



Authentication in Access Networks (Track #4: Broadband access networks concepts)

robotiker
tecnalia

eman ta zabal zazu



Universidad Euskal Herriko
del País Vasco Unibertsitatea

Enrique Areizaga
Eduardo Jacob
Purificación Sáiz



MUSE Autumn School 2006
(October 19-20, Bilbao)

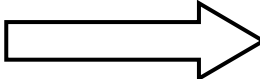
AGENDA



- > Authentication and access control in LAN (Puri Sáiz)
- > Authentication and access control in WLAN (Puri Sáiz)
- > Authentication in Broadband Access Networks (Enrique Areizaga)

- > **Authentication and access control in LAN**
 - **Original LAN**
 - **IEEE 802.1X: Authentication and Access Control**
- > Authentication and access control in WLAN
- > Authentication in Broadband Access Networks

- > Original LAN definition: connectivity oriented

- > No access control
 - Switch port enabled
 - Device connected to switch port  Access granted

- > Security concerns
 - LAN deployment in easily accessible areas
 - No authentication / authorization / access control mechanisms

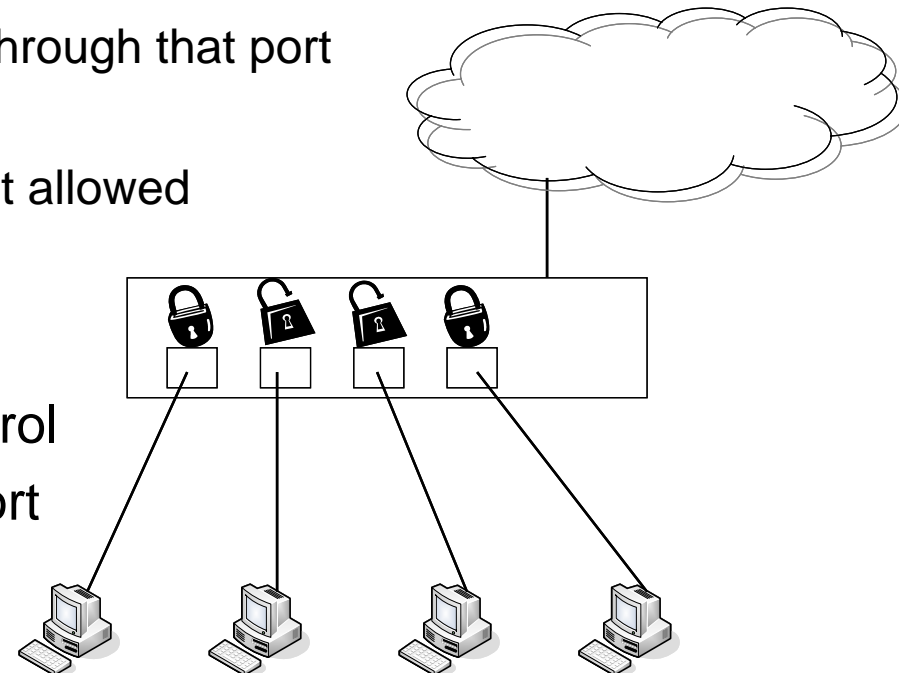
↳ Any device can attach to the network

> A very simple idea:

- Initially, access through a port is disabled (blocked)
- When a user attaches to that port → authentication phase
- If successful authentication → user authorized
 - Port is enabled: traffic allowed through that port
- If not → user not authorized
 - Port remains disabled: traffic not allowed

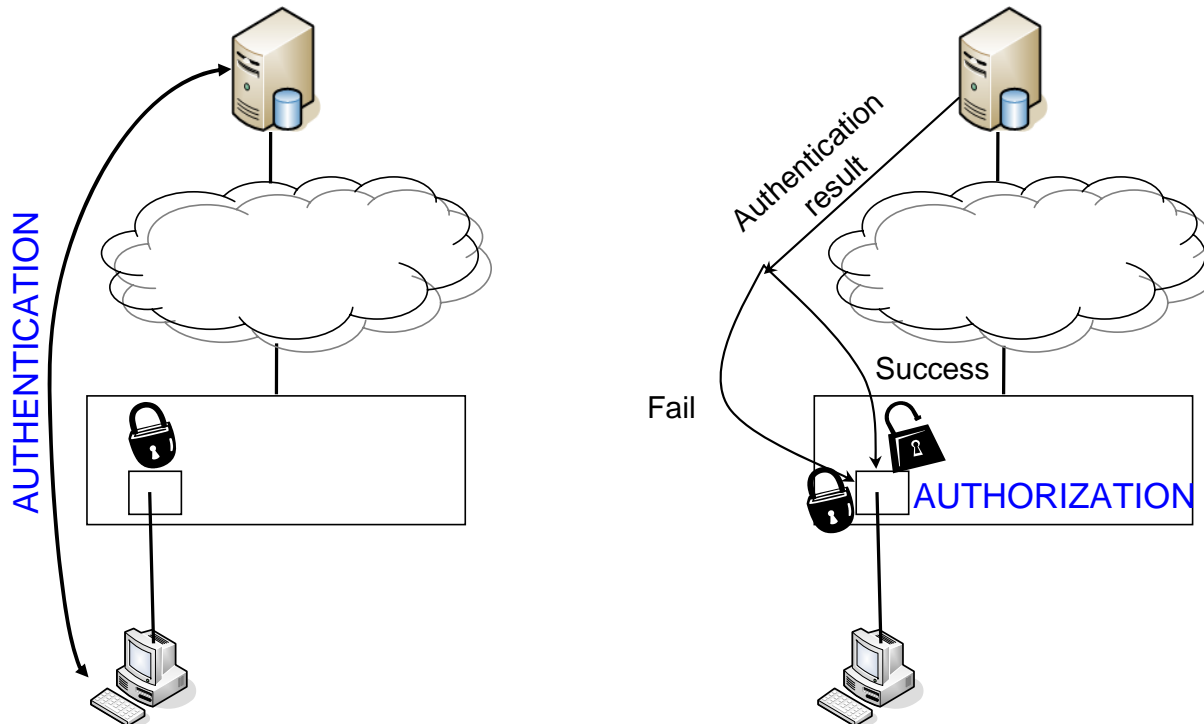
> This is done port-by-port

- Port-based network access control
- One device connected to one port

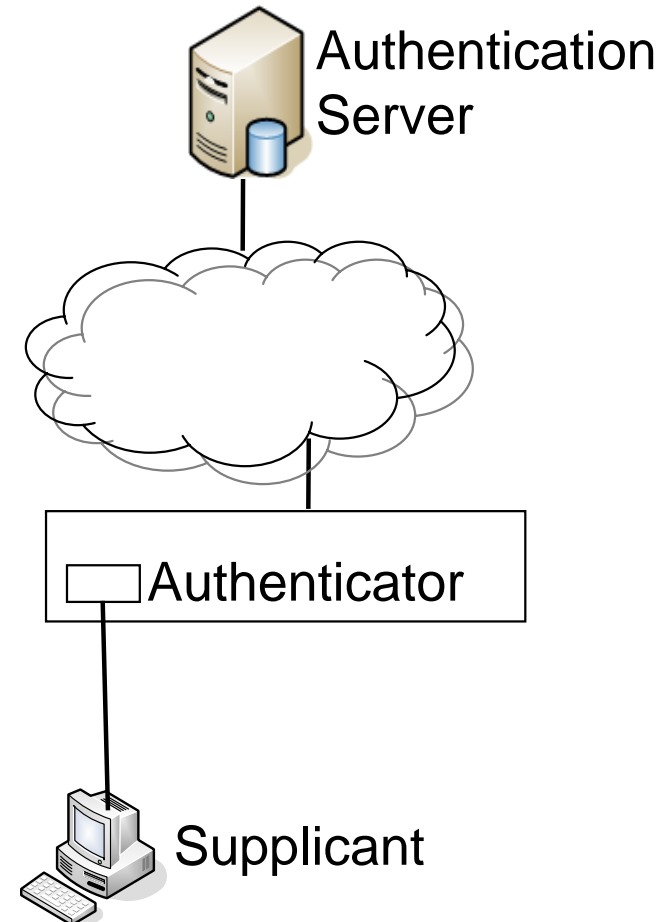


IEEE 802.1X – Authentication-Authorization

- > Clear separation Authentication – Authorization
 - Possible use of a back-end Authentication Server
 - Easy to integrate with existing AAA equipment



- > Supplicant:
 - It wants to access the services accesible via the Authenticator
- > Authenticator:
 - It enforces authentication before allowing access to the services accessible via itself
- > Authentication Server:
 - It performs the authentication functions to verify the credentials of the Supplicant on behalf of the Authenticator
 - ...and then indicates to the Authenticator whether or not the Supplicant is authorized to access the Authenticator's services



> Splitting of a port into two access ports:

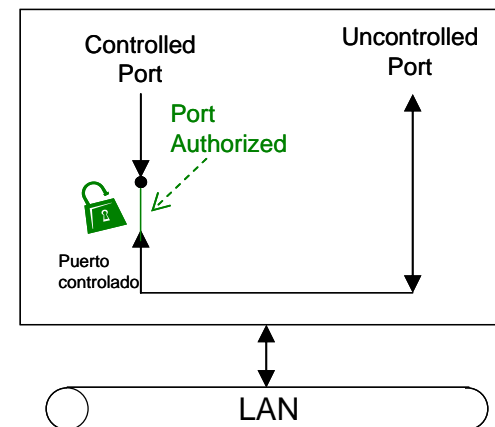
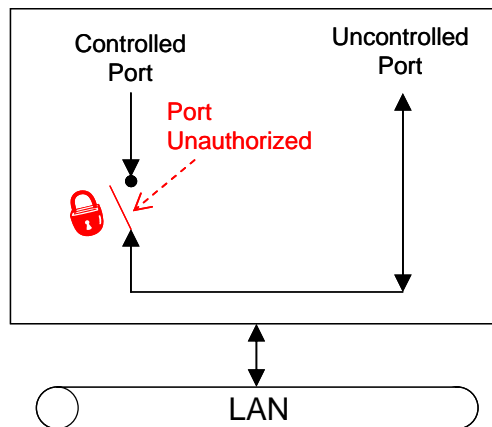
- Uncontrolled Port

It allows the uncontrolled exchange of traffic at any time, regardless the authorization state of the port.

