

TAP All The Things

Using the BSidesDFW 9 Badge to View Network Traffic



Presented by @alt_bier



What is a TAP?

A network TAP is an external monitoring device that mirrors the traffic that passes between two network nodes. A TAP (test access point) is a hardware device inserted at a specific point in the network to monitor data.

A passive Ethernet TAP like the BSidesDFW badge is limited to speeds of 100Mb since the 1Gb protocol would require active components in the TAP. The BSidesDFW badge uses capacitors to force the inline devices to autonegotiate a speed of 100Mb or below.







Connecting Devices to the TAP

The BSidesDFW badge has two "Inline" RJ45 ports that should be connected between the two network nodes that you wish to monitor.

You should not need to modify speed settings on these "Inline" node connections as they will auto-negotiate to 100Mb or less.

For the Demo we will be connecting two laptops together using static IP's. In the real world you would most likely place the TAP in-between a single device and the switch port it connects to.







Connecting Devices to the TAP

The BSidesDFW badge has two "TAP" RJ45 ports that are hardwired to see traffic in one direction. To view traffic from both directions you must monitor both.

Since the "TAP" ports are only receiving traffic, autonegotiation will not work. The monitor interfaces must have the port speed manually configured.

For the Demo we will be monitoring both "TAP" ports connected to the same laptop. In the real world you would most likely monitor one or the other direction, moving the monitor port as needed.







Wireshark Protocol Analyzer

Wireshark is a free open source network protocol analyzer (formerly known as Ethereal) that captures packets in real time and display them in human-readable format. It is available for download here:



https://www.wireshark.org/

Wireshark will display the packets seen on one or more interfaces and "decode" this information providing details about the protocols being used and the state of the traffic in real time.





After downloading and installing Wireshark, you can launch it and double-click the name of a network interface under Capture to start capturing packets on that interface.

As soon as you click the interface's name, you'll see the packets start to appear in real time.

