Controleer en identificeer pakketverlies in het WAN voor SD-WAN

Inhoud

Inleiding Voorwaarden Vereisten Gebruikte componenten Achtergrond Proces voor probleemoplossing Overzicht proces Markeer het gewenste verkeer met DSCP Leg het verkeer vast met de ingesloten vastlegging Analyse via Wireshark Filter het gewenste verkeer op ESP Sequence Gerelateerde informatie

Inleiding

Dit document beschrijft hoe u gegevens kunt identificeren en verzamelen wanneer het verkeer over het WAN is kwijtgeraakt, maar er geen dalingen worden gezien op de SD-WAN Edge.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Cisco softwaregedefinieerde Wide Area Network (SD-WAN)
- Ingesloten pakketvastlegging voor vManager-pakketvastlegging
- draadhaai
- Microsoft Excel

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- C800V versie 17.03.04
- vManager versie 20.3.4
- Wireshark versie 2.6.3

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Achtergrond

Om bij deze uitdaging te helpen, tonen de stappen die in dit document worden beschreven hoe u specifiek verkeer kunt markeren met gedifferentieerde services code point (DSCP) om te helpen de gewenste pakketten te identificeren. DSCP kan worden gebruikt om het verkeer te identificeren aangezien deze waarde van de binnen pakketheader aan de kopbal IPsec wordt gekopieerd. Zodra de gewenste pakketten worden geïdentificeerd, toont het hoe te om het verkeer over twee WAN aan te passen vangt om verkeer te verzekeren dat van bron tot bestemming wordt gemaakt.

Twee enige routerplaatsen worden gebruikt om deze probleemoplossingtechniek aan te tonen. In dit geval, ICMP verkeer van 10.0.0.10 tot 10.0.2.10 in de vorm van 100 pings zoals getoond in het beeld. Er is geen verlies in dit voorbeeld maar deze zelfde probleemoplossingtechniek wordt gebruikt in het geval waar er een verlies is om het te identificeren.



Proces voor probleemoplossing

Overzicht proces

- Voor het verkeer dat over WAN wordt overgetrokken, is een Toegangslijst (ACL) (of gecentraliseerd beleid) nodig om verkeer met wat ongebruikte DSCP-waarde te markeren. In dit voorbeeld wordt DSCP 27 gebruikt.
- 2. Zodra het verkeer wordt gemarkeerd, wordt de ingesloten pakketvastlegging gebruikt om de pakketten op de transportinterface van de bron en de bestemmingsrouter op te nemen.

Opmerking: vManager-pakketvastlegging kan ook worden gebruikt, hoewel er een beperking is van 5 MB aan gegevens of 5 minuten looptijd.

- 1. Nadat de opnamen zijn genomen, open ze in Wireshark om te bekijken.
- 2. De filter wordt toegepast in Wireshark om te tonen welke pakketten worden gewenst en dan worden zij vergeleken.
- 3. Microsoft Excel wordt gebruikt voor grote opnamen om nauwkeurigheid te garanderen.

Markeer het gewenste verkeer met DSCP

Een toegangslijst zoals het voorbeeld wordt geconfigureerd op de bronrouter (cEdge1 in dit voorbeeld) en toegepast op de interface in het SD-WAN-gedeelte van de routerconfiguratie zoals getoond.

Een optionele teller wordt toegepast om te verifiëren dat het verkeer het beleid raakt zoals verwacht. Dit kan worden gecontroleerd met de opdracht **tonen sdwan beleid access-list-tellers**.

```
policy
access-list mark_dscp_27
sequence 10
match
source-ip 10.0.0.10/32
destination-ip 10.0.2.10/32
1
action accept
count MARK_DSCP_27_COUNT (optional counter to verify packets that hit the policy)
set
dscp 27
1
1
1
default-action accept
sdwan
 interface GigabitEthernet3
 access-list mark_dscp_27 in
```

Leg het verkeer vast met de ingesloten vastlegging

Opmerking: hoe u een ingesloten pakketopname in Cisco IOS XE configureert om de versleutelde pakketten op te nemen die via het WAN worden verzonden, naar het <u>voorbeeld</u> Ingesloten pakketvastlegging voor Cisco IOS en Cisco IOS XE Configuration

Opmerking: er moet een ACL worden gebruikt om de EPC op het WAN te beperken, aangezien er meer dan de 1000 PPS-snelheidslimiet voor de EPC zou kunnen zijn.

