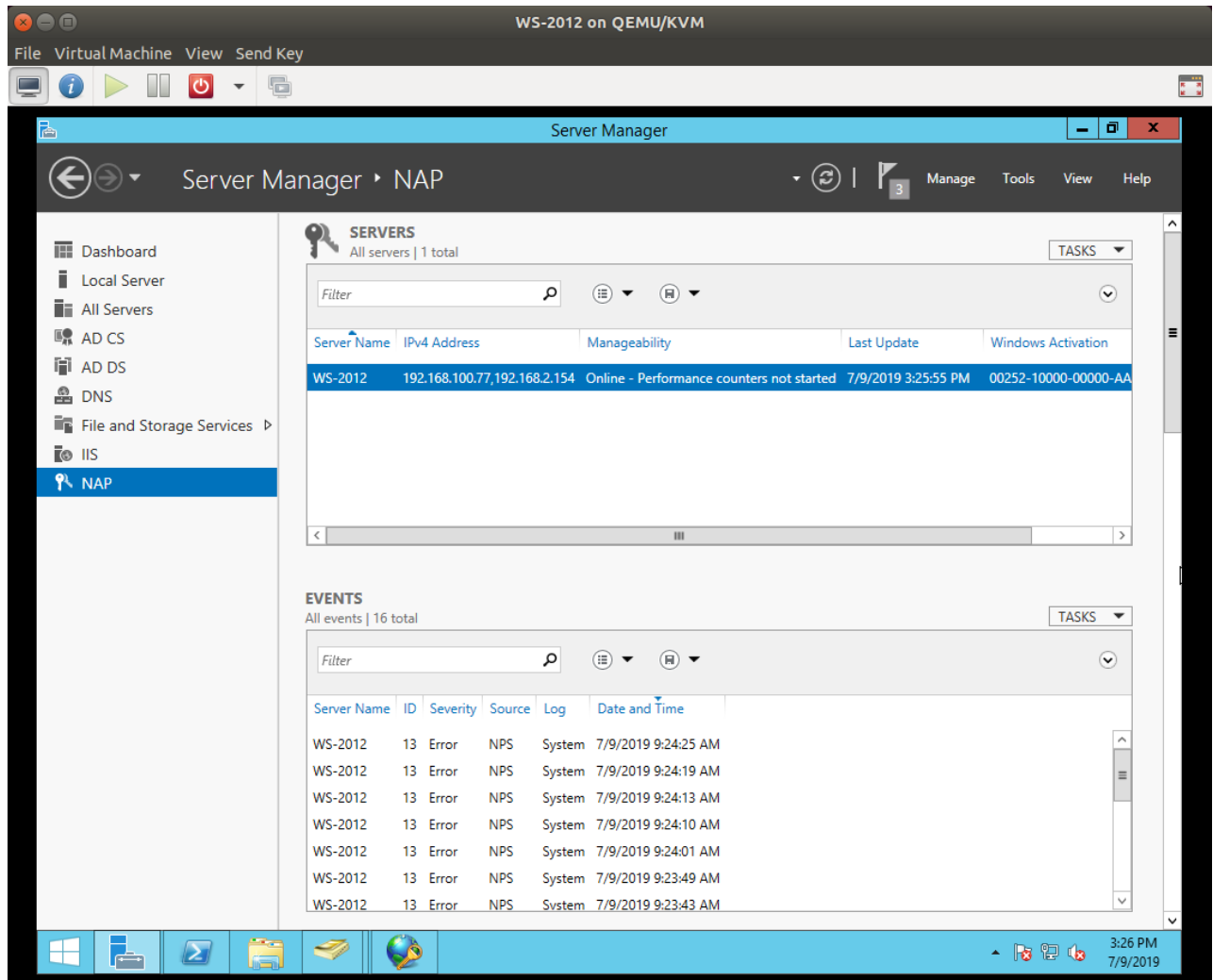


EAP-PEAP AND MSCHAPv2 Configuration

Goal: To set up a lanforge wireless station with EAP-PEAP AND MSCHAPv2 authentication.