ile	Edi	t	Viev	V	Go	Cap	ture	Ana	lyze	Statis	stics	Telep	hony	Wir	reless	To	ols	Help
0	1	5 6	•		5	×	6	9	-	- EE	1	8		Đ,	Q	2	EF.	
A.	weby a	die	day	filter		tel./		-										
1.4	1017.0	Gray	ind y	1115040														
				141														
	N	/elc	om	e to	Wire	sha	rk											
	Ca	ap	tur	е														
	u	sing	this	filte	r: 🔳	Ent	er a c	apture	filter									
					-													
	Vi	tua	IBOX	Ho	st-Or	ily N	etwo	rik			L							
	VN	Awa	are N	letw	ork A	dapt	ter VN	Ine	A	г Г	M	Ĩ						
	Et	herr	net 2									_						
	VN	/wa	are N	letw	ork A	dapt	ter VN	Anet1			1							
	E+I	harr	toot															
G	apturi	ng f	rom	Wi-	Fi				_									
Ca	<mark>epturi</mark> Edit	ng f Vi	rom ew	Wi-l Go	Fi	oture	An	alvze	Statis	tics	Telepi	hony	Wireles	5 Te	ools	Help		
Ca le	Edit	ng f Vi	rom ew	Wi-l Go	Fi Caj	oture	An	alyze	Statis	tics	Telep	hony	Wireles:	s To	ools	Help		
Ca le	Edit	ng f Vi ()	ew	Go	Fi Caj	oture	An Q	alyze	Statis	tics	Telep	hony	Wireles:	s To ©	ools	Help		
le App	Edit	ng f Vi © ispla	ew y filte	Go	Caj	oture	An Q	alyze	Statis	tics	Telepi	hony	Wireles: ⊙_⊖_	s To Q	ools III rotocol	Help	nath	Info
le App	Edit Edit I <u>C</u> Ny a d	ng f Vi () ispla Time 36.	rom ew y filte	Wi-I Go	Fi Caj	oture	An Q e :f8b	alyze ⊛ ∉	Statis	tics	Telepi	hony	Wireles: @ @ @	s To @	rotocol LSv1.	Help Le	ngth 120	Info Applic
Са Іе Арр 2	Edit Edit Diy a d	ng f Vi () ispla Time 36. 36.	rom ew y filte 9514 9515	Wi-l Go Er	Fi Caj	Source 2607	An 9 :f8b(:1c0	alyze	Statis	tics	Telepl stinati 01:10	hony on c0:cf0 8b0:40	Wireles: () () () () () () () () () ()	s To @ P : T	rotocol LSv1. CP	Help Le	ngth 120 74	Info Applic 58841
е [Edit	ng f Vi () ispla 36. 36. 36.	rom ew y filte 9514 9515	Wi-l Go F 443 504 770	Caj	oture	An 9 :f8b0 :1c0 :1c0	alyze	Statis	tics	stinati 01:10 07:fi	hony on c0:cf0 8b0:40 8b0:40	Wireles: () () () () () () () () () ()	с Тс (С) С С С С С С С С С С С С С	rotocol LSv1. CP	Help Le 2	ngth 120 74 120	Info Applic 58841 Applic
Calle App 2 2 2 2 2 2 2	Edit Edit My a d 031 032 033 034 035	ng f Vi () ispla 36. 36. 36. 37. 37.	rom ew y filte 9514 9515 9517 9517 2160	Wi-l Go Go 443 504 770 L75 574	Caj	bture	An 2 :f8b :1c0 :f8b :1c0	alyze @	Statis	tics	Telepi stinati 01:1 07:fi 07:fi 01:1	hony on c0:cf0 8b0:40 8b0:40 c0:cf0 8h0-40	Wireles: () () () () () () () () () ()	с То е г г т т т т т т т т т	rotocol LSv1. CP LSv1. CP	Help Le 2	ngth 120 74 120 74	Info Applic 58841 Applic 443 → [TCP =