Voorbeeld

Een ACL wordt geconfigureerd op cEdge1 en cEdge3 omdat verkeer alleen is geselecteerd in de richting van bron naar bestemming in dit voorbeeld.

Opmerking: de WAN IP-adressen worden gebruikt om de opname te filteren. Er zijn meerdere uitgangen die kunnen worden gebruikt om het pad dat het verkeer neemt te identificeren, zodat de juiste WAN IP's kunnen worden geïdentificeerd voor het ACL-filter. De opdrachten die kunnen worden gebruikt om deze uitvoer te genereren zijn de **show sdwan app-fwd cflowd flows** en **toon sdwan policy service path**. Blader naar <u>Conditional Packet</u> <u>Trace</u> om de debug-voorwaarde te controleren.

ip access-list extended CAP-Filter

10 permit ip host 192.168.23.149 host 192.168.28.240

Op dit punt worden de opnamen gestart op beide routers en worden 100 pings over de overlay verzonden.

Success rate is 100 percent (100/100), round-trip min/avg/max = 1/1/4 ms Nadat de opnamen zijn gestopt en van beide routers zijn verzameld, moeten ze worden geopend in Wireshark om ze te kunnen bekijken.

Analyse via Wireshark

Als de cEdge1-opname eenmaal is geopend in Wireshark, wordt gezien dat al het verkeer is versleuteld en het is niet eenvoudig te ontcijferen welke pakketten de pings zijn die zijn verzonden.

Ē	Apply a display filter <ctrl-></ctrl->		1 1 1 1 1 1 1	alda							
No.	Time	Source	Destination	Protocol Length	ESP Sequence	Differentiated Services Codepoint	Source Port	Destination Port	Sequence Number	Info	
-	1 0.000000	192.168.23.149	192.168.28.240	UDP	175	Class Selector 6				12386 + 12407 Len=133	
т	2 0.563966	192.168.23.149	192.168.28.240	UDP	168	Class Selector 6				12386 + 12407 Len=126	
	3 0.903996	192.168.23.149	192.168.28.240	UDP	175	Class Selector 6				12386 + 12407 Len=133	
	4 1.428978	192.168.23.149	192.168.28.240	UDP	168	Class Selector 6				12386 + 12407 Len=126	
	5 1.896993	192.168.23.149	192.168.28.240	UDP	175	Class Selector 6				12386 + 12407 Len=133	
	6 2.417977	192.168.23.149	192.168.28.240	UDP	168	Class Selector 6				12386 + 12407 Len=126	
	7 2.792958	192.168.23.149	192.168.28.240	UDP	175	Class Selector 6				12386 + 12407 Len=133	
	8 3.323973	192.168.23.149	192.168.28.240	UDP	168	Class Selector 6				12386 + 12407 Len=126	
	9 3.781957	192.168.23.149	192.168.28.240	UDP	175	Class Selector 6				12386 + 12407 Len=133	
	10 4.145988	192.168.23.149	192.168.28.240	UDP	168	Class Selector 6				12386 + 12407 Len=126	
	11 4.769949	192.168.23.149	192.168.28.240	UDP	175	Class Selector 6				12386 + 12407 Len=133	