1. RADIUS Server is a Windows Server 2012 VM using its internal RADIUS Server specifically on interface 192.168.2.154.

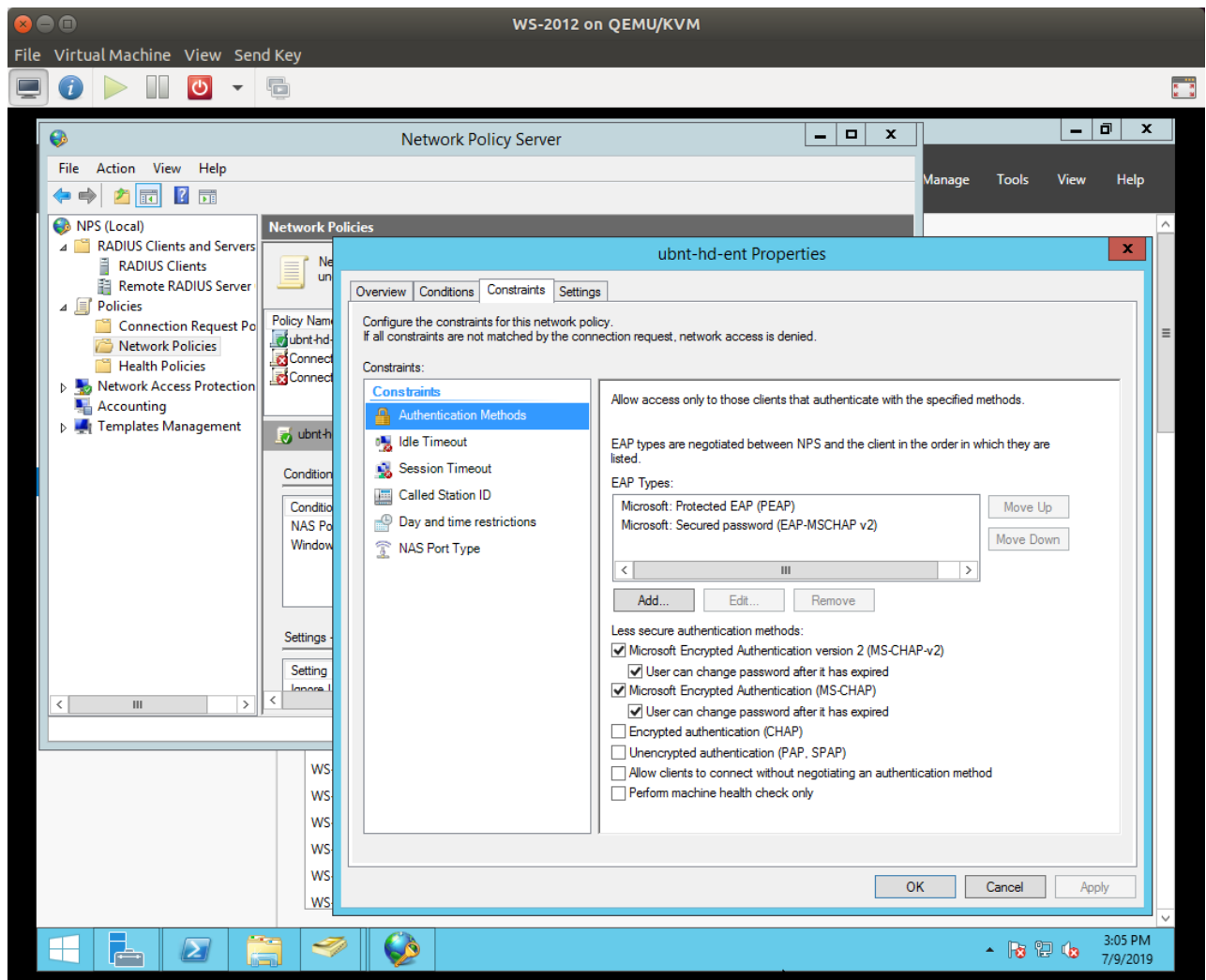


The screenshot shows the Windows Server 2012 Server Manager console. The left-hand navigation pane is expanded to show the 'NAP' (Network Access Protection) section. The main area displays the 'SERVERS' section, which lists all servers. There is one server listed: 'WS-2012' with an IPv4 address of '192.168.100.77, 192.168.2.154'. The server status is 'Online - Performance counters not started'. Below the servers list, there is an 'EVENTS' section showing a list of events. The events are all errors related to NPS (Network Policy Server) on the WS-2012 server.

