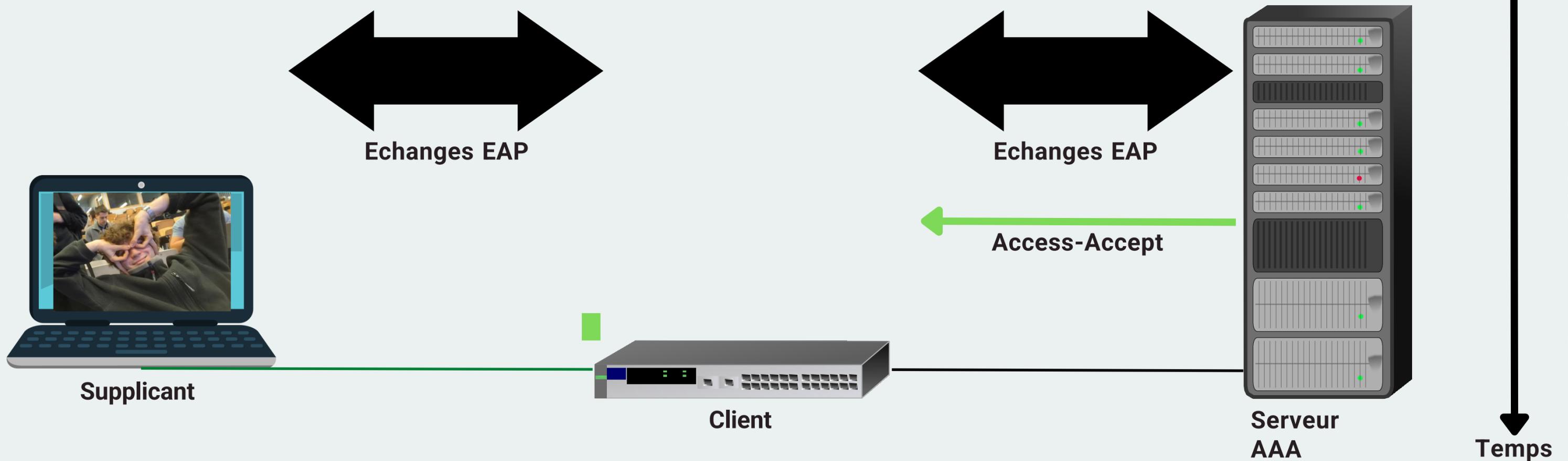
- 1 - Initialisation
- 2 - Identification
- 3 - Négociation
- 4 - Authentification**



AUTHENTIFICATION

CONNEXION À UN RÉSEAU 802.1X

- 1 - Initialisation
- 2 - Identification
- 3 - Négociation
- 4 - Authentification

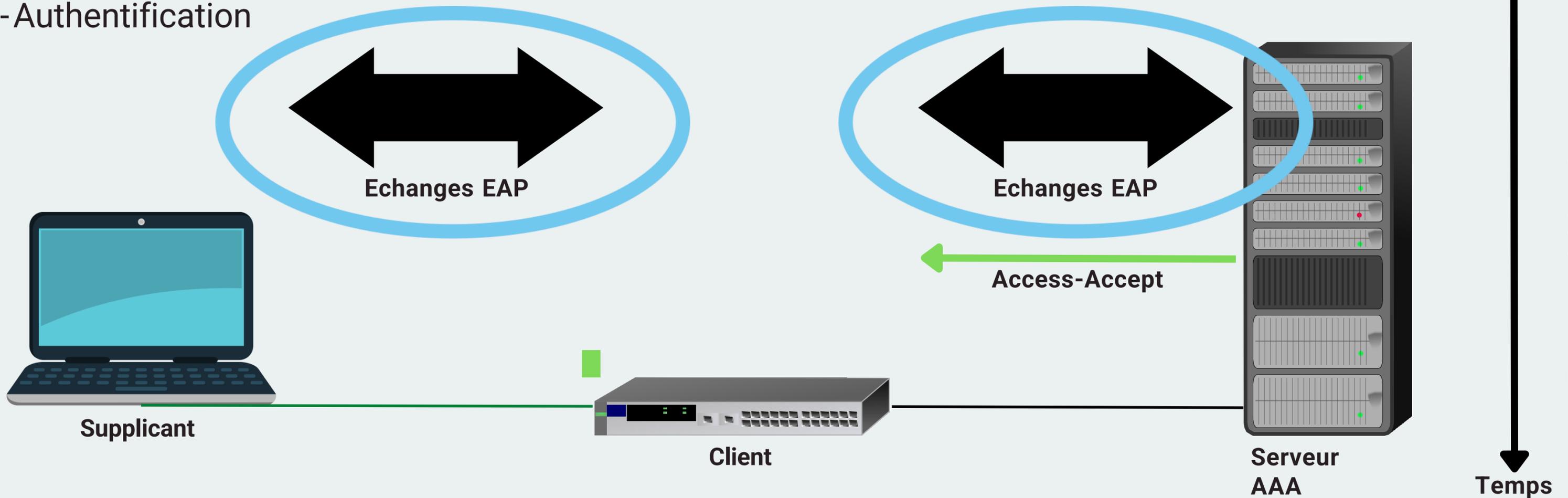


AUTHENTIFICATION

CONNEXION À UN RÉSEAU 802.1X

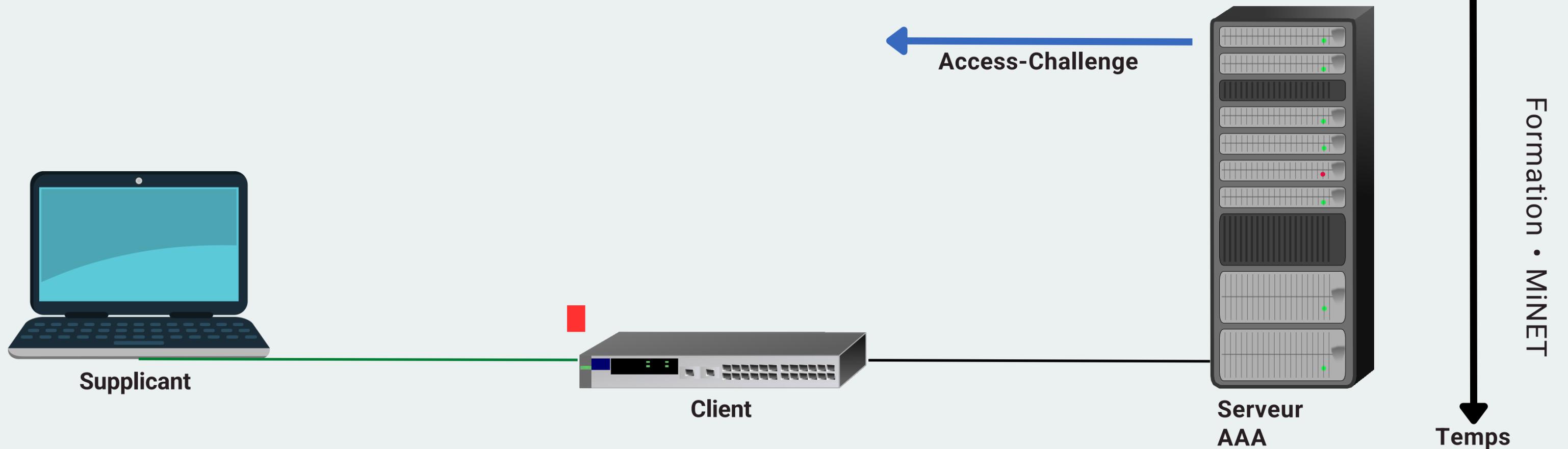
- 1 - Initialisation
- 2 - Identification
- 3 - Négociation
- 4 - Authentification

C'est quoi ?