	12 4.981995	192.168.23.149	192.168.28.240	UDP	168	Class Selector 6				12386 + 12407 Len=126	
	13 5.722954	192.168.23.149	192.168.28.240	UDP	175	Class Selector 6				12386 + 12407 Len=133	
	14 5.970994	192.168.23.149	192.168.28.240	UDP	168	Class Selector 6				12386 + 12407 Len=126	
	15 6.532961	192.168.23.149	192.168.28.240	UDP	175	Class Selector 6				12386 + 12407 Len=133	
	16 6.949999	192.168.23.149	192.168.28.240	UDP	168	Class Selector 6				12386 + 12407 Len=126	
	17 7.348980	192.168.23.149	192.168.28.240	UDP	175	Class Selector 6				12386 + 12407 Len=133	
	18 7.923999	192.168.23.149	192.168.28.240	UDP	168	Class Selector 6				12386 + 12407 Len=126	
	19 8.193990	192.168.23.149	192.168.28.240	UDP	175	Class Selector 6				12386 + 12407 Len=133	
	20 8.774953	192.168.23.149	192.168.28.240	UDP	168	Class Selector 6				12386 + 12407 Len=126	
	21 9.111993	192.168.23.149	192.168.28.240	UDP	175	Class Selector 6				12386 + 12407 Len=133	
	22 9.653957	192.168.23.149	192.168.28.240	UDP	168	Class Selector 6				12386 + 12407 Len=126	
	23 10.082988	192.168.23.149	192.168.28.240	UDP	175	Class Selector 6				12386 + 12407 Len=133	
	24 10.564957	192.168.23.149	192.168.28.240	UDP	168	Class Selector 6				12386 + 12407 Len=126	
	25 10.949999	192.168.23.149	192.168.28.240	UDP	175	Class Selector 6				12386 + 12407 Len=133	
	26 11.416970	192.168.23.149	192.168.28.240	UDP	168	Class Selector 6				12386 + 12407 Len=126	
	27 11.937991	192.168.23.149	192.168.28.240	UDP	175	Class Selector 6				12386 + 12407 Len=133	
	28 12.400964	192.168.23.149	192.168.28.240	UDP	168	Class Selector 6				12386 + 12407 Len=126	
	29 12.836998	192.168.23.149	192.168.28.240	UDP	175	Class Selector 6				12386 + 12407 Len=133	
	30 13.266984	192.168.23.149	192.168.28.240	UDP	168	Class Selector 6				12386 + 12407 Len=126	
	31 13.779958	192.168.23.149	192.168.28.240	UDP	175	Class Selector 6				12386 + 12407 Len=133	
	32 14.171988	192.168.23.149	192.168.28.240	UDP	176	Default				12386 + 12407 Len=134	
	33 14.173986	192.168.23.149	192.168.28.240	UDP	176	Default				12386 + 12407 Len=134	
	34 14.174978	192.168.23.149	192.168.28.240	UOP	176	Default				12386 + 12407 Len=134	
	35 14.175985	192.168.23.149	192.168.28.240	UDP	176	Default				12586 + 12407 Len=134	
	36 14.176977	192.168.23.149	192.168.28.240	UOP	176	Default				12386 + 12407 Len=134	
	37 14.176977	192.168.23.149	192.168.28.240	UDP	176	Default				12386 + 12407 Len=134	
	38 14.178991	192.168.23.149	192.168.28.240	UOP	176	Derault				12386 + 12407 Len+134	

