

The different Versions of

802.11X

Karsten Iwen

 @KarstenIwen



The different Versions of

802.1X

Karsten Iwen




 @KarstenIwen

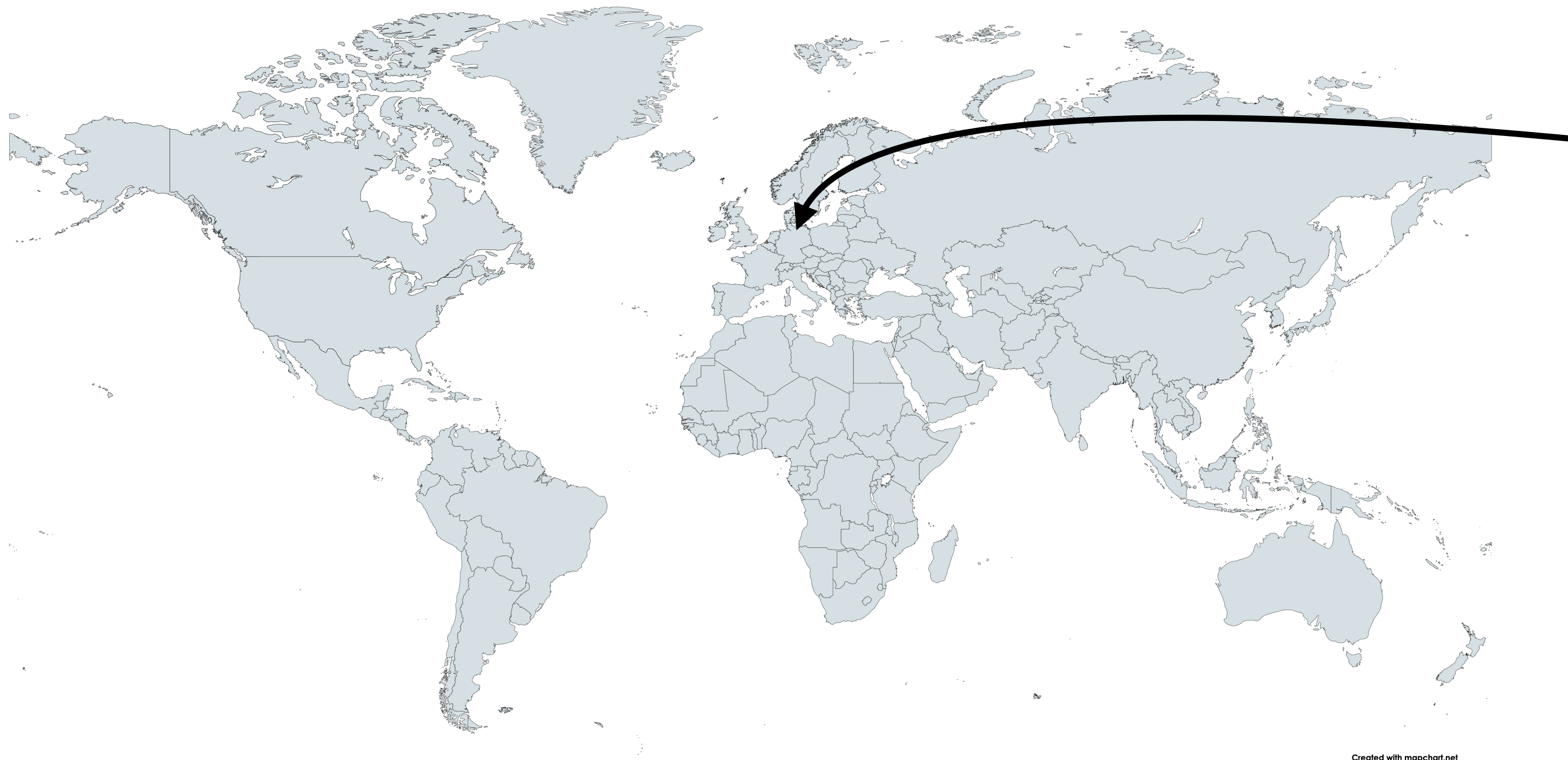


About Me

Karsten Iwen

• Freelance Consultant/Trainer

-  @KarstenIwen
-  <https://www.iwen.de>
-  <https://cyber-fi.net> (Blog)



Created with mapchart.net



IEEE Standard for Local and Metropolitan Area Networks Port-Based Network Access Control

1 1 or 1, x or X
What's in the name?