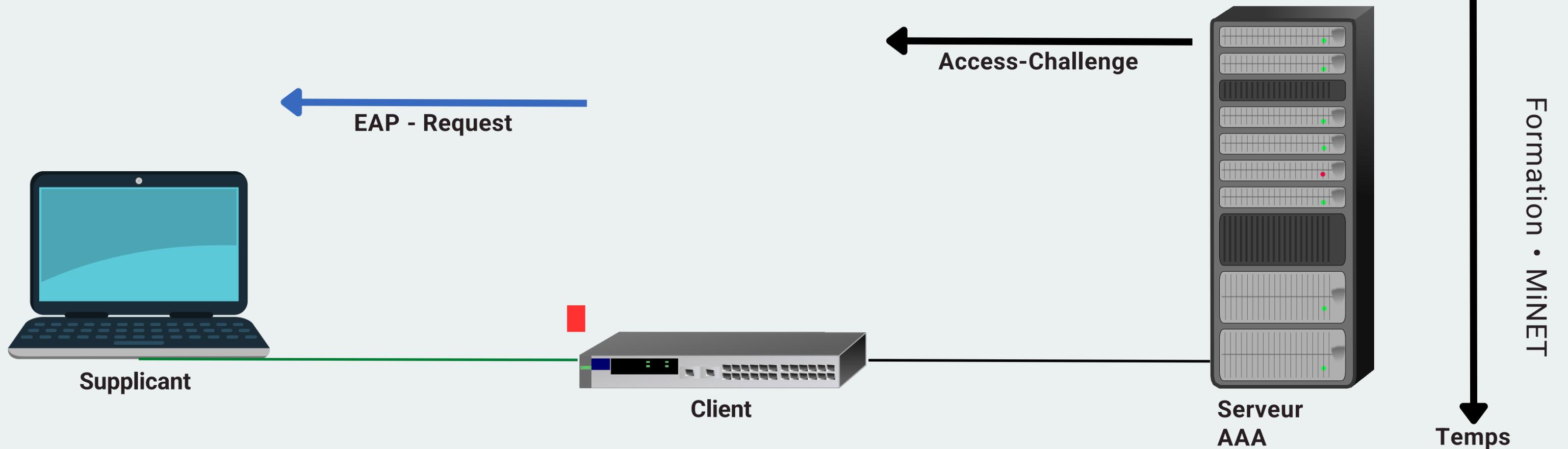
AUTHENTICATION

LE PROTOCOLE EAP-MD5



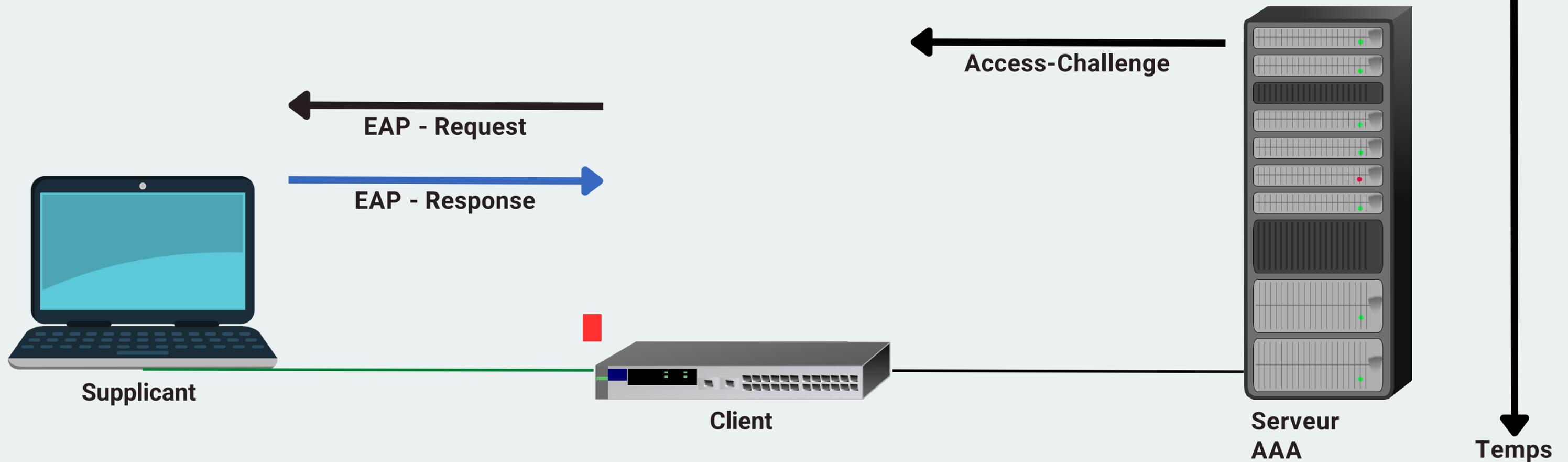
AUTHENTICATION

LE PROTOCOLE EAP-MD5



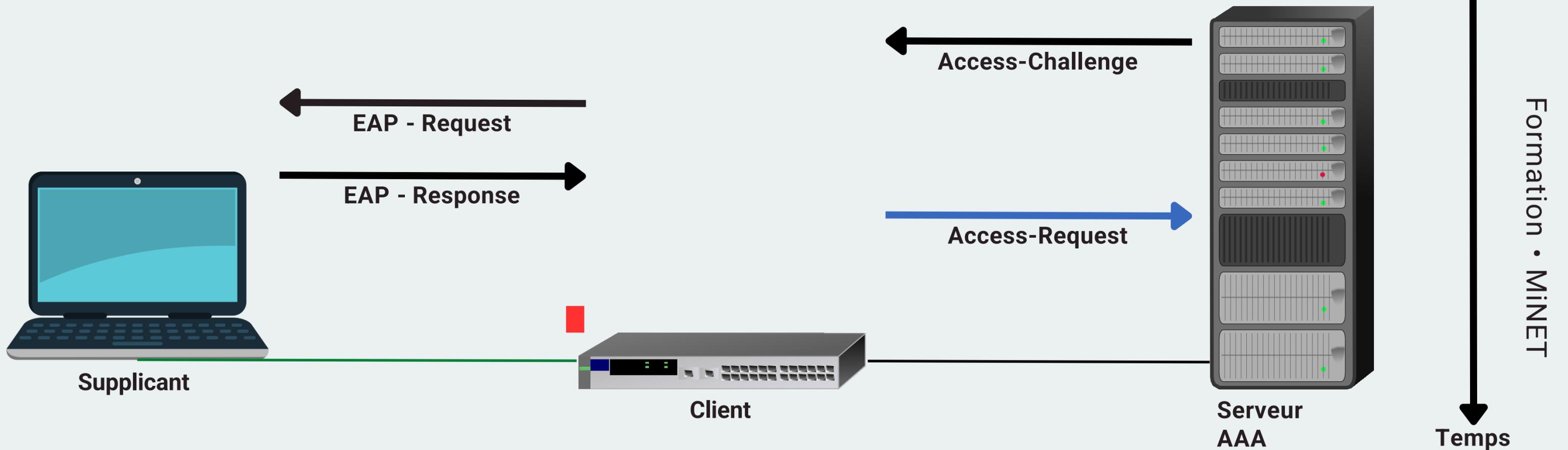
AUTHENTICATION

LE PROTOCOLE EAP-MD5



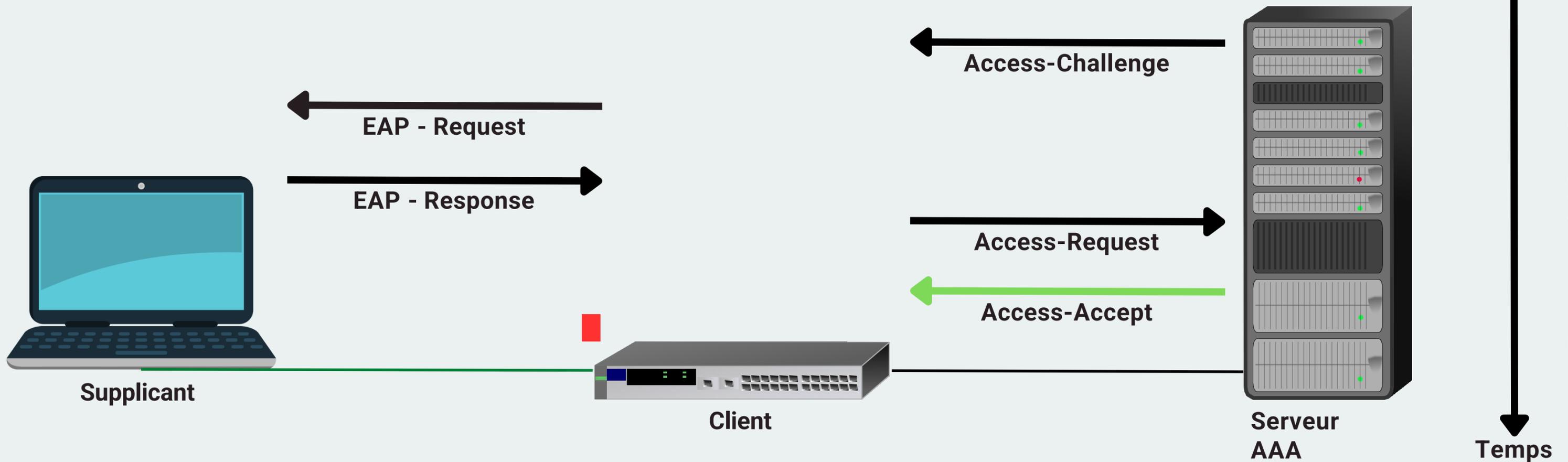
AUTHENTICATION

LE PROTOCOLE EAP-MD5



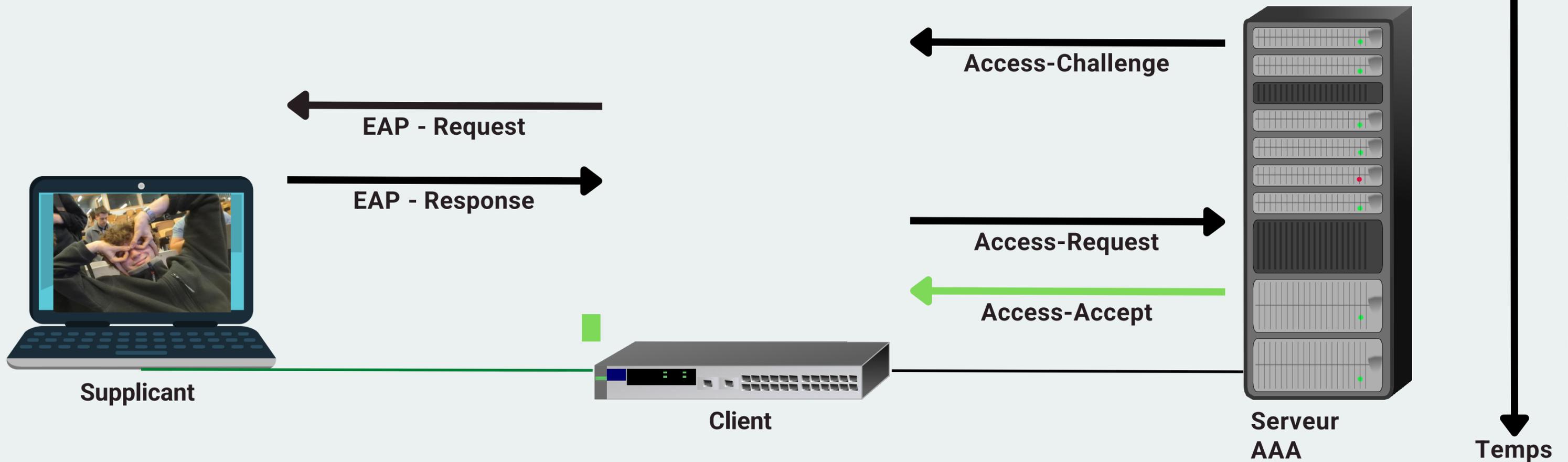
AUTHENTICATION

LE PROTOCOLE EAP-MD5



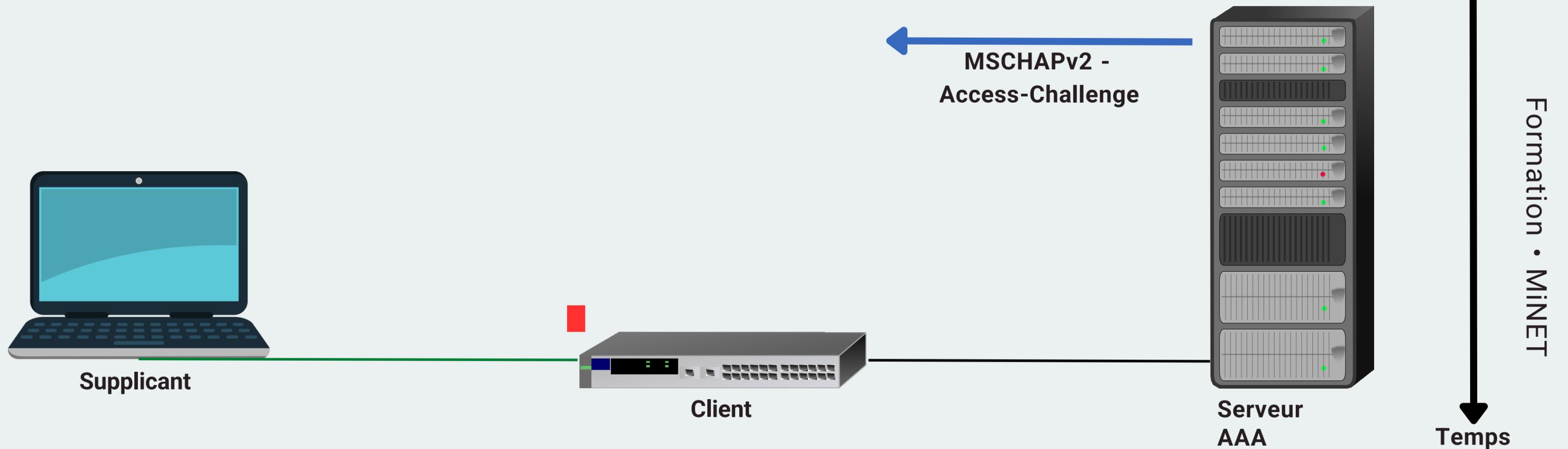
AUTHENTICATION

LE PROTOCOLE EAP-MD5



AUTHENTICATION

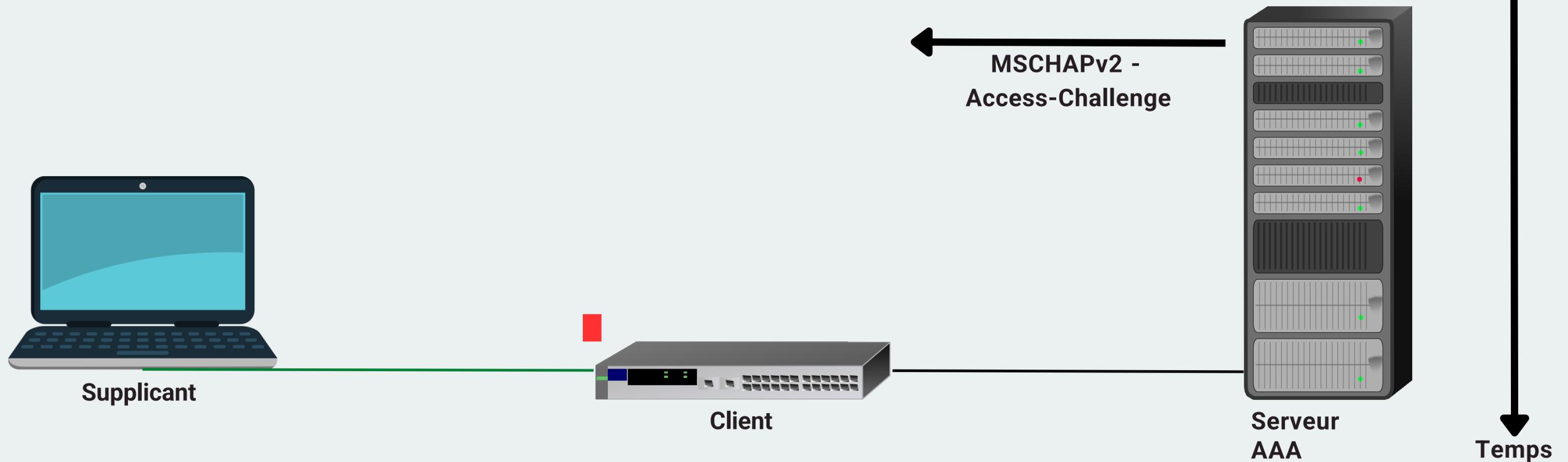
LE PROTOCOLE EAP-MSCHAPV2



AUTHENTIFICATION

LE PROTOCOLE EAP-MSCHAPV2

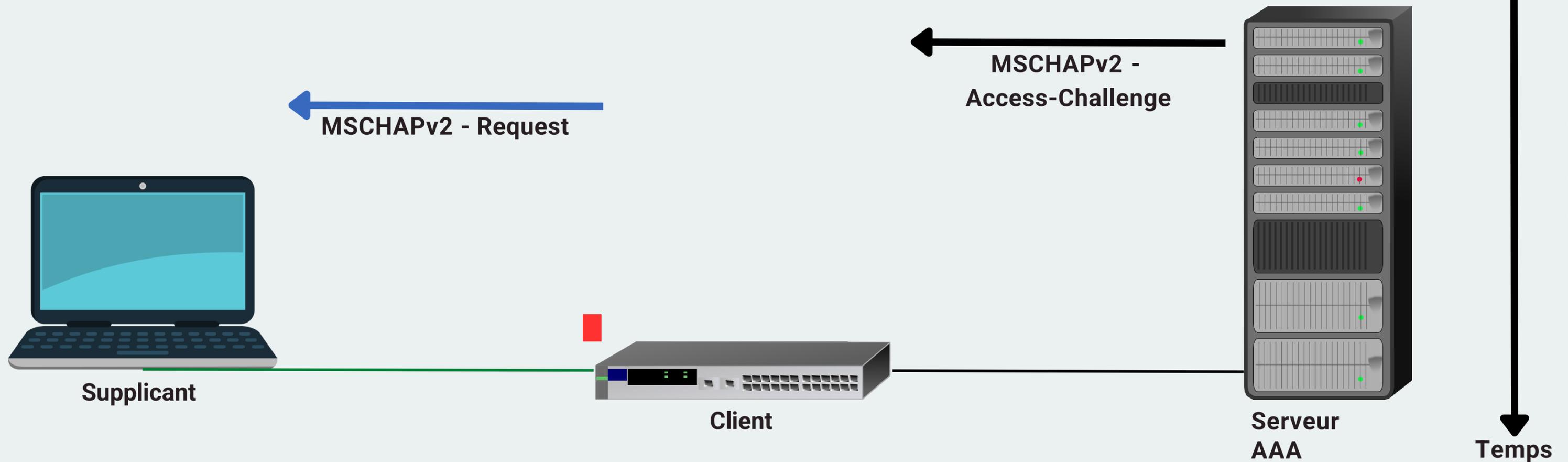
Le défi est un nombre généré aléatoirement.
À partir de ce défi et de son mot de passe,
le correspondant effectue des calculs.
Le résultat est envoyé à l'authentificateur.



AUTHENTIFICATION

LE PROTOCOLE EAP-MSCHAPV2

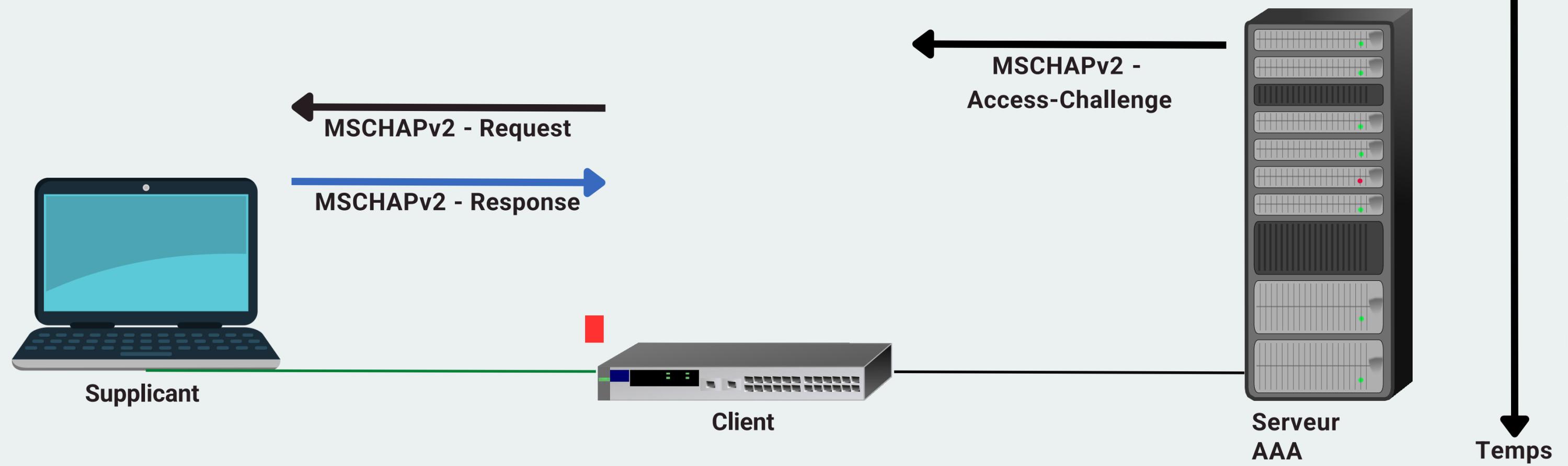
Le défi est un nombre généré aléatoirement.
À partir de ce défi et de son mot de passe,
le correspondant effectue des calculs.
Le résultat est envoyé à l'authentificateur.



AUTHENTIFICATION

LE PROTOCOLE EAP-MSCHAPV2

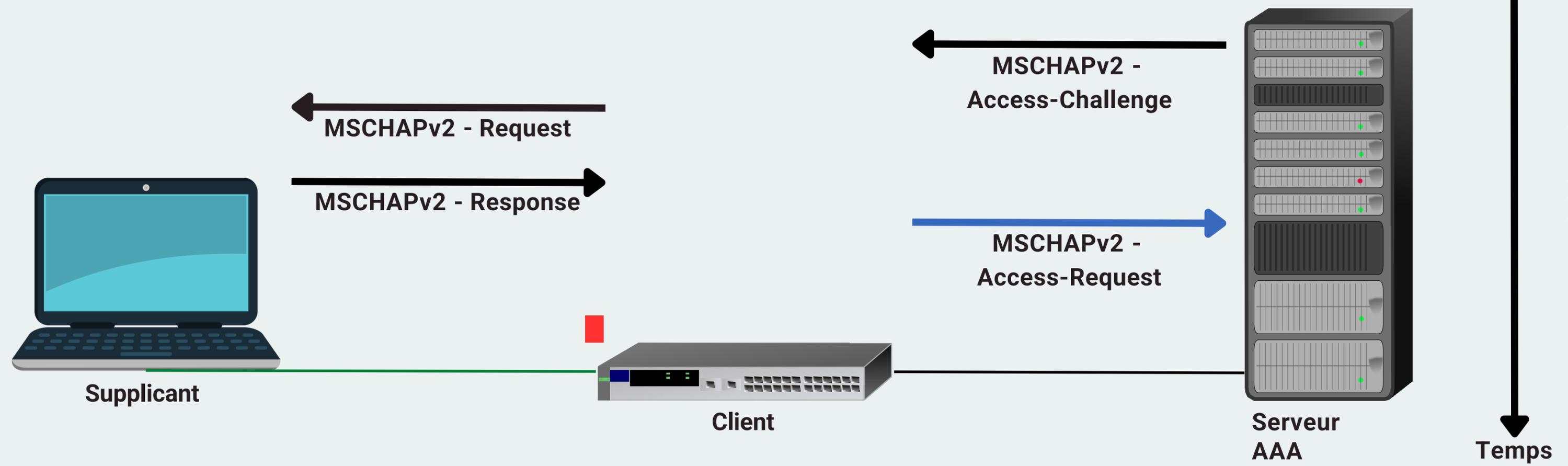
Le défi est un nombre généré aléatoirement.
À partir de ce défi et de son mot de passe,
le correspondant effectue des calculs.
Le résultat est envoyé à l'authentificateur.