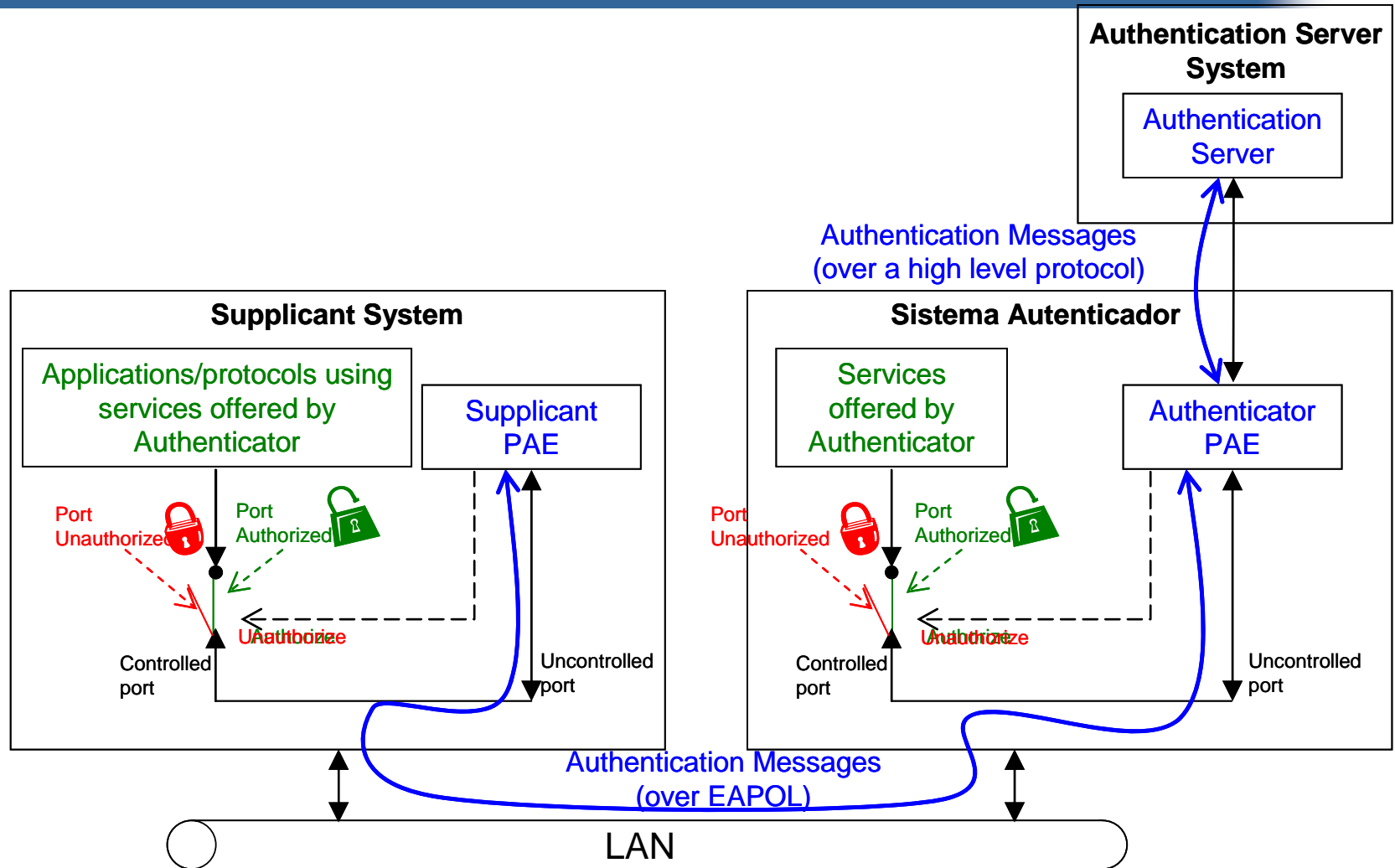
To exchange authentication protocol messages

- Controlled Port

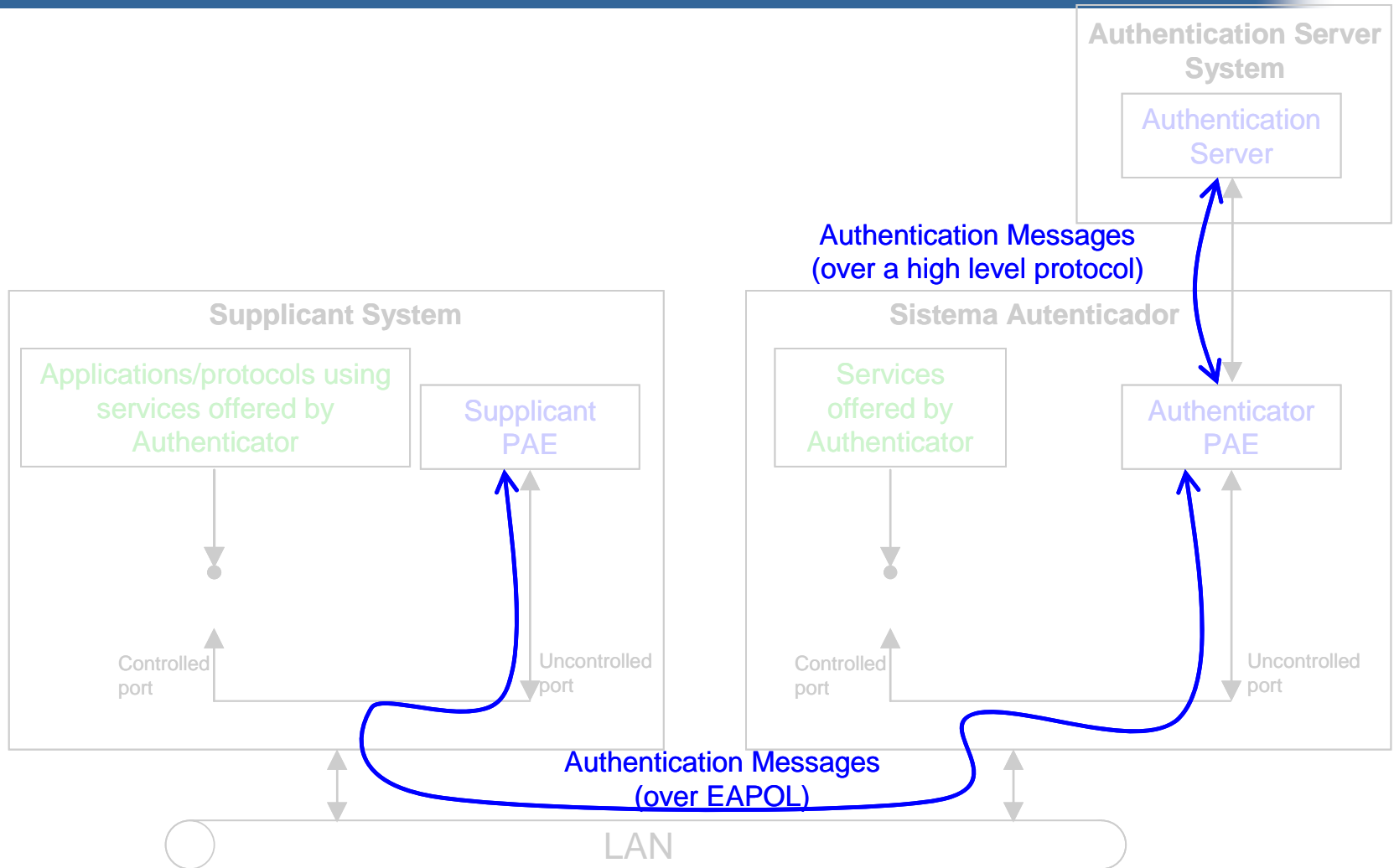
It allows the exchange of traffic only when the port is in an Authorized state



IEEE 802.1X – Everything together



IEEE 802.1X – Authentication



WHAT IS OUTSIDE IEEE 802.1X SPECIFICATION

- > IEEE 802.1X doesn't specify:
 - the type of authentication
 - the contents of authentication messages.
- > Instead, it makes use of EAP (Extensible Authentication Protocol) to exchange authentication messages.
- > EAP doesn't specify, either, an authentication procedure.
 - EAP is a common framework...
 - ...that supports multiple authentication methods (EAP-MD5, EAP-TLS, EAP-TTLS, PEAP, EAP-SIM...)
 - EAP-method messages are transported within EAP messages

WHAT IS WITHIN IEEE 802.1X SPECIFICATION

> IEEE 802.1X specifies:

- That EAP will be used to exchange authentication messages
- A protocol to transport EAP over LAN: EAPOL
EAP transport between Authenticator - Supplicant

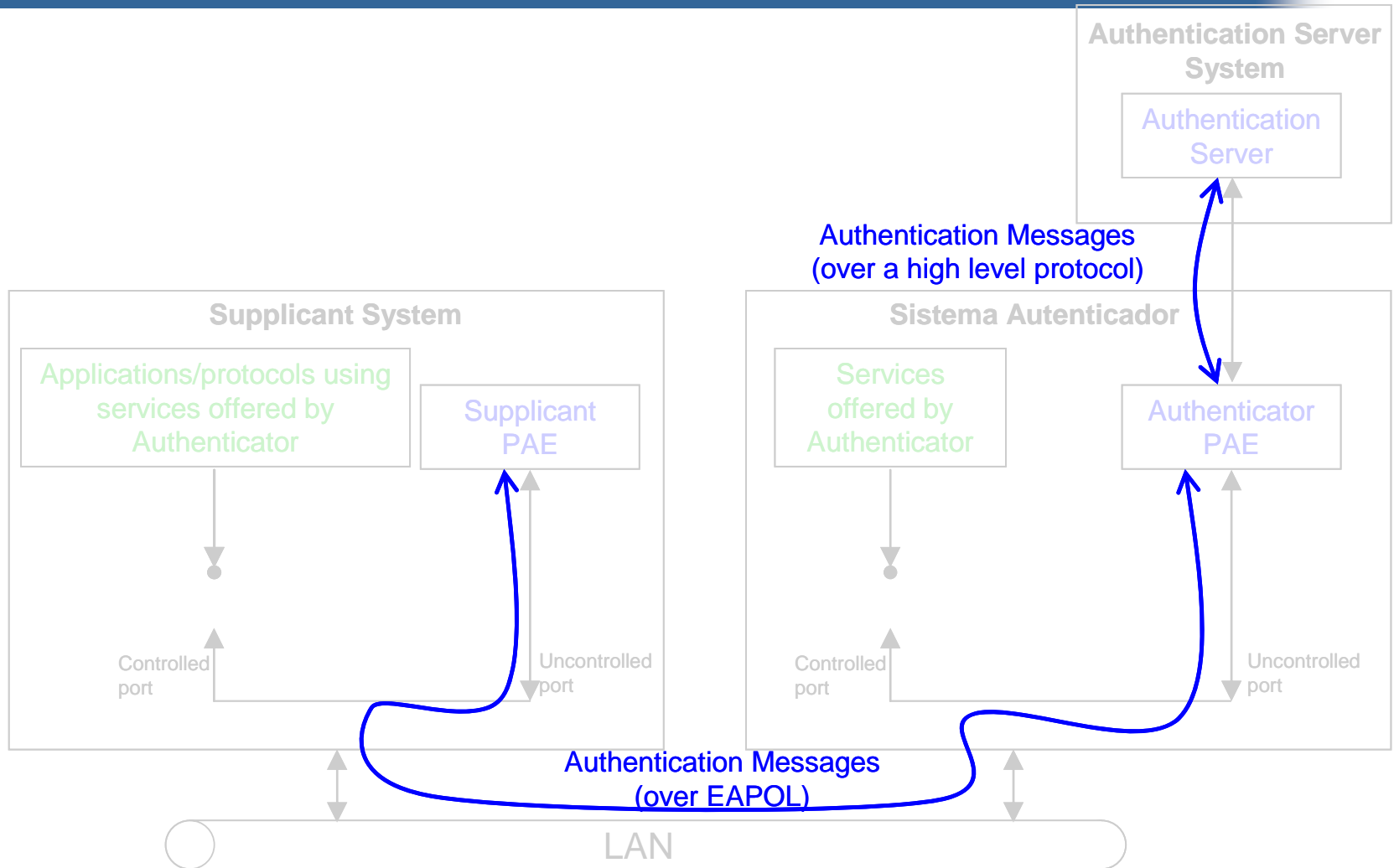
AGAIN, WHAT IS OUTSIDE IEEE 802.1X SPECIFICATION