Calle App 2 2 2 2 2 2 2 2	Edit Edit My a d 031 032 033 034 034	ng f Vi ispla 36. 36. 37.	rom ew 9514 9515 9517 2164	Wi- Go 443 504 770 175 574	Fi Caj	bture	An 9 :f8b(:1c0 :f8b(:1c0	alyze	Statis	tics	Telepi stinati 01:10 07:fi 07:fi 01:10 07:fi	hony on c0:cf0 8b0:40 c0:cf0 sb0:40 c0:cf0	Wireles: () () () () () () () () () ()	5 To 9 11 11 11 11 11 11 11 11 11	rotocol LSv1. CP LSv1. CP	Help Le 2	ngth 120 74 120 74	Info Applic 58841 Applic 443 → [TCP <
2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2	Edit Edit 031 032 033 034 034 035	ng f Vi ispla 36. 36. 37. 37. 37.	rom ew 9514 9515 9517 2164 2175	Wi-l Go 1 1 1 1 4 4 3 5 0 4 1 7 5 5 7 4 1 2 4 1 5	Caj Caj Caj	bture	An e ::f8bi :1c0 ::f8bi :1c0 ::f8bi :1c0	alyze al	Statis e:c04 :8961 e:c04 ·8961 bits	tics	Telepi stinati 01:11 07:fi 01:11 07:fi 01:11 07:fi	hony on c0:cf0 8b0:40 c0:cf0 8h0:40 c0:cf0 8h0:40 c0:cf0	Wireles: (),	s To @ P := T := T := T := T (592	rotocol LSv1. CP CP CP bits	Help Le 2 2	ngth 120 74 127 74 127	Info Applic 58841 Applic 443 → [TCP < erface
App 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2	Edit Edit 031 032 033 034 034 035	ng f Vi () ispla 36. 36. 36. 37. 37. 37. 37.	rom ew 9514 9515 9517 2160 217 2160 217 217 217 217 217 217 217 217 217 217	Wi-l Go Fr 443 504 770 L75 574 574 574	Call Call CCtrl-	bture	An e ::f8bb ::1c0 ::f8b ::1c0 ::f8b ::1c0 ::f8b ::1c0 ::f8b ::1c0 ::f8b ::1c0 ::f8b ::1c0 ::f8b ::1c0 ::f8b ::1c0 ::1c0 ::f8b ::1c0 :	alyze	Statis	tics	Telepi stinati 01:11 07:fi 01:11 07:fi 01:11 07:fi 01:11 07:fi 01:12	hony on c0:cf0 8b0:40 8b0:40 c0:cf0 8h0:40 c0:cf0 8h0:40 c0:cf0 8h0:40 c0:cf0 8h0:40 c0:cf0 8h0:40 c0:cf0 8h0:40 c0:cf0 8h0:40 c0:cf0 8h0:40 c0:cf0 8h0:40 c0:cf0 8h0:40 sh0 sh0:40 sh0:40 sh0:40 sh0:40 sh0:40 sh0:40 sh0	Wireles: () () () () () () () () () ()	s To Q P : T : T : T (592 t: A	ools rotocol LSv1. CP CP CP bits suste	Help Le 2) on kC_3	ngth 120 74 127 int 5:e4	Info Applic 58841 Applic 443 → ITCP = erface :c8 (1)
App 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2	Edit Edit 031 032 033 034 034 034 034 034	ng f Vi () ispla 15 15 15 15 15 15 15 15 15 15	rom ew y film 9514 9515 216/ 216/ 216/ 216/ 216/ 216/ 216/ 216/	Wi- Go 443 504 770 175 574 576 576 576	Cap Cap Corri- ytes : In l Ver	Source 2607 2601 2601 2601 2607 2601 2607 2601 2607 2601 2607 2601 2607 2601 2607 2601 2607 2601 2607 2601 2607 2607 2607 2607 2607 2607 2607 2607	An e ::f8bb ::1c0 ::f8bb ::1c0 ::f8bb ::1c0 ::f8bb ::1c0 ::f8bb ::1c0 ::f8bb	alyze @ @ 0:400 :cf00 :cf00 0:400 (592 3:be: Src: 	Statis Statis e:c04 :8961 :8961 :8961 bits; od (7) 2601 c Port	Dee Dee 26 26 26 26 26 26 26 26 26 26 26 26 26	Telepi stinati 01:1: 07:fi 07:fi 01:1: 07:fi 00:1: 01:1: 07:fi 00:1: 01:1: 07:fi 00:1: 01:1: 07:fi 00:1: 01:1: 07:fi 00:1: 01:1: 07:fi 00:1: 01:1: 07:fi 00:1: 0:: 0:	hony on c0:cf0 8b0:40 c0:cf0 8h0:40 c0:cf0 8h0:40 c0:cf0 8h0:40 c0:cf0 8h0:40 c0:cf0 8h0:40 c0:cf0 8h0:40 c0:cf0 8h0:40 c0:cf0 c0:cf0 8h0:40 c0:cf0 b1 b1 b1 b1 b1 b1 b1 b1 b1 b1 b1 b1 b1	Wireless (), (), ():8961 ()	s To e r r r r r r r r r r r r r	rotocol LSv1. CP rp bits sustel c103: ¹ Sea:	Help Le 2) on kC_3 5336 3873	ngth 120 74 127 int 5:e4 , Ds	Info Applic 58841 Applic 443 → [TCP = erface :c8 (1) t: 260 k: 728
App App 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2	Edit Edit 031 032 033 034 034 034 034 034 034 034 034 034	ng f Vi ispla 36. 36. 37. 37. 37. 203. et 1 iss:	rom ew 9514 9512 9512 9512 9512 9512 9512 9512 9512	Wi- Go 443 504 770 175 574 24 b Src 5000 Con	Caj Caj X Ctri- ytes : Int l Ver trol	bture Source 2607 2601 2607 2601 2607 2601 2607 2601 2607 2601 2607 260	An 9 1:f8bi 1:c0 1:f8bi 1:c0 0:f8bi 1:c0 1	alyze al	Statis Statis	titics De 26 26 26 26 26 26 26 26 26 26	Telep stinati 01:1: 07:fi 07:f	hony c0:cf0 8b0:40 c0:cf0 b0:cf0 b0:cf0 c0:cf0 c0 c0 c0 c0 c0 c0 c0 c0 c0 c0 c0 c0 c0	Wireless (), (), (), (), (), (), (), (), (), (),	s To Q P := T := T := T (592 t: A 669: 43, 1	rotocol LSv1. CP LSv1. CP bits sustel c103:1 Seq:	Lep 2 2 () on kC_3 55336 3873	ngth 120 74 127 int 5:e4 , Ds , Ac	Info Applic 58841 Applic 443 → [TCP = erface :c8 (1) t: 260 k: 728
App App 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2	Edit Edit 031 032 033 034 034 035 034 035	ng f Vi ispla 36. 36. 36. 37. 37. 37. 37. 203. 203. 203. 203. 203. 203. 203. 203	rom ew 9514 9515 2160 2175 2160 2175 2160 2175 2160 2175 2160 2217 2160	Wi-1 Go Go 443 5604 770 L75 574 574 574 574 574 574 574 574 574 5	Fi Caj X V V V V V V S V S V S V S V S V S V S	bture Source 2607 2601 2601 2607 260	An e ::f8bd :1c0 ::f8bd ::r6bd :	alyze alyze a):400 :cf00 :cf00 0:400 :cf00 0:400 :cf00 0:400 :cf00 0:400 :cf00 0:400 :cf00 :	Statis Statis Second	tics De 26 26 26 26 26 26 26 26 26 26	Telepi stinati 01:11 07:fi 01:11 byte f8:38 cf00: 841, dd 6	hony on c0:cf0 8b0:40 8b0:40 c0:cf0 8b0:40 sb0:40 sb0:40 sb0:40 b0:cf0 sb0:40 s	Wireless @ @ 0:8961 0e:c04 0e:c04 0:8961 0e:c04 0:8961 do:c05 tured d), Ds e182:3 ort: 4 ,5	s To e r r T r T T T (592 t: A 669: 43, 1 	rotocol LSv1. LSv1. LSv1. CP CP rp bits sustel c103:! Seq: :	Help 2 2) on kC_3 3873	ngth 120 74 127 74 127 int 5:e4 , Ac	Info Applic 58841 Applic 443 → fTCP = erface :c8 (1: t: 260 k: 728