AUTHENTIFICATION

LE PROTOCOLE EAP-MSCHAPV2

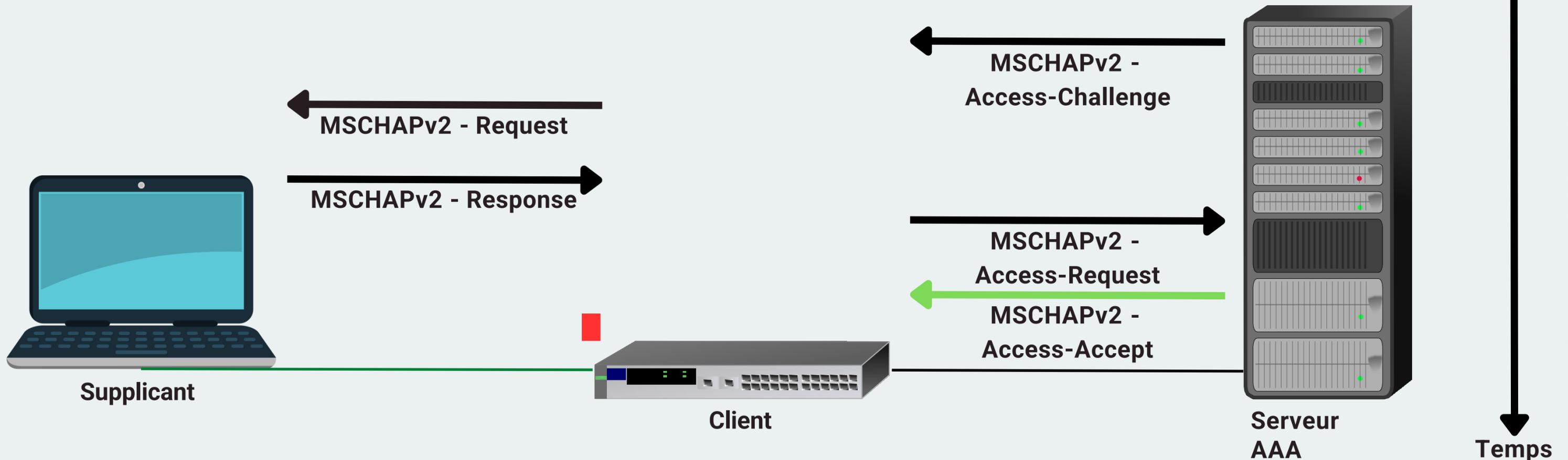
Le défi est un nombre généré aléatoirement.
À partir de ce défi et de son mot de passe,
le correspondant effectue des calculs.
Le résultat est envoyé à l'authentificateur.



AUTHENTIFICATION

LE PROTOCOLE EAP-MSCHAPV2

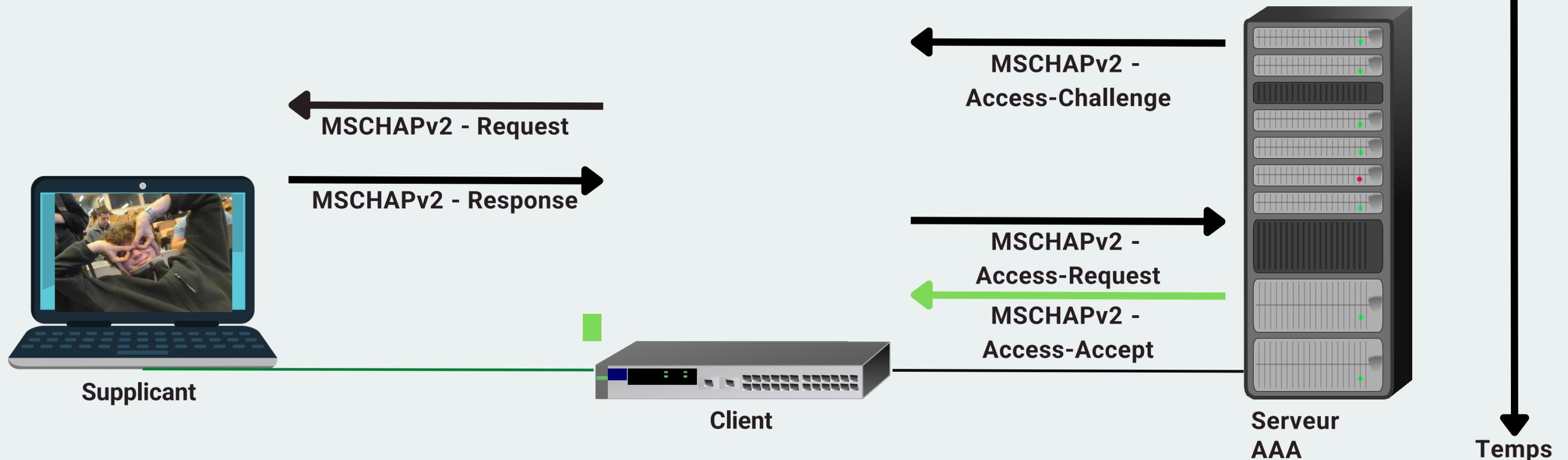
Le défi est un nombre généré aléatoirement.
À partir de ce défi et de son mot de passe,
le correspondant effectue des calculs.
Le résultat est envoyé à l'authentificateur.



AUTHENTIFICATION

LE PROTOCOLE EAP-MSCHAPV2

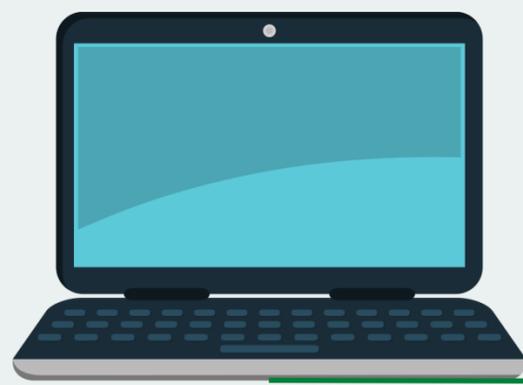
Le défi est un nombre généré aléatoirement.
À partir de ce défi et de son mot de passe,
le correspondant effectue des calculs.
Le résultat est envoyé à l'authentificateur.



AUTHENTICATION

LE PROTOCOLE EAP-TLS

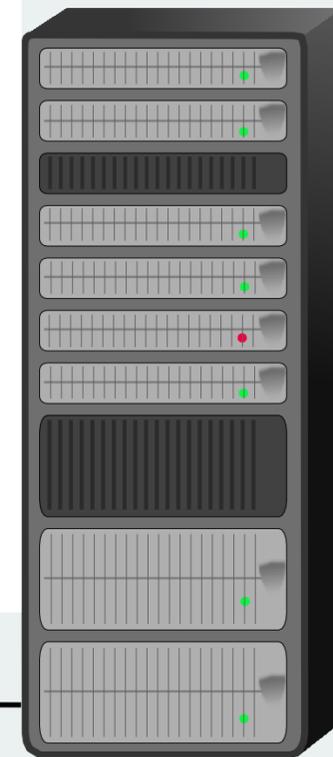
1 - Création/échange certificats



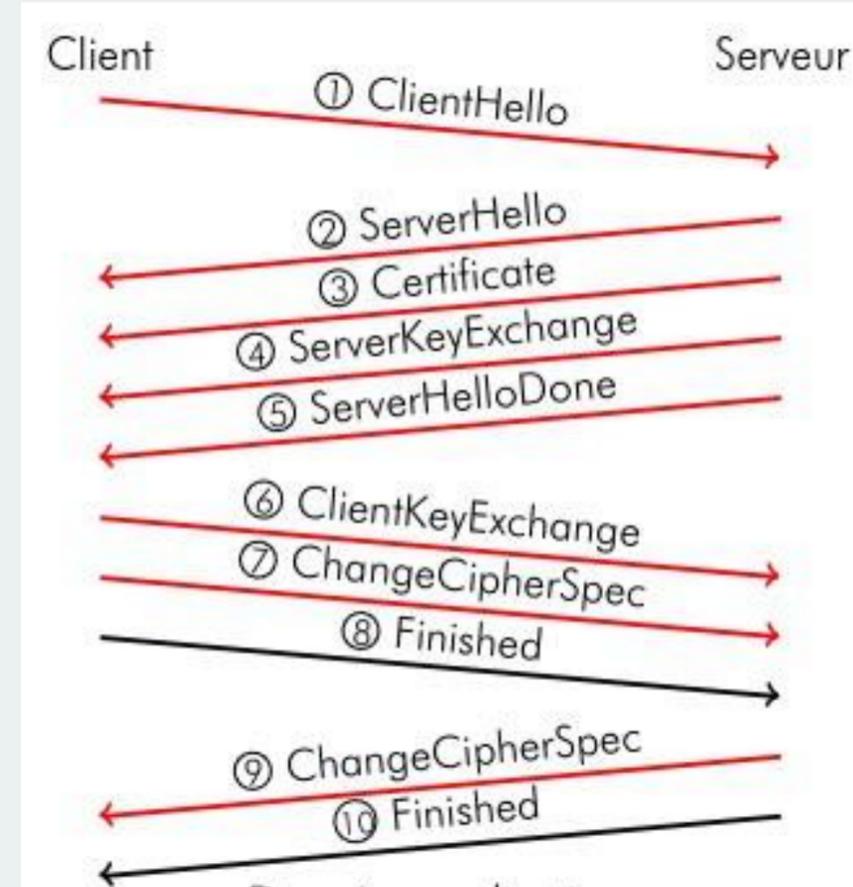
Supplicant



Client



Serveur
AAA

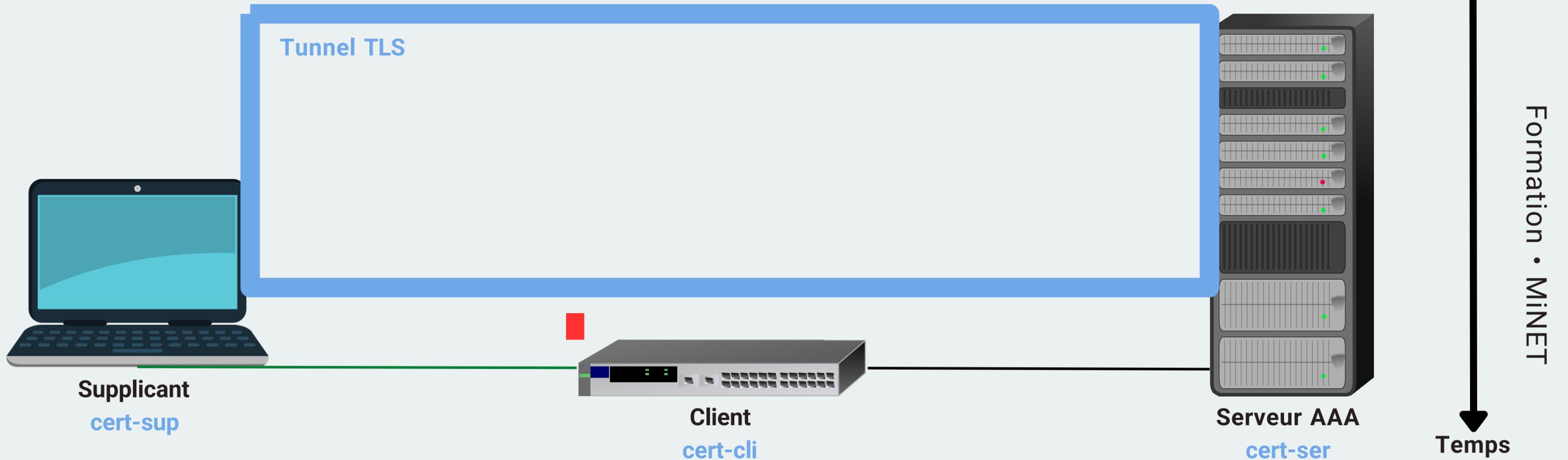


Temps

AUTHENTIFICATION

LE PROTOCOLE EAP-TLS

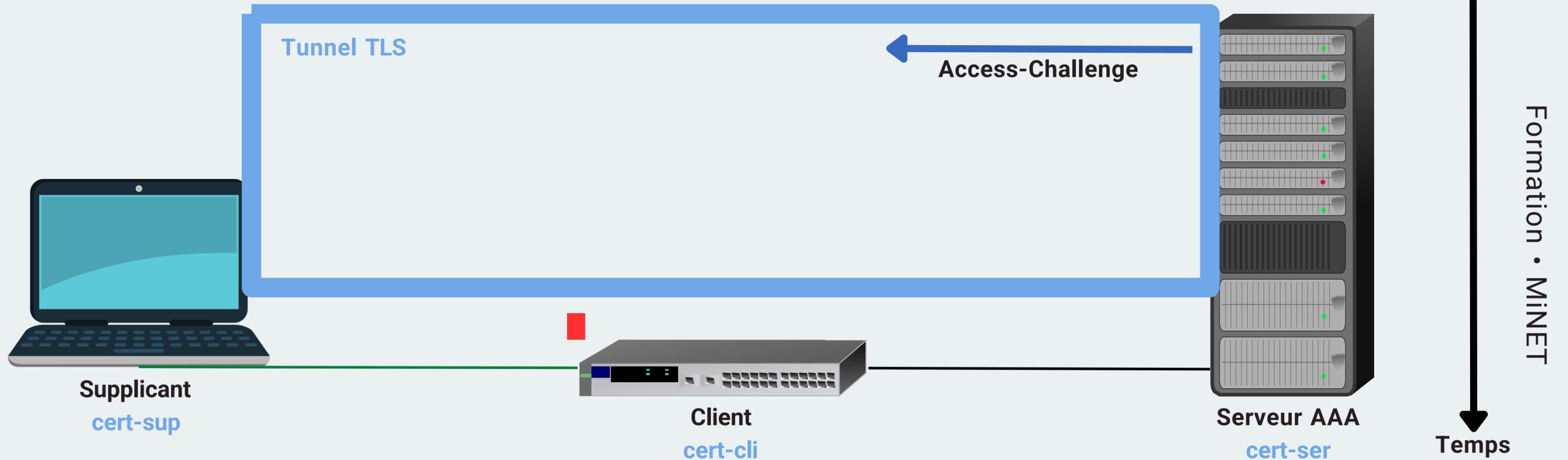
- 1 - Création/échange certificats
- 2 - Echanges de trames EAP dans le tunnel TLS