1 1 or 1, x or X
What's in the name?

802.1 1X

1 1 or 1, x or X

What's in the name?

802.1 1X



11 or 1, x or X What's in the name?

802.11X

The screenshot shows a Twitter thread. The top tweet is from Jennifer (JJ) Minella (@jjx) dated 1. Nov. 2021, stating: "It's ONE X. 802.1X not 802.11X. Save the world. Right this wrong. #WIFI #8021X #RADIUS #NetworkRehab". Below it is a tweet from Ekahau (@ekahau) dated 25. Okt. 2021 at 10:31 nachm., which includes a link to a resource and a thumbnail image of a diagram titled "802.1X & EAP Ladder Diagram". The diagram shows a sequence of messages between a client and a server. The Ekahau logo and "WIRELESS DESIGN" are visible in the bottom right of the diagram thumbnail.

1 1 or 1, x or X

What's in the name?

802~~1~~ 1X

802~~1~~ x

802~~1~~ 1 x

802.1X ✓

The different versions of 802.1X

```
> Frame 3: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface en7, id 0
> Ethernet II, Src: (Client)WLAN-Pi-eth0 (02:01:5b:f0:f9:20), Dst: Nearest-non-TPMR-bridge (01:80:c2:00:00:03)
< 802.1X Authentication
  Version: 802.1X-2001 (1)
  Type: EAP Packet (0)
  Length: 14
> Extensible Authentication Protocol
```

```
> Frame 8: 187 bytes on wire (1496 bits), 187 bytes captured (1496 bits)
> Prism capture header
> 802.11 radio information
> IEEE 802.11 QoS Data, Flags: .....F.
> Logical-Link Control
< 802.1X Authentication
  Version: 802.1X-2004 (2)
  Type: EAP Packet (0)
  Length: 5
> Extensible Authentication Protocol
```

```
> Radiotap header v0, Length 25
> 802.11 radio information
> IEEE 802.11 QoS Data, Flags: .....F.C
> Logical-Link Control
< 802.1X Authentication
  Version: 802.1X-2010 (3)
  Type: EAP Packet (0)
  Length: 6
> Extensible Authentication Protocol
```

```
> Frame 189: 211 bytes on wire (1688 bits), 211 bytes captured (1688 bits) on interface wlanp:
> Radiotap Header v0, Length 56
> 802.11 radio information
> IEEE 802.11 QoS Data, Flags: .....F.
> Logical-Link Control
< 802.1X Authentication
  Version: 802.1X-2004 (2)
  Type: Key (3)
  Length: 117
  Key Descriptor Type: EAPOL RSN Key (2)
  [Message number: 1]
> Key Information: 0x008a
  Key Length: 16
  Replay Counter: 0
  WPA Key Nonce: bce46804f541f994513d090857e6602d5c4b882b4988ae6d266cdd659f1e40d2
  Key IV: 00000000000000000000000000000000
  WPA Key RSC: 0000000000000000
  WPA Key ID: 0000000000000000
  WPA Key MIC: 00000000000000000000000000000000
  WPA Key Data Length: 22
> WPA Key Data: dd14000fac04504ca5be4f8834b6f1a55abc85200450
```