App App 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2	epturi Edit 031 032 033 034 034 035 ame terni ansm	ng f Vi ispla 36. 36. 37. 37. 37. 2033 et 1 iss: 87. 87. 87. 87. 87.	rom ew 9514 9512 9512 9512 9512 9512 9512 9512 9512	Wi-l Go 443 504 770 L75 574 574 574 574 574 574 574 574 574 5	Fi Cap Vtes : In trol	50000 50000 2607 2601 2607 2007 2007 2007 2007 2007 2007 200	An 9 168 110 110 110 110 100 100 100 10	alyze alyze al;400 cf00 cf00 0;400 cf00 0;400 0;592 cf00 0;400 0;592 cf00 0;400	Statis Stati	tics De 26 26 26 26 26 26 26 26 26 26	Telepl stinati 01:11 07:fi 07:fi 01:11 07:fi 8:38 cf00: 841, dd 6 61 6	hony on c0:cf0 8b0:40 8b0:40 c0:cf0 b0:c0 c0:cf0 b0:c0 c0:cf0 b0:c0 c0:cf0 b0:c0 c0 c0 c0 c0 c0 c0 c0 c0 c0 c0 c0 c0 c	Wireless @ @ 0:8961 0e:c04 0e:c04 0:8961 ae-co5 tured d), Ds e182:3 ort: 4 ,5 1,5	s To e P := T := T := T (592 t: A 669: 43, 1 	ools rotocol LSv1. CP Dits sustel c103:1 Seq: .8	Help Le 2 2) on kC_3 5336 3873	ngth 120 74 127 74 127 int 5:e4 , Ac	Info Applic 58841 Applic 443 → fTCP = erface :c8 (1) t: 260 k: 728
2 Ce App 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2	Edit Edit 031 032 033 034 034 034 034 034 034 034 1cc 31 36 00	ng f Vi ispla 36. 36. 37. 37. 37. 203. et 1 iss: 87. 87. 87. 87. 87. 89. 00	ew y filt 9514 9513 9513 9513 2160 2177 21777 2177 2177 2177 2177 2177 2177 2177 2177 2177	Wi-1 Go 443 504 770 L75 574 44 b Src cor Con 35 14 03 00	Cap Cap ytes : I Ne trol e4 ct 00 64	oture Source 2607 2601 2607 2601 2607 2601 2607 2601 2607 2601 2607 2601 2607 2601 2607 2601 2607 260	An 9 1100 1100 1100 1100 1100 1100 1000	alyze alyze alyze cf60 cf6	Statis Stat	tics De 26 26 26 26 26 26 26 26 26 26	Telepl stinati 01:1 07:fi 01:1 byte f8:38 cf00: 841, dd 6 f1 e 61 e 64 e c3 4	hony on c0:cf0 8b0:40 8b0:40 c0:cf0 75 c0:cf0 c0:cf0	Wireless @ @ @ 0:8961 0e:c04 0e:c04 0:8961 ae:c04 0:8961 do:c04 0:8961 do:c04 0:8961 0:100 0:1	s To @ P := T := T := T (592 t: A 669: 43, 1 	rotocol LSV1. CP LSV1. CP bits sustel c103: Seq: @.	Help Le 2 2) on kC_3 55366 3873 	ngth 120 74 127 127 127 127 127 127	Info Applic 58841 Applic 443 → [TTCP = erface :c8 (1) t: 260 k: 728