Filter deze opname met een weergavefilter **ip.dsfield.dscp == 27**, men ziet dat er slechts 100 pakketten worden weergegeven aan de onderkant van het scherm en men ziet dat de DSCP kolom waarde allen 27 toont.

Time						1			81-
	Source	Destination	Protocol Leng	h ESP Sequence	Differentiated Services Codepoint	Source Port Destination Port	Sequence Number	Info	
451 55.441963	192.168.23.149	192.168.28.240	UDP	176	27			12386 + 12407 Len=134	
452 55.445976	192.168.23.149	192.168.28.240	UDP	176	27			12386 + 12407 Len=134	
453 55.448966	192.168.23.149	192.168.28.240	UDP	176	27			12386 + 12407 Len=134	
454 55.450965	192.168.23.149	192.168.28.240	UDP	176	27			12386 → 12407 Len=134	
455 55.452964	192.168.23.149	192.168.28.240	UDP	176	27			12386 → 12407 Len=134	
456 55.454963	192.168.23.149	192.168.28.240	UDP	176	27			12386 → 12407 Len=134	
457 55.455970	192.168.23.149	192.168.28.240	UDP	176	27			12386 + 12407 Len=134	
458 55.456977	192.168.23.149	192.168.28.240	UDP	176	27			12386 + 12407 Len=134	
459 55.457968	192.168.23.149	192.168.28.240	UDP	176	27			12386 + 12407 Len=134	
468 55.458975	192.168.23.149	192.168.28.240	UDP	176	27			12386 + 12407 Len=134	
461 55.461966	192.168.23.149	192.168.28.240	UDP	176	27			12386 + 12407 Len=134	
462 55.463965	192.168.23.149	192.168.28.240	UDP	176	27			12386 + 12407 Len=134	
463 55.465964	192.168.23.149	192.168.28.240	UDP	176	27			12386 + 12407 Len=134	
464 55.466971	192.168.23.149	192.168.28.240	009	176	27			12386 + 12487 Len=134	
405 55.467962	192.168.23.149	192.100.28.240	100	1/6	27			12300 + 12407 Len=134	
400 55.469961	192.168.23.149	192.166.28.240	000	176	27			12360 + 12407 Len=134	
407 55.470968	192.168.23.149	192.168.28.240	000	176	27			12300 + 12407 Len+154	
408 55.471975	192.168.23.149	192.168.28.248	000	170	27			12300 + 12407 Len=134	
407 55.472907	192.100.23.149	192.100.20.240	100	176	27			12306 * 12407 Len=134	
470 55.474900	192.100.23.149	102.100.20.240	100	176	27			12300 * 1240/ Len=134	
471 33.473973	192.100.23.149	192.100.20.240	100	176	27			12366 + 12407 Len-134	
472 33.470303	192.100.23.149	102 168 28 240	100	176	27			12386 + 12407 Lene134	
473 55.478963	192.108.23.149	102.168.28.240	100	176	27			12386 + 12407 Len-134	
475 55 481060	102 168 23 140	102 168 28 240	100	176	27			12386 + 12407 Len=134	
476 55 484075	103 168 33 140	103 168 38 340	100	176	27			13386 - 13467 Len-134	
477 55.485967	192.168.23.149	192.168.28.240	LIDP	176	27			12386 a 12487 Len=134	
478 55 487966	192.168.23.149	192,168,28,240	109	176	27			12386 a 12407 Lenal34	
479 55,488973	192.168.23.149	192.168.28.240	LIDP	176	27			12386 # 12407 Len=134	
488 55,491963	192.168.23.149	192.168.28.240	LIDP	176	27			12386 + 12407 Len=134	
481 55,588961	192, 168, 23, 149	192.168.28.240	LIDP	176	27			12386 + 12407 Len=134	
482 55,518959	192.168.23.149	192.168.28.240	LIDP	176	27			12386 + 12407 Len=134	
483 55,511966	192,168,23,149	192.168.28.240	LIDP	176	27			12386 + 12407 Len=134	
484 55, 513965	192, 168, 23, 149	192,168,28,240	LIDP	176	27			12386 + 12407 Len=134	
485 55, 514972	192,168,23,149	192,168,28,240	UDP	176	27			12386 + 12407 Len=134	
486 55, 516971	192, 168, 23, 149	192,168,28,240	LIDP	176	27			12386 + 12407 Len=134	
487 55,517963	192,168,23,149	192,168,28,240	UDP	176	27			12386 + 12407 Len=134	
488 55,523959	192,168,23,149	192,168,28,248	UDP	176	27			12386 + 12407 Len=134	
489 55,524966	192.168.23.149	192,168,28,248	UDP	176	27			12386 + 12407 Len=134	

In sommige gevallen waarin DSCP-waarde over het WAN wordt behouden, kan dezelfde filter op de doelopname worden gebruikt.

In andere gevallen is dit niet mogelijk, zoals een situatie waarin DSCP-waarde via een openbare internetverbinding wordt gewist.

Filter het gewenste verkeer op ESP Sequence

In beide gevallen kan het verkeer worden geïdentificeerd met de ESP-volgnummers.

Om de ESP opeenvolgingsaantallen in het pakket te zien, klik op de opname met de rechtermuisknop en kies **Decoderen zoals** getoond.

			12386
			12386
	Mark/Upmark Packet	Ctrl+M	12386
		current a	12386
	Ignore/Unignore Packet	Ctrl+D	12386
	Set/Unset Time Reference	Ctrl+T	12386
	Time Shift	Ctrl+Shift+T	12386
	Packet Comments	•	12386
	Packet comments		12386
	Edit Resolved Name		12386
			12386
	Apply as Filter	+	12386
	Prepare as Filter	•	12386
	Conversion Filter		12386
	Conversation Filter	,	12386
	Colorize Conversation	•	12386
	SCTP	•	12386
	Follow	•	12386
	TONOW		12386
	Сору	•	12386
			12386
	Protocol Preferences	•	12386
	Decode As		12386
	Channel De allant in Maria Maria		12386
	Show Packet in New Window		12386

Selecteer het vervolgkeuzemenu **Huidige** veld en selecteer in dat veldtype **UDPENCAP** of selecteer het in de vervolgkeuzelijst.



