

Kernel TLS and hardware TLS offload in FreeBSD 13

by

Mellanox, Chelsio and Netflix



Why crypto?

- Bob and Alice and the secret message
- Mathematical dependance on a relatively small pre-shared key
- When used right:
 - Prevents eavesdropping
 - Prevents data tampering
- When used wrong:
 - Makes denial of service easier

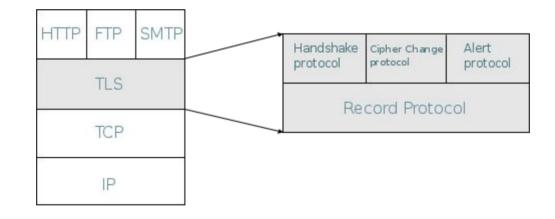


What is TLS ?

- Transport Layer Security, TLS
- Used behind https:// (TCP port 443)
- Supports multiple crypto codecs among others
 AES 128B / 256B
- Supports multiple key exchange protocols
 - DiffieHellman, DH
 - Ron Rivest, Adi Shamir, Leonard Adleman, RSA
- Most recent version is v1.3



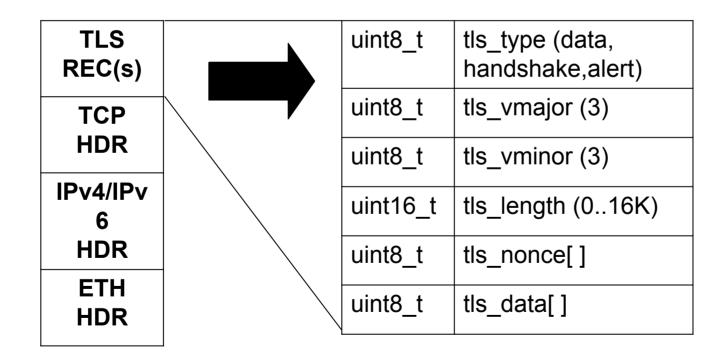
What is TLS ?





TLS v1.2

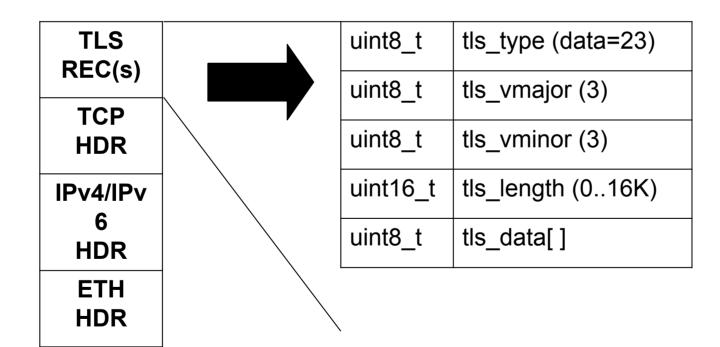
- Layout of a TLS record
- More detailed information at: https://tls.ulfheim.net/





TLS v1.3

- Layout of a TLS record
- More detailed information at: https://tls.ulfheim.net/





AES 128B / 256B

- Advanced Encryption Standard, AES
 - See: <u>https://en.wikipedia.org/wiki/Advanced_Encryption_Standard</u>
- A 16-byte block cipher
- The stream version can stop and resume encryption at any arbitrary point in the TLS record
 - Supports the concept of a crypto cursor
- FreeBSD also supports CBC



TLS implementations

- Current FreeBSD alternatives (OpenSSL based)
 - Generic user-space, AES-NI
 - SW kernel TLS, AES-NI
 - Open Crypto Framework kernel backend
 - TCP Offload Engine for TLS
 - NIC kernel TLS







A look inside OpenSSL

- Datapath is oriented around:
 - typedef struct bio_st BIO;
 - o BIO_read()
 - o BIO_write()
- All data must have a pointer in user-space in order to be encrypted
- Based on the source and sink methodology
- Refer to the bio(3) manual page



OpenSSL and kTLS

- 16 patches have been submitted by: Boris Pismenny <<u>borisp@mellanox.com</u>>
- FreeBSD userspace APIs:
 - o #include <sys/ktls.h>
 - setsockopt(TCP_TXTLS_ENABLE)
 - setsockopt(TCP_TXTLS_MODE)
- FreeBSD kernel support added in r351522:
 - <u>https://svnweb.freebsd.org/changeset/base/351522</u>



Netflix kTLS

- Kernel TLS Motivation
 - Handle 100Gb/s of TLS with nginx
 - Retain performance advantages of async sendfile(9) (fewer context switches, no nginx thread pool, no extra memory copy)
 - Eliminate any possible inefficiency



- Not ready flag
- Unmapped mbufs
- Send Tags



not ready mbuf flag

- mbuf flag M_NOTREADY tell socket buffers if mbufs are ready for transmission or not.
- Added to support async sendfile in r275329
- Sendfile(9) adds mbuf to socket buffer marked M_NOTREADY
 - Until M_NOTREADY is cleared, tcp cannot send it
- disk reads are issued into those mbufs
- M_NOTREADY cleared and tcp_usr_ready() routine called after disk read is complete
- Allows a simple mbuf filter routine, like TLS encryption, to process the mbufs before they are submitted to the network driver via the TCP stack.

Netflix "unmapped" mbufs

- Called "unmapped" because they carry an array of pointers to unmapped physical addresses.
- Initially envisioned for sendfile, not TLS
- Dramatically reduces the length of socket buffer mbuf chains, thus reducing cache misses. For a 16K TLS record, it compresses chains by about 6:1 (TLS hdr, trailer and 4 buffers). For unencrypted sendfile, it can compress mbuf chains up to 19:1
 - 5-20% CPU reduction in Netflix unencrypted workloads
- Describes a TLS record entirely, including TLS header, trailer, message data, and pointers to kernel TLS session state in a single mbuf
- A single reference counted entity per TLS record is key for NIC TLS offload to be able to easily handle TCP retransmissions.



Netflix Software kTLS

Software Kernel TLS Implementation, TLS 1.0 -> TLS 1.3

- Plaintext data passed to kernel via sendfile() or sosend().
- The kernel frames TLS records into M_NOMAP mbufs at sendfile() or sosend() time and places them into socket buffers.
- Mbuf chains are marked with M_NOTREADY
- Framed records are queued for encryption when they would previously be marked "ready"
- Encryption is done by a pool of kernel threads (1 per core)
- Once encrypted, mbufs are marked "ready" & sent to TCP



mbuf send tags

- A property of mbufs which tell the underlying network interface about dedicated packet processing and queues.
- A quick and efficient way to demultiplex data traffic.
- Allows for traversal through VLAN and LAGG (Link Aggregation).
- Safe against route changes.



mbuf send tag APIs

- Control path methods:
 - struct mbuf_snd_tag *mst;
 - struct ifnet

*ifp;

- Allocate(ifp, &mst)
- Modify(mst, arg)
- Query(mst, arg)
- Free(ifp, mst)



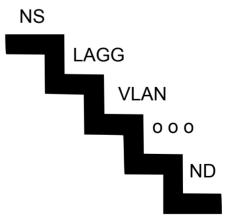
mbuf send tags

- From Network Stack, NS, perspective:
 - struct mbuf *mb;
 - struct ifnet *ifp;
 - o m_pkthdr.snd_tag = mst;
 - m_pkthdr.csum_flag |= CSUM_SND_TAG;
 - o ifp->if_output(mb);



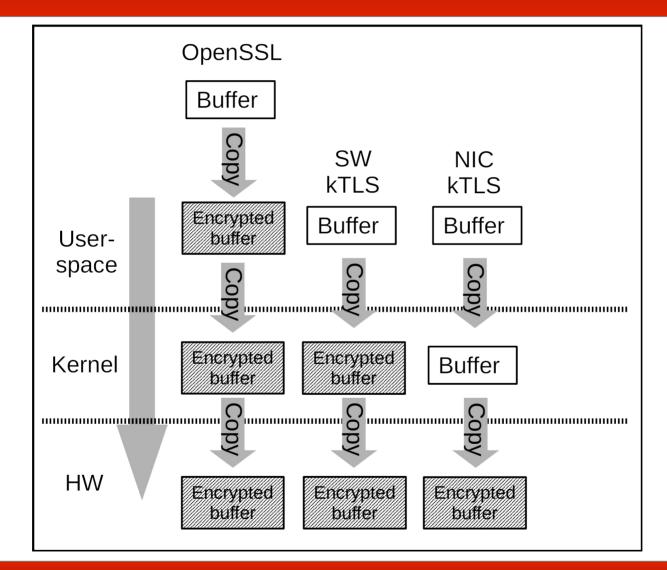
mbuf send tags

- From Network Driver, ND, perspective:
 - struct mbuf *mb;
 - struct xxx_send_tag *st;
 - o st = container_of(m_pkthdr.snd_tag, ...)
 - select queue by st->queue;