2 Calle App 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2	Edit Edit 031 032 033 034 034 035 034 034 035 034 035 1cm 31 36 00 b8	ng f Vi ispla 36. 36. 37. 37. 37. 2033 et 1 iss: 87. 87. 87. 87. 87. 87. 87. 900 21.	rom ew 9514 9512 9517 2164 21777 2164 21777 2164 21777 2164 21777 2164 21777 2164 21777 2164 21777 2164 21777 2164 21777 2164 21777 2164 21777 2164 21777 2164 21777 2164 21777 2164 21777 2164 21777 2164 21777 2164 21777 2164 217777 2164 217777 2164 2177777 2164 21777777777777777777777777777777777777	Wi- Go 443 504 770 L75 574 24 b Src 574 24 b Src Con Con 35 14 03 00 10	Fi Caj V V V V V V V V V V V V V V V V V V V	on 1 2607	An e ::f8bb :1c0 ::f8bb :1ca wire or_38 n 6, 1 toco] 5c 01 07 d9 42	alyze al	Statis Statis	tics De 26 26 26 26 26 26 26 26 26 26	Telep stination 01:11 07:ff 01:11 07:ff 01:11 07:ff 01:11 07:ff 01:11 07:ff 01:11 07:ff 01:11 07:ff 01:120 07:ff 01:12 00:12 00:12 00:12 00:12 00:12 00:12 00:12 00:12 00:12 00:12 00:12 0	hony on c0:cf0 8b0:40 8b0:40 c0:cf0 c0:cf0 8b0:40 c0:cf0 c0:c	Wireless @ @ @ @:8961 @e:c04 @e:c04 0:8961 @e:c04 d), Ds e182:3 ort: 4 ,5 1 61 	s To Q P IIIIIIIIIIIIIIIIIIIIIIIIIIIIIIII	rotocol LSv1. CP LSv1. CP bits susted c103: Seq: 	Help Le 2 5336 3873 	ngth 120 74 127 74 127 int 5:e4 , Ac	Info Applic 58841 Applic 443 → [TCP = :c8 (1) t: 260 k: 728
Etl 1000 1	Edit Edit 031 032 033 034 034 034 034 034 034 034 034 034	ng f Vi ispla 36. 36. 37. 37. 37. 2033 et 1 iss: 87. 87. 87. 87. 87. 87. 87. 87. 87. 900. 21.	rom ew 9514 9515 9517 2160 217 2160 217 2160 217 2160 217 2160 217 2160 217 2160 217 2160 217 2160 217 2160 217 2160 217 2160 200 217 2160 200 200 200 200 200 200 200 200 200 2	Wi-l Go 443 504 770 L75 574 24 b Src Con Con 35 14 03 00 10	Fi Cap Cap Cap Cap Cap Cap Cap Cap Cap Cap	2601 2601 2601 2601 2601 2601 2601 2601	An e ::f8bi :1c0 ::f8bi :1c0 wire or_38 n 6, tocol 07 d9 42	alyze a:400 :cf00 :cf00 0:400 :cf00 0:400 :cf00 0:400 :cf00 0:400 :cf00 0:400 :cf00 0:400 :cf00 0:400 :cf00 :c	Statis Stati	tics De 26 26 26 26 26 26 26 26 26 26	Telepl stinati 01:11 07:ff 01:11 07:ff 01:11 07:ff 841, 07:ff 841, 04:e 61:e 61:e 61:e 63:4	hony on c0:cf0 8b0:40 c0:cf0 c0:c	Wireless () () () () () () () () () () () () () (s To Q IIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIII	rotocol LSv1. CP LSv1. CP LSv1. CP LSv1. CP LSv1. CP Sustel Sustel : Seq: 	Help Le 2) on kC_3 5336 3873 Ny	ngth 120 74 127 int 5:e4 , Ds , Ac	Info Applic 58841 Applic 443 → fTCP < erface :c8 (1) t: 260 k: 728