> IEEE 802.1X doesn't specify:

- How to transport EAP between Authenticator–Authentication Server

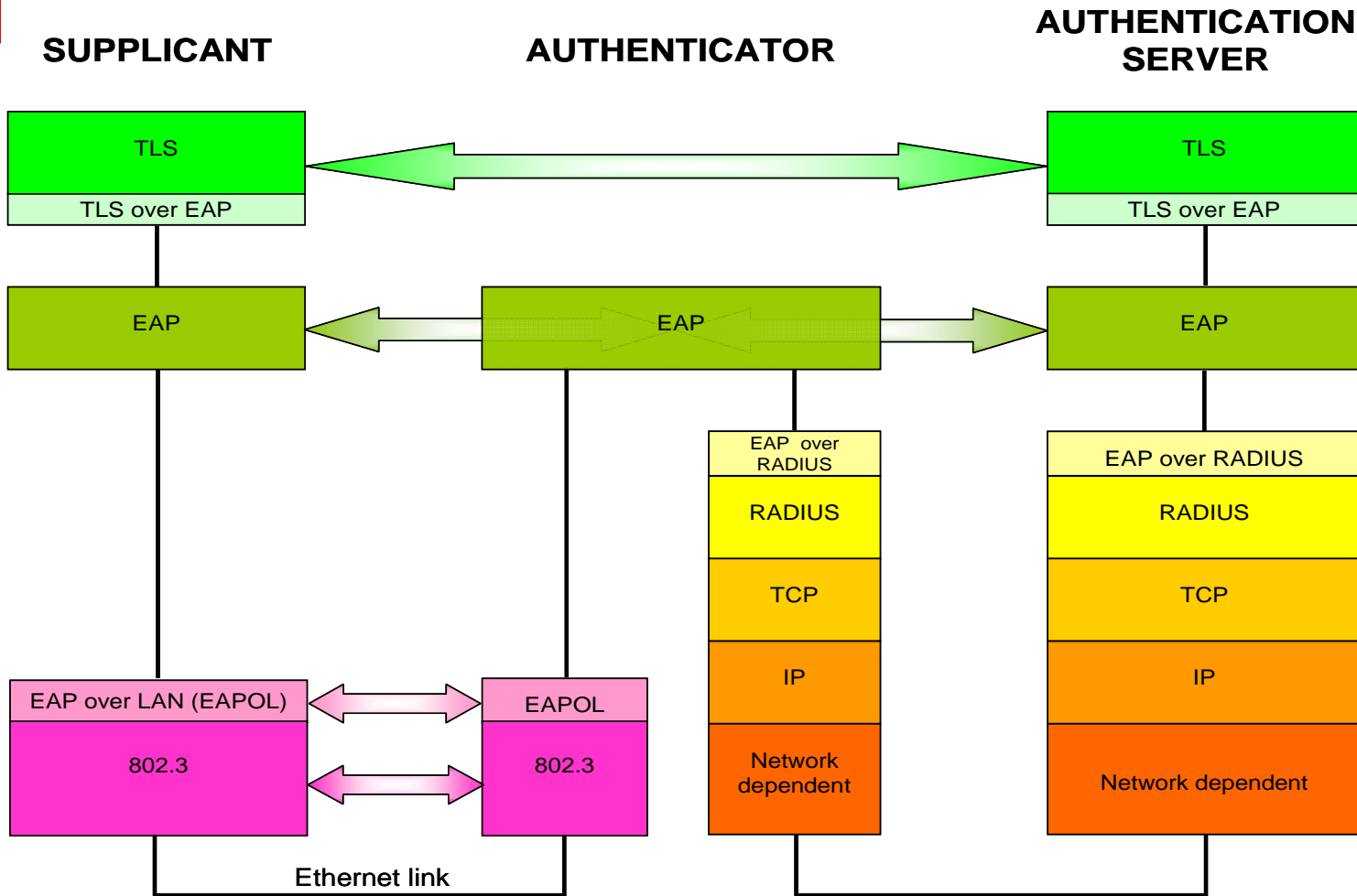
RADIUS is the most deployed, but Diameter, PANA... can be used.

IEEE 802.1X – Authentication

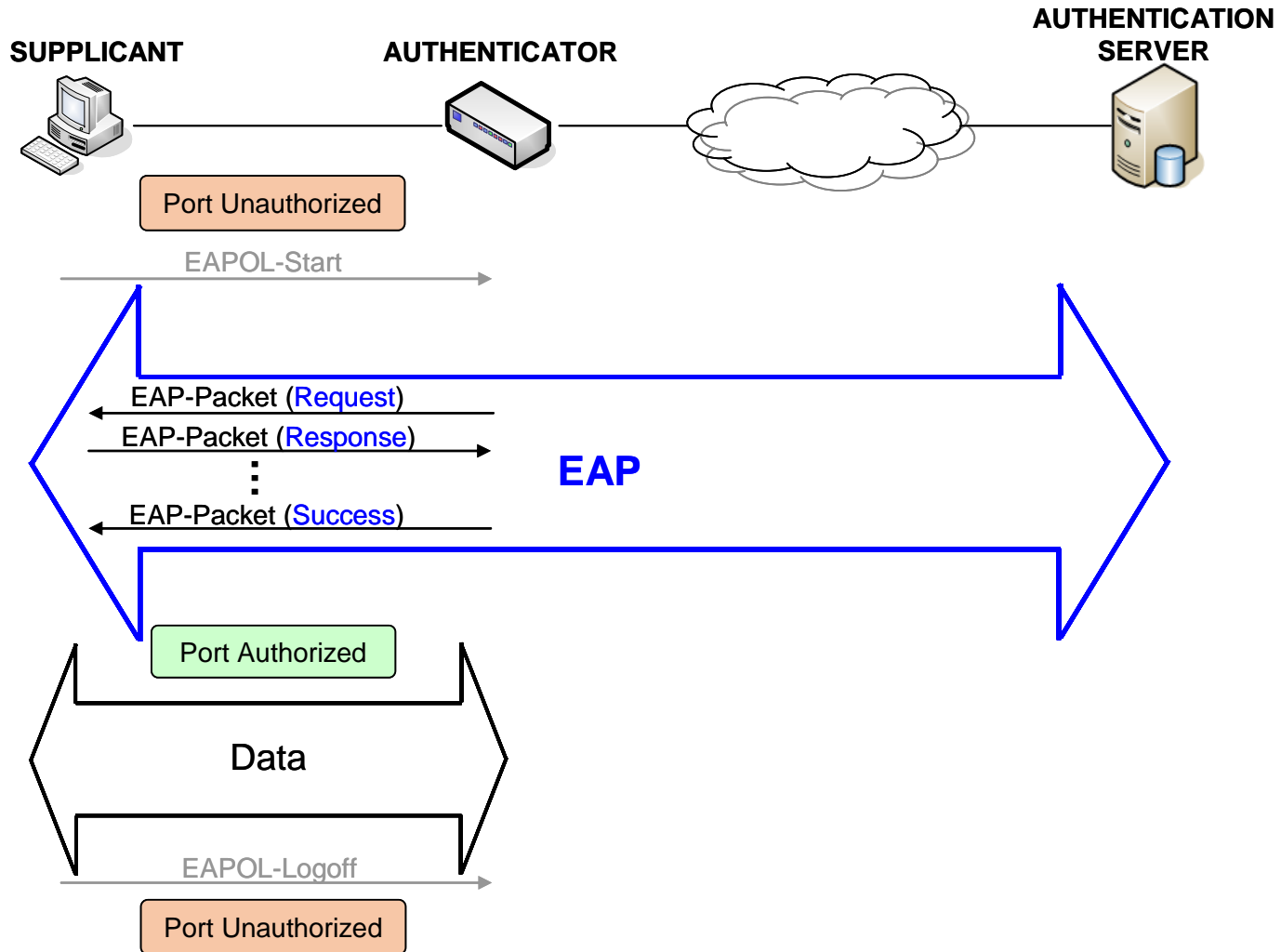


IEEE 802.1X – Authentication protocol stack

Example

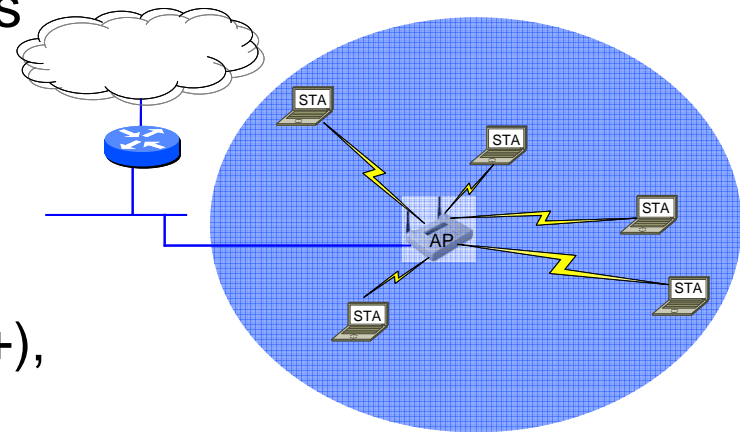


IEEE 802.1X – Authentication exchange



- > Authentication and access control in LAN
- > **Authentication and access control in WLAN**
 - **Similarities and differences with wired LANs**
 - **IEEE 802.11i**
- > Authentication in Broadband Access Networks