Dataflow overview

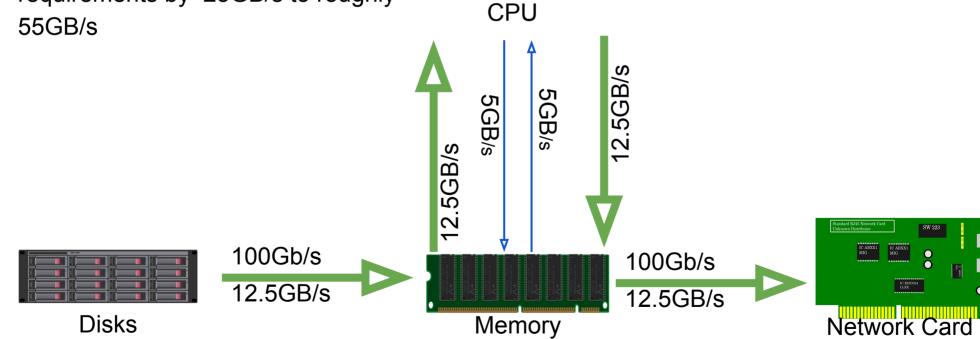




Using sendfile and software kTLS, data is encrypted by the host CPU.

This increases our bandwidth requirements by 25GB/s to roughly 55GB/s



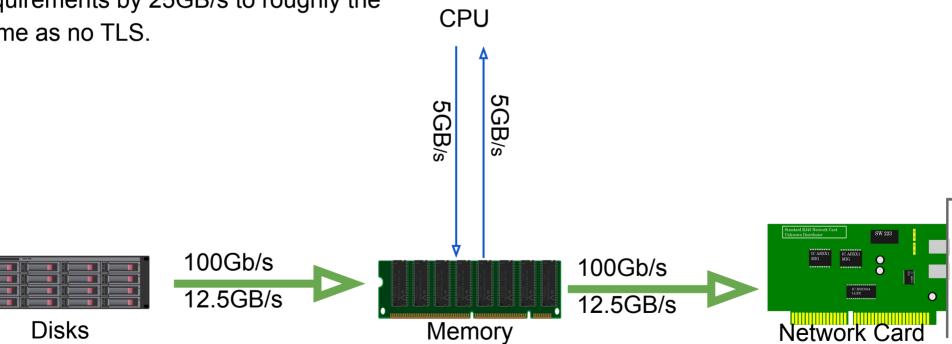




Using sendfile and inline kTLS, data is encrypted by the NIC.

This reduces our bandwidth requirements by 25GB/s to roughly the same as no TLS.