Wireshark color coding: You'll probably see packets highlighted in a variety of different colors.

Wireshark uses colors to help you identify the types of traffic at a glance. By default, light purple is TCP traffic, light blue is UDP traffic, and black identifies packets with errors



TARDWARE TACKING THULLAGE

Packet filtering: If you want to inspect something specific, such as an application or destination, you can apply a filter to only show this data.

The most basic way to apply a filter is by typing it into the filter box at the top of the window and clicking Apply (or pressing Enter).

Wireshark · Display Filters	?	×
Name	Filter	^
IPX only	ipx	
TCP only	tcp	
UDP only	udp	
Non-DNS	!(udp.port == 53 tcp.port == 53)	
TCP or UDP port is 80 (HTTP)	tcp.port == 80 udp.port == 80	
HTTP	http	
No ARP and no DNS	not arp and !(udp.port == 53)	
Non-HTTP and non-SMTP to/from 192.0.2.1	ip.addr == 192.0.2.1 and not tcp.pd	DI



8

TAP All The Things

Follow a TCP Stream: Another interesting thing you can do is right-click a packet and select Follow > TCP Stream.

You'll see the full TCP conversation between the client and the server.

4	*Wi-Fi					=
Fi	le Edit	View Go Ca	apture Analyze Statistics	Telephony Wireless	Tools He	elp
1	🔳 🙇	•	ि ९ 🗢 🕾 🖗	👲 📃 📃 ପ୍ ପ୍ ପ୍		
I	tcp.strea	am eq 35				× 🛋 🗸
No		Time	Source	Destination	Protocol	Length Info
×	1054	2.798483	192.168.29.250	131.253.61.66	TCP	66 60375 → 443
	1078	2.891263	131.253.61.66	192.168.29.250	TCP	58 443 → 60375
Т	1079	2.891359	192.168.29.250	131.253.61.66	TCP	54 60375 → 443
	1080	2.891527	192.168.29.250	131.253.61.66	TLSv1.2	288 Client Hell
	1103	2.992980	131.253.61.66	192.168.29.250	TCP	1514 [TCP segmen
_	1104	2 992980	131 253 61 66	192 168 29 250	тср	1514 [TCP segmen
>	Frame	1078: 58 bytes	on wire (464 bits),	58 bytes captured (46	4 bits)	on interface 0
>	Ethern	et II, Src: As	sustekC_35:e4:c8 (1c:8	7:2c:35:e4:c8), Dst:	IntelCor	_38:be:bd (7c:5c:
>	Intern	et Protocol Ve	ersion 4, Src: 131.253	.61.66, Dst: 192.168.	29.250	
>	Transm	ission Control	Protocol, Src Port:	443, Dst Port: 60375,	Seq: 0,	Ack: 1, Len: 0



Inspect a Packet: If you click on a packet to select it you can dig down to view its details in the middle portion of the screen.

Clicking on any of those detail lines expands its view and provides any additional detail available.

The bottom portion of the screen shows the raw packet data being decoded.

	0			G	२ 👄	e) 5	2 👔	T			Ð	Q	a, 1						
tcp.	stream eo	ı 35															×	-) •]
lo.	Time	•	5	Source				Des	tinatio	n			Pr	otocol	Len	ngth	Info		
- 10	054 2.7	98483	1	192.16	8.29.	250		131	.253	.61.	66		T	P		66	60375	→ 44	3
10	078 2.8	91263	1	131.25	3.61.	66		192	2.168	.29.	250		T	IP .		58	443 →	6037	5
10	079 2.8	91359	1	192.16	8.29.	250		131	1.253	.61.	66		T	P		54	60375	→ 44	3
10	080 2.8	91527	1	192.16	8.29.	250		131	1.253	.61.	66		TI	Sv1.2	2	288	Clien	t Hel	1
	circups	ulatio	п туре	: Eth	ernet	(1)				_		_							
	Arriva [Time Epoch	l Time shift Time:	n type : Jun for th 149703	9, 2 is pa 7204.	017 12 cket: 140142	(1) 2:40:0 0.000	04.14 00000 secor	4014 300 nds	1000 secor	Pac: ds]	ific	Day	ligh	t Tim	e				
3000	Arriva [Time Epoch 1c 87	l Time shift Time: 2c 35	n type : Jun for th 149703 e4 c8	9, 20 is pa 7204.	017 12 cket: 140142 c f8	2:40:0 0.000 1000 9 38 b	04.14 00000 secon	4014 000 nds 08	1000 secor 00 45	Pac: ids]	ific	Day	ligh . \	t Tim .8	е .Е.				
0000 0010	Arriva [Time Epoch 1c 87 00 34	l Time shift Time: 2c 35 0b 5d	n type : Jun for th 149703 e4 c8 40 00	9, 20 is pa 7204.	017 12 cket: 140142 c f8 6 4f	2:40:0 0.000 1000 38 bo 85 c0	04.14 00000 secor	4014 000 nds 08 1d	1000 secor 00 45 fa 83	Pac: ids]	ific 	Day .,5. 4.]@	ligh . \ 	t Tim .8	e .E.				
0000 0010 0020	Arriva [Time Epoch 1c 87 00 34 3d 42	l Time shift Time: 2c 35 0b 5d eb d7	n type : Jun for th 149703 e4 c8 40 00 01 bb	9, 20 is pa 7204. 7c 5 80 0 22 5	017 12 cket: 140142 c f8 6 4f 2 7b	2:40:0 0.000 1000 : 38 b0 85 c0 69 00	04.14 00000 secon e bd 0 a8 0 00	4014 000 nds 08 1d 00	1000 secor 00 45 fa 83 00 80	Pac: ids] 5 00 5 fd 0 02	ific =!	Day .,5. 4.]@ B	ligh . \ 	t Tim .8 0 {i	e .E. 				
0000 0010 0020 0030 0040	Arriva [Time Epoch 1c 87 00 34 3d 42 fa f0 04 02	l Time shift Time: 2c 35 0b 5d eb d7 48 ef	n type : Jun for th 149703 e4 c8 40 00 01 bb 00 00	9, 20 is pa 7204. 7204. 80 0 22 5 02 0	017 12 cket: 140142 c f8 6 4f 2 7b 4 05	2:40:0 0.000 1000 3 38 b 85 c 69 0 b4 0	04.14 00000 secon e bd 0 a8 0 00 1 03	4014 000 nds 08 1d 00 03	1000 secor 00 45 fa 83 00 80 08 01	Pac: ds] 6 00 8 fd 9 02 1 01	ific	Day .,5. 4.]@ B	ligh . \ ."R	t Tim .8 0 {i	e .E. 				