- > An infrastructure WLAN can be seen as an evolution of an Ethernet access network where:
 - The access switch is replaced by a wireless access point (AP)
 - The access link is a radio access
 - The devices accessing the network have mobility capabilities within the AP area
- > Therefore, IEEE 802.1X authentication and access control model is valid, in its basics, for WLANs:
 - The AP (Authenticator) controls the access of the mobile stations (Supplicants) to the network
 - After a successful authentication (and +), the AP authorizes the station's traffic



IEEE 802.11: differences with wired LAN



> But there exist also some substantial differences:

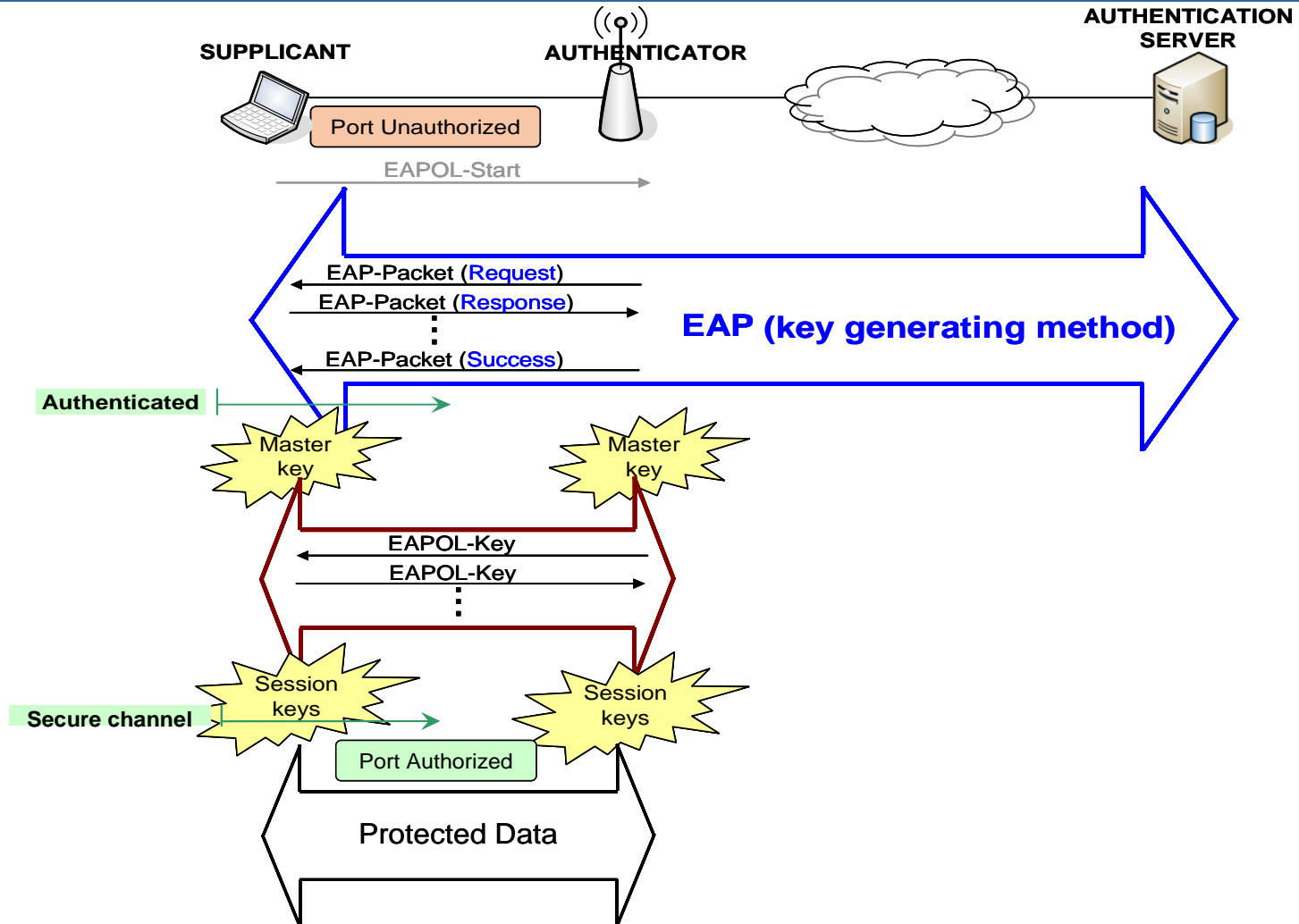
Wired LAN	WirelessLAN	Issue in WLAN	Measure
Point-to-point links... between each station and the switch.	Shared access link... for every station to access the AP.	If the physical port in the AP is authorized after a device successfully authenticates → several devices are authorized	Logical ports (one physical port → several logical ports, each one controlling the access of a different device)
Wired link. Dedicated	Wireless media. Shared	Exchanged traffic easily accesible to possible attackers → eavesdrop, modify contents, replay messages...	Traffic protection (confidentiality and integrity algorithms to protect traffic) (key management)

> WEP:

- Original security mechanisms for WLAN
- Soon proved to be easily vulnerable. Available tools (airsnort, wepcrack...)

> IEEE 802.11i (June 2004)

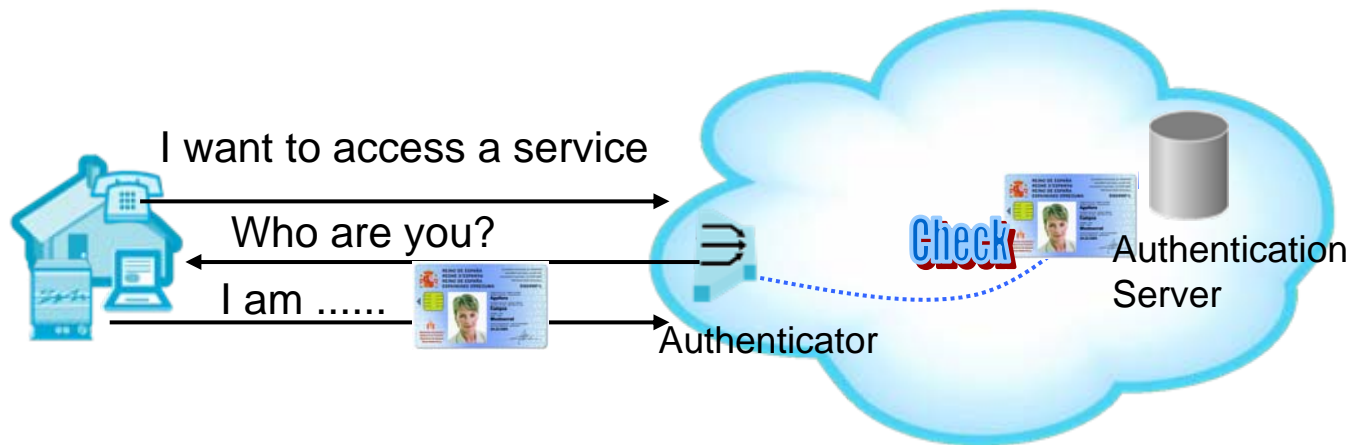
- Reuse of IEEE 802.1X for authentication and control access, per logical port
- Definition of key management protocols to derive session keys
- Definition of two confidentiality and integrity protocols
 - TKIP+Michael: new definition, to upgrade existing equipment (RC4)
 - AES-CCMP



- > Authentication and access control in LAN
- > Authentication and access control in WLAN
 - Similarities and differences with wired LANs
 - IEEE 802.11i
- > **Authentication in Broadband Access Networks**

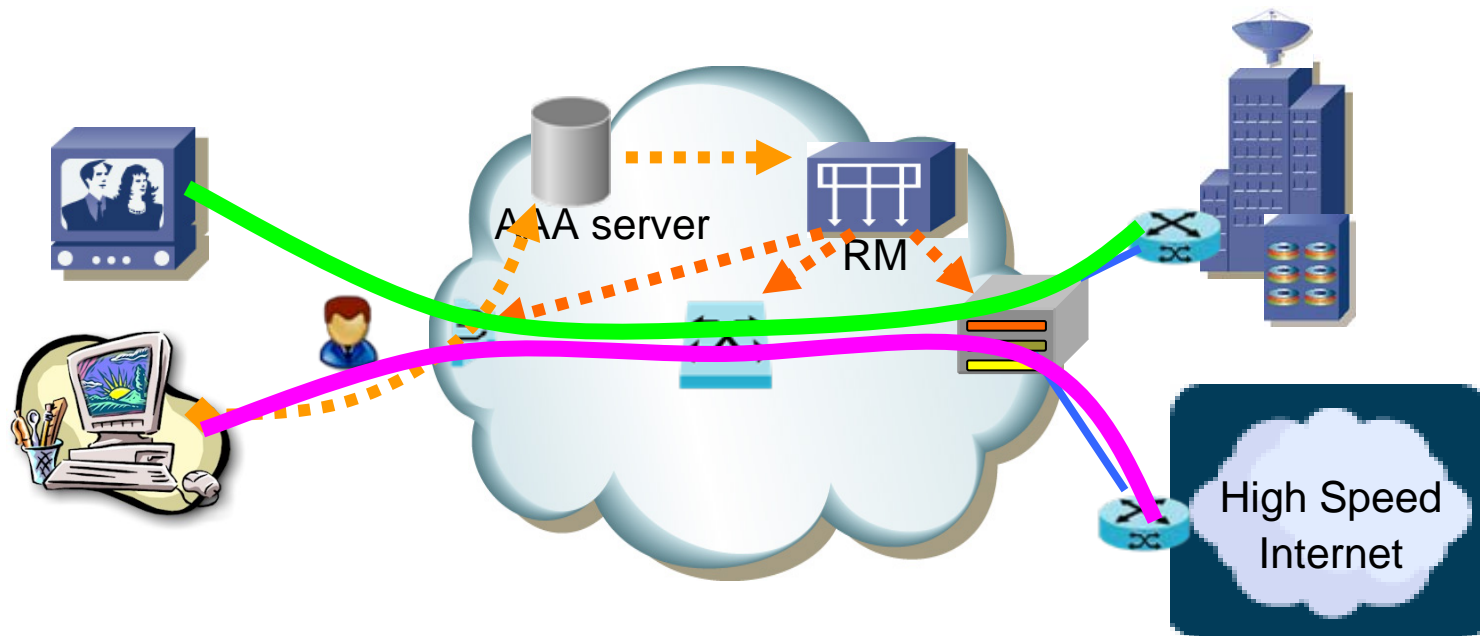
What is authentication in an Access Network

- > It is the process of controlling, recognizing in a reliable way, the identity claimed by another entity.