TLS before and after

		iperf_tls_serve	er.pcap			× 🚄			iperf_tls	_client.pca	p		0 - E
e <u>E</u> dit <u>V</u> iew <u>G</u> o	<u>Capture</u> <u>A</u> nalyze	e <u>S</u> tatistics Teleph	on <u>y W</u> ireless <u>T</u> ools	<u>H</u> elp		Eil	e <u>E</u> dit <u>V</u> iew <u>G</u> o	<u>Capture</u> <u>A</u> nal	yze <u>S</u> tatistics	Felephony <u>N</u>	<u>W</u> ireless <u>T</u> ools <u>H</u>	elp	
	📄 🖹 🖹 🙆	۹ 🔶 警	₹ 🛓 其 📕					💼 🗈 🖹	ء 🔶 🌔 🔯) 🔮 有	₹	e e e 🏢	
Apply a display filte	r <ctrl-></ctrl->				 Expression 	+	Apply a display filte	er <ctrl-></ctrl->					Expression
Time	Source	Destination Prot	tocol Length Info			A No.	Time	Source	Destination	Protocol	Length Info		
7 0.108610	11.215.5.66			nt Key Exchange,	Change Cipher		8 0.108653	11.215.5.66	11.215.5.65	TLSv1.2	339 Client	Key Exchange, C	hange Cipher
8 0.215088	11.215.5.65	11.215.5.66 TCP		→ 24791 [ACK] Se			9 0.216265			TCP		24791 [ACK] Seq	
9 0.636250	11.215.5.66	11.215.5.65 TLS		/pted Handshake №			10 0.636028			TLSv1.2		ed Handshake Me	
10 0.636405	11.215.5.65	11.215.5.66 TLS		Session Ticket, C			11 0.637301			TLSv1.2		sion Ticket, Ch	
11 0.736667	11.215.5.66	11.215.5.65 TCP		$I \rightarrow 5001 [ACK] Set$			12 0.736716			TCP		5001 [ACK] Seq	
12 1.079358	11.215.5.65	11.215.5.66 TLS		/pted Handshake M		~	13 1.080408			TLSv1.2		ed Handshake Me	
13 1.081282		11.215.5.65 TCP		l → 5001 [ACK] Se			14 1.081042			TCP		5001 [ACK] Seq	
14 1.184810	11.215.5.65	11.215.5.66 TCP		→ 24791 [ACK] Se			15 1.185996			TCP		24791 [ACK] Seq	
15 1.186756	11.215.5.66	11.215.5.65 TCP		L → 5001 [ACK] Se			16 1.186043			TCP		5001 [ACK] Seq	
16 1.186772	11.215.5.65	11.215.5.66 TCP		→ 24791 [ACK] Se			17 1.187430			TCP		24791 [ACK] Seq	
17 1.188830	11.215.5.66	11.215.5.65 TCP	2962 2479	L → 5001 [ACK] Se		-	18 1.187444	11.215.5.66	11.215.5.65	TCP	2962 24791 -	5001 [ACK] Seq	
					•								•
thernet II, Src: nternet Protocol	: RealtekU_55:15 l Version 4, Src	:75 (52:54:00:55:1 : 11.215.5.66, Dst		kU_f3:64:3f (52:			Frame 14: 1514 b Ethernet II, Src Internet Protoco Transmission Con	: RealtekU_55: l Version 4, S	15:75 (52:54:0 Src: 11.215.5.6	0:55:15:75) 6, Dst: 11.), Dst: RealtekU 215.5.65	_f3:64:3f (52:54	
thernet II, Src nternet Protoco ransmission Cont	: RealtekU_55:15 l Version 4, Src trol Protocol, S	::75 (52:54:00:55:1 :: 11.215.5.66, Dst :rc Port: 24791, Ds	15:75), Dst: Realte t: 11.215.5.65 st Port: 5001, Seq:	kU_f3:64:3f (52: 454, Ack: 1173,			Ethernet II, Src Internet Protoco Transmission Con	: RealtekU_55: l Version 4, S trol Protocol,	15:75 (52:54:0 Src: 11.215.5.6 Src Port: 247	0:55:15:75) 6, Dst: 11. 91, Dst Por), Dst: RealtekU 215.5.65 rt: 5001, Seq: 4	_f3:64:3f (52:54	
thernet II, Src nternet Protocol ransmission Cont 0 52 54 00 f3 64	: RealtekU_55:15 l Version 4, Src trol Protocol, S 4 3f 52 54 00 55	:75 (52:54:00:55:1 : 11.215.5.66, Dst rc Port: 24791, Ds 5 15 75 08 00 45 00	15:75), Dst: Realte t: 11.215.5.65 st Port: 5001, Seq: RT·d?RT U·u·E	kU_f3:64:3f (52: 454, Ack: 1173,			Ethernet II, Src Internet Protoco Transmission Con 30 52 54 00 f3 6	: RealtekU_55: l Version 4, S trol Protocol, 4 3f 52 54 00	15:75 (52:54:0 Src: 11.215.5.6 Src Port: 247 55 15 75 08 00	0:55:15:75) 6, Dst: 11. 91, Dst Por 45 00 RT), Dst: RealtekU 215.5.65 rt: 5001, Seq: 4	_f3:64:3f (52:54	
thernet II, Src nternet Protocol ransmission Cont 0 52 54 00 f3 64 0 05 dc 00 00 40	: RealtekU_55:15 l Version 4, Src trol Protocol, S 4 3f 52 54 00 55 0 00 40 06 12 ec	:75 (52:54:00:55:1 : 11.215.5.66, Dst arc Port: 24791, Ds 5 15 75 08 00 45 00 c 0b d7 05 42 0b d7	15:75), Dst: Realte t: 11.215.5.65 st Port: 5001, Seq: RT· d?RT · U·u· E @.@B	kU_f3:64:3f (52: 454, Ack: 1173,			Ethernet II, Src Internet Protoco Transmission Con 00 52 54 00 f3 6 10 05 dc 00 00 4	: RealtekU_55 l Version 4, 5 trol Protocol, 4 3f 52 54 00 0 00 40 06 00	15:75 (52:54:0 Src: 11.215.5.6 Src Port: 247 55 15 75 08 00 00 0b d7 05 42	0:55:15:75) 6, Dst: 11. 91, Dst Por 45 00 RT 0b d7), Dst: RealtekU 215.5.65 rt: 5001, Seq: 4 • d?RT U u E • @ @ · · · · B	_f3:64:3f (52:54	
thernet II, Src nternet Protocol ransmission Cont 0 52 54 00 f3 64 0 05 dc 00 00 40 0 05 41 60 d7 13	: RealtekU_55:15 l Version 4, Src trol Protocol, S 4 3f 52 54 00 55 0 00 40 06 12 ec 3 89 50 26 6d 48	:75 (52:54:00:55:1 : 11.215.5.66, Dst irc Port: 24791, Ds 5 15 75 08 00 45 00 c 0b d7 05 42 0b d7 3 33 db dd 59 80 10	15:75), Dst: Realte t: 11.215.5.65 st Port: 5001, Seq: RT·d?RT·U·u·E @@B. @@B. 	454, Ack: 1173,		000 000 000 000	Ethernet II, Src Internet Protoco Transmission Con 00 52 54 00 f3 6 10 05 dc 00 00 4 20 05 41 60 d7 1	: RealtekU_55: l Version 4, 5 trol Protocol, 4 3f 52 54 00 0 00 40 06 00 3 89 50 26 6d	15:75 (52:54:0 Src: 11.215.5.6 Src Port: 247 55 15 75 08 00 00 0b d7 05 42 48 33 db dd 59	0:55:15:75) 6, Dst: 11. 91, Dst Por 45 00 RT 0b d7 80 10 A), Dst: RealtekU 215.5.65 rt: 5001, Seq: 4 	_f3:64:3f (52:54	
thernet II, Src nternet Protocol ransmission Cont 0 52 54 00 f3 64 0 05 dc 00 00 44 0 05 41 60 d7 11 0 04 02 7c 0b 00	RealtekU_55:15 l Version 4, Src trol Protocol, S 4 3f 52 54 00 55 0 00 40 06 12 ec 3 89 50 26 6d 46 0 00 01 01 08 0a	:75 (52:54:00:55:1 : 11.215.5.66, Dst irc Port: 24791, Ds 5 15 75 08 00 45 00 c 0b d7 05 42 0b d7 3 33 db dd 59 80 10 a 10 12 c2 5f 27 96	15:75), Dst: Realte t: 11.215.5.65 st Port: 5001, Seq: RT d?RT U.u.E @.@B. A`P& mH3.Y.	<pre>kU_f3:64:3f (52: 454, Ack: 1173, </pre>			Ethernet II, Src Internet Protoco Transmission Con 00 52 54 00 f3 6 10 05 dc 00 04 2 00 541 60 d7 1 30 04 02 27 ff 0	: RealtekU_55 l Version 4, 5 trol Protocol, 4 3f 52 54 00 00 00 40 06 00 3 89 50 26 6d 00 00 01 01 08	15:75 (52:54:0 Src: 11.215.5.6 Src Port: 247 55 15 75 08 00 00 0b d7 05 42 48 33 db dd 59 0a 10 12 c2 5f	0:55:15:75) 6, Dst: 11. 91, Dst Por 45 00 RT 0b d7 80 10 A 27 96), Dst: RealtekU 215.5.65 rt: 5001, Seq: 4 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.	_f3:64:3f (52:54	