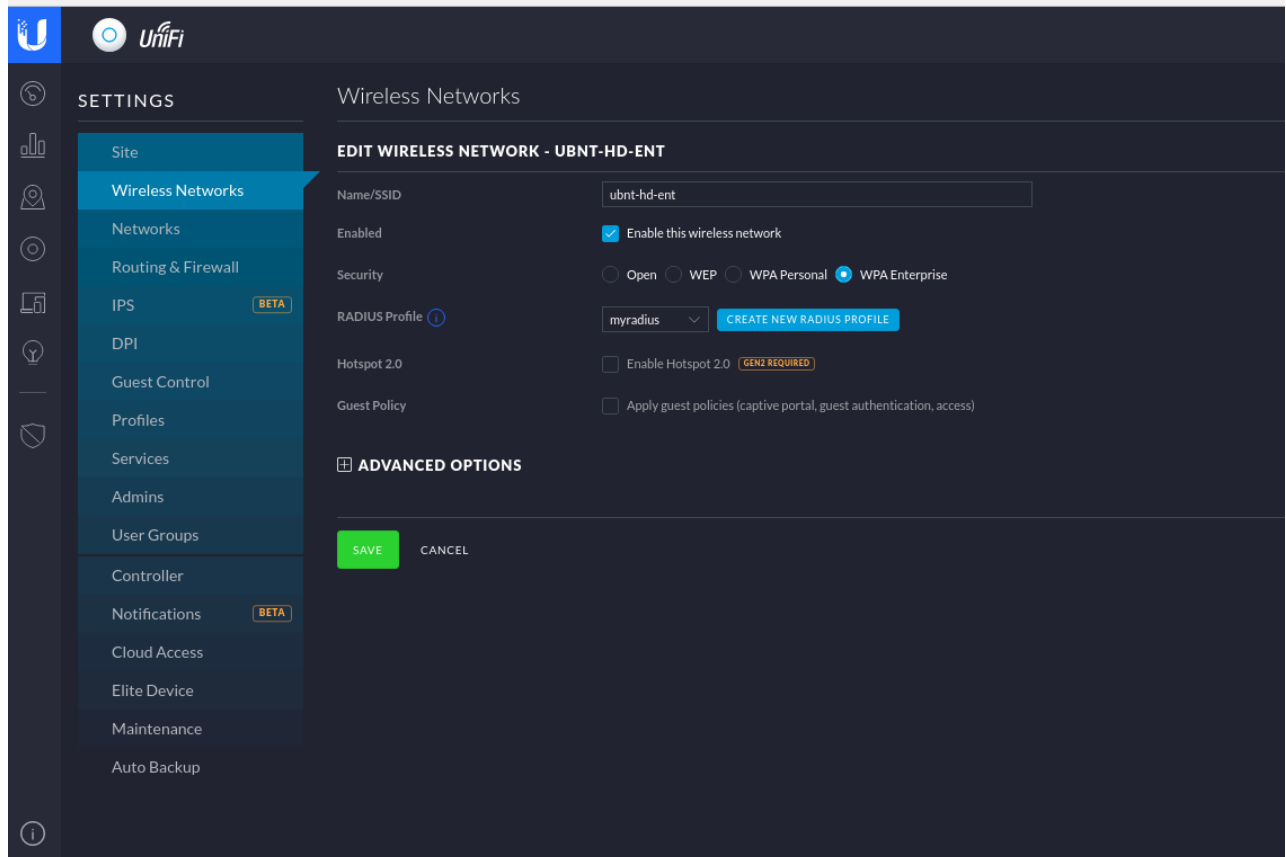
Server Name	IPv4 Address	Manageability	Last Update	Windows Activation
WS-2012	192.168.100.77, 192.168.2.154	Online - Performance counters not started	7/9/2019 3:25:55 PM	00252-10000-00000-AA

