802.1x认证过程及EAPOL帧格式

帧号	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23
内容示例	01	80	c2	00	00	03	00	22	FA	F5	58	38	88	8e	01	01								
说明		目	的MAC	(固定)				源!	MAC			帧 (固		协议 版本	报文 类型	帧七	长度	通信 类型	EAP 通信 id	EAP数扩		EAP协 商类 型	EAP数据
标注 			I	A					I	3					D	E	F	7	G	Н]	[J	K
以太网帧						Et	hernet	:-Head	er										EAI	Po1特7	有			
对标注的解	· 2释																							
	A	目的地址MAC地址,一般为广播地址: 01-80-c2-00-00-03																						
	В	源MAC:	地址																					
	С	帧类型	₹. EAP	o1帧为	0x888e																			
	D	协议版	(本,固	固定为0	x01。																			
	Е	报文类	栏型。耳	攻值为:	①, E	EAPOL-	Packet	: 0x0	0 2	EAPO	L-Star	t: 0x0	1 3,	EAPOI	L-Logo	ff: 0x	02							
解释	F	帧长度	Ë o																					
	G	EAP通	信类型	。取值	: 1,	EAP-R	equest	: 0x01	2,	EAP-Re	esopns	e: 0x0	2 3,	EAP-S	Succes	s: 0x0	3 4.	EAP-	-Failu	re: 0x	x04			
	Н	EAP通	信id。	通常由	服务器	发来的	力报文指	定,在	上连续	的报文	内使用	这个id	来协商	或者计	十算MD5	值的数	据之一	0						
	I	EAP数	据长度	0																				
	J	EAP协	商类型	。取值	: 1)	. Iden	tity:	0x01	2, MD	05_Cha]	llenge	: 0x04												
	K	EAP扩	展数据	0																				

认证过程		(详细:	数据包续	如下)																								
1,	主机向	1服务器	器(多技	番或广扫	番地址)发送	EAPOL-	-Start																				
构造的帧。	。假设	源地址	为: 00	-1E-90)-76-A	1-40。																						
帧号	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23 · · · · ·				
内容示例	01	80	c2	00	00	03	00	1E	90	76	A1	40	88	8e	01	01	00	00										
说明		目	的MAC	(固定)				源	MAC		A1																
标注			I	A		A																						
以太网帧																												
主机向服组	以太网帧 Ethernet-Header EAPo1特有 E机向服务器发送的帧数据为: 01-80-C2-00-00-03-00-1E-90-76-A1-40-88-8E-01-01-00-00																											
2,	服务器	导向主机	l发送E	CAP-REG	QUEST-	Identi	ty要求	验证身	份的词	青 求。											EAP EAP数据长度							
构造的帧。	服务器向主机发送EAP-REQUEST-Identity要求验证身份的请求。 的帧。假设源地址为: 00-21-D7-16-B0-18。数据长度一般为60字节。假设通信ID为0C。																											
帧号	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	EAP协商类 EAP数据 21 22 23····· 21 05 01 00····· EAP协商类型 EAP数据					
内容示例	01	80	c2	00	00	03	00	21	D7	16	В0	18	88	8e	02	00	00	05	01	0C	00	05	01	00				
说明	0												通信	EAP数?	居长度	商类	EAP数据											
标注				A						В			(D	E]	-	G	Н	-	_	J	К				
以太网帧						Et	herne	t-Head	er							•			EA	· Po1特7	· 有							

3、 主机向服务器发送EAP-RESPONSE-Identity回应。

构造的帧。假设源地址为: 00-1E-90-76-A1-40。数据长度为28字节。通信ID为: 05,用户名为: cdzq,其ASCII码(十六进制)为: 63,64,7A,71。

帧号	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23
内容示例	01	80	c2	00	00	03	00	1E	90	76	A1	40	88	8e	01	00	00	09	02	0C	00	09	01	63 64 7A 71
说明		目	的MAC	(固定)				源	MAC			帧 <i>学</i> (固			报文 类型	帧七	长度	进信 迷刑	EAP 通信 id	EAP数打		EAP协 商类 型	EAP数据
标注			1	A]	В			(D	E	F	ſ _Ŧ	G	Н]	[Ј	K
以太网帧						Et	hernet	t-Head	er										EAF	Po1特有				

