

Implementation of A Dissector for ForCES Protocol in Ethereal

Fenggen Jia, jfg@mail.zjgsu.edu.cn Chuanhuang Li, chuanhuang_li@pop.zjgsu.edu.cn Ming Gao, gmyyqno1@pop.zjgsu.edu.cn Ligang Dong, donglg@mail.zjgsu.edu.cn Bin Zhuge, zhugebin@mail.zjgsu.edu.cn

> IETF 76th Meeting Nov 9, 2009, Hiroshima Japan



What We Have Implemented

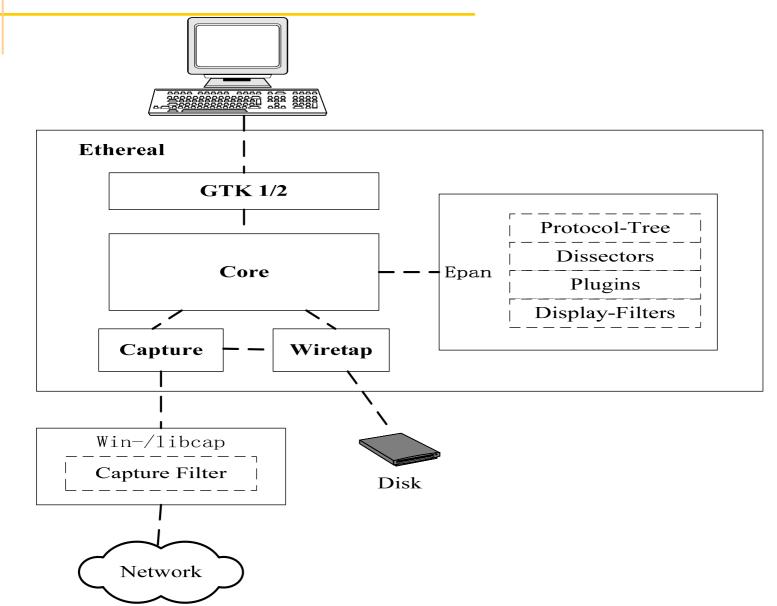
- Analyzing the ForCES protocol encapsulated in TCP/IP, SCTP TML;
- Decode all the fields of ForCES Main Header;
- Decode and show all the fields of LFBselect-TLV included in Main TLV;

- Oper-TLV included in LFBselect-TLV as well.

- Decode and show all the fields of REDIRECT-TLV included in Main TLV;
- Decode and show all the fields of ASResult-TLV and ASTreason-TLV included in Main TLV;
- All the above are displayed as a tree in Ethereal;



Function Blocks in Ethereal

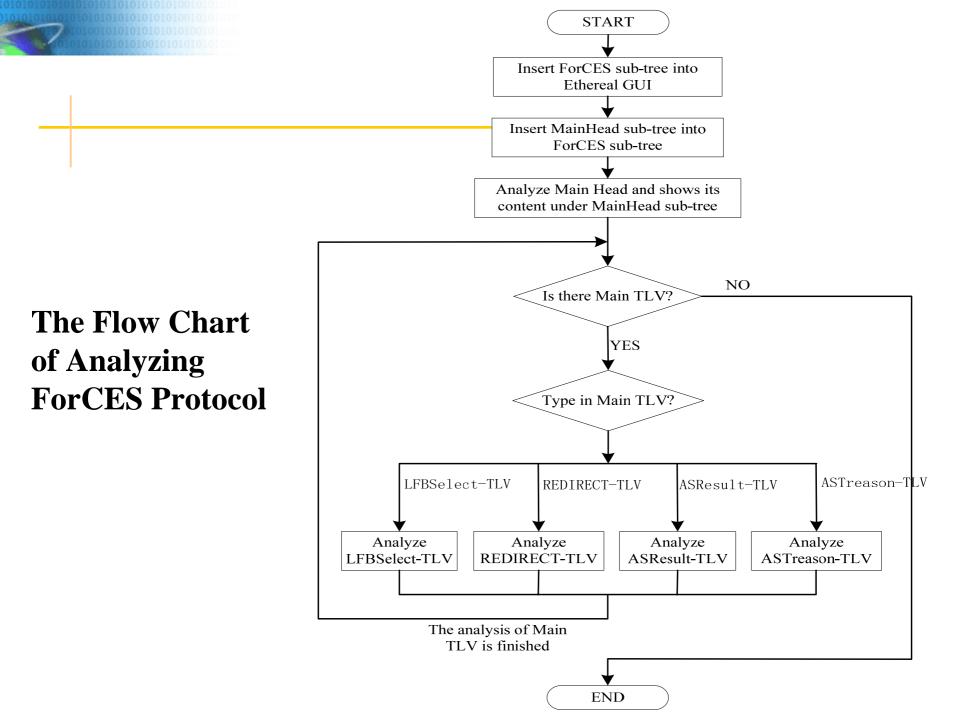


Insert A "ForCES" Dissector into Ethereal

- Parent-node of ForCES sub-tree is TCP/UDP /SCTP;
- Implement the routine which is used for decoding the message head in the ForCES protocol and shows its protocol tree;
- Register all the fields and parameters in the ForCES protocol to ethereal;
- Implement routine which is used for registering decoding function of the ForCES protocol.