Server Name	ID	Severity	Source	Log	Date and Time
WS-2012	13	Error	NPS	System	7/9/2019 9:24:25 AM
WS-2012	13	Error	NPS	System	7/9/2019 9:24:19 AM
WS-2012	13	Error	NPS	System	7/9/2019 9:24:13 AM
WS-2012	13	Error	NPS	System	7/9/2019 9:24:10 AM
WS-2012	13	Error	NPS	System	7/9/2019 9:24:01 AM
WS-2012	13	Error	NPS	System	7/9/2019 9:23:49 AM
WS-2012	13	Error	NPS	System	7/9/2019 9:23:43 AM

2. RADIUS Server has both EAP-PEAP and MSCHAPv2 configured for use.



3. AP is a Ubiquiti HD AP with SSID ubnt-hd-ent with WPA Enterprise security.



4. The AP controller points to the RADIUS server at 192.168.2.154.

The screenshot displays the UniFi Settings interface. On the left, a sidebar menu lists various settings categories: Site, Wireless Networks, Networks, Routing & Firewall, IPS (marked BETA), DPI, Guest Control, Profiles (highlighted), Services, Admins, User Groups, Controller, Notifications (marked BETA), Cloud Access, Elite Device, Maintenance, and Auto Backup. The main content area is titled 'EDIT RADIUS PROFILE - MYRADIUS' and features two tabs: 'RADIUS' (selected) and 'SWITCH PORTS' (marked BETA). Under the 'RADIUS' tab, the configuration for the 'myradius' profile is shown. It includes fields for 'Profile Name' (myradius), 'VLAN Support' (with checkboxes for wired and wireless networks), 'RADIUS Auth Server' (with fields for IP Address: 192.168.2.154, Port: 1812, and Password/Shared Secret: lanforge), and 'Accounting' (with a checkbox to enable accounting). At the bottom of the configuration section are 'SAVE' and 'CANCEL' buttons.

5. LANforge STA1 basic configuration:

sta1 (ct523-3n-f20) Configure Settings

Port Status Information

Current: LINK-UP GRO Authorized

Driver Info: Port Type: WIFI-STA Parent: wiphy0 wiphy0...

Port Configurables

Standard Configuration **Advanced Configuration** Misc Configuration Corruptions Custom WiFi

Advanced WiFi Settings

Select 'WPA2' on the Standard Configuration screen to enable Advanced/802.1x and enable Advanced/802.1x to enable most of these. Enabling 802.11u enables others.

Key Management: WPA-EAP HESSID: 00:00:00:00:00:00

Pairwise Ciphers: DEFAULT Realm:

Group Ciphers: DEFAULT Client Cert:

WPA PSK: IMSI:

EAP Methods: EAP-PEAP Milenage:

EAP Identity: lanforge01 Domain:

EAP Anon Identity: Consortium:

EAP Password: !!lanforge123 Phase-1:

EAP Pin: Phase-2:

Private Key: PK Password:

CA Cert File: PAC File:

Network Auth: IEEE80211w: Disabled (0)

☒ Advanced/802.1x ☐ Enable 802.11u ☐ HotSpot 2.0 ☐ Enable PKC

Print
Display
Probe
Display Scan
Sync
Apply
OK
Cancel

7. Wireshark capture of STA1 EAPOL authentication.

sta1-eap-peap-pcap.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Filter: eapol