Why to authenticate?

- The network access provider needs to know your profile, your SLAs (Service Level Agreements):
 - What services you have contracted
 - How they have to be provided

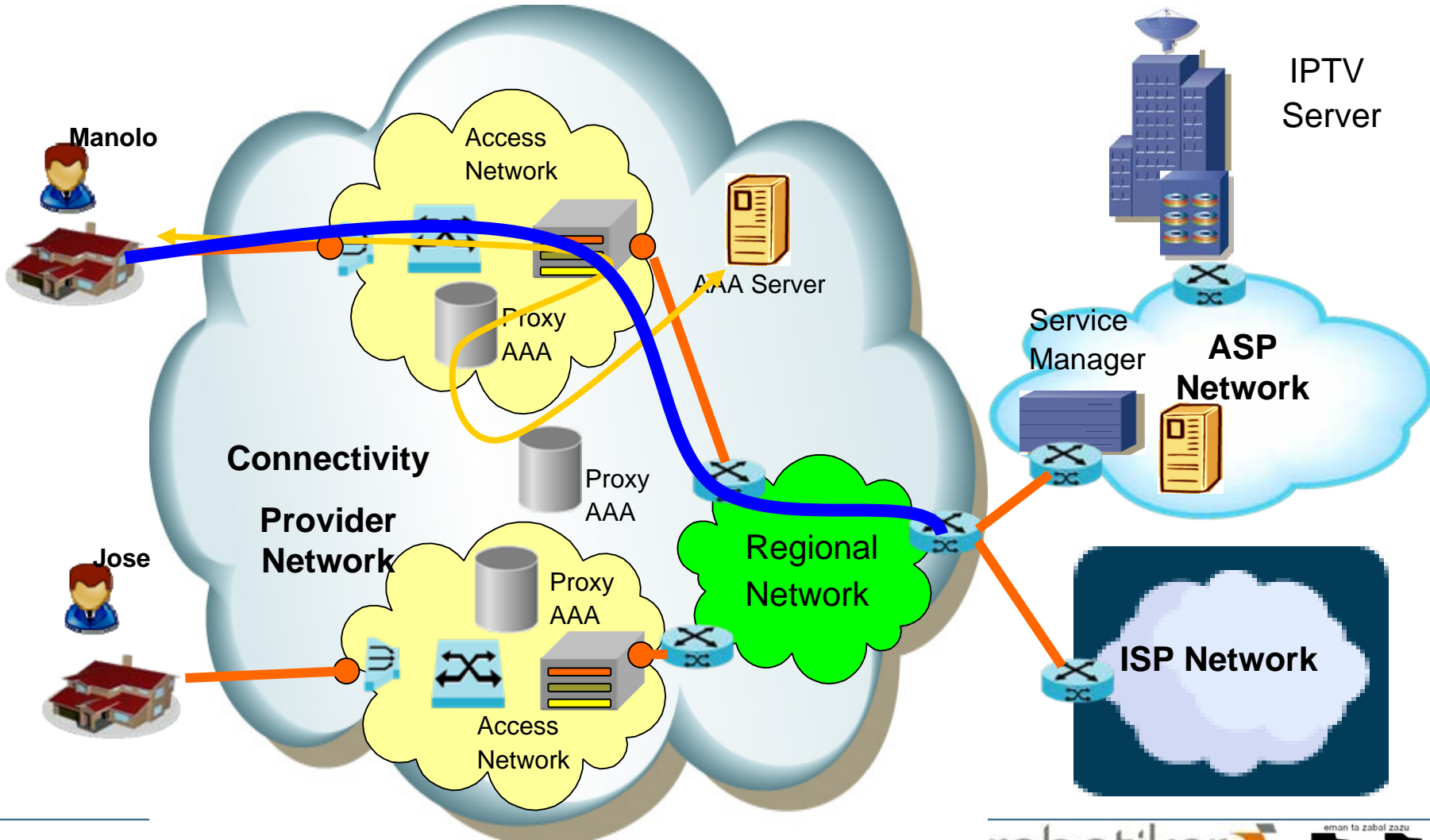


How to authenticate in a BB Access Network?

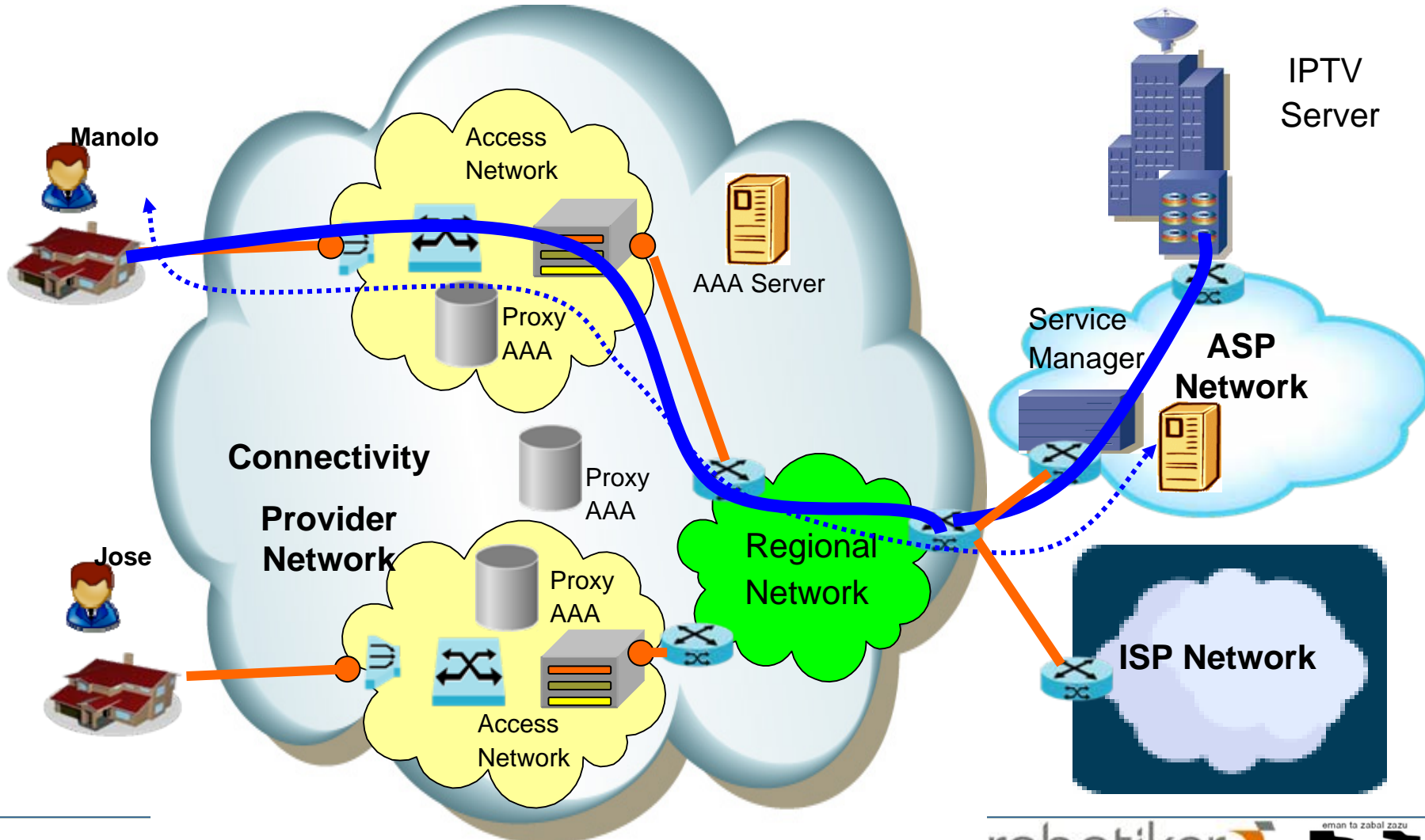


- > By means of:
 - **An Authenticator** -> Collects the authentication credentials from end user's side
 - **An Authentication Server** -> Determines whether those credentials match a known entity, and deduces the authorization rights related to that entity.
- > The entity to be authenticated needs to have some credentials (i.e. unique authentication key) provided by the Authentication server.
- > The credentials will be transmit to the network using devices (i.e. A user giving his/her credentials to a modem).
- > The combination of the device plus the entity's credentials determine the rights to use the network.