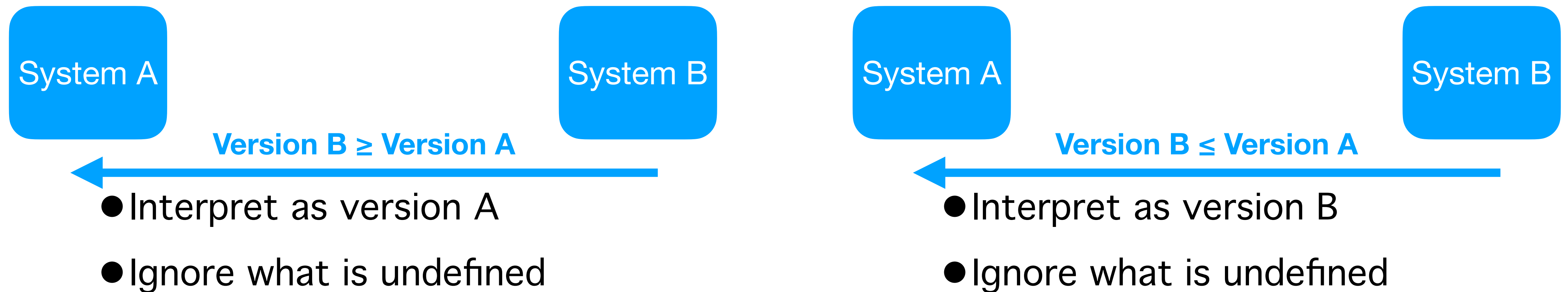
Is this relevant for us?

NOT AT ALL!

The different versions of 802.1X

- IEEE 802.1X-2001
- IEEE 802.1X-2004
- IEEE 802.1X-2010
 - 802.1Xbx-2014 - Amendment 1: MAC Security Key Agreement Protocol (MKA) Extensions
 - 802.1Xck-2018 - Amendment 2: YANG Data Model
- IEEE 802.1X-2020

Handling of different Versions



IEEE Std 802.1X-2001, IEEE Std 802.1X-2004

7.5.7 Validation of received EAPOL frames and EAPOL protocol version handling

IEEE Std 802.1X-2010, IEEE Std 802.1X-2020

11.5 EAPOL protocol version handling

Handling of different Versions

Window title: eapol and wlan.ta == 7c:21:0d:9d:84:e9

No.	Time	Transmitter	Receiver	Frame Type	Version
16	0.143352	(AP)-9120-9k8	(Client)-iPhone13Pro	EAP	802.1X-2010
19	0.196647	(AP)-9120-9k8	(Client)-iPhone13Pro	EAP	802.1X-2010
27	0.264693	(AP)-9120-9k8	(Client)-iPhone13Pro	EAP	802.1X-2010
30	0.297336	(AP)-9120-9k8	(Client)-iPhone13Pro	EAP	802.1X-2010
161	3.565297	(AP)-9120-9k8	(Client)-iPhone13Pro	EAP	802.1X-2010
168	3.597655	(AP)-9120-9k8	(Client)-iPhone13Pro	EAP	802.1X-2010
171	3.630276	(AP)-9120-9k8	(Client)-iPhone13Pro	EAP	802.1X-2010
178	3.748148	(AP)-9120-9k8	(Client)-iPhone13Pro	EAP	802.1X-2010
181	3.780846	(AP)-9120-9k8	(Client)-iPhone13Pro	EAP	802.1X-2010
188	3.872547	(AP)-9120-9k8	(Client)-iPhone13Pro	EAP	802.1X-2010
189	3.876516	(AP)-9120-9k8	(Client)-iPhone13Pro	EAPOL	802.1X-2004
196	3.903581	(AP)-9120-9k8	(Client)-iPhone13Pro	EAPOL	802.1X-2004