No.	Time	Source	Destination	Protocol	Length	Current Channel	SSID	Authentication SEQ	Info
772	19.516524412	f2:9f:c2:69:55:12	00:aa:aa:aa:aa:01	EAP	95				Request, Identity
774	19.517453382	00:aa:aa:aa:aa:01	f2:9f:c2:69:55:12	EAP	165				Response, Identity
787	19.701494244	f2:9f:c2:69:55:12	00:aa:aa:aa:aa:01	EAP	96				Request, Protected EAP (EAP-PEAP)
789	19.792729402	00:aa:aa:aa:aa:01	f2:9f:c2:69:55:12	TLV1	345				Client Hello
801	20.069986287	f2:9f:c2:69:55:12	00:aa:aa:aa:aa:01	TLV1	1486				Server Hello, Certificate, Certificate Request, Server Hello Done
803	20.093782105	00:aa:aa:aa:aa:01	f2:9f:c2:69:55:12	EAP	96				Response, Protected EAP (EAP-PEAP)
814	20.326253297	f2:9f:c2:69:55:12	00:aa:aa:aa:aa:01	TLV1	363				Server Hello, Certificate, Certificate Request, Server Hello Done
816	20.329190427	00:aa:aa:aa:aa:01	f2:9f:c2:69:55:12	TLV1	438				Certificate, Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
828	20.596931079	f2:9f:c2:69:55:12	00:aa:aa:aa:aa:01	TLV1	159				Change Cipher Spec, Encrypted Handshake Message
830	20.597130389	00:aa:aa:aa:aa:01	f2:9f:c2:69:55:12	EAP	96				Response, Protected EAP (EAP-PEAP)
841	20.877143184	f2:9f:c2:69:55:12	00:aa:aa:aa:aa:01	TLV1	133				Application Data
843	20.878191725	00:aa:aa:aa:aa:01	f2:9f:c2:69:55:12	TLV1	170				Application Data, Application Data
862	21.142284222	f2:9f:c2:69:55:12	00:aa:aa:aa:aa:01	TLV1	149				Application Data
864	21.143333554	00:aa:aa:aa:aa:01	f2:9f:c2:69:55:12	TLV1	170				Application Data, Application Data
876	21.409454669	f2:9f:c2:69:55:12	00:aa:aa:aa:aa:01	TLV1	165				Application Data
878	21.419634798	00:aa:aa:aa:aa:01	f2:9f:c2:69:55:12	TLV1	234				Application Data, Application Data
899	21.675999119	f2:9f:c2:69:55:12	00:aa:aa:aa:aa:01	TLV1	181				Application Data
901	21.677938558	00:aa:aa:aa:aa:01	f2:9f:c2:69:55:12	TLV1	170				Application Data, Application Data
911	21.941181166	f2:9f:c2:69:55:12	00:aa:aa:aa:aa:01	TLV1	197				Application Data
913	21.942376527	00:aa:aa:aa:aa:01	f2:9f:c2:69:55:12	TLV1	234				Application Data, Application Data
927	22.211661467	f2:9f:c2:69:55:12	00:aa:aa:aa:aa:01	EAP	94				Success
930	22.222145337	f2:9f:c2:69:55:12	00:aa:aa:aa:aa:01	EAPOL	207				Key (Message 1 of 4)
932	22.223407689	00:aa:aa:aa:aa:01	f2:9f:c2:69:55:12	EAPOL	207				Key (Message 2 of 4)
934	22.234758865	f2:9f:c2:69:55:12	00:aa:aa:aa:aa:01	EAPOL	241				Key (Message 3 of 4)
936	22.235731584	00:aa:aa:aa:aa:01	f2:9f:c2:69:55:12	EAPOL	185				Key (Message 4 of 4)

Frame 772: 95 bytes on wire (760 bits), 95 bytes captured (760 bits) on interface 0

- Ethernet II, Src: Radiotap Header v0, Length 48
- IEEE 802.11 radio information
- IEEE 802.11 QoS Data, Flags:F.C
- Logical-Link Control
- 802.1X Authentication
- Extensible Authentication Protocol

```

0000  00 00 30 00 2f 40 00 a0 20 00 00 a0 20 00 00 a0  ..0/0.....
0010  20 08 00 00 00 00 00 00 0b 79 01 00 00 00 00  ..y.....
0020  10 0c 50 14 40 01 e4 00 00 00 0b 00 01 e2 02    ..P@.....
0030  88 02 3c 00 00 aa aa aa 01 f2 9f c2 69 55 12    ..<.....10..
0040  f2 9f c2 69 55 12 00 00 00 00 aa 03 00 00 00    ..10.....
0050  88 0e 02 00 00 05 01 5a 00 05 01 a1 cf e8 bd    ..Z.....

```

sta1-eap-peap-pcap.pcapng Packets: 1186 - Displayed: 25 (2.1%) Profile: Default

8. LANforge STA2 basic configuration:

sta2 (ct523-3n-f20) Configure Settings

Port Status Information

Current: LINK-UP GRO Authorized

Driver Info: Port Type: WIFI-STA Parent: wiphy0 wiphy0...