Network Authentication

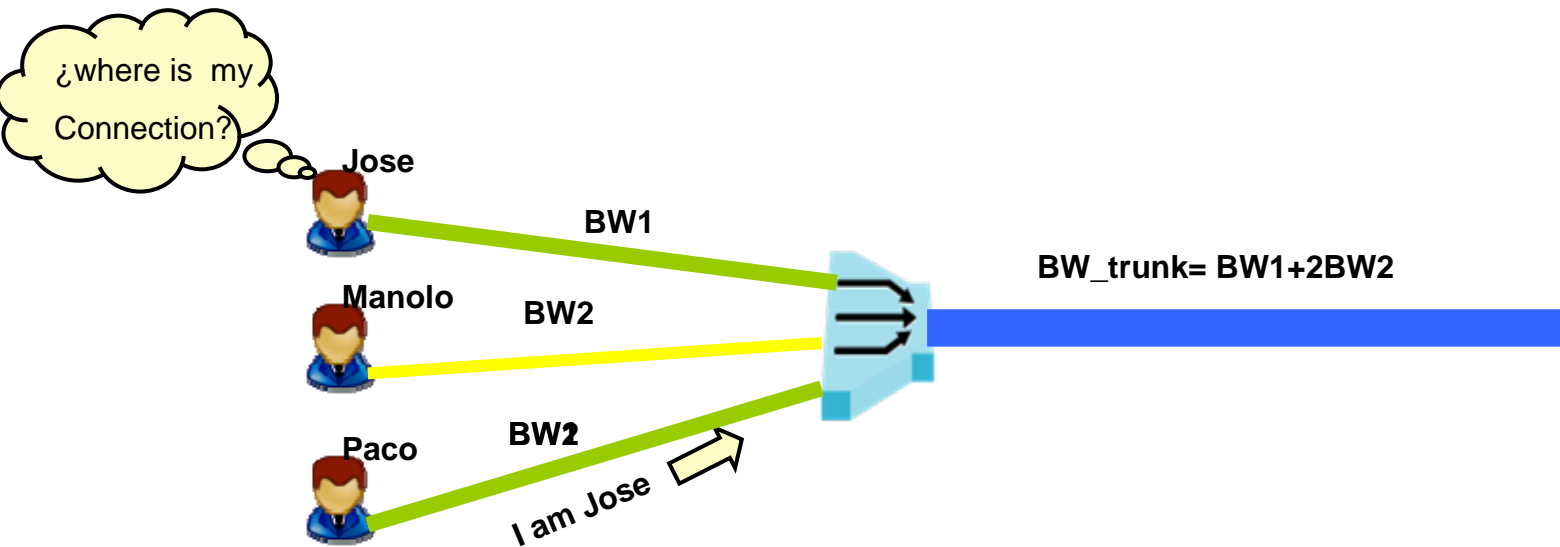


Service Authentication



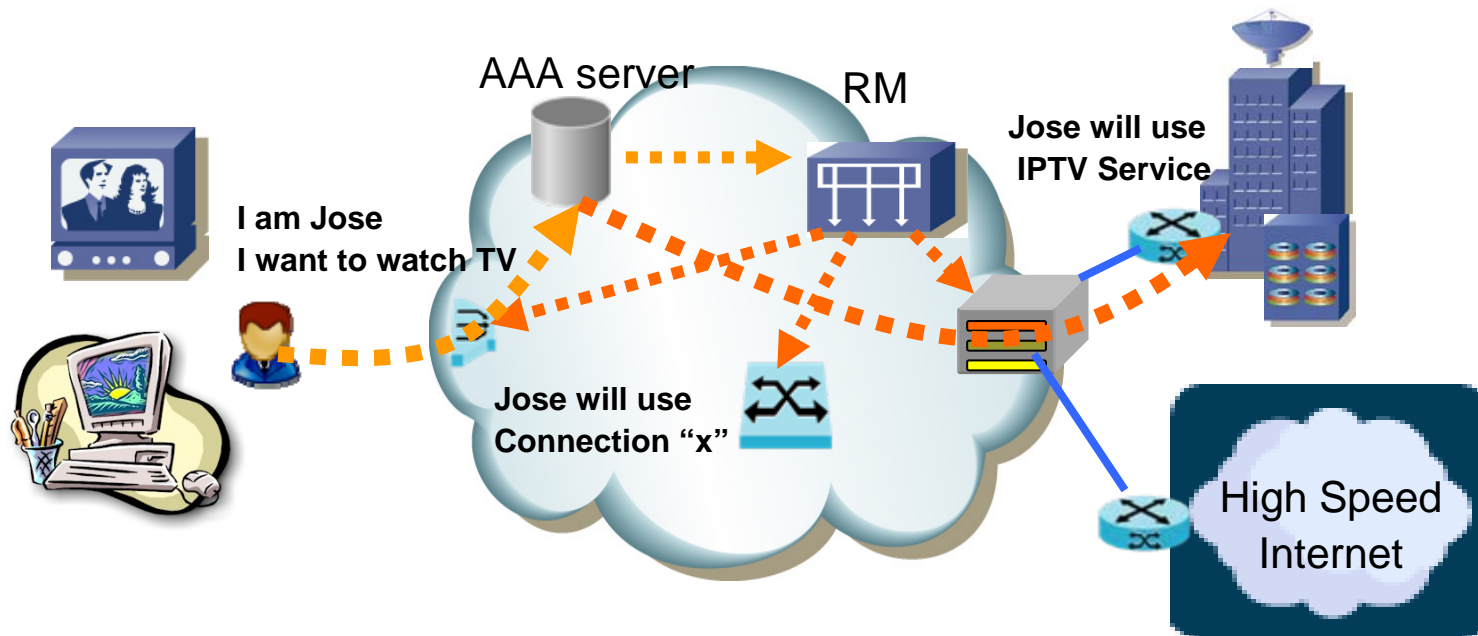
Benefits of Authentication (I)

- > Protect the network and services against unauthorized usage of resources (Bandwidth, access to service servers, IP addresses).



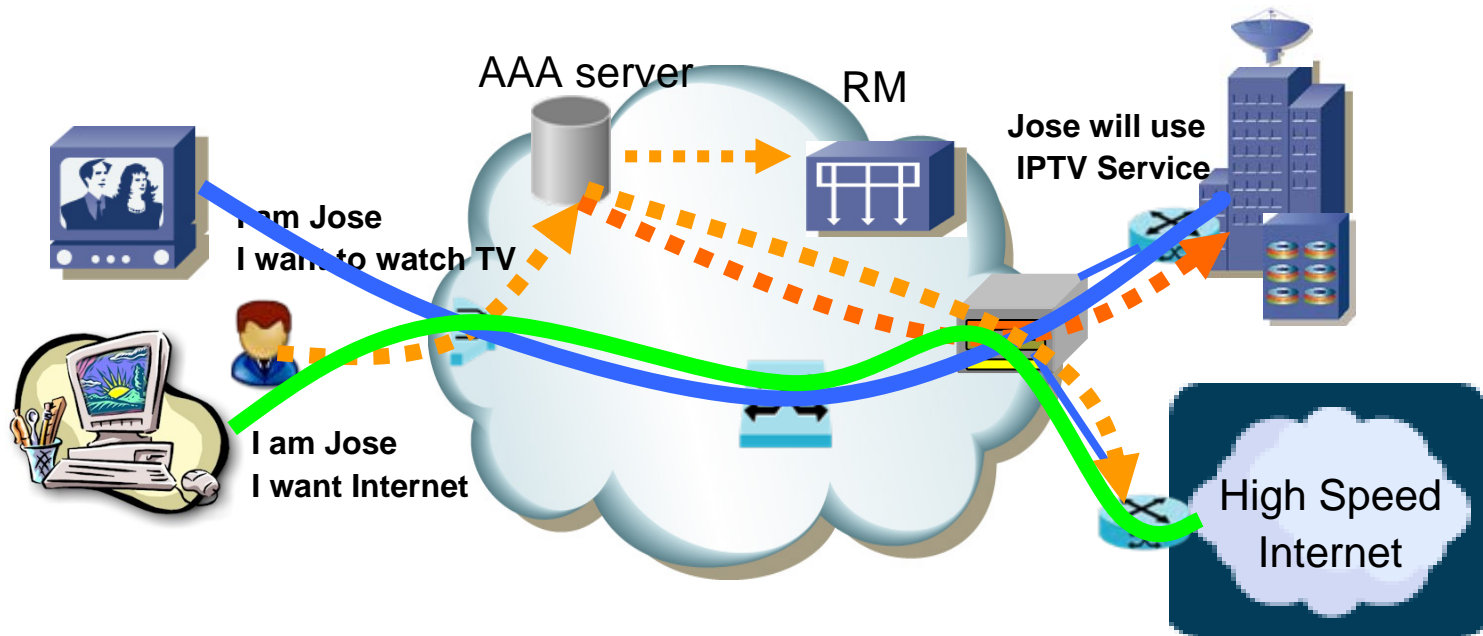
Benefits of Authentication (II)

- Support the collection of billing data and to provide traceability in the network.
 - Traceability can be use for legal interception
 - Traceability can be use for forensics in case of a security failure



Benefits of Authentication (III)

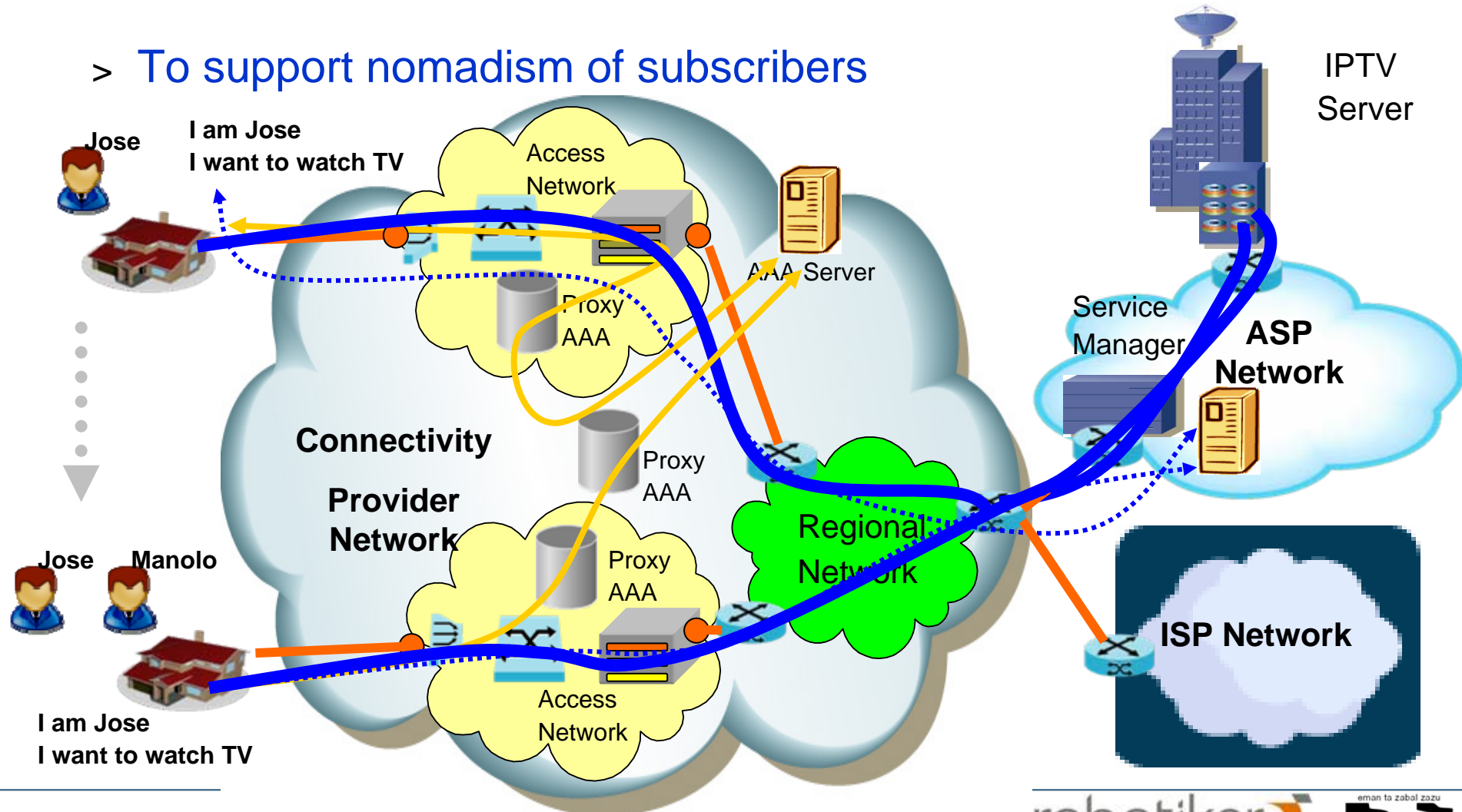
- > To authenticate the network connections needed for different services (possible for different service providers)



Benefits of Authentication (IV)