AUTHENTIFICATION

LE PROTOCOLE EAP-TLS

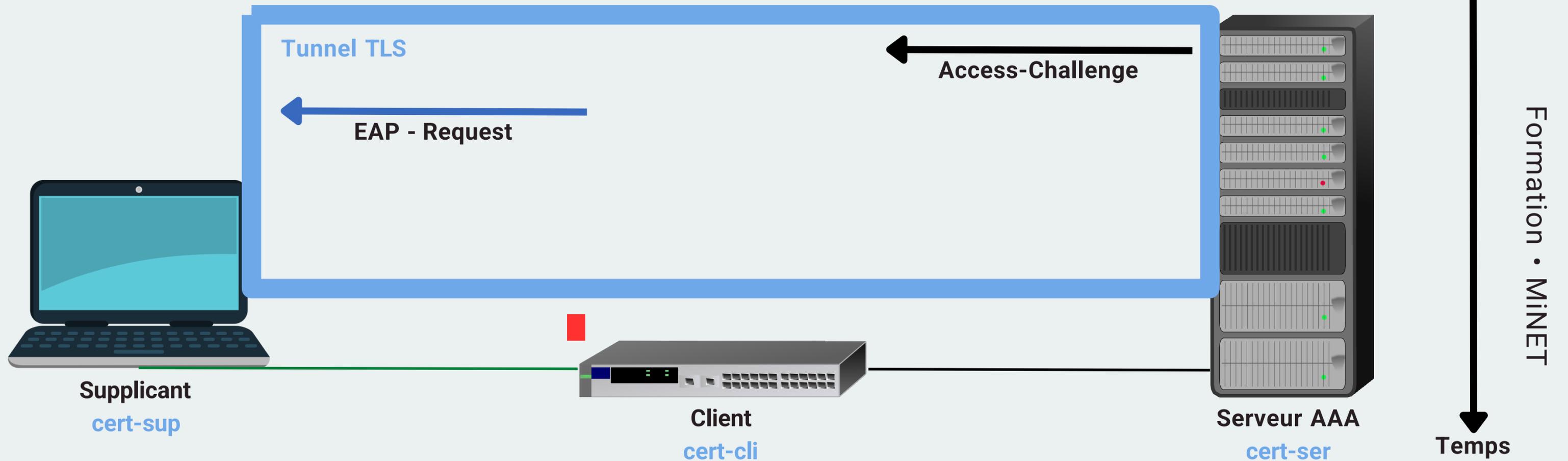
- 1 - Création/échange certificats
- 2 - Echanges de trames EAP dans le tunnel TLS



AUTHENTIFICATION

LE PROTOCOLE EAP-TLS

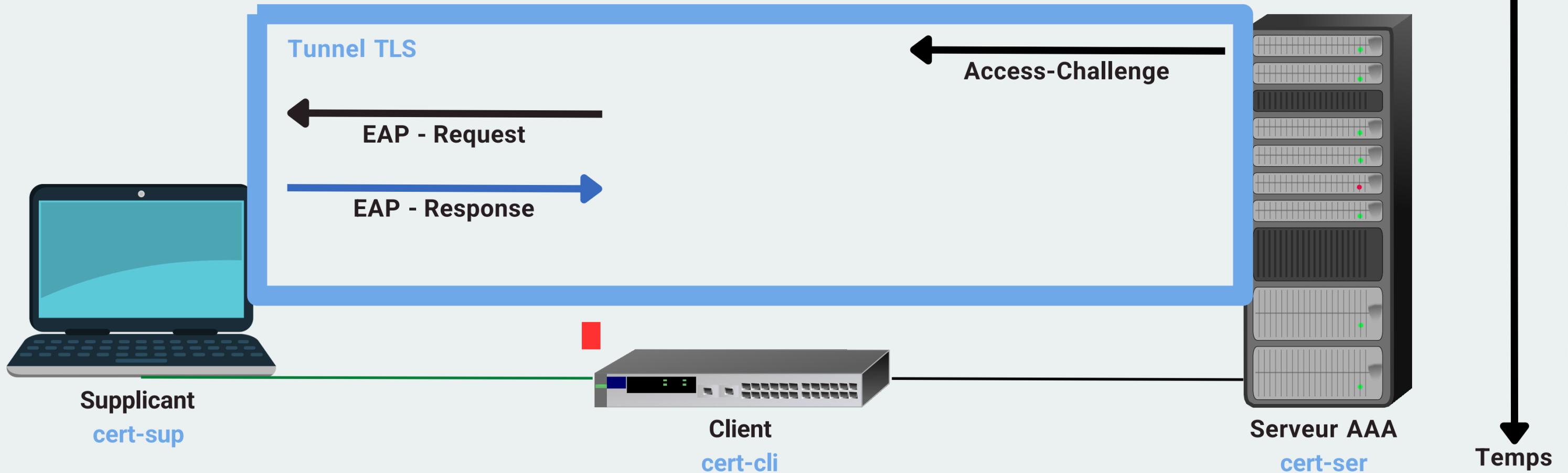
- 1 - Création/échange certificats
- 2 - Echanges de trames EAP dans le tunnel TLS



AUTHENTIFICATION

LE PROTOCOLE EAP-TLS

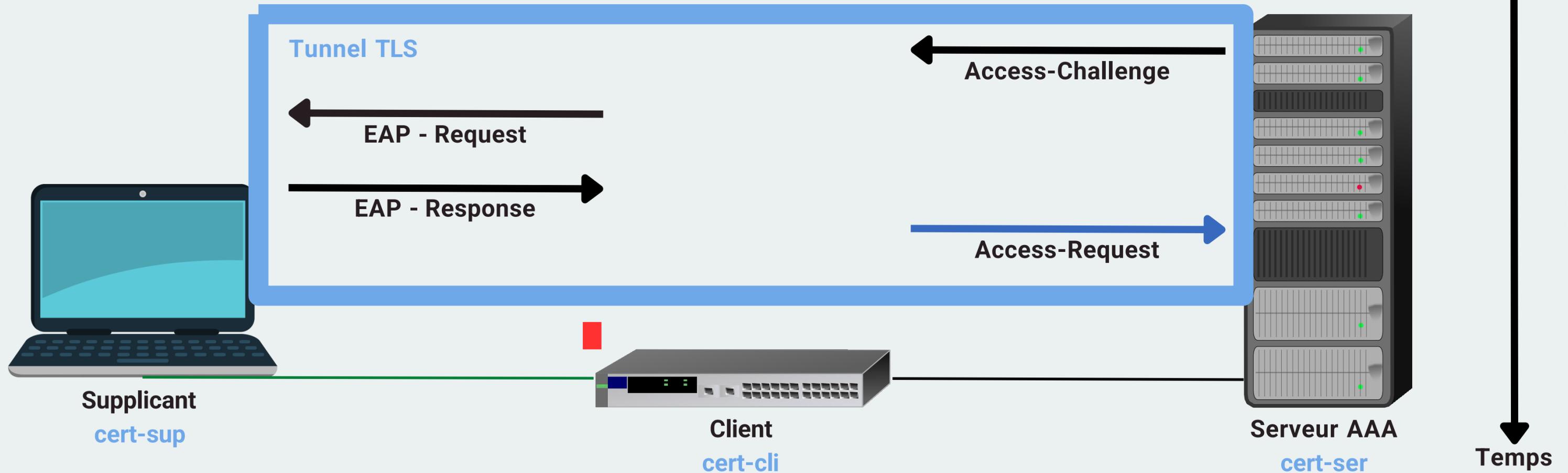
- 1 - Création/échange certificats
- 2 - Echanges de trames EAP dans le tunnel TLS



AUTHENTIFICATION

LE PROTOCOLE EAP-TLS

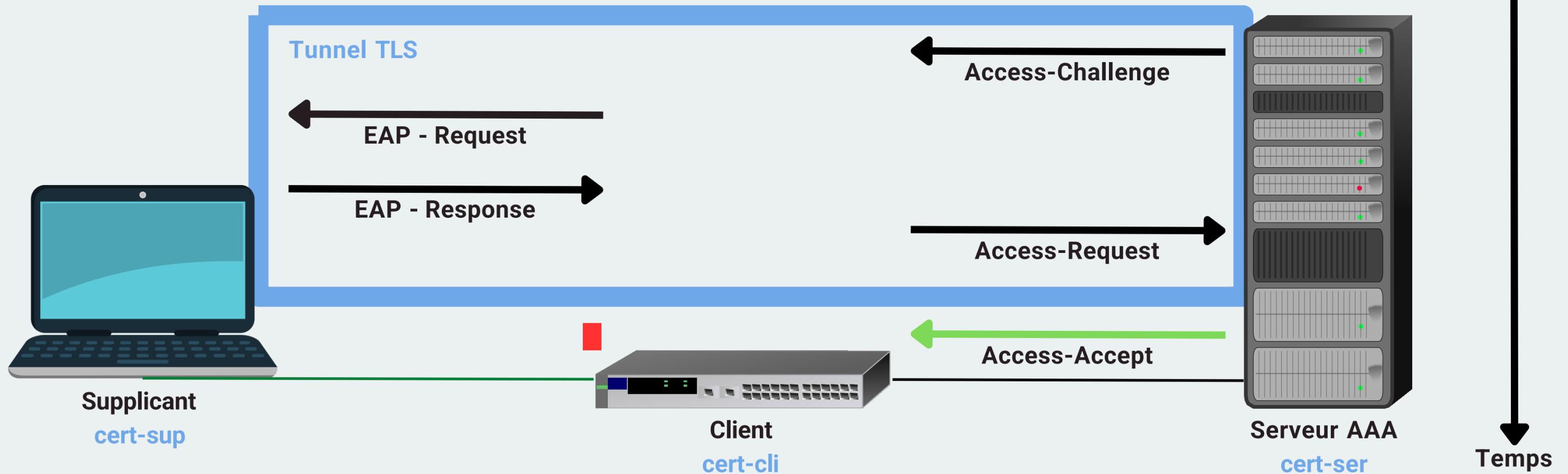
- 1 - Création/échange certificats
- 2 - Echanges de trames EAP dans le tunnel TLS



AUTHENTIFICATION

LE PROTOCOLE EAP-TLS

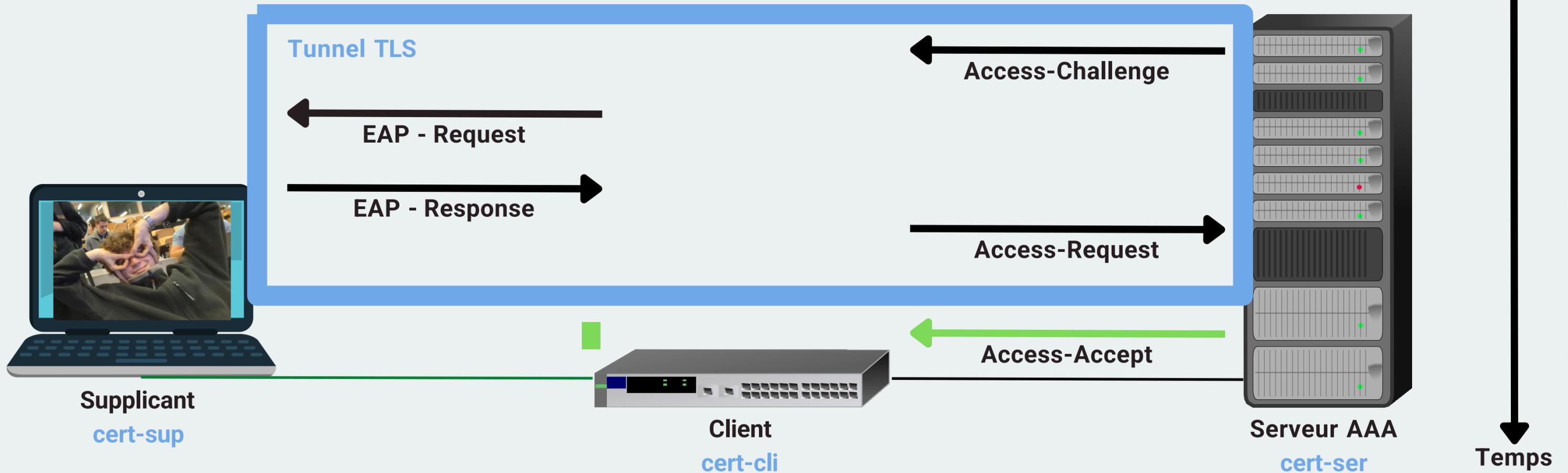
- 1 - Création/échange certificats
- 2 - Echanges de trames EAP dans le tunnel TLS



AUTHENTIFICATION

LE PROTOCOLE EAP-TLS

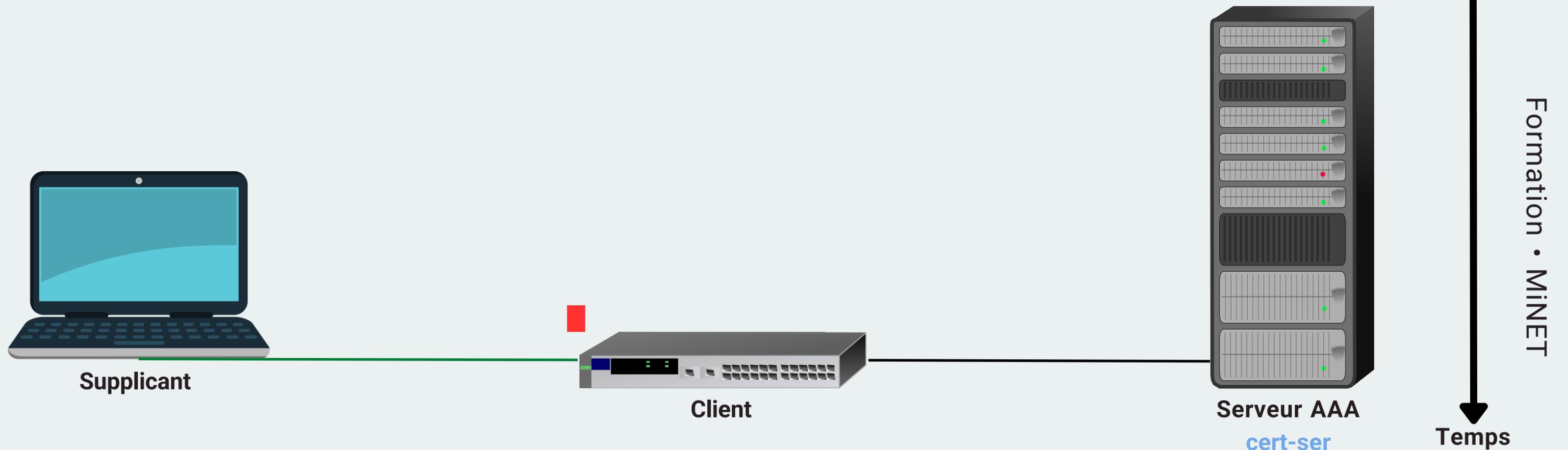
- 1 - Création/échange certificats
- 2 - Echanges de trames EAP dans le tunnel TLS



AUTHENTIFICATION

LE PROTOCOLE EAP-PEAP

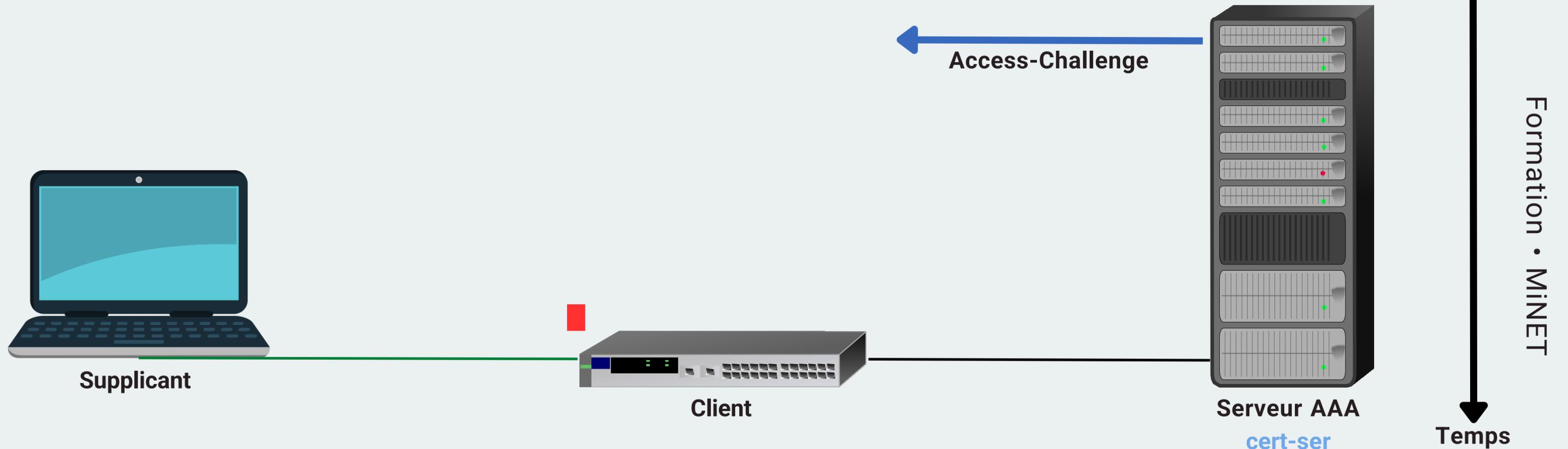
PEAP = Protected EAP → L'idée, c'est d'avoir un protocole EAP encapsulé dans un tunnel TLS créé à l'aide d'un seul certificat serveur.