Port Configurables

Standard Configuration
Advanced Configuration
Misc Configuration
Corruptions
Custom WiFi

Advanced WiFi Settings

Select 'WPA2' on the Standard Configuration screen to enable Advanced/802.1x and enable Advanced/802.1x to enable most of these. Enabling 802.11u enables others.

Key Management: WPA-EAP

Pairwise Ciphers: DEFAULT

Group Ciphers: DEFAULT

WPA PSK:

EAP Methods: MSCHAPV2

EAP Identity: lanforge02

EAP Anon Identity:

EAP Password: !!lanforge123

EAP Pin:

Private Key:

CA Cert File:

Network Auth:

HESSID: 00:00:00:00:00:00

Realm:

Client Cert:

IMSI:

Milenage:

Domain:

Consortium:

Phase-1:

Phase-2:

PK Password:

PAC File:

ieee80211w: Disabled (0)

☒ Advanced/802.1x
☐ Enable 802.11u
☐ HotSpot 2.0
☐ Enable PKC

Print
Display
Probe
Display Scan
Sync
Apply
OK
Cancel

10. Wireshark capture of STA2 EAPOL authentication.

sta2-mschapv2-pcap.pcapng									
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help									
eapol									
No.	Time	Source	Destination	Protocol	Length	Current Channel	SSID	Authentication SEQ	Info
370	8.328336015	f2:9f:c2:69:55:12	00:aa:aa:aa:aa:02	EAP	95				Request, Identity
372	8.329898380	00:aa:aa:aa:aa:02	f2:9f:c2:69:55:12	EAP	105				Response, Identity
385	8.598459105	f2:9f:c2:69:55:12	00:aa:aa:aa:aa:02	EAP	96				Request, Protected EAP (EAP-PEAP)
387	8.599562282	00:aa:aa:aa:aa:02	f2:9f:c2:69:55:12	EAP	96				Response, Legacy Nak (Response Only)
389	8.865832262	f2:9f:c2:69:55:12	00:aa:aa:aa:aa:02	EAP	123				Request, MS-Authentication EAP (EAP-MS-AUTH)
401	8.867272942	00:aa:aa:aa:aa:02	f2:9f:c2:69:55:12	EAP	150				Response, MS-Authentication EAP (EAP-MS-AUTH)
412	9.132674916	f2:9f:c2:69:55:12	00:aa:aa:aa:aa:02	EAP	141				Request, MS-Authentication EAP (EAP-MS-AUTH)
414	9.133888858	00:aa:aa:aa:aa:02	f2:9f:c2:69:55:12	EAP	96				Response, MS-Authentication EAP (EAP-MS-AUTH)
420	9.401831405	f2:9f:c2:69:55:12	00:aa:aa:aa:aa:02	EAP	94				Success
428	9.412393830	f2:9f:c2:69:55:12	00:aa:aa:aa:aa:02	EAPOL	207				Key (Message 1 of 4)
430	9.414099490	00:aa:aa:aa:aa:02	f2:9f:c2:69:55:12	EAPOL	207				Key (Message 2 of 4)
434	9.425894636	f2:9f:c2:69:55:12	00:aa:aa:aa:aa:02	EAPOL	241				Key (Message 3 of 4)
436	9.426624481	00:aa:aa:aa:aa:02	f2:9f:c2:69:55:12	EAPOL	185				Key (Message 4 of 4)

Frame 370: 95 bytes on wire (760 bits), 95 bytes captured (760 bits) on interface 0

RadioTap Header v0, Length 48

IEEE 802.11 radio information

IEEE 802.11 QoS Data, Flags:F.C

Logical-Link Control

802.1X Authentication

Extensible Authentication Protocol

```

0000  00 00 30 00 2f 40 00 a0 20 08 00 a0 20 08 00 a0  ..0/0...
0010  20 08 00 00 00 00 00 00 4a a8 8a 17 00 00 00 00  ..J.....
0020  10 0c 50 14 40 01 e3 00 00 00 db 00 dc 01 e1 02  ..P@.....
0030  88 02 3c 00 00 aa aa aa 02 f2 9f c2 69 55 12  ..<.....10..
0040  f2 9f c2 69 55 12 00 00 00 00 00 00 00 00 00  ..10.....
0050  88 0e 02 00 00 05 01 4e 00 05 01 33 7c 15 0f  ..N...3...

```