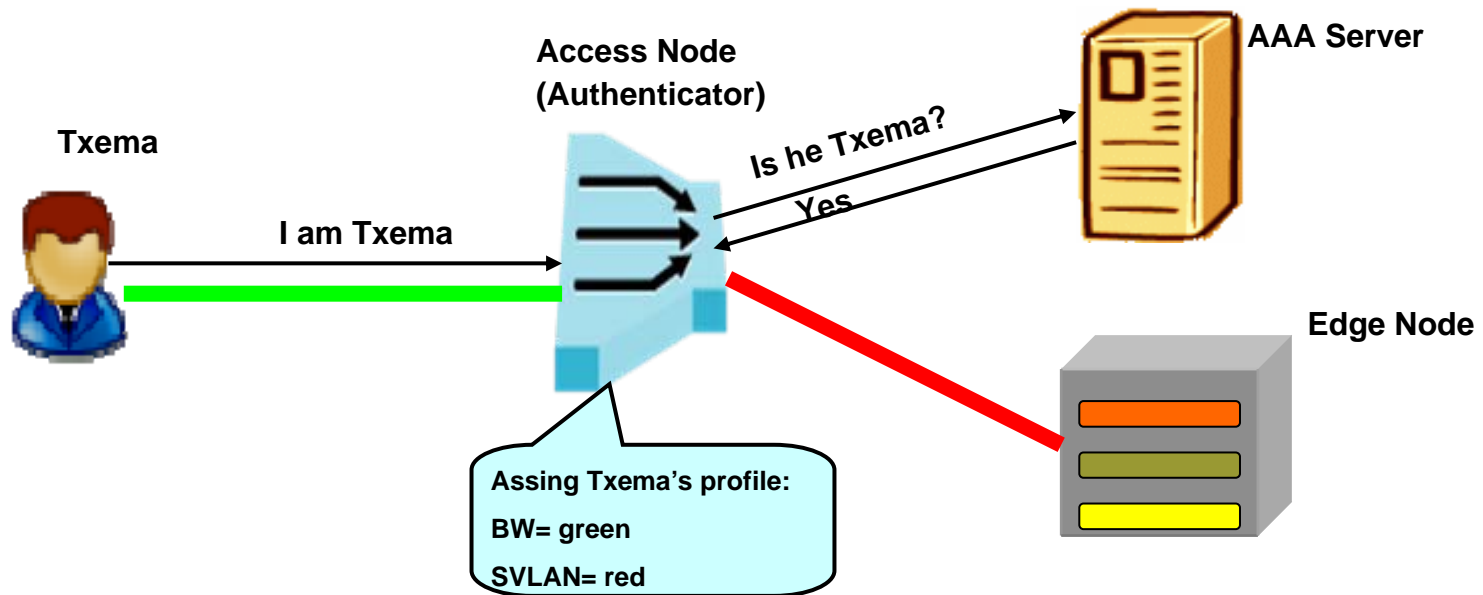


> To support nomadism of subscribers



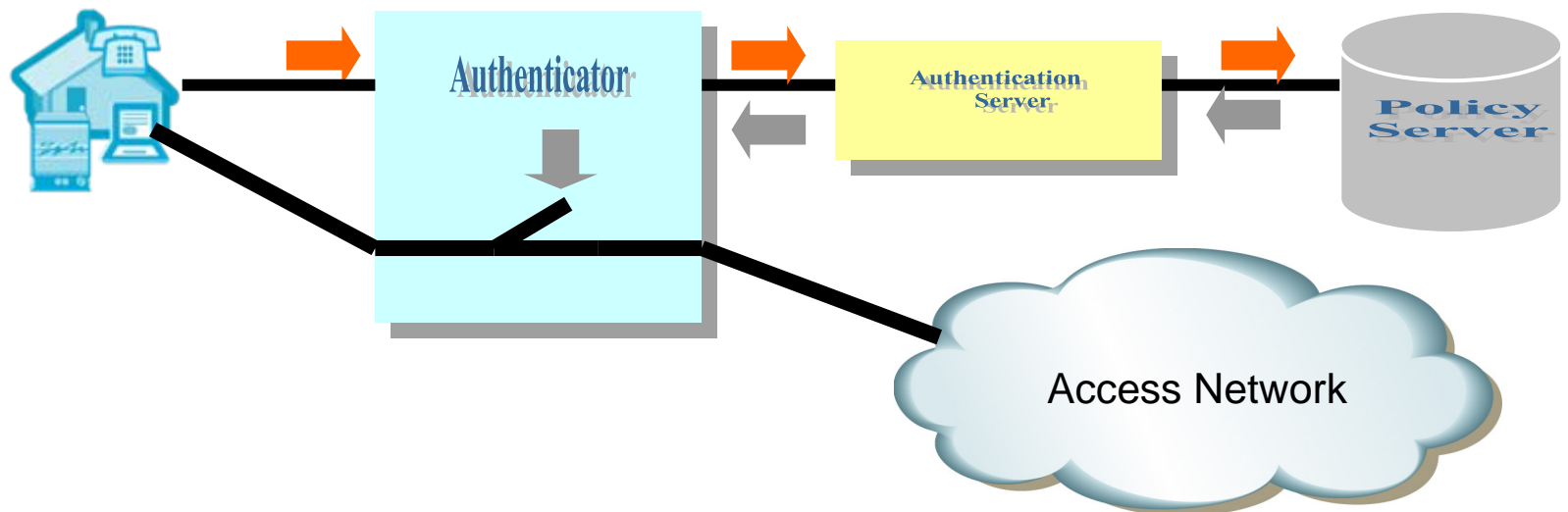
Benefits of Authentication (V)

- > To automate the Access Node (AN) configuration. Upon authentication the AN will dynamically adapt to the customer needs according to the services he/she has subscribed, making more easy the management of the Access Network.



Authorization

- > Is the process of allowing and forbidding an entity to perform a certain set of actions.
- > When performed by a network operator, it is the process of determining and enforcing different network policies for the different clients of the network.



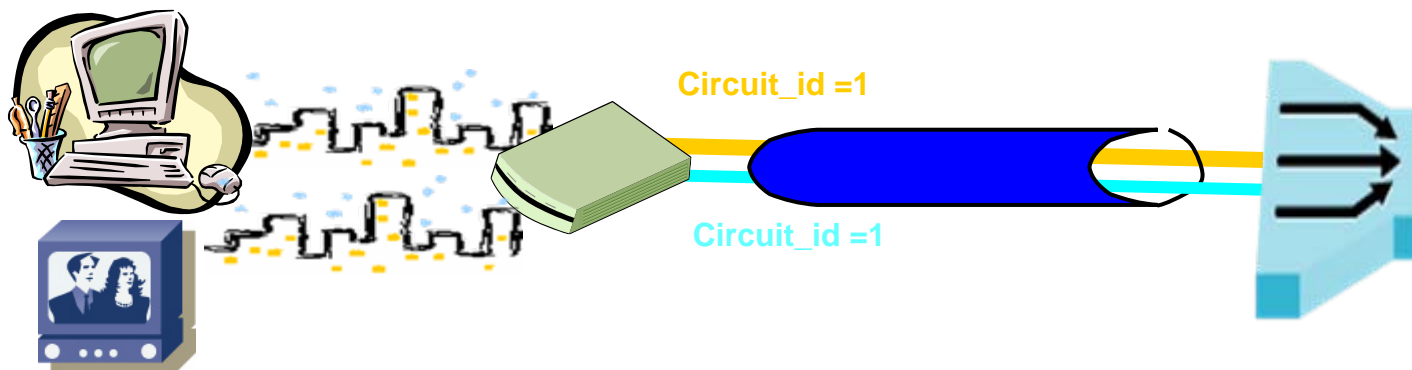
- > Operators implement “Authentication mechanisms” to authorize the authenticated entities the use of its network resources.
- > Authorization take the form of a authorization profile, returned by a policy server to the network node which endorses the role of the authenticator, after the authentication process is completed.
- > The Authorization profile contain a collection of network policies as:
 - Accepted/rejected
 - Access list (list of permitted/forbidden network destinations)
 - Bandwidth for each class of service

What can be authenticated in a BB access network?



- > Subscriber authentication per-line and per-circuit
- > Subscriber authentication per-RG and per-device
- > End-user authentication per device
- > Physical device authentication and subscriber authentication per-physical-device
- > Device type authentication

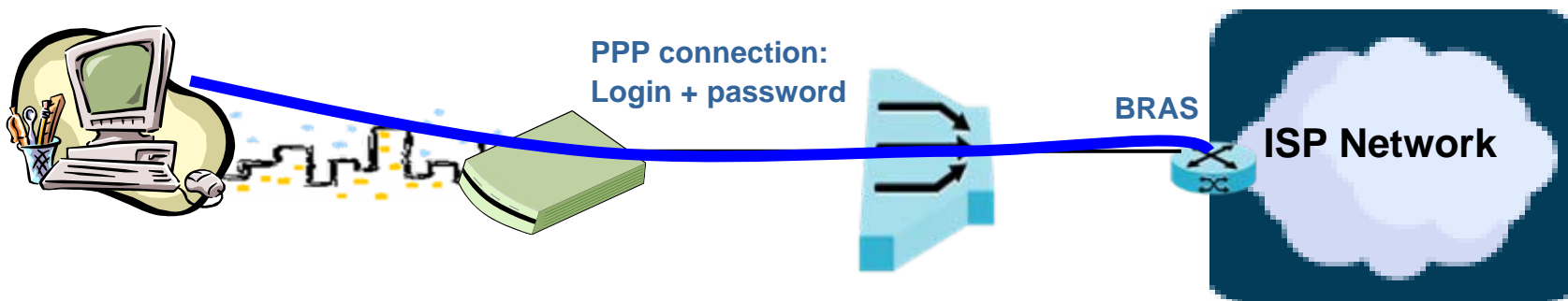
- > This is typically done today for point-to-point connections
- > The Access Node provides a circuit identifier to the client.
- > Any device connected to that circuit is authenticated.
- > Examples of circuit_id: PVCs in ATM or VLANs in Ethernet.



- > When there is a single circuit per access loop, **the identification is per line.**

Subscriber authentication per-RG and per-device

- > The device which exchanges its credentials with the network is controlled by the subscriber.
- > If the device is the **Residential Gateway** the effect is the same as with per-line identification (no distinction between devices)
- > The subscriber can change the credentials in the device corresponding to his service subscriptions.



- > If **multiple devices** at home exchange individually their credentials with the network, they will be identified individually.