AUTHENTIFICATION

LE PROTOCOLE EAP-PEAP

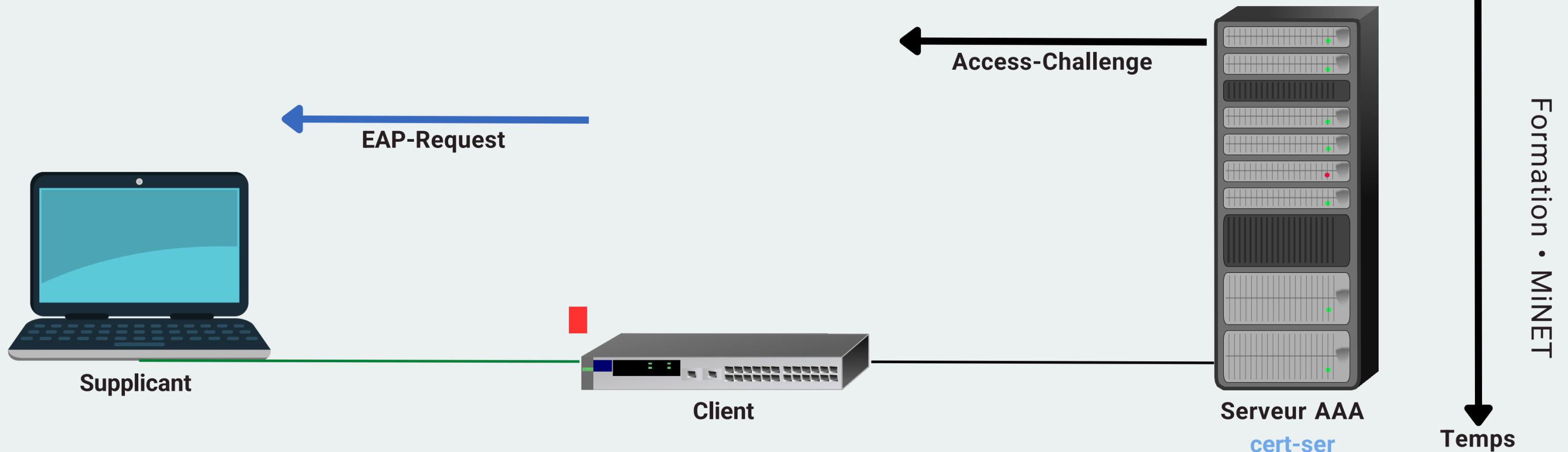
PEAP = Protected EAP → L'idée, c'est d'avoir un protocole EAP encapsulé dans un tunnel TLS créé à l'aide d'un seul certificat serveur.



AUTHENTIFICATION

LE PROTOCOLE EAP-PEAP

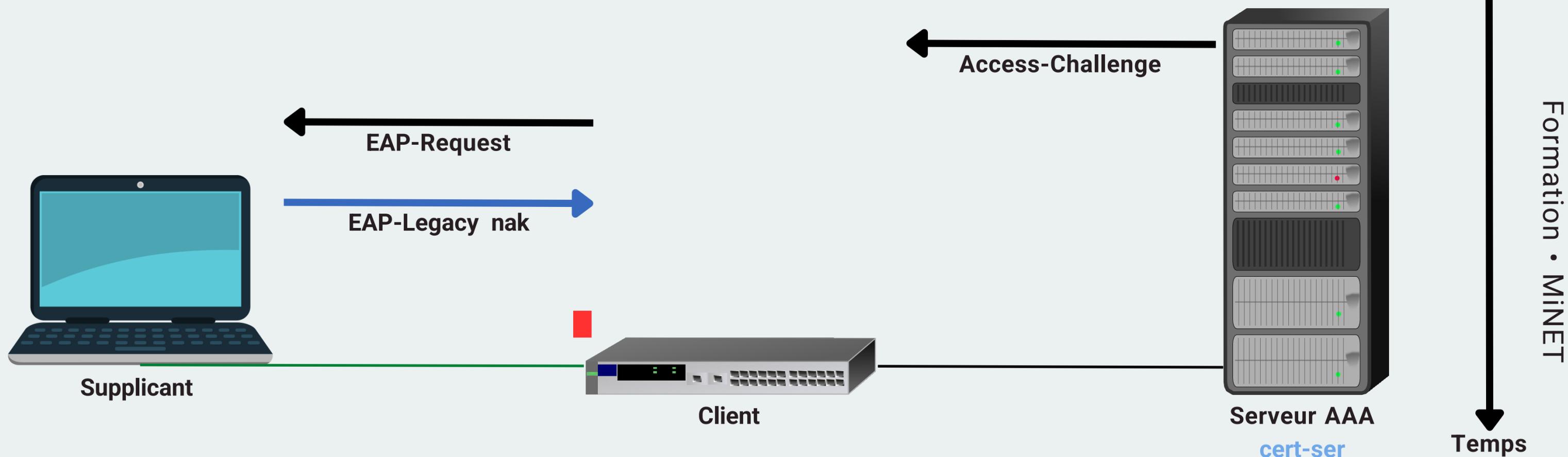
PEAP = Protected EAP → L'idée, c'est d'avoir un protocole EAP encapsulé dans un tunnel TLS créé à l'aide d'un seul certificat serveur.



AUTHENTIFICATION

LE PROTOCOLE EAP-PEAP

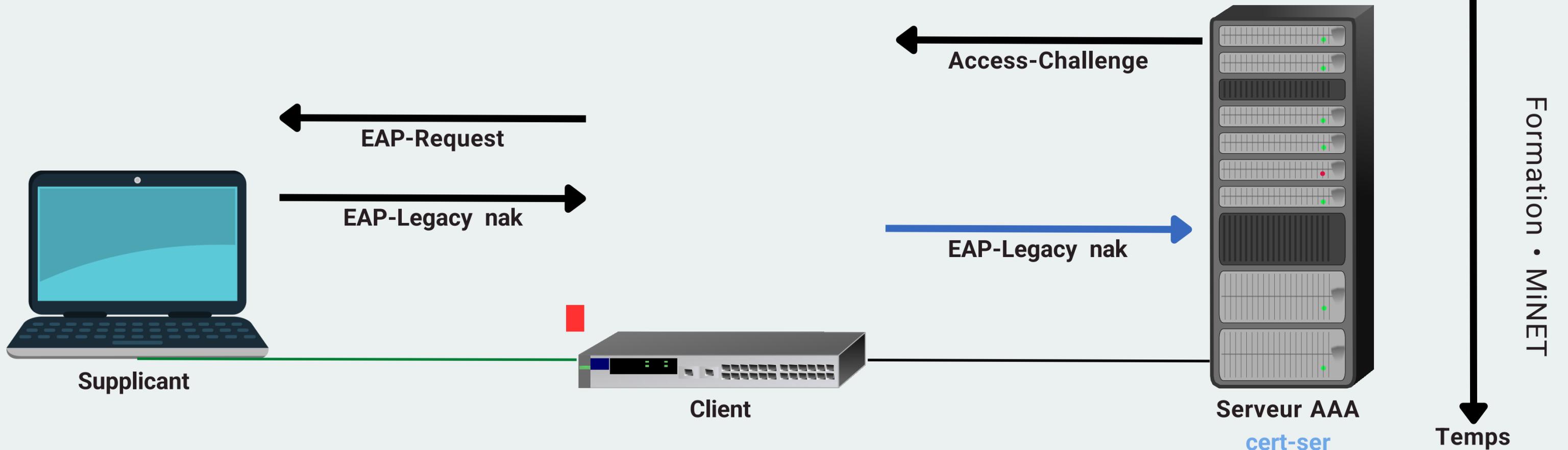
PEAP = Protected EAP → L'idée, c'est d'avoir un protocole EAP encapsulé dans un tunnel TLS créé à l'aide d'un seul certificat serveur.



AUTHENTIFICATION

LE PROTOCOLE EAP-PEAP

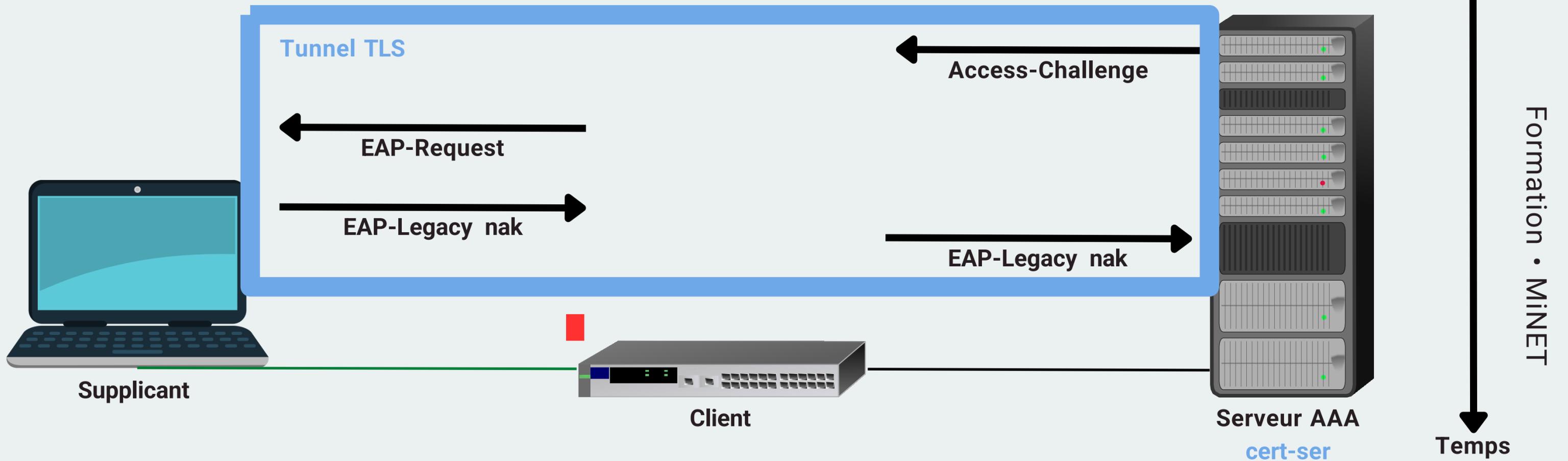
PEAP = Protected EAP → L'idée, c'est d'avoir un protocole EAP encapsulé dans un tunnel TLS créé à l'aide d'un seul certificat serveur.



AUTHENTIFICATION

LE PROTOCOLE EAP-PEAP

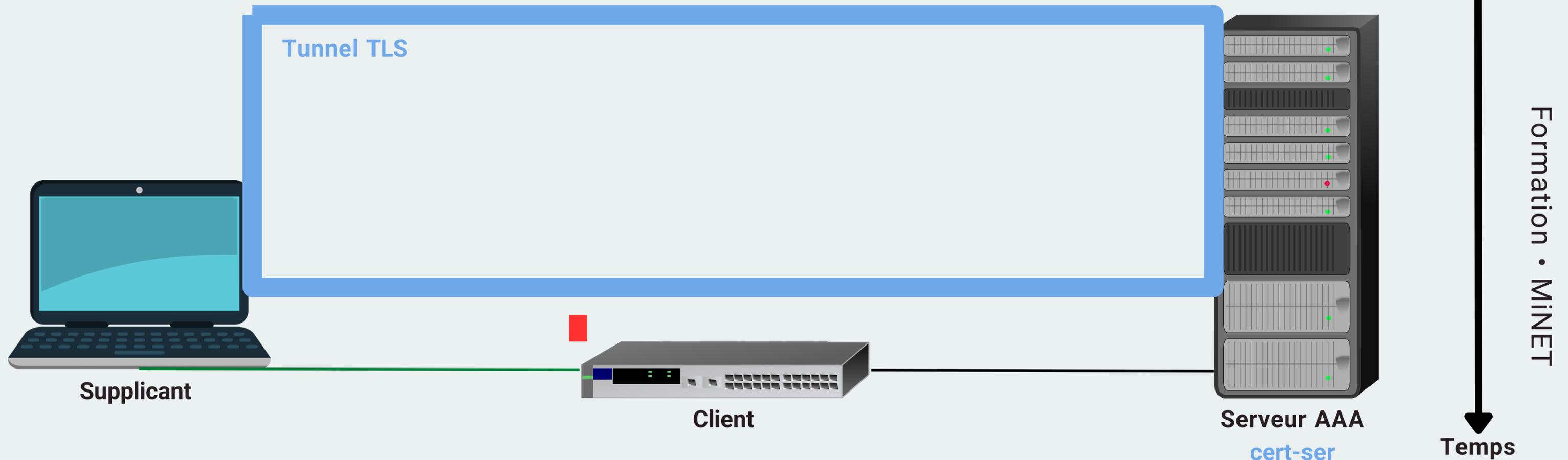
PEAP = Protected EAP → L'idée, c'est d'avoir un protocole EAP encapsulé dans un tunnel TLS créé à l'aide d'un seul certificat serveur.



AUTHENTIFICATION

LE PROTOCOLE EAP-PEAP

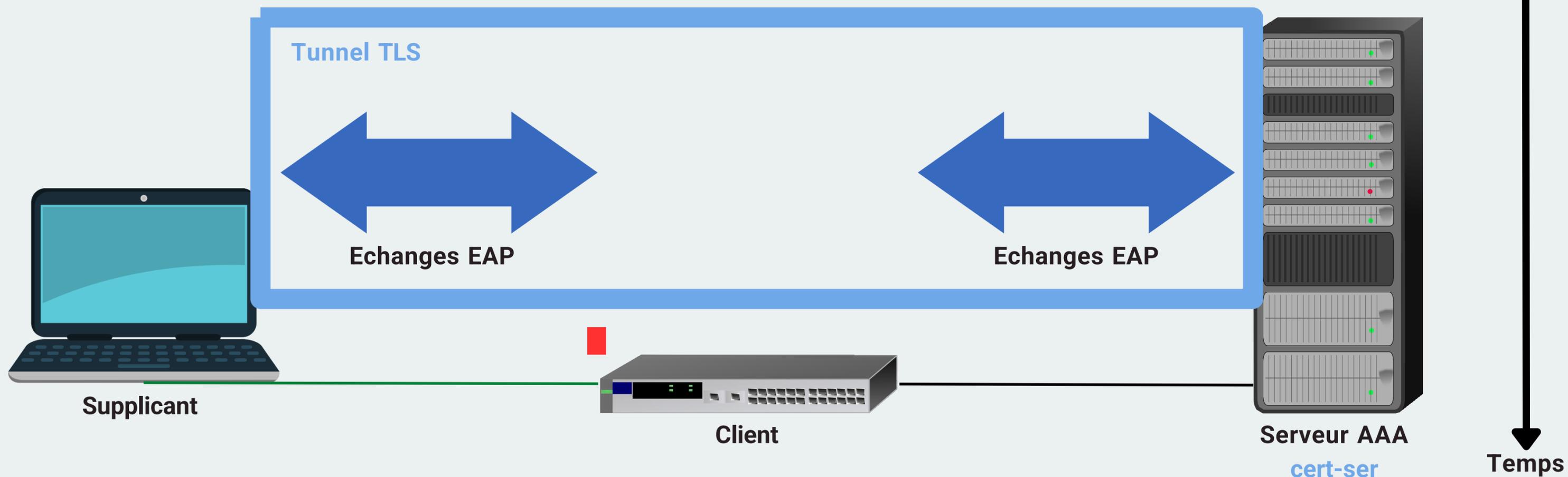
PEAP = Protected EAP → L'idée, c'est d'avoir un protocole EAP encapsulé dans un tunnel TLS créé à l'aide d'un seul certificat serveur.