ithernet II, Src internet Protocol ransmission Cont 0 52 54 00 f3 64 0 05 dc 00 00 44 0 54 160 07 13 0 04 02 7c 0b 06 0 6e 25 17 03 03	RealtekU_55:15 l Version 4, Src trol Protocol, S 4 3f 52 54 00 55 0 00 40 06 12 ec 3 89 50 26 6d 46 0 00 01 01 08 06 3 40 18 00 00 06	:75 (52:54:00:55:1 : 11.215.5.66, Dst irc Port: 24791, Ds 5 15 75 08 00 45 00 c 0b d7 05 42 0b d7 3 33 db dd 59 80 10 a 10 12 c2 5f 27 96 9 00 00 00 00 01 0a	15:75), Dst: Realte t: 11.215.5.65 st Port: 5001, Seq: @.@. 	kU_f3:64:3f (52: 454, Ack: 1173,		000 000 000 000	Ethernet II, Src Internet Protoco Transmission Con 00 52 54 00 f3 6 10 05 dc 00 00 4 20 05 41 60 d7 1 30 04 02 27 ff 0 40 6e 25 17 03 0	: RealtekU_55 l Version 4, S trol Protocol, 4 3f 52 54 00 00 00 40 06 00 3 89 50 26 6d 00 00 01 01 08 3 40 18 00 00	15:75 (52:54:0 Src: 11.215.5.6 Src Port: 247 55 15 75 08 00 00 0b d7 05 42 48 33 db dd 59 0a 10 12 c2 5f 00 00 00 00 00 00	0:55:15:75) 6, Dst: 11. 91, Dst Por 45 00 RT 0b d7 80 10 A 27 96 0 01 04 N%), Dst: RealtekU 215.5.65 rt: 5001, Seq: 4 	_f3:64:3f (52:54	
thernet II, Src: internet Protocol ransmission Cont 052 54 00 f3 60 05 dc 00 00 40 05 41 60 d7 11 06 402 7c 0b 90 6 62 51 7 03 03 6 22 df ac 0a	RealtekU_55:15 l Version 4, Src trol Protocol, S 4 3f 52 54 00 55 0 000 40 06 12 ec 3 89 50 26 6d 44 0 00 01 01 08 0c 3 40 18 00 00 06 a 77 87 17 44 cC	:75 (52:54:00:55:1 : 11.215.5.66, Dst irc Port: 24791, Ds 5 15 75 08 00 45 00 c 0b d7 05 42 0b d7 3 33 db dd 59 80 10 a 10 12 c2 5f 27 96 000 00 00 01 0a 0 d4 61 35 b3 13 86	15:75), Dst: Realte 11:215.5.65 st Port: 5001, Seq: RT. d?RT U.u.E 	kU_f3:64:3f (52: 454, Ack: 1173,			Ethernet II, Src Internet Protoco Transmission Con 00 52 54 00 f3 6 10 05 dc 00 04 2 20 05 41 60 07 1 30 04 02 27 ff 0 40 62 51 17 03 05 60 00 00 00 00 00	: RealtekU_55 l Version 4, S trol Protocol, 4 3f 52 54 00 0 00 40 06 00 3 89 50 26 6d 0 00 01 01 08 3 40 18 00 00 0 00 01 00 00	15:75 (52:54:0 Src: 11.215.5.6 Src Port: 247 55 15 75 08 00 00 0b d7 05 42 48 33 db dd 59 0a 10 12 c2 5f	0:55:15:75) 6, Dst: 11. 91, Dst Por 45 00 RT 0b d7 A 80 10 A 27 96 0 01 04 N%), Dst: RealtekU 215.5.65 rt: 5001, Seq: 4 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.	_f3:64:3f (52:54	
ithernet II, Sro nternet Protocol ransmission Cont 52 54 00 f3 60 0 52 54 00 f3 60 0 55 64 00 00 40 0 54 160 47 11 0 64 02 7c 0b 00 6 25 17 03 00 6 23 24 fac 04 fac 05 76 a8 36 93 56	RealtekU_55:15 l Version 4, Src trol Protocol, S 4 3f 52 54 00 55 0 00 40 06 12 ec 3 89 50 26 6d 44 0 00 01 01 08 06 3 40 18 00 00 06 4 77 87 17 44 cc 6 88 32 38 fa 47	:75 (52:54:00:55:1 : 11.215.5.66, Dst irc Port: 24791, Ds 5 15 75 08 00 45 00 c 0b d7 05 42 0b d7 3 33 db dd 59 80 10 a 10 12 c2 5f 27 96 9 00 00 00 00 01 0a	15:75), Dst: Realte 11:215.5.65 st Port: 5001, Seq:	kU_f3:64:3f (52: 454, Ack: 1173,		00 00 00 00 00 00 00	Ethernet II, Src Internet Protoco Transmission Con 00 52 54 00 f3 6 10 05 dc 00 00 4 00 054 160 d7 1 30 04 02 27 ff 0 40 6e 25 17 03 0 50 00 00 00 00 6 50 00 00 00 0f ff	: RealtekU_55 l Version 4, 5 trol Protocol, 4 3f 52 54 00 0 00 40 06 00 3 89 50 26 6d 0 00 01 01 08 3 40 18 00 00 10 00 01 00 00 f ff 9c 00 00	15:75 (52:54:0 Src: 11.215.5.6 Src Port: 247 55 15 75 08 00 00 0b d7 05 42 48 33 db dd 59 0a 10 12 c2 5f 00 00 00 00 00 13 89 00 00 00	0:55:15:75) 6, Dst: 11. 91, Dst Por 45 00 RT 0b d7 80 10 A 27 96 01 04 N% 00 00), Dst: RealtekU .215.5.65 rt: 5001, Seq: 4 d?RT U u E 0.0 	_f3:64:3f (52:54	
thernet II, Src nternet Protocol ransmission Cont 52 54 00 f3 64 05 dc 00 00 44 0 54 160 d7 13 0 44 02 7c 0b 00 6 62 5 17 03 03 a 2 32 df ac 02 76 a8 36 93 52 38 56 2c 1c 22	RealtekU_55:15 l Version 4, Src trol Protocol, S 4 3f 52 54 00 55 0 00 40 06 12 ec 3 89 50 26 6d 42 0 00 01 01 08 06 3 40 18 00 00 06 a 77 87 17 d4 c6 6 88 32 38 fa 4 2 26 cb 63 dc 40	:75 (52:54:00:55:1 : 11.215.5.66, Dst irc Port: 24791, Ds 5 15 75 08 00 45 00 c 0b d7 05 42 0b d7 3 3 db dd 59 80 10 a 10 12 c2 5f 27 96 0 00 00 00 01 0a 10 41 35 b3 13 86 7 d2 05 82 d0 84 b9	15:75), Dst: Realter t: 11.215.5.65 st Port: 5001, Seq: RT d?RT Uuue 	kW_f3:64:3f (52: 454, Ack: 1173,		00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	Ethernet II, Src Internet Protoco Transmission Con 0 52 54 00 f3 6 0 5 dc 00 00 4 0 5 dc 00 00 4 0 65 41 60 d7 1 30 04 02 27 ff 0 40 6e 25 17 03 0 50 00 00 00 00 ff f 70 33 34 35 36 3 39 30 31 32 3	RealtekU_55 l Version 4, 5 trol Protocol, 43 35 52 54 00 389 50 26 6d 10 00 11 01 08 34 418 00 00 00 00 10 00 00 ff fc c 00 00 738 39 30 31 34 35 36 37	15:75 (52:54:0 Src: 11.215.5.6 Src Port: 247 55 15 75 08 00 00 0b d7 05 42 48 33 db dd 59 0a 10 12 c2 5f 00 00 00 00 00 13 89 00 00 00 02 33 34 35 36 38 39 30 31 32	0:55:15:75) 6, Dst: 11. 91, Dst Por 45 00 RT 0b d7 80 10 A 27 96 10 01 04 n% 00 00 37 38 344 33 34 90), Dst: RealtekU .215.5.65 rt: 5001, Seq: 4 d?RT U.u. E @ @B. 	_f3:64:3f (52:54	
thernet II, Src nternet Protocol ransmission Cont 52 54 00 f3 60 05 4c 00 00 40 05 41 60 47 11 0 44 02 7c 0b 00 6 62 51 7 03 00 1 42 32 4f ac 00 76 a8 36 93 56 38 5e 2c 1c 22 0 ec df 0f a1 93 2 25 2 af 8b ac	RealtekU_55:15 l Version 4, Src trol Protocol, S 4 3f 52 54 00 55 0 00 40 06 12 ec 3 40 18 00 00 6 4 00 01 01 08 02 3 40 18 00 00 06 6 88 32 38 fa 47 2 26 cb 63 dc 46 3 49 09 e5 40 05 d 86 e0 78 01 55	:75 (52:54:00:55:1 : 11.215.5.66, Dst irc Port: 24791, Ds 5 15 75 08 00 45 00 c 0b d7 05 42 0b d7 3 3 db dd 59 80 10 a 10 12 c2 5f 27 96 0 00 00 00 00 01 0a 10 41 25 b3 13 86 7 d2 05 82 d0 84 b9 0 b2 9f 6c 6d bf cc 0 a3 f2 2d 07 45 61 3 16 8e 99 bd c5 df	15:75), Dst: Realte 11:215.5.65 st Port: 5001, Seq: RT d?RT U.u.E 	kW_f3:64:3f (52: 454, Ack: 1173,			Ethernet II, Src Internet Protoco Transmission Con 00 52 54 00 f3 6 10 05 dc 00 00 4 00 054 160 d7 1 130 04 02 27 ff 0 40 6e 25 17 03 0 50 00 00 00 00 ff f 70 33 34 35 36 3 80 39 30 31 32 3 03 53 63 7 38 3	RealtekU_55 l Version 4, 5 trol Protocol, 4 3f 52 54 00 00 00 40 06 00 3 89 50 26 6d 00 00 101 08 3 40 18 00 00 00 00 01 00 00 ff fc 00 00 73 83 93 30 31 3 43 53 63 77 93 03 13 23	15:75 (52:54:0 Src: 11.215.5.6 Src Port: 247 55 15 75 08 00 00 0b d7 05 42 48 33 db dd 59 00 00 00 00 00 13 89 00 00 00 03 83 93 30 32 33 34 35 36 38 39 30 31 32 34 35 36 37 38	0:55:15:75) 6, Dst: 11. 91, Dst Por 45 00 RT 0b d7 A 80 10 A 27 96 1 00 00 A 31 32 3 31 32 3 33 34 90: 56), Dst: RealtekU .215.5.65 rt: 5001, Seq: 4 	_f3:64:3f (52:54	