10

Demo Configuration

The "Inline" nodes are two laptops configured with static IP's using normal Ethernet auto-negotiation. The first is set up as a web server and the second as a client.

The "TAP" ports are connected to a monitor laptop that has been configured with no IP address information and manually assigned port speed with auto-negotiation



11/3/2018



Demo Configuration - Web Server

The web server is an Ubuntu laptop running Apache/PHP to serve a simple web page that displays a random image.

- The web page has been configured to prevent caching which might otherwise cause the client to serve local content instead of pulling from the server.
- A bash script will display the web server logs during the demo.

index.php

head>

<title>Test page</title>

<h1>Test Page</h1>

<?php

// display random image with inline php for a random image number and time added to prevent caching

11

/ DownLoaded random images from <u>https://picsum.photos/</u>
/ and stored them in a local images dir so this can work while lisconnected from internet

?>

<img src="/images/400/picsum.photos.<?php \$random = rand(1,20); echo \$random; ?>.jpeg?nocache=<?php echo time(); ?>" />

</body>
</html>



TAP All The Things

11/3/2018

Demo Configuration - Web Client

The web client is an Ubuntu laptop running a Firefox web browser.

A Python script will be running to automate the web page calls to the server and display them in the Firefox browser during the demo.

Since a simple kill would cause Firefox to enter safe mode I used xdotool to close it cleanly.



TAP All The Things

Demo Configuration - TAP Monitor

The TAP Monitor is an Ubuntu laptop running Wireshark to view the network traffic.

Wireshark will be running on both "TAP" monitor interfaces thus seeing both directions of the connection.

The application ethtool will be used to disable auto-negotiation and set the port speed on the monitor interfaces.

	setnet100.sh
1	#!/bin/bash
2	echo ""
3	sudo ethtool enp0s25
4	<pre>sudo ethtool -s enp0s25 autoneg off</pre>
5	<pre>sudo ethtool -s enp0s25 speed 100 duplex full</pre>
6	sudo ethtool enp0s25
7	echo ""
8	sudo ethtool enx001060230c4e
9	<pre>sudo ethtool -s enx001060230c4e autoneg off</pre>
10	<pre>sudo ethtool -s enx001060230c4e speed 100 duplex full</pre>
	sudo ethtool enx001060230c4e
	echo ""



TAP All The Things

Demo

The Demo will be set up in the Hardware Hacking Village area.

We encourage everyone to check out this demo. Since the laptops must be kept unlocked, we ask that this be done with eyes only and not hands.

The demo should look something like the picture to the right.





TAP All The Things

11/3/2018