How to Analyze ForCES Protocol

- ForCES sub-tree is inserted under TCP or UDP\SCTP parentnode;
- Create MainHead sub-tree under ForCES sub-tree;
- Analyze the content of MainHead, and show the meaning of special values;
- Create multiple Main TLV sub-trees under ForCES sub-tree according to the number and type of Main TLV. The type of Main TLV is LFBselect-TLV, REDIRECT-TLV, ASResult-TLV, or ASTreason-TLV;
- If the type of Main TLV is LFBselect-TLV, then
 - Analyze LFBCLASSID and LFBInstance in this TLV;
 - Create multiple OPER-TLV sub-tree under LFBselect-TLV sub-tree;
 - Analyze the type of OPER-TLV, and show its type name and length.
- If the type of Main TLV is REDIRECT-TLV, ASResult-TLV, or ASTreason-TLV, then the content in the TLV is shown.

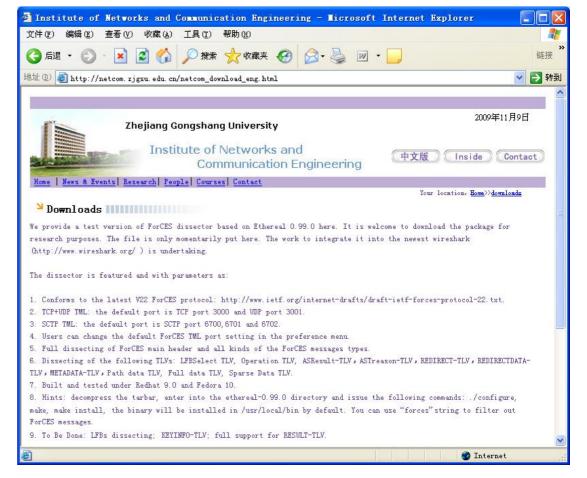


Interface of Ethereal with ForCES Plugin

10 00	<u>E</u> dit <u>V</u> iew	<u>G</u> o <u>C</u> apture	<u>A</u> nalyze	Statistics	<u>H</u> elp														
16	u 🔍 🤮	f 🕍 i 📄 I	X	6			> 20	$\overline{\Delta}$			9 0				¥ 🗹] 🍪	×	8	
<u>F</u> ilter	r: forces &&	ospf					▼ 4	<u>E</u> xpres	sion	> 清除(0	应用(A)	1						
	Time	Source		Destinati	on		Protocol	-					<u> </u>						
51	31.863215	192.168.10.3		192.168	.10.1		ForCES	Messag	ge Type	: Pack	etRedirect	t,Total L	ength:	560 B	vtes				
52	2 31.864734	192.168.10.1		192.168	.10.3		ForCES	Messag	ge Type	: Pack	etRedirect	t,Total L	ength:	496 B	ytes				
54	1 31.893450	192.168.10.3		192.168	.10.1		ForCES	Messag	ge Type	: Pack	etRedirect	t,Total L	ength:	496 B	ytes				
	5 31.895533	192.168.10.1		192.168	.10.3		ForCES	Messag	ge Type		etRedirect			576 B	ytes				
	31.912913	192.168.10.3		192.168				Messag			etRedirect			656 B					
	7 31.920692	192.168.10.1		192.168				Messag			etRedirect	-		496 B					
	3 32.033297	192.168.10.3		192.168				Messag	0 71		etRedirect	The second s		496 B					
	32.040624	192.168.10.1		192.168				Messag	<u> </u>		etRedirect			496 B					
	32.050282	192.168.10.1		192.168				Messag			etRedirect			560 B					
	32.283780	192.168.10.3		192.168				Messag			etRedirect			816 B					
	2 32.284782	192.168.10.1		192.168				Messag			etRedirect		- V	512 B					
	3 32.294989 5 32.427280	192.168.10.3		192.168				Messag			etRedirect			624 B	1				
	32.427280 7 32.794468	192.168.10.3 192.168.10.3		192.168				Messag			etRedirect etRedirect			672 B 608 B	-				
	32.794468	192.168.10.3		192.168				Messag			etRedirect			560 B	-				
	32.870493	192.168.10.1		192.168	a second second second			Messag			etRedirect			624 B	A CONTRACTOR OF A CONTRACTOR OFTA CONTRACTOR O				
		s on wire, 182 ga-Byt_4e:bf:5f (Giga-By	vt_32:58	8:3d (00:1	6:e6:32:	:58:3d)										
Ethern > Des > Sou Typ Interne Ver Hes 7 Diff	et II, Src: Gij stination: Giga- urce: Giga-Byt ce: IP (0x080) et Protocol, Sr rsion: 4 ader length: 20 ferentiated Ser	ga-Byt_4e:bf:5f (-Byt_32:58:3d (0 _4e:bf:5f (00:0f:a 0) c: 192.168.10.3 0 bytes vices Field: 0x00	00:0f:ea:4e: 0:16:e6:32: ea:4e:bf:5f) (192.168.1)	bf:5f), Dst 58:3d) 0.3), Dst: :00: Defau	192.168. lt; ECN:	10.1 (1 0x00)			58:3d)										