AUTHENTIFICATION

LE PROTOCOLE EAP-PEAP

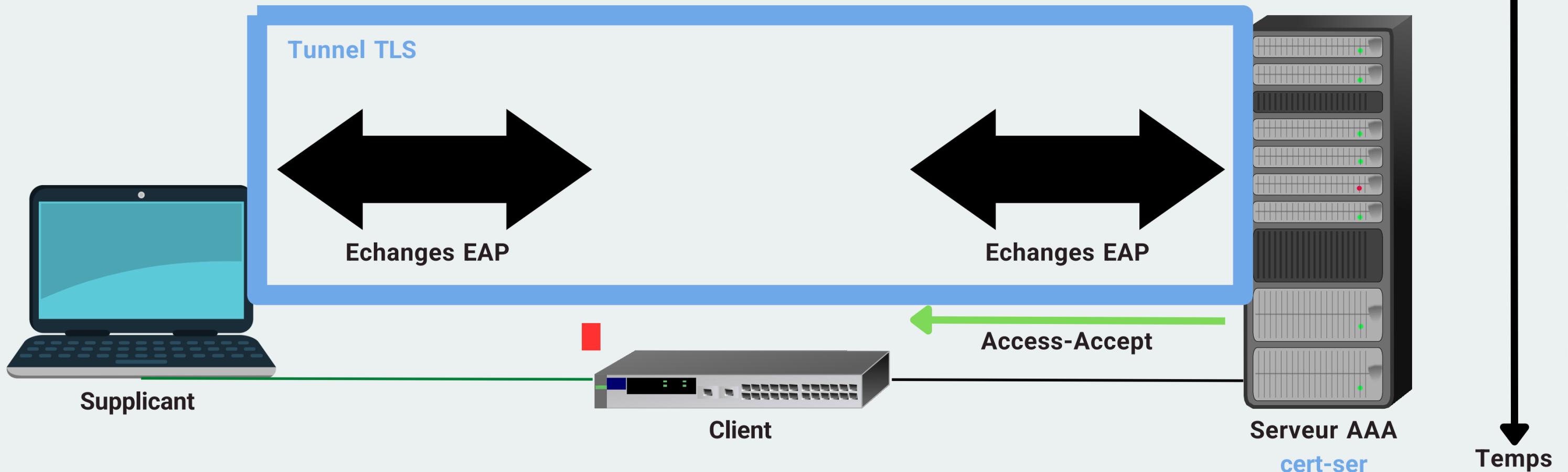
PEAP = Protected EAP → L'idée, c'est d'avoir un protocole EAP encapsulé dans un tunnel TLS créé à l'aide d'un seul certificat serveur.



AUTHENTIFICATION

LE PROTOCOLE EAP-PEAP

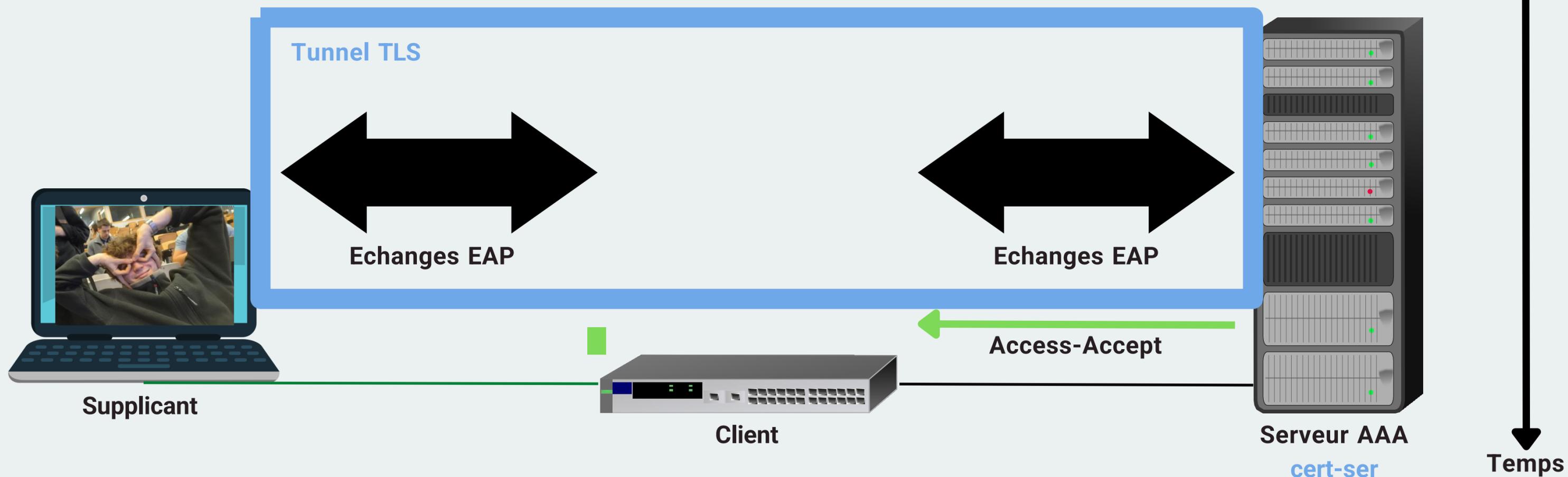
PEAP = Protected EAP → L'idée, c'est d'avoir un protocole EAP encapsulé dans un tunnel TLS créé à l'aide d'un seul certificat serveur.



AUTHENTIFICATION

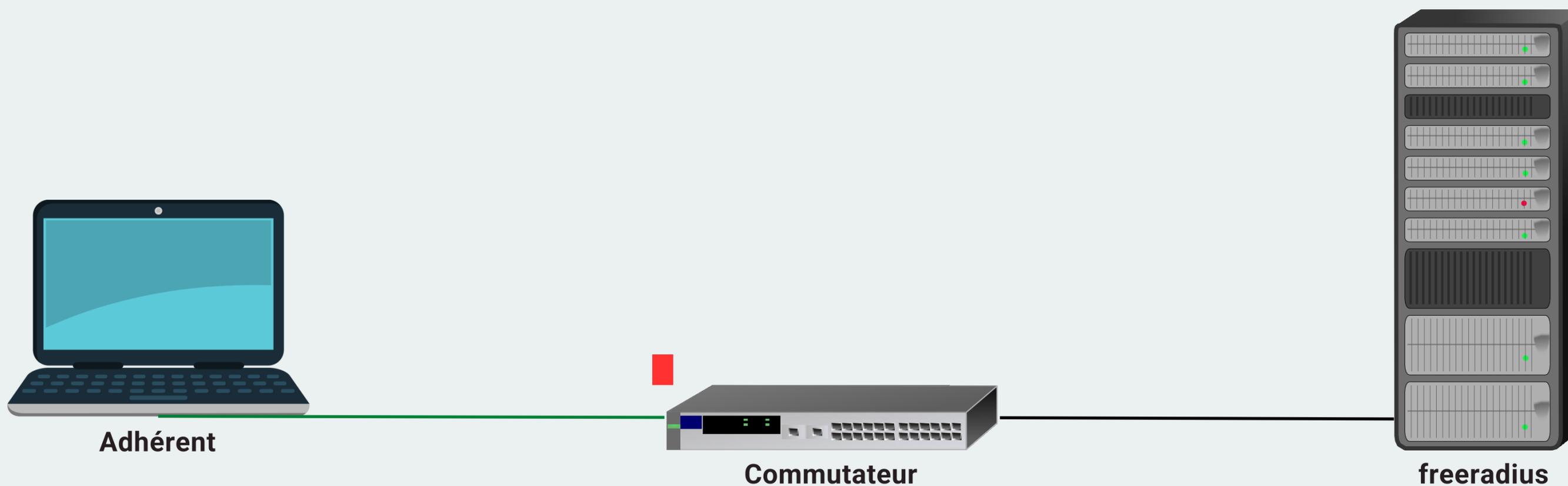
LE PROTOCOLE EAP-PEAP

PEAP = Protected EAP → L'idée, c'est d'avoir un protocole EAP encapsulé dans un tunnel TLS créé à l'aide d'un seul certificat serveur.



ET CHEZ NOUS ?

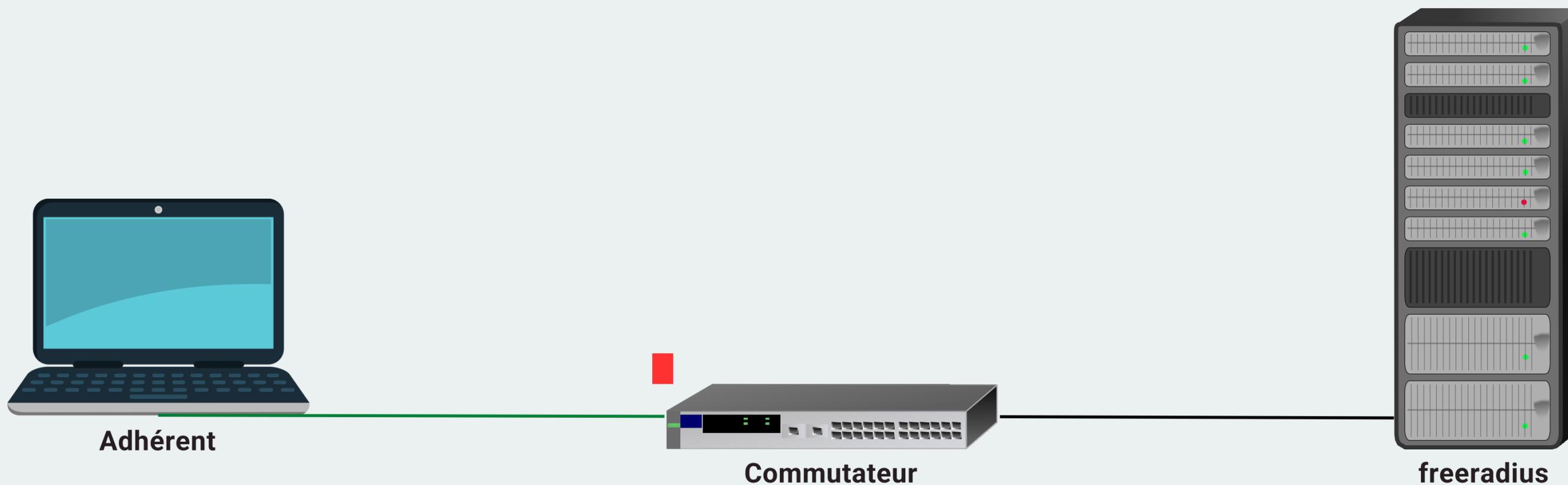
PROTOCOLE EAP UTILISÉ



ET CHEZ NOUS ?

PROTOCOLE EAP UTILISÉ

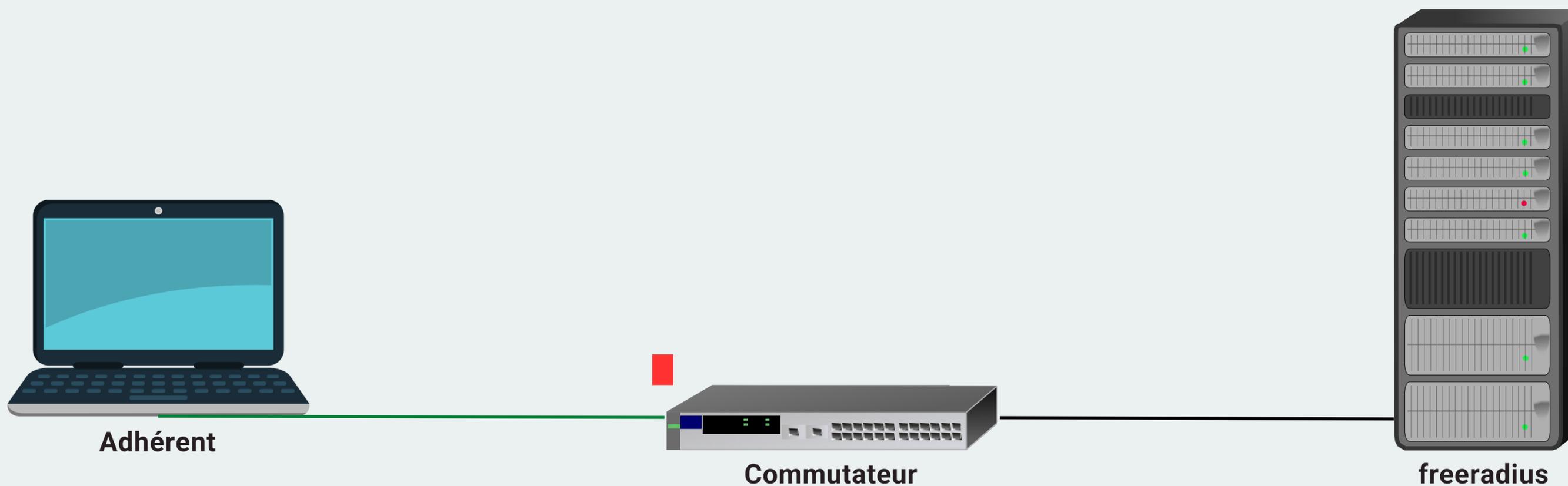
LE GRAND



ET CHEZ NOUS ?

PROTOCOLE EAP UTILISÉ

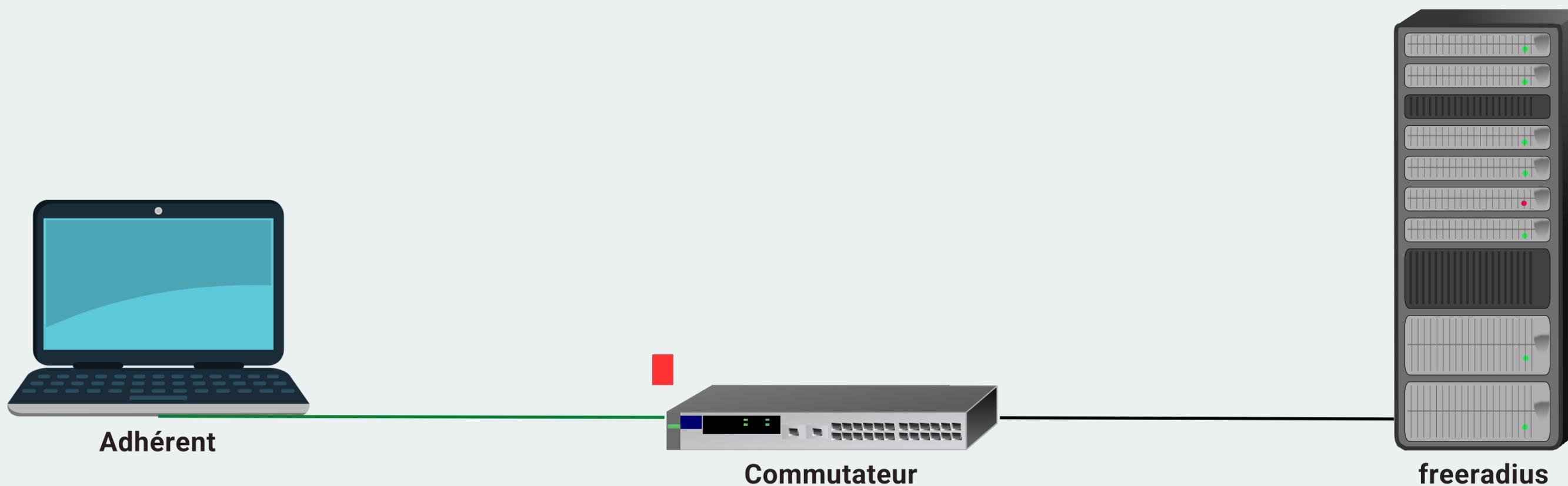
LE GRAND
LE SEUL



ET CHEZ NOUS ?