Window title: eapol and wlan.ta == d6:08:7a:89:54:38

No.	Time	Transmitter	Receiver	Frame Type	Version
17	0.148696	(Client)-iPhone13Pro	(AP)-9120-9k8	EAP	802.1X-2001
24	0.221450	(Client)-iPhone13Pro	(AP)-9120-9k8	EAP	802.1X-2001
25	0.221934	(Client)-iPhone13Pro	(AP)-9120-9k8	EAP	802.1X-2001
28	0.266697	(Client)-iPhone13Pro	(AP)-9120-9k8	EAP	802.1X-2001
159	3.525544	(Client)-iPhone13Pro	(AP)-9120-9k8	EAP	802.1X-2001
162	3.567670	(Client)-iPhone13Pro	(AP)-9120-9k8	EAP	802.1X-2001
169	3.599951	(Client)-iPhone13Pro	(AP)-9120-9k8	EAP	802.1X-2001
172	3.633084	(Client)-iPhone13Pro	(AP)-9120-9k8	EAP	802.1X-2001
179	3.750373	(Client)-iPhone13Pro	(AP)-9120-9k8	EAP	802.1X-2001
182	3.782849	(Client)-iPhone13Pro	(AP)-9120-9k8	EAP	802.1X-2001
190	3.877610	(Client)-iPhone13Pro	(AP)-9120-9k8	EAPOL	802.1X-2004
197	3.904581	(Client)-iPhone13Pro	(AP)-9120-9k8	EAPOL	802.1X-2004



IEEE 802.1X-2001

- Initial Version
- 7.5.3 Protocol version = 1
- Only Key Descriptor for RC4
- 7.8 „This standard refers to EAP carried in RADIUS as a basis of these exchanges; however, the use of other protocols to achieve these exchanges is permitted.“
- D.1 „Although RADIUS support is optional within IEEE Std 802.1X-2001, it is expected that most IEEE Std 802.1X-2001 Authenticators will function as RADIUS clients.“

IEEE 802.1X-2004

- Same purpose as IEEE 802.1X-2001
- More detailed purpose and scope
- More Definitions and abbreviations explained
- New IEEE 802.11 Key Descriptor Type => RSN
- RC4 Key Descriptor Type defined as „deprecated“
- Mentions also Diameter as an example of an AAA protocol

IEEE 802.1X-2004

- Same purpose as IEEE 802.1X-2001
- More detailed purpose and scope
- More Definitions and abbreviations explained
- New IEEE 802.11 Key Descriptor Type => RC4
- RC4 Key Descriptor Type defined as „deprecated“
- Mentions also Diameter as an example of an AAA protocol

```
> Frame 189: 211 bytes on wire (1688 bits), 211 bytes captured (1688 bits) on interface wlanp:
> Radiotap Header v0, Length 56
> 802.11 radio information
> IEEE 802.11 QoS Data, Flags: .....F.
> Logical-Link Control
< 802.1X Authentication
  Version: 802.1X-2004 (2)
  Type: Key (3)
  Length: 117
  Key Descriptor Type: EAPOL RSN Key (2)
  [Message number: 1]
  > Key Information: 0x008a
  Key Length: 16
  Replay Counter: 0
  WPA Key Nonce: bce46804f541f994513d090857e6602d5c4b882b4988ae6d266cdd659f1e40d2
  Key IV: 00000000000000000000000000000000
  WPA Key RSC: 0000000000000000
  WPA Key ID: 0000000000000000
  WPA Key MIC: 00000000000000000000000000000000
  WPA Key Data Length: 22
  > WPA Key Data: dd14000fac04504ca5be4f8834b6f1a55abc85200450
```