End-user authentication per-device



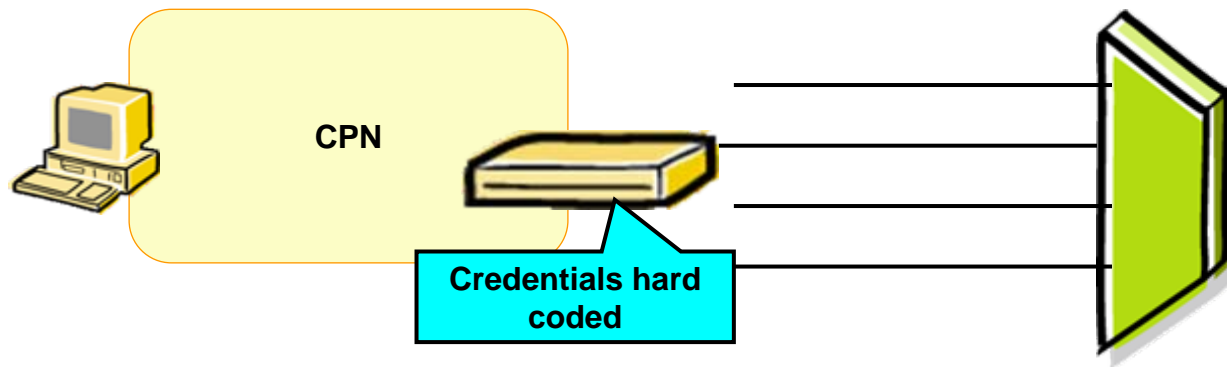
- > An end-user can enter his/her credentials into a device by means of an smart card, dongle or even manually.
- > Those credentials belong to the users, and they do not leave them permanently on a device, quite the opposite the user carries the credentials with him/her. Thus, **the end-user is always authenticated per device.**
- > In other words, when the credentials can be entered by the temporary user of a terminal the entity authenticated is the end-user.
- > However, when the device which exchanges its credentials with the network is a given terminal in the home network, **the authentication is per-device.**

End-user authentication per-device



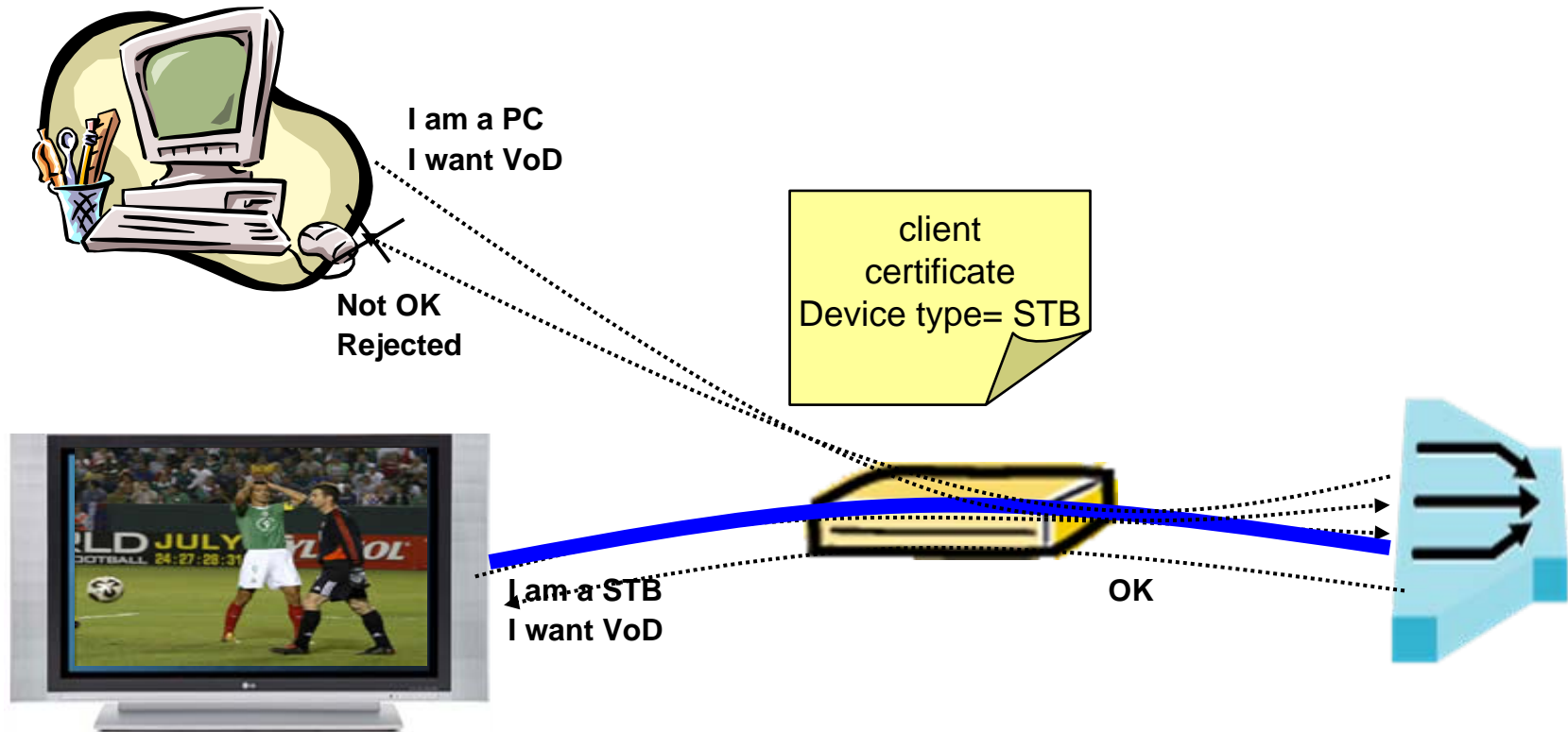
Physical device authentication and subscriber authentication per-physical-device

- > The entity authenticated can be the physical device if there are unique credentials hard-coded into the Residential Gateway.
- > From the point of view of a network operator, authenticating the physical device does not replace a subscriber or an end-user authentication.
- > If the operator trusts the associations between each physical device and subscriber, then the subscriber can be authenticated per-physical-device.



- > If the intention is to authenticate a device as pertaining to a particular type of devices, not to authenticate the individual physical device itself, then the entity authenticated is the device type.
- > The device type can be part of the credential which are provided by the device to the authenticator.
- > The device type must be hard-coded or only configurable by operator.
- > Example, an operator may want to restrict access to a premium VoD service only to a STB of a certified type and block the service from being provide to a PC.

Device type authentication



Summary of the factors impacting the authenticated entities



		1/ What is the device which provides the credentials to the network ?		
		Access Node	Residential Gateway	Individual device behind RG
2/ How are the credentials provided to that device ?	Hard coded in factory or Configurable by the operator only	Subscriber per line or Subscriber per circuit	Physical RG ; Type of RG ; Subscriber per physical RG ,	Physical device ; Type of device ; Subscriber per physical device ;
	Configurable by the subscriber or From a smart card per subscriber	N/A	Subscriber per RG	Subscriber per device
	Configurable by individual end users or From a smart card per end user	N/A	N/A	End user per device
		→ What entity can a network operator authenticate from the credentials ?		

- > **Use Case 1:** Dynamic configuration of the access network according to the subscriber profile.
 - **Use case 1.1: Subscriber dynamic authentication** to allow dynamic configuration of the Access Node, and ease the provisioning of triple play services.
 - **Use case 1.2: Subscriber authentication** to allow nomadism. If not done dynamically it will take too long to reconfigure the network.
 - **Use case 1.3: End-user authentication** to allow Network-level Parental control. Different members of the family can have different policies to access the network (i.e. restriction in some network destinations).

- > **Use Case 2:** Denying access to stolen or hacked devices, or allowing only certain device type.
 - **Use case 2.1: Device type authentication** to allow only a device type (i.e. an specific STB) or to only trusted network entities (i.e. check that the RG is the one provided by the operator)
 - **Use case 2.2: Physical device authentication** denying access to stole RG/devices. Checking if the credentials provided by the RG/device authenticate an authorized equipment or not.

- > **Use Case 3: Authentication used for accounting.**
 - **Use case 3.1: Subscriber authentication** to allow charging on their use of the network (per GB, time, traffic, ..)
 - **Use case 3.2: End-user authentication** to allow charging per user (i.e. to differentiate between business use and private, or to charge nomadic or visiting users).
 - **Use case 3.3: Subscriber authentication** to allow charging other Service subscribers. To allow the network provider to charge the Service providers for the use of the network.

- > **Use Case 4:** Authentication used for other reasons.
 - **Use case 4.1: Subscriber authentication** is mandatory for ISPs, who must be able to know and to remember at all time what IP address was allocated to what subscriber at what time.
 - **Use case 4.2: Subscriber authentication:** Legal interceptions. The authorities may request to intercept or duplicate traffic originating from or destined to some particular subscribers, and thus subscriber authentication is required.

Use cases classification



		Use cases								
		1.1 Dynamic network provisioning	1.2 Allow nomadism	1.3 Parental control	2.1 Device type (trusted)	2.2 Stolen device	3 Charge subscriber	4 ISP Legal intercept	Deduction over the levels of importance	
Entities required to be Authenticated	Subscriber per line	Required					Required	Required	1	
	Subscriber per circuit	Required					Optional	Optional	1	
	Subscriber per RG	Required	Optional				Required	Required	1	
	Subscriber per device	Optional	Required				Required	Required	2	
	End user per device	Optional	Optional	Required			Optional	Optional	3	
	Physical device				Optional	Required	Optional		4	
	Device type				Required				2	
	Order of priorities	1	2	3	2	4	1	1		

Order of priorities: probability to be deploy by network operators in the short term

Different alternatives to provide “AA”



> Some comparisons:

Method	Layer i NW stack	[D]raft/[S]table	EAP support	X-SIM compatible	Mutual authentication	L2 switch traversal	Router traversal	NAT traversal	Secure comm. channel
802.1x	2	S	Y	Y	Possible	Y (but with restrictions)	N	N	N (802.11i does provide)
PANA	3	D	Y	Y	Possible	Y	N (but probably soon)	N	Can be bootstrapped
DHCP option 90	2-3	S	Y (only indirectly)	Y	Possible	Y	N	N	-
Capture portal	5	Propreitary solutions	Y	N	Typically not possible	Y	Y	Y	N

> EAP as framework for performing AA

- EAP-SIM, EAP-AKA, EAP-TTLS, ...

- Authentication in access networks is a must in order to setup correctly the connections to the subscribers.
- Authentication can be done in different ways, depending on the granularity required and the services provided.
- The trend in broadband networks towards multiservice multiprovider access networks makes authentication per circuit not sufficient and requiring an identification of the end user.
- The trend towards the separation between the Service providers and Connectivity providers requires a correct accounting of the resources consumed.

The future of Broadband networks lies on the new Authentication