Ethern Des Sou Typ Interne Ver Hea T Diff	tet II, Src: Gij stination: Giga-Byt we: IP (0x080) et Protocol, Sr rsion: 4 ader length: 20 ferentiated Ser 0000 00 = 1 0. = ECN	ga-Byt_4e:bf:5f (-Byt_32:58:3d (0 _4e:bf:5f (00:0f:a 0) c: 192.168.10.3 0 bytes vices Field: 0x00 Differentiated Ser I-Capable Transp	00:0f:ea:4e: 0:16:e6:32: :ea:4e:bf:5f) (192.168.1)) (DSCP 0: vices Codep	bf:5f), Dst 58:3d) 0.3), Dst: 00: Defau oint: Defau	192.168. lt; ECN:	10.1 (1 0x00)			58:3d)										
Ethern > Des > Sou Typ Interne Ver Hes 7 Diff (tet II, Src: Gig stination: Giga- rce: Giga-Byt ve: IP (0x080) et Protocol, Sr rsion: 4 ader length: 24 ferentiated Ser 0000 00 = 1 0. = ECN	ga-Byt_4e:bf:5f (-Byt_32:58:3d (0 _4e:bf:5f (00:0f:a 0) c: 192.168.10.3 0 bytes vices Field: 0x00 Differentiated Ser I-Capable Transp I-CE. 0	00:0fiea:4e: 0:16:e6:32: 2:a:4e:bf:5f) (192.168.1)) (DSCP 0) vices Codep ort (ECT): (bf:5f), Dst 58:3d) 0.3), Dst: 000: Defau oint: Defau)	192.168. lt: ECN: lt (0x00)	10.1 (1 0x00)	92.168.10		58:3d)										
Ethern > Des > Sou Typ Interne Ver Hea - Diff (the II, Src: Gi stination: Giga- rce: Giga-Byt, be: IP (0x080) et Protocol, Sr rsion: 4 ader length: 20 ferentiated Ser 0000 00 = 1 0. = ECN 0 - ECN 0 16 e6 32 0 a8 00 00 a 01 80 05 0 03 40 00	ga-Byt_4e:bf:5f (-Byt_32:58:3d (0 _4e:bf:5f (00:0f:a 0) c: 192.168.10.3 0 bytes vices Field: 0x00 Differentiated Ser I-Capable Transp	00:0f:ea:4e: 0:16:e6:32: ea:4e:bf:5f) (192.168.1)) (DSCP 0) vices Codep ort (ECT): (ea 4e bf 5f a4 f0 c0 a 81 9f 10 (00 00 00	bf:5f), Dst 58:3d) 0.3), Dst: 000: Defau oint: Defau 0 708 00 4 8 0a 03 6 00 8c 00 00 00	192.168. lt; ECN: lt (0x00) 5 00 c0 a8 00 00 00 00	10.1 (1 0x00)) 2X= @.@.	92.168.10 .NE.		58:3d)										
Etherm > Des > Sou Typ Typ Nerman Ver Hes 7 Diffi (aet II, Src: Gigastination: Giga- arce: Giga-Byt, arce: Giga-Byt, be: IP (0x080) et Protocol, Sr rssion: 4 ader length: 20 ferentiated Ser 0.0000 00 = 1	ga-Byt_4e:bf:5f (-Byt_32:58:3d (0 _4e:bf:5f (00:0f:a 0) c: 192.168.10.3 0 bytes vices Field: 0x00 Differentiated Ser I-Capable Transp I-CE: 0 58 3d 00 0f (40 00 40 11 00 b9 00 94 00 00 00 00	00:0f:ea:4e: 0:16:e6:32: ea:4e:bf:5f) (192.168.1) (DSCP 0) vices Codep ort (ECT): (ea 4e bf 5f a4 f0 c0 a 81 9f 10 0 00 00 00 00 02 00	bf:5f), Dst 58:3d) 0.3), Dst: 00: Defat 00: Defat 0 1 000 0 4 8 0a 03 16 00 8c 00 00 00 00 00 01 00 00 0c	192.168. lt: ECN: lt (0x00) 5 00 c0 a8 00 00 00 00 00 00	10.1 (1 0x00)) 2X= @.@.	92.168.10		58:3d)										

Ethereal with ForCES Plugin Download

- Download web:
 - <u>http://netcom.zjgsu.edu</u>
 <u>.cn/netcom_download</u>
 <u>eng.html</u>
- File:
 - <u>ethereal-</u> 0.99.0 forces.tar.gz





Thanks!