thernet II, Src nternet Protocol ransmission Cont 52 54 00 f3 64 05 dc 00 00 44 05 41 60 d7 13 0 40 27 c 0b 06 6 e 25 17 03 03 0 a 2 32 df ac 04 76 a 8 5e 2c 1c 22 38 5e 2c 1c 22 2 e c df 0f a 1 93 2 22 52 a f 8b ac 78 7c c9 32 et	RealtekU_55:15 l Version 4, Src trol Protocol, S 4 3f 52 54 00 55 0 00 40 06 12 ec 3 89 50 26 6d 42 0 00 01 01 08 06 3 40 18 00 00 06 a 77 87 17 d4 cc 6 88 32 38 fa 47 2 26 cb 63 dc 46 3 49 09 e5 40 01 d 86 e0 78 01 b5 b a9 26 b3 b1 60	:75 (52:54:00:55:1 : 11.215.5.66, Dst irc Port: 24791, Ds 5 15 75 08 00 45 00 c 0b d7 05 42 0b d7 3 33 db dd 59 80 10 a 10 12 c2 5f 27 96 0 00 00 00 00 10 a 0 d4 61 35 b3 13 86 0 44 61 35 b3 13 86 7 42 05 82 d0 84 b9 0 b2 9f 6c 6d bf cc o a 3 f2 2d 07 45 61 3 16 8e 99 bd c5 df 9 9f c7 a0 57 9a 1d	15:75), Dst: Realter 11:215.5.65 st Port: 5001, Seq: RT d?RT Uuue A`-P& mH3.Y. -A`-P& mH3.Y. -N	<pre>:kU_f3:64:3f (52:</pre>			Ethernet II, Src Internet Protoco Transmission Con 0 52 54 00 f3 6 10 05 dc 00 00 4 20 05 41 60 d7 1 30 04 02 27 ff 0 40 6e 25 17 03 0 60 00 00 00 ff 70 33 34 35 36 3 80 39 30 31 32 3 90 35 36 37 38 3 31 32 33 34 3	: RealtekU_55 l Version 4, S trol Protocol, 4 3f 52 54 00 0 00 40 06 00 0 00 40 06 00 0 00 01 01 08 13 40 18 00 00 10 00 01 00 00 10 00 01 00 00 17 38 39 30 31 13 34 35 36 37 19 30 31 32 33	15:75 (52:54:0 Src: 11.215.5.6 Src Port: 247 55 15 75 08 00 00 0b d7 05 42 48 33 db dd 54 00 00 00 00 00 13 89 00 00 00 01 38 90 00 00 00 00 38 93 00 32 33 34 35 36 38 39 30 31 32 34 35 36 37 38 30 31 32 33 34	0:55:15:75) 6, Dst: 11. 91, Dst Por 45 00 RT 0b d7 80 10 A 27 96 27 96 91 04 N% 00 00 31 32 37 38 34! 33 34 90: 39 30 56 122), Dst: RealtekU .215.5.65 -t: 5001, Seq: 4 -0.0	_f3:64:3f (52:54	
thernet II, Src nternet Protocol ransmission Cont 52 54 00 f3 64 05 41 60 07 11 04 02 7c 0b 06 6 e25 17 03 05 16 e25 17 03 05 7 6 a8 36 93 56 7 6 a8 36 93 56 7 6 a8 36 e2 c 1c 22 e c df 0f a1 93 2 e5 2 af 8b ac 7 87 c c 9 32 ef 3 94 fe 6 ef 44	RealtekU_55:15 l Version 4, Src trol Protocol, S 4 3f 52 54 00 55 0 000 40 06 12 ec 3 89 50 26 6d 4f 0 00 01 01 08 06 3 40 18 00 00 06 a 77 87 17 d4 cC 6 88 32 38 fa 47 2 26 cb 63 dc 46 3 49 09 e5 40 01 d 86 e0 78 01 b5 b a9 26 b3 b1 66 a 52 70 bb 8e c4	:75 (52:54:00:55:1) :11.215.5.66, Dst :rc Port: 24791, 5 15 75 08 00 450 00 5 15 75 08 00 450 00 70 33 db d5 98 10 3 33 db d5 98 10 10 10 12 c2 57 27 96 00 00 00 10	15:75), Dst: Realte 11:215.5.65 st Port: 5001, Seq:	<pre>kU_f3:64:3f (52: 454, Ack: 1173,</pre>			Ethernet II, Src Internet Protoco Transmission Con 05 25 400 f3 6 05 dc 00 00 4 05 dc 00 00 4 06 25 17 03 0 60 00 00 00 00 ff f 03 34 35 36 3 39 36 31 32 33 34 3 03 7 38 39 30 31 32 3 03 7 38 39 30 31 32 30 30 37 38 39 30 31 32 30 30 31 32 30 31 32 30 31 32 30 30 31 32 30 30 30 30 30 30 30 30 30 30 30 30 30	RealtekU_55: l Version 4, S trol Protocol, 43 35 52 54 00 389 50 26 6d 10 00 01 01 08 34 01 80 00 00 00 01 01 08 00 00 100 00 6f ff 9c 000 03 34 35 36 37 13 34 35 36 37 13 32 33 34 35	15:75 (52:54:0 Src: 11.215.5.6 Src Port: 247 55 15 75 08 00 00 0b d7 05 42 48 33 db dd 59 0a 10 12 c2 5f 00 00 00 08 39 30 13 89 00 00 00 02 33 34 35 36 38 39 30 31 32 34 35 36 37 38 30 31 32 33 44	0:55:15:75) 6, Dst: 11. 91, Dst Por 45 00 RT 0b d7 A 27 96 10 80 10 A 27 96 10 00 00 31 32 33 34 90: 39 30 56: 35 36 122 785), Dst: RealtekU .215.5.65 -rt: 5001, Seq: 4 -0.00 -0.	_f3:64:3f (52:54	
thernet II, Src nternet Protocol ransmission Cont 52 54 00 f3 60 05 dc 00 00 40 05 41 60 d7 11 0 40 22 7c 0b 00 6 62 51 77 03 05 0 42 32 df ac 00 76 a8 36 93 50 38 5e 2c 1c 22 0 ec df 0f al 9 2 es 22 af 8b ac 78 7c c9 32 et 39 4f e6 ef 44 30 2c c1 0e 00	RealtekU_55:15 l Version 4, Src trol Protocol, S 4 3f 52 54 00 55 0 00 40 06 12 ec 3 40 18 00 00 66 3 40 18 00 00 66 4 77 87 17 44 cc 6 88 32 38 fa 47 2 26 cb 63 dc 46 3 49 09 e5 40 01 d 86 e0 78 01 b5 b a9 26 b3 16 66 a 52 70 bb 8e cc 84 56 cc 9d 06	:75 (52:54:00:55:1 : 11.215.5.66, Dst irc Port: 24791, Ds 5 15 75 08 00 45 00 c 0b d7 05 42 0b d7 3 33 db dd 59 80 10 a 10 12 c2 5f 27 96 0 00 00 00 00 01 0a 10 4 61 35 b3 13 86 7 d2 05 82 d0 84 b9 0 b2 9f 6c 6d bf cc 0 a3 f2 2d 07 45 61 3 16 8e 99 bd c5 df 0 9f c7 a0 57 9a 1d 4 3a da b2 c5 a5 30 3 d0 f1 16 4a 01 0a	15:75), Dst: Realte 11:215.5.65 st Port: 5001, Seq: A'P& mH3.Y. A'P& mH3.Y. 	<pre>kkU_f3:64:3f (52: 454, Ack: 1173,</pre>			Ethernet II, Src Internet Protoco Transmission Con 00 52 54 00 f3 6 10 05 dc 00 00 4 00 05 16 00 7 130 04 02 27 ff 0 40 66 25 17 03 0 50 00 00 00 00 ff f 70 33 34 35 36 3 30 31 32 33 34 3 30 31 32 33 34 3 30 31 32 33 34 3 30 37 38 39 30 3 33 34 35 36 3	RealtekU_55 l Version 4, 5 trol Protocol, 4 3f 52 54 00 0 00 40 66 00 3 89 50 26 6d 0 00 01 10 3 40 18 00 00 0 00 00 01 00 00 ff fg c 00 00 rd 38 3 30 31 3 34 35 36 37 9 30 31 32 33 15 36 37 38 39 13 22 33 34 35 7 38 39 30 31	15:75 (52:54:0 Src: 11.215.5.6 Src Port: 247 55 15 75 08 00 00 0b d7 05 42 08 33 db d5 9 00 00 00 00 00 13 89 00 00 00 00 00 83 93 30 32 33 34 35 36 38 39 30 31 32 34 35 36 37 38 30 31 32 33 44 36 37 38 39 30 32 33 44 35 36	0:55:15:75) 6, Dst: 11. 91, Dst Por 45 00 RT 0b d7 A 27 96 1 80 10 A 27 96 1 00 00 3 31 32 3 33 34 900 35 36 12 31 32 788 344), Dst: RealtekU .215.5.65 rt: 5001, Seq: 4 	_f3:64:3f (52:54	
thernet II, Src nternet Protocol ransmission Cont 52 54 00 f3 64 05 dc 00 00 44 05 41 60 d7 11 0 44 02 7c 0b 00 6 e 25 17 03 00 a 23 2d ff ac 04 76 a8 36 93 56 38 5e 2c 1c 22 0 e cd f of al 93 2 e 52 af 8b at 78 7c c9 32 ef 39 4f e6 ef 44 39 4f c6 b6 49 7 d 1d bc 6b 83	RealtekU_55:15 Version 4, Src trol Protocol, S 4 3f 52 54 00 55 0 00 40 06 12 ec 3 40 18 00 00 06 a 77 87 17 44 cc 6 88 32 38 fa 47 2 26 cb 63 dc 46 3 49 09 e5 40 00 d 86 e0 78 01 b5 b a9 26 b3 b1 66 a 52 70 bb 8e c2 e 84 56 cc 9d 06 4 94 fe 6f 47 f4	:75 (52:54:00:55:1 : 11.215.5.66, Dst irc Port: 24791, Ds 5 15 75 08 00 45 00 c 0b d7 05 42 0b d7 3 33 db dd 59 80 10 a 10 12 c2 5f 27 96 0 00 00 00 00 01 0a 0 d4 61 35 b3 13 86 7 d2 05 82 d0 84 b9 0 b2 9f 6c 6d bf cc 0 a3 f2 2d 07 45 61 3 16 8e 99 bd c5 df 0 9f c7 a0 57 9a 1d 4 3a da b2 e5 a5 30 a d0 f1 16 4a 01 0a 4 d1 39 3e e8 09 fb	15:75), Dst: Realter 11:215.5.65 st Port: 5001, Seq: A' P& mH3. Y. - A' P&	<pre>skU_f3:64:3f (52:</pre>			Ethernet II, Src Internet Protoco Transmission Con 00 52 54 00 f3 6 10 05 dc 00 00 4 20 05 41 60 d7 1 30 04 02 27 ff 0 40 6e 25 17 03 0 60 00 00 00 00 60 60 00 00 00 00 ff 70 33 34 35 36 3 30 31 32 33 34 3 31 32 33 34 35 36 3 30 33 34 35 36 3 30 33 34 35 36 3 30 39 30 31 32 3	RealtekU_55 l Version 4, S trol Protocol, 4 3f 52 54 00 00 00 40 06 00 3 89 50 26 6d 0 00 1 01 08 3 4 01 8 00 00 60 00 01 00 00 7 38 39 30 31 3 34 35 36 37 7 38 39 30 31 3 34 35 36 37 7 38 39 30 31 3 34 35 36 37 3 34 35 36 37	$\begin{array}{c} 15:75 & (52:54:0\\ \text{Src:} & 11.215.5.6\\ \text{Src:} & 12.215.5.6\\ \text{Src:} & 247\\ \hline 55 & 15 & 75 & 08 & 00\\ 00 & 0b & d7 & 05 & 42\\ 48 & 33 & db & dd & 59\\ 00 & 00 & 00 & 00 & 00\\ 13 & 89 & 00 & 00 & 00\\ 00 & 03 & 39 & 30\\ 32 & 33 & 44 & 35 & 36\\ 38 & 39 & 30 & 31 & 32\\ 34 & 35 & 36 & 37 & 38\\ 30 & 31 & 32 & 33 & 44\\ 36 & 37 & 38 & 39 & 30\\ 32 & 33 & 44 & 55 & 36\\ 38 & 39 & 30 & 31 & 32\\ \hline \end{array}$	0:55:15:75) 6, Dst: 11. 