PROTOCOLE EAP UTILISÉ

LE GRAND
LE SEUL
L'UNIQUE



ET CHEZ NOUS ?

PROTOCOLE EAP UTILISÉ

LE GRAND
LE SEUL
L'UNIQUE

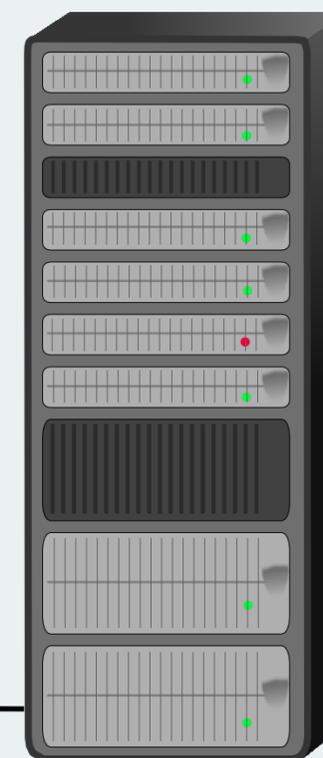
PEAP-MSCHAPv2



Adhérent



Commutateur

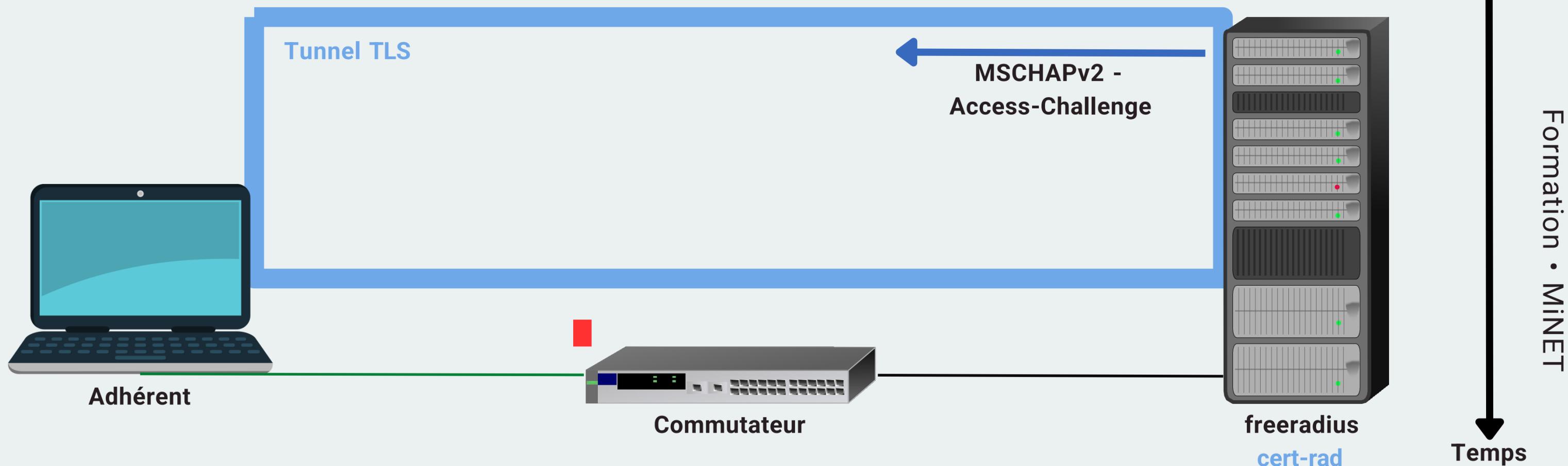


freeradius

ET CHEZ NOUS ?

PEAP-MSCHAPV2

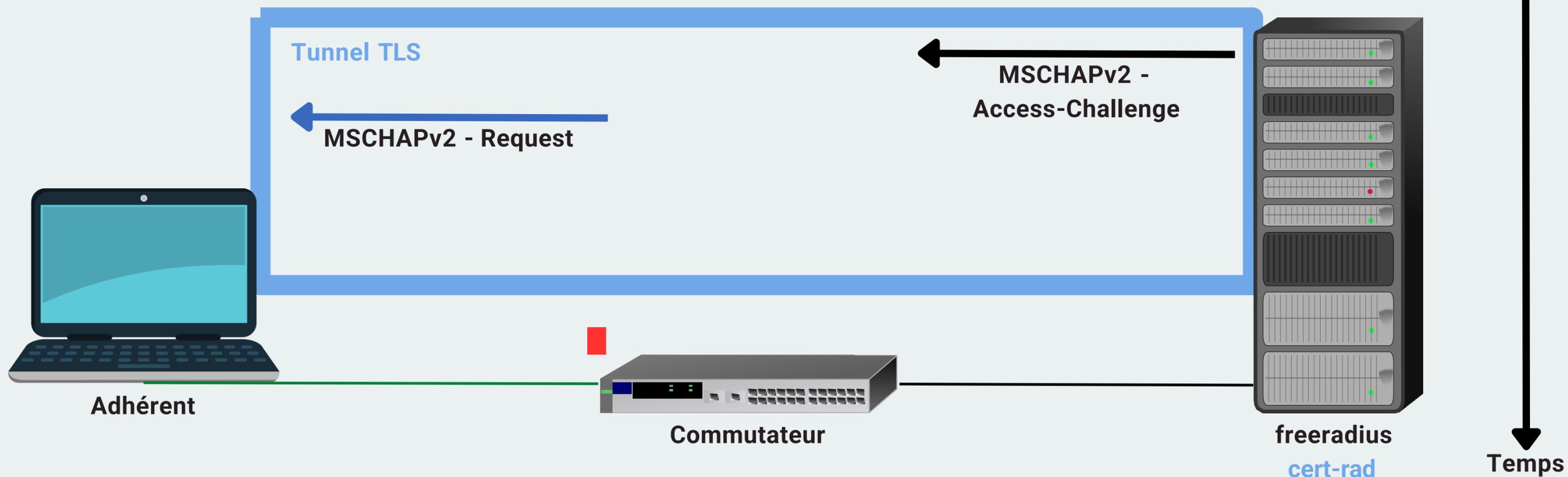
C'est un PEAP où les échanges EAP au sein du tunnel TLS correspondent aux échanges du protocole MSCHAPv2 !



ET CHEZ NOUS ?

PEAP-MSCHAPV2

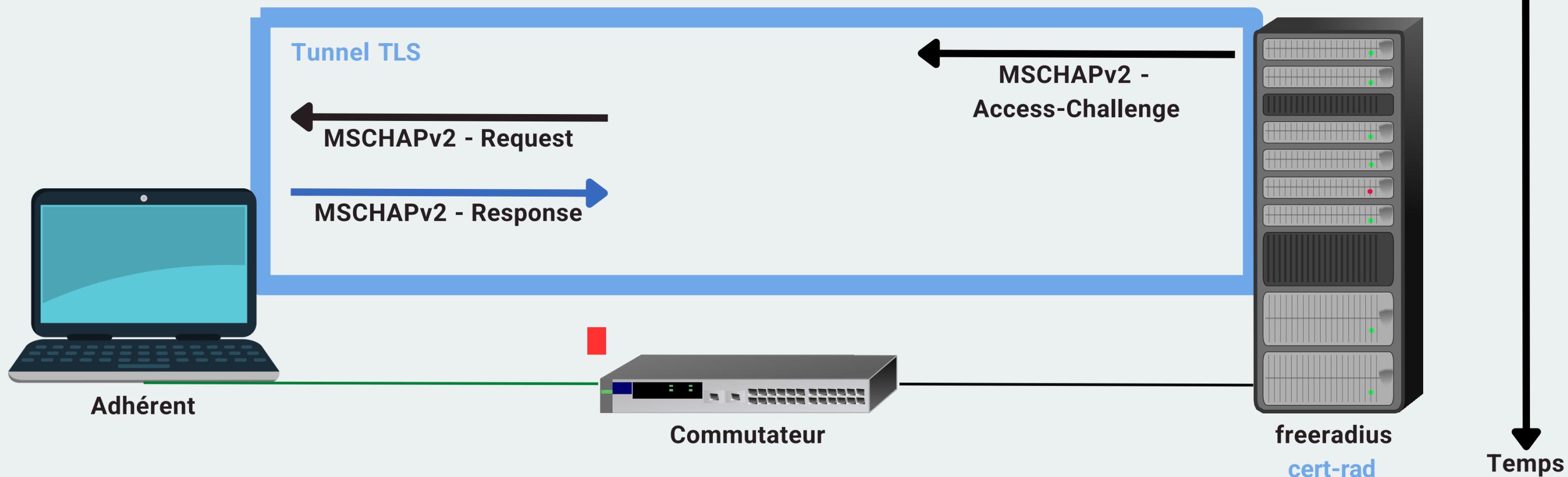
C'est un PEAP où les échanges EAP au sein du tunnel TLS correspondent aux échanges du protocole MSCHAPv2 !



ET CHEZ NOUS ?

PEAP-MSCHAPV2

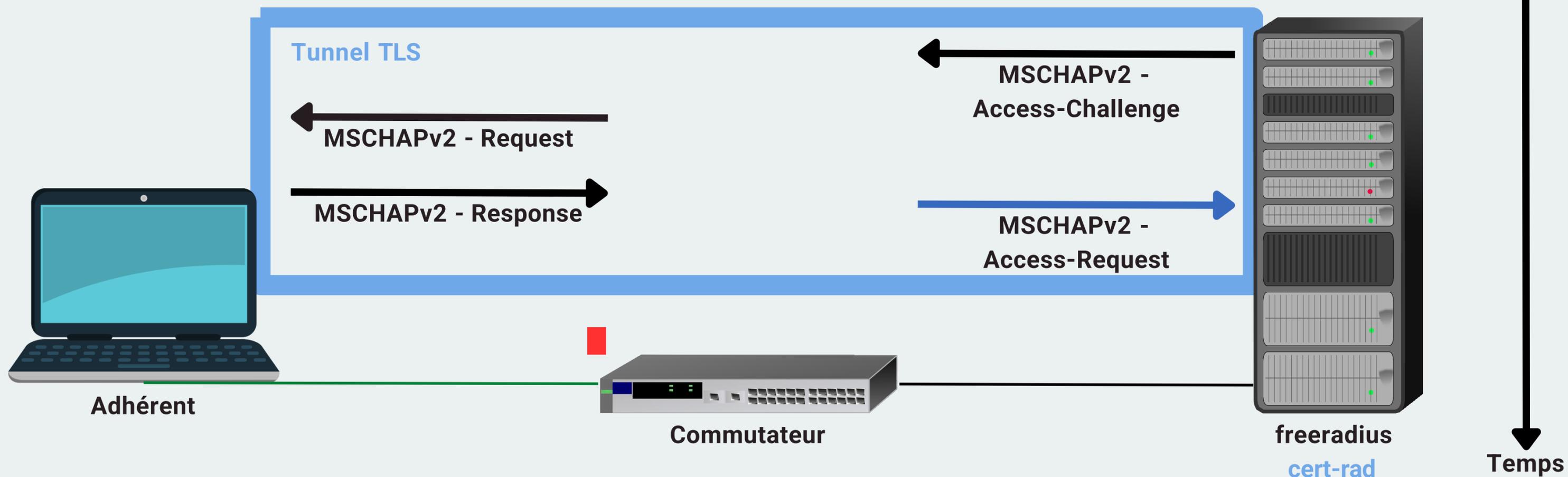
C'est un PEAP où les échanges EAP au sein du tunnel TLS correspondent aux échanges du protocole MSCHAPv2 !



ET CHEZ NOUS ?

PEAP-MSCHAPV2

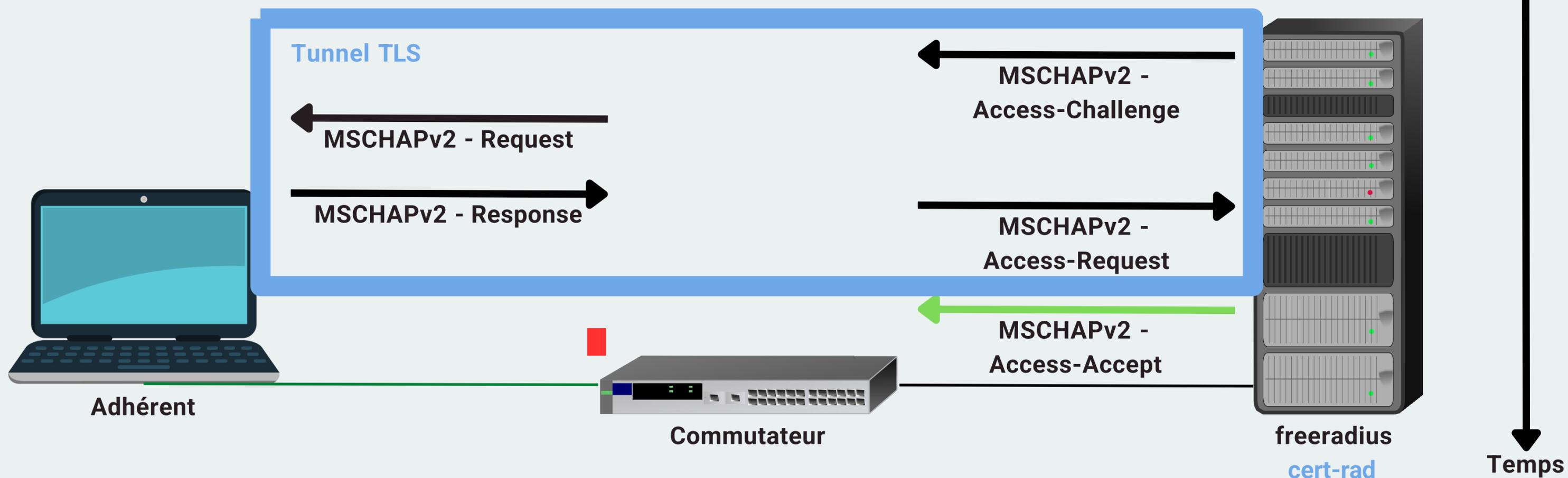
C'est un PEAP où les échanges EAP au sein du tunnel TLS correspondent aux échanges du protocole MSCHAPv2 !



ET CHEZ NOUS ?

PEAP-MSCHAPV2

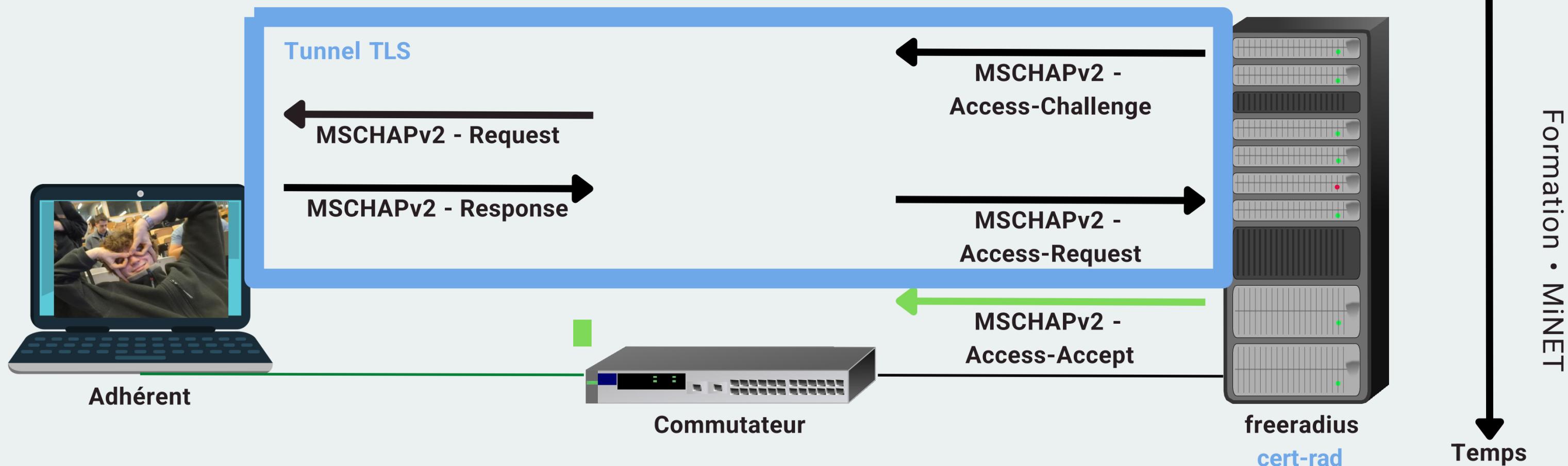
C'est un PEAP où les échanges EAP au sein du tunnel TLS correspondent aux échanges du protocole MSCHAPv2 !