主机向服务器发送的帧数据为: 01-80-C2-00-00-03-<mark>00-1E-90-76-A1-40</mark>-88-8E-01-00-00-09-02-0C-00-09-01-**63-64-7A-71**

1、 服务器向主机发送EAP-REQUEST-MD5_Challenge要求验证密码的MD5校验值

构造的帧。假设源地址为: 00-21-D7-16-B0-18。

帧号	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23
内容示例	01	80	c2	00	00	03	00	21	D7	16	ВО	18	88	8e	02	00	00	19	01	OD	00	19	04	10
说明		目	「的MAC	(固定)				源	MAC			帧学 (固			报文 类型	帧书	长度	17H1/I	EAP 通信 id	EAP数技	居长度	EAP协 商类 型	EAP数据
标注	A								I	В			(D	Е	F	-	G	Н	I	-	J	K

以太网帧						Et	hernet	-Head	er										EAl	Po1特有	与 言											
服务器返回 52-56-00 -										E-02-0	0-00-1	9-01-0)D-00-	19-04-	10-B4-	-9E-26-	-95–F3	3 –A5– D)9-AA-1	E8-26-	A8-8B-	-FB-F3	-CB-01	-56-								
5、	主机向	刀服务器	8发送E	AP-RES	SPONSE-	-MD5_C	hallen	ge回应	:																							
构造的帧。	假设	源地址	为: 00	-1E-90	0-76-A]	1-40。																										
帧号	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23 · · · · ·								
内容示例	01	80	c2	00	00	03	00	1E	90	76	A1	40	88	8e	01	00	00	1A	A													
说明	Hand Hand															商类																
标注		A B C D E F G H I J															К															
以太网帧	帧 Ethernet-Header EAPol特有																															
主机向服约 D4-C2-63 -			数据为	: 01-	-80-C2-	-00-00	-03- <mark>00</mark>	-1E-90)-76-A	1-40-8	8-8E-0	1-00-0)0-1A-(02-0D-	-00-1A-	-04- <mark>10</mark> -	-F4-21	36-9	A-CA-2	26-DD-	24-BC-	-79–D3	-C2-20	-D9-								
6、	服务器	导向主机	几发送E	AP–Suc	cess。																											
构造的帧。	假设	源地址	为: 00	-21-D7	′-16-B(0-18。																										
帧号	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23								
内容示例	01	80	c2	00	00	03	00	21	D7	16	В0	18	88	8e	02	00	00	04	03	OD	00	04	00	00								
说明		E	的MAC	(固定)				源M	ИАС			帧 (固			报文 类型	帧七	长度	通信 类型		EAP数i			EAP数据								

标注			1	A					F	3				C	D	E	F	7	G	Н]	[J	K
以太网帧						Et	hernet	t-Head	er										EA	Po1特有	ij			
服务器返[00-00-00-										E-02-0	0-00-0	4-03-0)D-00-(04-00-	-00-00-	-00-00-	-00-00)-00-0	0-00-0	00-00-	00-00-	-00-00	-00-00	-00-
9、	服务器	8务器向主机发送EAP-Failure。(若认证失败时发送的数据,例如密码错。)																						
构造的帧。	b帧。假设源地址为: 00−21−D7−16−B0−18。																							
帧号	- 0 1 2 3 4 5 6 7 8 9 10 11 12 13								14	15	16	17	18	19	20	21	22	23						
内容示例	01	80	c2	00	00	03	00	21	D7	16	В0	18	88	8e	02	00	00	04	04	0F	00	04	00	00
说明	目的MAC(固定) 源MAC (固定)														协议 版本	报文 类型	帧书	长度	通信 类型	EAP 通信 id	EAP数扩		EAP协 商类 型	EAP数据
标注	A B												(C	D	Е	F	7	G	Н]	[Ј	К
以太网帧						Et	hernet	t-Head	er							•			EA	· Po1特有	<u> </u>		•	
	 可的数:	——— 据为:	01-80-		-00-03-	-00-21	 -D7-16	 	 8-88-8F	E-02-0	0-00-0	4-04-0)F-00-(04-00-	-00-00-	-00-00-	-00-00)-00-0	00-00-	00-00-	00-00-	-00-00	-00-00	-00-