91, Dst Por 45 00 RT 0b d7 A 27 96 1 01 04 n% 00 00 A 31 32 3 31 32 3 39 30 56 35 36 12: 37 38 34 90 37 38 34 90), Dst: RealtekU .215.5.65 rt: 5001, Seq: 4 d?RT U.u.E. .0.0 .0.89012 567890 12345678 123456 78901234 789012 3456789 345678 9012345 567890 12345678 90123456789012 567890 12345678	_f3:64:3f (52:54	
Ethernet II, Src Internet Protocol Transmission Cont 052 54 00 f3 64 0 05 dc 00 00 44 0 05 d1 60 d7 11 0 62 21 7 03 03 0 62 22 df ac 04 0 63 54 c0 03 38 52 cc 1c 22 0 64 02 7c 04 60 0 64 02 7c 04 60 0 62 21 7 03 03 0 76 a8 36 93 56 0 76 a8 36 93 52 0 26 25 2 af 8b ac 0 39 4f 66 ef 41 0 39 4f 66 ef 44 0 30 2c c1 06 06 0 7d 1d bc 6b 34 0 90 dc 44 5b	RealtekU_55:15 l Version 4, Src trol Protocol, S 4 3f 52 54 00 55 0 000 40 06 12 ec 3 89 50 26 6d 4f 0 00 01 01 08 06 3 40 18 00 00 06 a 77 87 17 d4 cC 6 88 32 38 fa 47 2 26 cb 63 dc 46 3 49 09 e5 40 01 d 86 e0 78 01 b5 b a9 26 b3 b1 66 a 52 70 bb 8e c2 e 84 56 cc 9d 06 4 94 fe 6f 47 f2 2 1f 1b ed fc 21	:75 (52:54:00:55:1) :1.215.5.66, Dst :rc Port: 24791, Ds 5 15 75 08 00 45 06 5 15 75 08 00 45 06 07 3 3d dd 59 80 10 a 10 12 c2 57 79 80 10 a 10 12 c2 57 27 96 90 00 00 01 0a a 10 12 c2 57 27 96 10 04 61 35 b3 13 86 7 42 05 82 d0 84 b9 b2 96 c6 64 b7 c0 a3 f2 d0 74 51 13 16 84 91 a3 a4 b2 54 54 30 34 d1 39 ae 89 b0 ad 14 40 14 a4 47 47	15:75), Dst: Realter 11:1215.5.65 st Port: 5001, Seq: RT d?RT U.U.E 	<pre>kU_f3:64:3f (52: 454, Ack: 1173,</pre>		O O	Ethernet II, Src Internet Protoco Transmission Con 0 52 54 00 63 6 0 65 dc 00 00 4 0 55 dc 00 00 4 0 65 dc 00 00 4 0 65 dc 00 00 4 0 66 25 17 03 0 60 00 00 00 00 0 60 00 00 00 00 ff f 0 33 44 35 36 3 39 35 36 37 38 3 0 31 32 33 34 35 30 33 34 35 36 3 31 32 33 34 35 36 3 30 39 30 31 32 3 0 35 36 37 38 3 0 37 38 39 30 31 32 3 0 35 36 37 38 3	RealtekU_55: l Version 4, S trol Protocol, 43 35 52 54 00 00 04 06 389 50 26 6d 00 00 1 01 08 33 40 18 00 00 60 00 01 01 08 34 39 30 31 35 36 37 38 39 13 2 33 34 35 13 34 35 36 37 13 32 33 34 35 13 34 35 36 37 13 2 33 34 35 13 34 35 36 37 13 3 34 35 36 37 38 39 34 35 36 37 33 34 35 36 37 34 35 36 37 34 35 36 37 35 36 37 38 39 36 31 32 33	$\begin{array}{c} 15:75 & (52:54:6)\\ \text{Src: } 11.215.5.6 \\ \text{Src Port: } 247 \\ \hline \\ 55 & 15 & 75 & 08 & 00 \\ 00 & 0b & d7 & 05 & 42 \\ 48 & 33 & db & dd & 59 \\ 0a & 10 & 12 & c2 & 5f \\ 00 & 00 & 00 & 00 & 00 \\ 00 & 00 & 38 & 39 & 30 \\ 38 & 39 & 30 & 31 & 32 \\ 34 & 35 & 36 & 37 & 38 \\ 30 & 31 & 32 & 33 & 44 \\ 35 & 36 & 37 & 38 & 39 & 30 \\ 32 & 33 & 34 & 35 & 36 \\ 38 & 39 & 30 & 31 & 32 \\ 34 & 35 & 36 & 37 & 38 \\ 39 & 30 & 31 & 32 \\ 34 & 35 & 36 & 37 & 38 \\ 39 & 30 & 31 & 32 \\ 34 & 35 & 36 & 37 & 38 \\ \end{array}$	0:55:15:75) 6, Dst: 11. 91, Dst Port 45 00 RT 0b d7 A 27 96 10 A 27 96 10 A 27 96 10 A 27 96 10 A 33 34 90 35 36 12 31 32 788 37 38 344 33 34 90 33 34 90 33 34 90 33 34 90 33 34 956), Dst: RealtekU .215.5.65 -rt: 5001, Seq: 4 -0.20 -0.	_f3:64:3f (52:54	
thernet II, Src nternet Protocol ransmission Cont 52 54 00 f3 6 0 55 cc 00 00 40 0 54 160 d7 13 0 04 02 7c 0b 00 6 e25 17 03 05 0 6 e25 17 03 05 0 76 a8 36 93 50 0 76 a8 36 93 50 0 76 a8 50 22 e1 2 2 52 af 8b a0 78 7c c9 32 e1 3 9 4f e6 ef 44 0 30 2c c1 0e 06 0 9 dc 44 5b 92 0 9 dc 44 5b 92	RealtekU_55:15 l Version 4, Src trol Protocol, S 4 3f 52 54 00 55 0 00 40 06 12 ec 3 40 18 00 00 64 4 36 23 88 50 26 6d 44 0 00 01 01 08 06 3 40 18 00 00 66 6 88 32 38 fa 47 2 26 cb 63 dc 46 3 49 09 26 40 01 d 86 e0 78 01 b5 b a9 26 b3 16 66 a 52 70 bb 8e cc 84 56 cc 9d 06 4 94 fe 6f 47 fz 2 1f 1b ed fc 2h 7 48 b5 fd 7e 92	:75 (52:54:00:55:1) :1.215.5.66, Dst :rc Port: 24791, Ds :5 15 75 08 00 45 00 :0 175 08 00 45 00 00 00 00 00 00 00 00 01 03 04 135 03 13 86 7 02 05 25 27 96 00 00 00 01 03 13 86 7 02 05 82 04 84 b9 02 04 61 35 03 13 86 7 02 03 72 24 07 45 61 31 86 99 b0 c5 df 04 61 35 31 86 99 b1 c5 df 05 c3 c2 c4 c7 c4 c7 c3 c4 c4 c5 df 05 c5 df c5 c6 c4 c4 c4 c4 c4 c4 c4	15:75), Dst: Realter 11:215.5.65 st Port: 5001, Seq: RT d?RT U.u.E 	<pre>kkU_f3:64:3f (52: 454, Ack: 1173, </pre>			Ethernet II, Src Internet Protoco Transmission Con 00 52 54 00 63 6 10 05 dc 00 00 4 00 54 60 27 16 00 7 130 04 02 27 ff 0 40 66 25 17 03 0 60 00 00 00 00 ff f 70 33 34 35 36 3 35 36 37 38 3 40 31 32 33 34 35 36 3 30 33 34 35 36 3 31 32 33 34 35 36 3 30 33 34 35 36 3 31 32 33 34 35 36 3 36 37 38 39 30 31 32 3 40 35 36 37 38 3 50 35 36 37 38 3 5	RealtekU_55 l Version 4, 5 trol Protocol, 4 3f 52 54 00 0 00 40 06 00 0 00 01 01 08 3 40 18 00 00 0 00 01 01 08 3 40 18 00 00 0 00 01 13 23 5 36 37 38 30 31 3 43 35 36 37 13 2 33 34 35 13 32 33 34 35 13 34 35 36 37 13 32 33 34 35 13 32 33 34 35 13 34 35 36 37 13 34 35 36 37 13 34 35 36 37 13 34 35 36 37 13 34 35 36 37 13 34 35 36 37 13 34 35 36 37 13 34 35 36 37 13 34 35 36 37 13 34 35 36 37 13 34 35 36 37 34 35 36 37 35 36 37 38 39	$\begin{array}{c} 15:75 & (52:54:6)\\ \text{Src: } 11.215.5.6 \\ \text{Src Port: } 247 \\ \hline \\ 55 & 15 & 75 & 08 & 00 \\ 00 & 0b & d7 & 05 & 42 \\ 48 & 33 & db & d59 \\ 0a & 10 & 12 & c2 & 5f \\ 00 & 00 & 00 & 00 & 00 \\ 13 & 89 & 00 & 00 & 00 \\ 00 & 00 & 38 & 39 & 30 \\ 32 & 33 & 34 & 35 & 36 \\ 38 & 39 & 30 & 31 & 32 \\ 34 & 35 & 36 & 37 & 38 \\ 30 & 31 & 32 & 33 & 44 \\ 53 & 36 & 37 & 38 \\ 30 & 31 & 32 & 33 & 44 \\ 53 & 36 & 37 & 38 \\ 30 & 31 & 32 & 33 & 34 \\ \end{array}$	0:55:15:75) 6, Dst: 11. 91, Dst Por 45 00 RT 0b d7 A 27 96 1 00 00 A 27 96 1 00 00 A 33 34 90 35 36 122 31 32 788 344 33 34 900 39 30 566 35 36 122 31 32 788 344 33 34 900 39 30 566 35 36 122 35 36 122), Dst: RealtekU .215.5.65 -rt: 5001, Seq: 4 	_f3:64:3f (52:54	