ET CHEZ NOUS ?

PEAP-MSCHAPV2

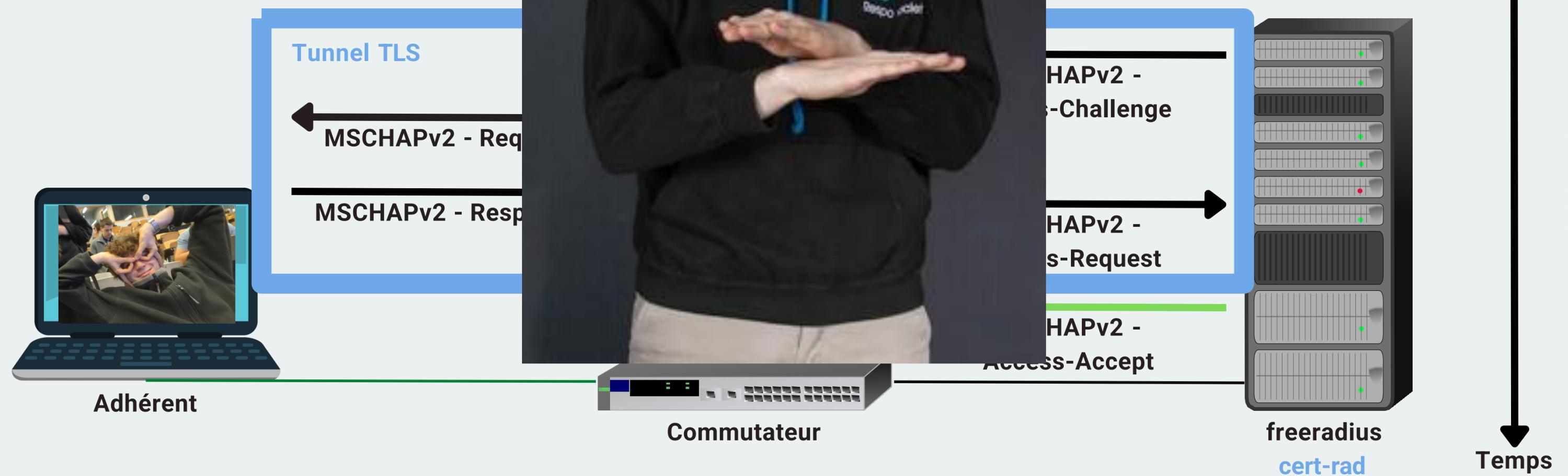
C'est un PEAP où les échanges EAP au sein du tunnel TLS correspondent aux échanges du protocole MSCHAPv2 !



ET CHEZ MINET

PEAP-MSCHAPV2

C'est un PEAP où les échanges EAP sont encapsulés dans un tunnel TLS et correspondent aux échanges du protocole MSCHAPv2 !



FREERADIUS

QU'EST-CE QUE C'EST ?

The logo for FreeRADIUS, featuring the word "free" in a blue script font and "RADIUS" in a dark blue, bold, sans-serif font.

Implémentation
open-source de
RADIUS



1/3 des utilisateurs dans le
monde s'authentifient grâce
à FreeRADIUS

FREERADIUS

À MiNET ?



Serveur RADIUS
utilisé à MiNET



Adhérent

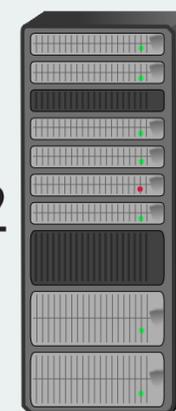


Contrôleur
d'accès

Politique de
basculement

radius2

radius



FREERADIUS

COMMENCER AVEC FREERADIUS

74

```
radius:/# ls -l /etc
```

```
drwxr-xr-x 4 root    root    4096 Jul 23  2022 fonts
drwxr-s--- 5 freerad freerad 4096 Jun  7  2022 freeradius
drwxr-xr-x 2 root    root    4096 Jul 23  2022 freetds
-rw-r--r-- 1 root    root     37 Oct 22  2012 fstab
```

← Configuration ici !

FREERADIUS

COMMENCER AVEC FREERADIUS

```
radius:/etc/freeradius/3.0# ls
```

```
README.rst  
certs  
clients.conf  
dictionary  
experimental.conf  
hints  
hunaroups  
mods-available  
mods-config  
mods-enabled  
panic.gdb  
policy.d  
proxv.conf  
radiusd.conf  
sites-available  
sites-enabled  
templates.conf  
trigger.conf  
users
```

Configuration des clients RADIUS

Modules de configuration

Paramètres de configuration du serveur

Gestion du serveur virtuel et du tunnel TLS

FREERADIUS

LES CLIENTS RADIUS

```
# Pour un commutateur
client 192.168.102.1 {
  ipaddr = 192.168.102.1
  secret = 0HaG8Fcvvg7E41KN
  shortname = switch-U1Routeur
  nastype = cisco
}

# Pour un WLC
client 192.168.102.219 {
  ipaddr = 192.168.102.219
  secret = 0HaG8Fcvvg7E41KN
  shortname = WLC_U7_WLC_Mif
}
```

Adresse IP du client

Secret partagé
avec le client

FREERADIUS

LES MODULES - CONFIGURATION DE EAP

```
# Configuration de EAP dans mods-available/eap
eap {
  default_eap_type = peap
  # ...
  peap {
    tls = tls-common
    default_eap_type = mschapv2
    copy_request_to_tunnel = no
    use_tunneled_reply = no
    virtual_server = "inner_tunnel"
  }
}
```

On veut du PEAP

Et même du PEAP-MSCHAPv2 !

Le serveur utilisé
pour le tunnel TLS
(dans *sites-enabled/*)

FREERADIUS

LES MODULES - CONFIGURATION DE L'AUTORISATION

78

```
# Configuration des modules
# personnalisés écrits en python
python3 {
    python_path=# ...
    module = freeradius
    # ...
}
```

Utilise le module présent dans
mods-config/python3/**freeradius.py**

```
radius:/etc/freeradius/3.0/mods-config/python3# ls
example.py
freeradius.py
radiusd.py
```

FREERADIUS

LES MODULES - CONFIGURATION DE L'AUTORISATION

79

```
# Configuration des modules
# personnalisés écrits en python
python3 {
    python_path=# ...
    module = freeradius
    # ...
}
```

Utilise le module présent dans
mods-config/python3/**freeradius.py**

```
radius:/etc/freeradius/3.0/mods-config/python3# ls
example.py
freeradius.py
radiusd.py
```

FREERADIUS

LES MODULES - CONFIGURATION DE L'AUTORISATION



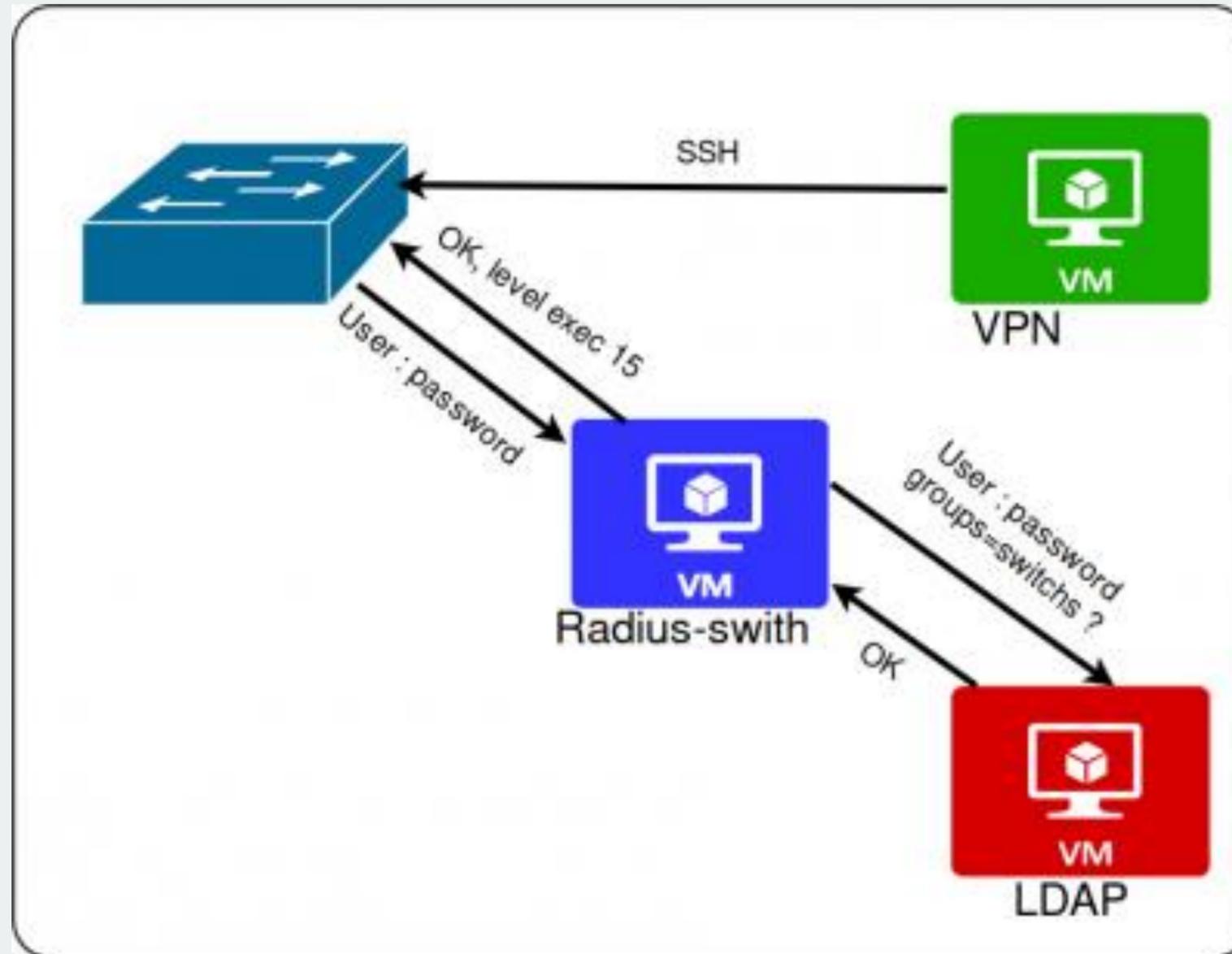
Radius sur la prod



Radius avec les switches

- LDAP pour Linux -> SSSD
- Explication en dessin
- Pas de PEAP mais LDAP

Radius avec les switches



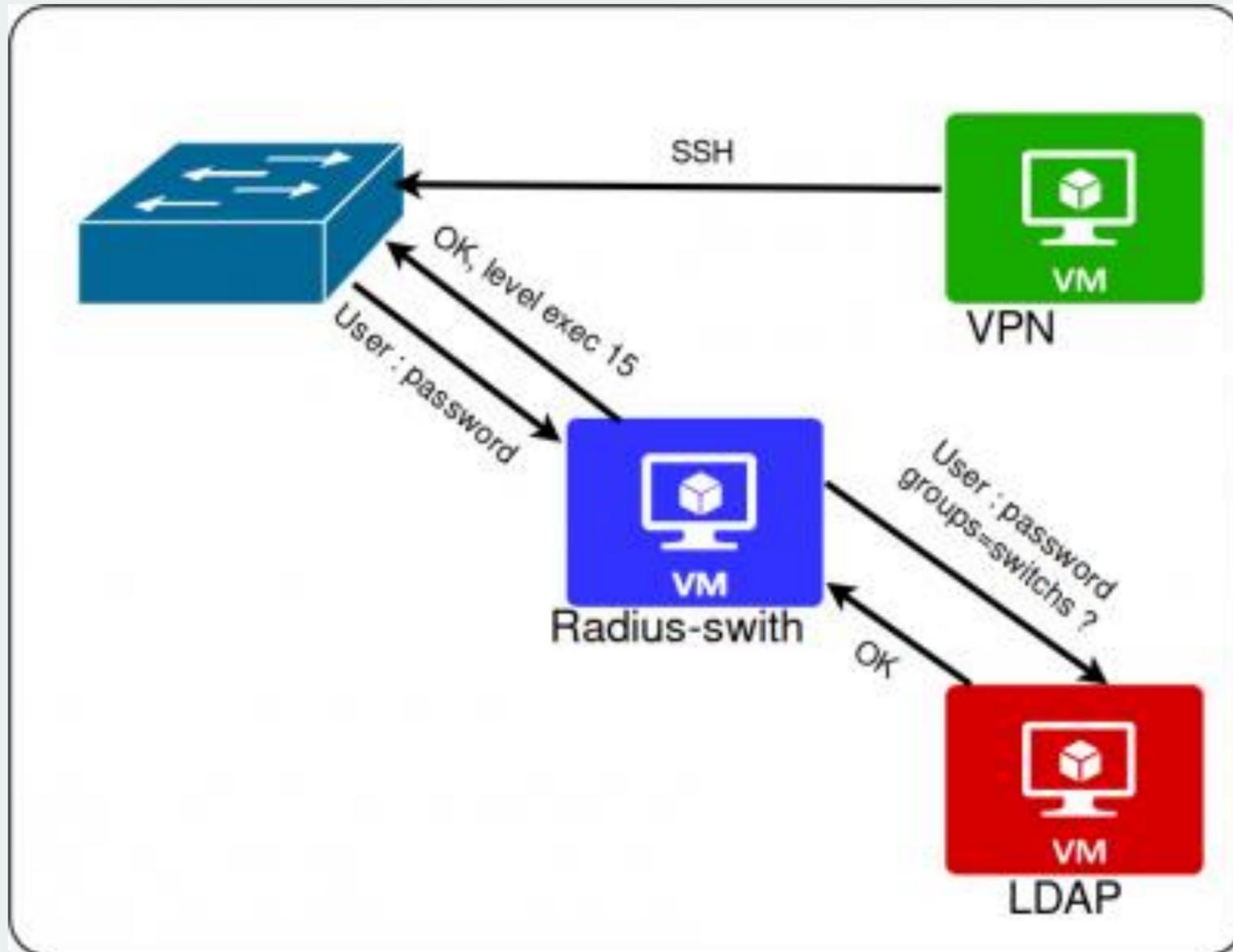
Radius avec les switches

82

```
1 | aaa group server radius radlogin
2 |   server-private 192.168.102.X auth-port 1812 acct-port 1813 key 7 CLERADIUS
3 |   cache expiry 48
4 |   cache authorization profile radcache
5 |   cache authentication profile radcache
6 |   deadtime 2
```

```
1 | aaa authentication login default group radlogin cache radlogin local
2 | aaa authorization exec default group radlogin cache radlogin local if-authenticated
```

Radius avec les switches



```
1 | update reply {  
2 |         cisco-avpair = "shell:priv-lvl=15"  
3 |     }
```