IEEE 802.1X-2004

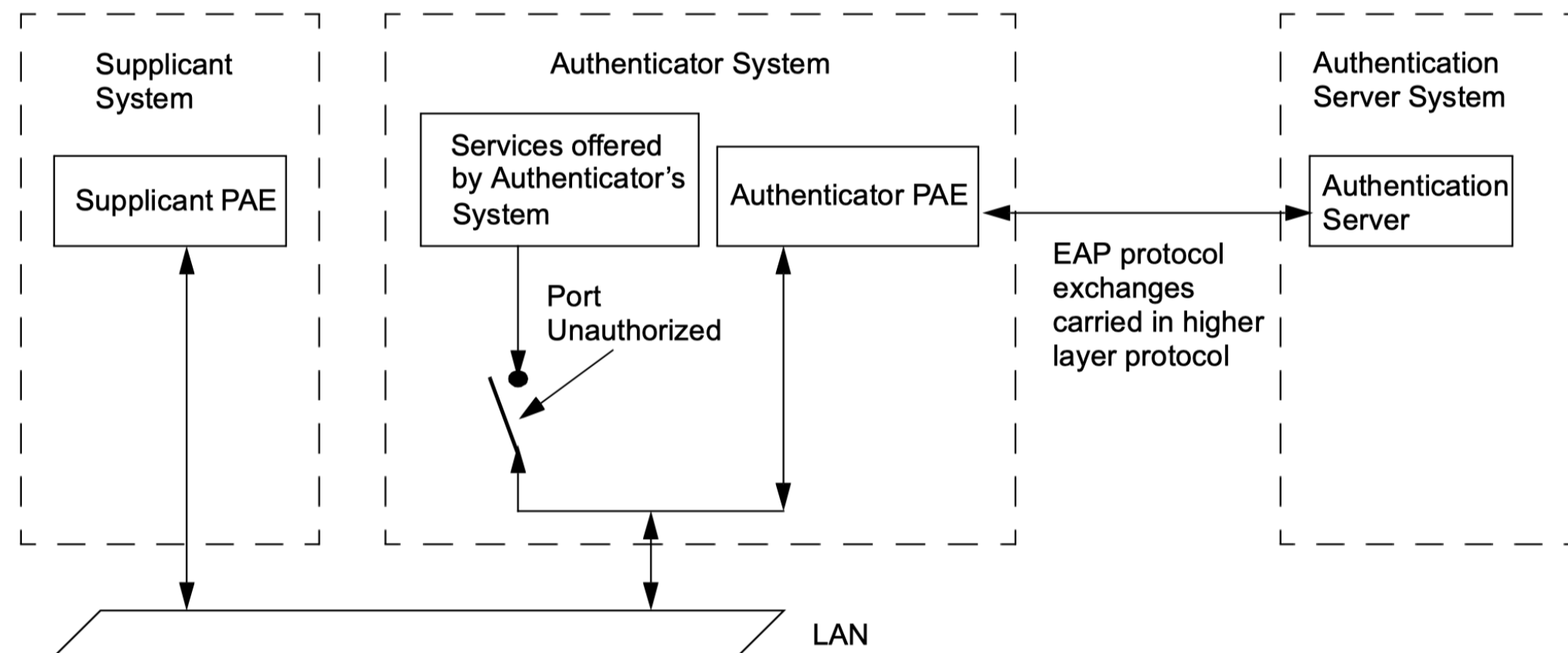


Figure 6-5—Authenticator, Supplicant, and Authentication Server roles

IEEE 802.1X-2001

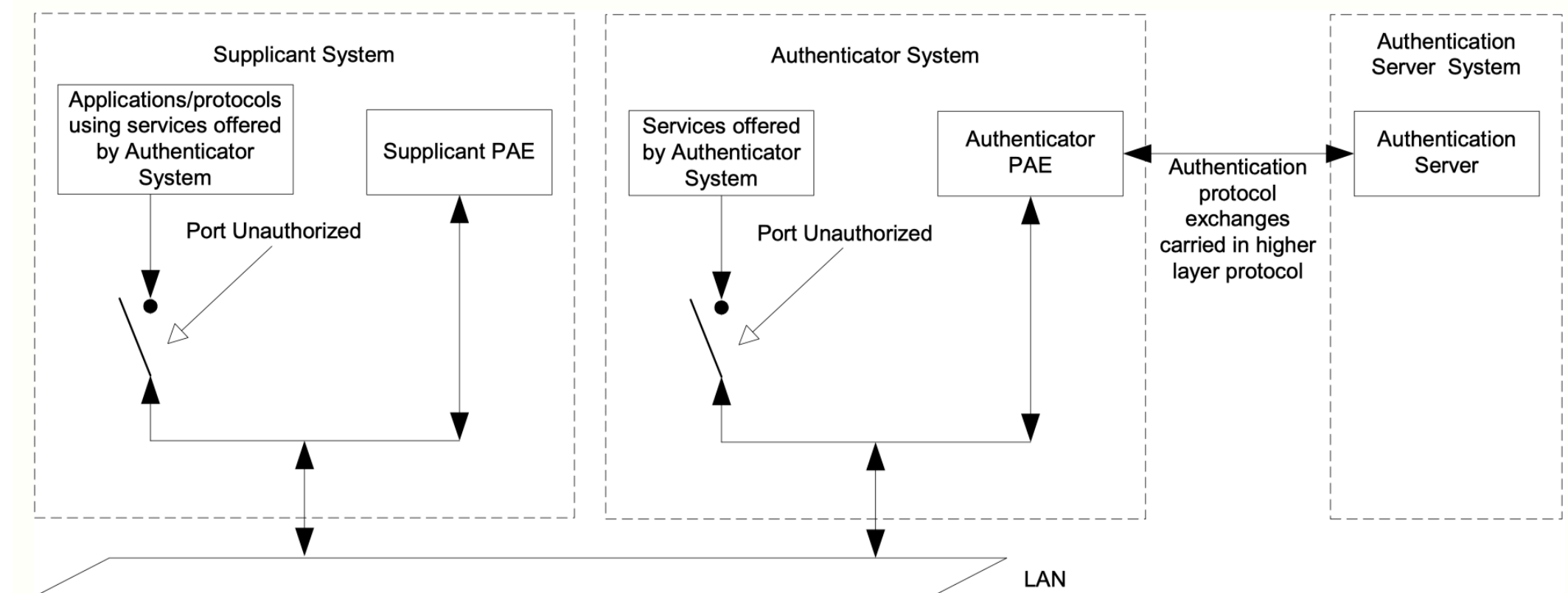


Figure 6-5—Authenticator, Supplicant, and Authentication Server roles

IEEE 802.1X-2004

- IEEE 802.1X-2004 defines that the Supplicant can also have a controlled/uncontrolled port:
 - 6.4 Controlled and uncontrolled access
 - 6.7 Coupling two EAPOL authentications

IEEE 802.1X-2004

- D.5 Security considerations (for RADIUS Integration)
 - D.5.6 IEEE 802.11 integration
- Standard grew from 134 to 169 pages
- 7.5.3 Protocol version = 2

IEEE 802.1X-2010

- Complete rewrite of IEEE 802.1X-2004:
„The extent of the changes necessary to IEEE Std 802.1X-2004 made it appropriate to revise IEEE Std 802.1X as a whole.“
- Addition of IEEE 802.1AE MAC Security (MACsec) and/or MKA (MACsec Key Agreement protocol)
- 6.6 Use of this standard by IEEE Std 802.11
[...] It is not the purpose of this standard to provide alternatives for the IEEE Std 802.11 specified functionality in 802.11 wireless networks.
- 5.22 Prohibitions
An implementation that is claimed to conform to this standard shall not
a) Support access to the MIB [...] using any version of SNMP prior to version 3.

IEEE 802.1X-2010

- RC4 Key Descriptor Type still only „deprecated“
- Standard grew from 169 to 205 pages
- 11.3.1 Protocol Version = 3

IEEE 802.1X-2020

- Very similar to IEEE 802.1X-2010
- Incorporating:
 - IEEE Std 802.1Xbx™-2014
Amendment 1: MAC Security Key Agreement Protocol (MKA) Extensions
 - IEEE Std 802.1Xck™-2018
Amendment 2: YANG Data Model
- RC4 Key Descriptor Type is not mentioned any more
- Standard grew from 205 to 287 pages
- 11.3.1 Protocol Version = 3

Thank you for listening