thernet II, Src nternet Protocol ransmission Cont 52 54 00 f3 64 05 dc 00 00 40 05 dc 00 00 40 05 d1 60 d7 11 0 40 02 7c 0b 00 a2 32 df ac 04 76 a8 36 93 56 38 5e 2c 1c 22 e c df 0f a1 93 2e 52 af 8b at 39 4f e6 ef 44 39 2c 10e 04 39 4f e6 65 30 4f e6 54 30 2c 10e 04 7d 1d bc 6b 34 09 dc 44 5b 92 16 87 7b 9c c1	RealtekU_55:15 Version 4, Src trol Protocol, S 4 3f 52 54 00 55 0 00 40 06 12 ec 3 89 50 26 6d 44 0 00 01 01 08 0a 3 40 18 00 00 06 a 77 87 17 44 cc 6 88 32 38 fa 47 2 26 cb 63 dc 46 3 49 09 e5 40 0b 4 86 e0 78 01 b5 b 89 26 b3 b1 66 a 52 70 bb 8e c2 e 84 56 cc 9d 0b 4 94 fe 6f 47 f2 2 1f be df 7e 92 b ae 50 40 43 45	:75 (52:54:00:55:1) :1.215.5.66, Dst irr Port: 24791, Ds 5 15 75 08 00 45 00 5 15 75 08 00 45 00 6 15 75 08 00 45 00 6 15 75 08 00 45 00 6 15 75 08 00 45 00 6 10 12 c2 5f 27 96 0 00 00 00 00 01 0a 10 12 c2 5f 27 96 0 00 00 00 00 01 0a 0 44 61 35 b3 13 86 7 d2 05 82 d0 84 b9 0 b2 9f 6c 6d bf cc 0 31 62 9f bc 5df 0 9f c7 a0 57 9a 1d 4 3a da b2 e5 a5 30 30 d0 f1 16 4a 01 0a 4 13 39 ae e8 09 fb 0 24 9f da a4 74 e7 2 2a 00 d5 a0 66 a1 e ff e0 e6 3c 6f 33	15:75), Dst: Realter 11:215.5.65 st Port: 5001, Seq: RT d?RT U.u.E @.@B. A`P& mH3.Y. 	<pre>kkU_f3:64:3f (52: 454, Ack: 1173,</pre>			Ethernet II, Src Internet Protoco Transmission Con 00 52 54 00 63 6 10 05 dc 00 00 4 00 54 60 27 16 00 7 130 04 02 27 ff 0 40 66 25 17 03 0 60 00 00 00 00 ff f 70 33 34 35 36 3 35 36 37 38 3 40 31 32 33 34 35 36 3 30 33 34 35 36 3 31 32 33 34 35 36 3 30 33 34 35 36 3 31 32 33 34 35 36 3 36 37 38 39 30 31 32 3 40 35 36 37 38 3 50 35 36 37 38 3 5	RealtekU_55 1 Version 4, S trol Protocol, 4 3f 52 54 00 00 00 40 06 00 3 89 50 26 6d 0 00 1 01 08 3 4 018 00 00 0 00 01 00 00 f ff 9c 00 00 7 38 39 30 31 3 4 35 36 37 38 39 13 34 35 36 37 35 36 37 38 39 34 35 36 37 35 36 37 38 39 34 35 36 37 35 36 37 38 39 34 35 36 37 35 36 37 38 39 31 32 33 34 35 35 36 37 38 39 31 32 33 34 35 35 36 37 38 39 34 35 36 37 35 36 37 38 39 33 34 35 36 37 35 36 37 38 39 36 37 38 39 37 38 39 34	$\begin{array}{c} 15:75 & (52:54:0\\ \text{Src: } 11.215.5.6\\ \text{Src: } 12.215.5.6\\ \text{Src: } 17.215.5.6\\ \text{Src: } 17.57 & 08.00\\ 00 & 0b & d7.05 & 42\\ 48 & 33 & db & dd & 59\\ 00 & 00 & 00 & 00 & 00\\ 13 & 89 & 00 & 00 & 00\\ 00 & 03 & 39 & 30\\ 32 & 33 & 44 & 55 & 63\\ 30 & 31 & 32 & 33 & 44\\ 36 & 37 & 38 & 39 & 30\\ 32 & 33 & 44 & 55 & 63\\ 38 & 39 & 30 & 31 & 32\\ 34 & 35 & 36 & 37 & 38\\ 30 & 31 & 32 & 33 & 44\\ 35 & 36 & 37 & 38 & 39 & 30\\ 30 & 31 & 32 & 33 & 44\\ 36 & 37 & 38 & 39 & 30\\ 30 & 31 & 32 & 33 & 44\\ 36 & 37 & 38 & 39 & 30\\ \end{array}$	0:55:15:75) 6, Dst: 11. 91, Dst Por 45 00 RT 0b d7 80 10 A 27 96 01 04 n% 00 00 31 32 37 38 344 33 34 90 35 36 12: 31 32 788 33 34 90 35 36 12: 31 32 788), Dst: RealtekU .215.5.65 -rt: 5001, Seq: 4 -0.20 -0.	_f3:64:3f (52:54	
Ethernet II, Sro Internet Protocol Transmission Cont 00 52 54 00 f3 64 10 05 dc 00 00 44 20 05 41 60 d7 13 130 04 02 7c 0b 00 40 62 51 77 03 05 60 a2 32 df ac 04 50 a2 32 df ac 04 50 a2 32 df ac 04 50 a8 58 22 12 23 60 a2 39 4f e6 ef 44 50 39 4f e6 ef 44 50 30 2c c1 0e 04 7d 1d bc 6b 34 20 9d c44 5b 93 60 16 87 7b 9c c1 50 dc da 08 7d 11	RealtekU_55:15 Version 4, Src trol Protocol, S 4 3f 52 54 00 55 0 00 40 06 12 ec 3 89 50 26 6d 44 0 00 01 01 08 0a 3 40 18 00 00 06 a 77 87 17 44 cc 6 88 32 38 fa 47 2 26 cb 63 dc 46 3 49 09 e5 40 0b 4 86 e0 78 01 b5 b 89 26 b3 b1 66 a 52 70 bb 8e c2 e 84 56 cc 9d 0b 4 94 fe 6f 47 f2 2 1f be df 7e 92 b ae 50 40 43 45	:75 (52:54:00:55:1) :1.215.5.66, Dst :rc Port: 24791, Ds :5 15 75 08 00 45 00 :0 175 08 00 45 00 00 00 00 00 00 00 00 01 03 04 135 03 13 86 7 02 05 25 27 96 00 00 00 01 03 13 86 7 02 05 82 04 84 b9 02 04 61 35 03 13 86 7 02 03 72 24 07 45 61 31 86 99 b0 c5 df 04 61 35 31 86 99 b1 c5 df 05 c3 c2 c4 c7 c4 c7 c3 c4 c4 c5 df 05 c5 df c5 c6 c4 c4 c4 c4 c4 c4 c4	15:75), Dst: Realter 11:215.5.65 st Port: 5001, Seq: RT d?RT U.u.E @.@B. A`P& mH3.Y. 	<pre>kkU_f3:64:3f (52: 454, Ack: 1173,</pre>			Ethernet II, Src Internet Protoco Transmission Con 00 52 54 00 f3 6 10 05 dc 00 00 4 20 05 41 60 d7 1 30 04 02 27 ff 0 40 6e 25 17 03 0 60 00 00 00 00 ff 70 33 34 35 36 3 30 39 30 31 32 3 30 31 32 33 34 3 31 32 33 34 35 36 3 31 32 33 34 35 36 3 39 30 31 32 33 34 3 30 39 30 31 32 3 31 32 33 34 3 30 37 38 39 30 3 31 32 33 34 3 30 37 38 39 30 3 31 32 33 34 3 30 37 38 39 30 3 37 38 39 30 31 32 3 37 38 39 30 30 31 32 3 37 38 39 30 31 32 3 37 38 39 30 31 32 3 37 38 39 30 31 32 3 37 38 39 30 30 30 31 32 3 37 38 39 30 30 30 30 30 30 30 30 30 30 30 30 30	RealtekU_55 1 Version 4, S trol Protocol, 4 3f 52 54 00 00 00 40 06 00 3 89 50 26 6d 0 00 1 01 08 3 4 018 00 00 0 00 01 00 00 f ff 9c 00 00 7 38 39 30 31 3 4 35 36 37 38 39 13 34 35 36 37 35 36 37 38 39 34 35 36 37 35 36 37 38 39 34 35 36 37 35 36 37 38 39 34 35 36 37 35 36 37 38 39 31 32 33 34 35 35 36 37 38 39 31 32 33 34 35 35 36 37 38 39 34 35 36 37 35 36 37 38 39 33 34 35 36 37 35 36 37 38 39 36 37 38 39 37 38 39 34	$\begin{array}{c} 15:75 & (52:54:0\\ \text{Src: } 11.215.5.6\\ \text{Src: } 12.215.5.6\\ \text{Src: } 17.215.5.6\\ \text{Src: } 17.57 & 08.00\\ 00 & 0b & d7.05 & 42\\ 48 & 33 & db & dd & 59\\ 00 & 00 & 00 & 00 & 00\\ 13 & 89 & 00 & 00 & 00\\ 00 & 03 & 39 & 30\\ 32 & 33 & 44 & 55 & 63\\ 30 & 31 & 32 & 33 & 44\\ 36 & 37 & 38 & 39 & 30\\ 32 & 33 & 44 & 55 & 63\\ 38 & 39 & 30 & 31 & 32\\ 34 & 35 & 36 & 37 & 38\\ 30 & 31 & 32 & 33 & 44\\ 35 & 36 & 37 & 38 & 39 & 30\\ 30 & 31 & 32 & 33 & 44\\ 36 & 37 & 38 & 39 & 30\\ 30 & 31 & 32 & 33 & 44\\ 36 & 37 & 38 & 39 & 30\\ \end{array}$	0:55:15:75) 6, Dst: 11. 91, Dst Por 45 00 RT 0b d7 80 10 A 27 96 01 04 n% 00 00 31 32 37 38 344 33 34 90 35 36 12: 31 32 788 33 34 90 35 36 12: 31 32 788), Dst: RealtekU .215.5.65 -rt: 5001, Seq: 4 -d?RT ·U·u·E ···P& mH3·Y. ···P& mH3·Y. ···· 2567890 12345678 123456 78901234 789012 34567890 345678 90123456 901234 56789012 34567890 123456780 13345678 90123456 901234 56789012 3456789 0123456	_f3:64:3f (52:54	

WIC kTLS offload challenges

- Minor OSI model violation.
- Packets are sent containing full headers, except for un-encrypted payload.
- Prior to retransmission, crypto cursor needs update by re-transmitting off-the-wire parts of the TLS record, if any.



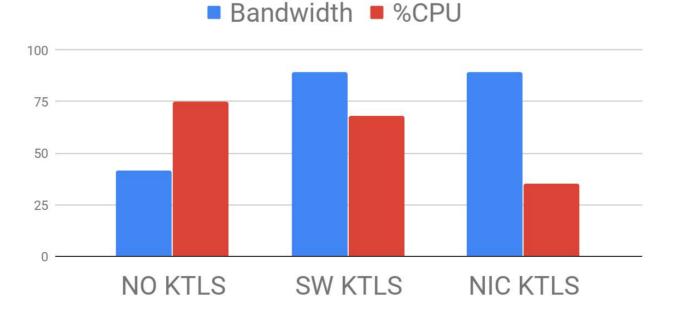
Benchmarks



Kernel TLS Performance: 90Gb/s, 68% CPU (SW), 35% CPU (T6 NIC kTLS)

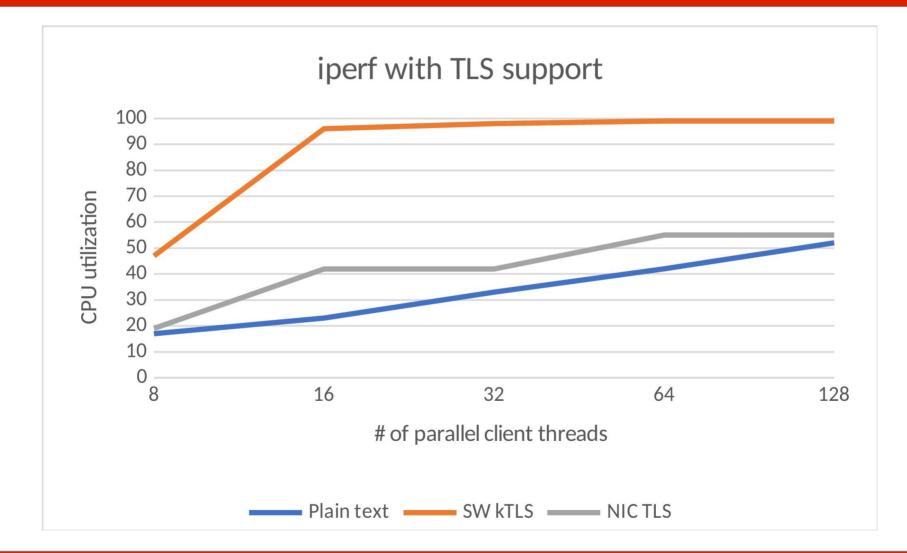
- Original (~2016) Netflix 100G NVME flash appliance
 - E5-2697A v4 @ 2.60GHz (16 core / 32 HTT), 128GB DDR4 2400MT/s, 1x100GbE, 4xNVME

kTLS vs Userspace





Mellanox NIC TLS





• ConnectX-6 DX (coming October 2019)

- <u>http://www.mellanox.com/page/ethernet_cards_overview</u>
- 16 000 000 simultaneous TLS connections (25, 50, 100 and 200 Gbit/s)





- T6 NIC TLS supports TLS v1.1 and v1.2 using both AES-CBC and AES-GCM.
- TOE TLS support for kTLS is in progress.
- ccr(4) can be used for AES-GCM via the OCF backend.



Q/A