Wires	hark	. D	ecod	eΑ	5
111103	11016	· •	ccou	~ ~	

Field	Value	Туре	Default	Current					
UDP port	12386	Integer, base 10	(none)	(none)					~
				(none) 3GPP2 A11 A21 AC DR ACtrace ADP ADwin ALC AMP					
+ -	ъ (
					OK	Save	Copy from	Cancel	Help

Selecteer **OK** zodra dit is voltooid.

ark • De	code As								>
Value	Туре	Default	Current						
12386	Integer, base 10	(none)	UDPENCAP						
D.									
	-0								
	Value 12386	ark · Decode As Value Type 12386 Integer, base 10	ark · Decode As Value Type Default 12386 Integer, base 10 (none)	Value Type Default Current 12386 Integer, base 10 (none) UDPENCAP	ark · Decode As Value Type Default Current 12386 Integer, base 10 (none) UDPENCAP	ark · Decode As Value Type Default Current 12386 Integer, base 10 (none) UDPENCAP	Value Type Default Current 12386 Integer, base 10 (none) UDPENCAP	ark · Decode As Value Type Default Current 12386 Integer, base 10 (none) UDPENCAP	ark - Decode As Value Type Default Current 12386 Integer, base 10 (none) UDPENCAP

Vouw in het gedeelte Wireshark Packet Details het gedeelte Encapsulating Security payload van het pakket uit om ESP Sequence te zien.

×

```
      479 55 488973 192 168 23 149
      192 168 28 240
      FSP
      176

      Frame 464: 176 bytes on wire (1408 bits), 176 bytes captured (1408 bits)
      192 168 28 240
      FSP
      176

      Ethernet II, Src: VMware_84:af:45 (00:50:56:84:af:45), Dst: VMware_84:e2:b7 (00:50:56:84:e2:b7)
      1nternet Protocol Version 4, Src: 192.168.23.149, Dst: 192.168.28.240

      User Datagram Protocol, Src Port: 12386, Dst Port: 12407
      UDP Encapsulation of IPsec Packets

      Encapsulating Security Payload
      ESP SPI: 0X0400010C (0/109340)

      ESP Sequence: 319
      ESP Sequence: 319
```

Klik met de rechtermuisknop op **ESP Sequence** en kies **toepassen als kolom** zodat de ESP Sequence kan worden gezien als een kolom in de sectie Packet List op het bovenste gedeelte van het Wireshark-scherm.

	07 IJ2.100.2J.17J	102.100.20.240	201
456 55.4	Frank I California		ESP
457 55.4	Expand Subtrees		ESP
458 55.4	Collapse Subtrees		ESP
459 55.4	Expand All		ESP
460 55.4	Collapse All		ESP
461 55.4	compservit		ESP
462 55.	Apply as Column	Ctrl+Shift+I	ESP
463 55.			ESP
464 55.4	Apply as Filter	•	ESP
465 55.4	Prepare as Filter	•	ESP
466 55.4	Conversation Filter		ESP
467 55.4	Conversation Filter	,	ESP
468 55.4	Colorize with Filter	•	ESP
469 55.4	Follow	•	ESP
470 55.4			ESP
471 55.4	Сору	•	ESP
472 55.4			ESP
473 55.4	Show Packet Bytes	Ctrl+Shift+O	ESP
474 55.4	Export Packet Bytes	Ctrl+Shift+X	ESP
Frame 464: 176 byt	Wiki Protocol Page		08 hits)
Ethernet II. Src:	Filter Field Reference		re 84:e2:b7 (0
Internet Protocol	Protocol Preferences	•	8.240
User Datagram Prot			
UDP Encapsulation	Decode As	Ctrl+Shift+U	
Encapsulating Secu	Go to Linked Packet		
ESP SPT · 0x0400		14C - 1	
ESP Sequence: 31	Show Linkid Packet in Nev	wwindow	

Opmerking: de ESP SPI voor de pakketten op cEdge1 is **0x040001dc**. Dit wordt gebruikt voor een filter op de doelopname.

```
> Frame 464: 176 bytes on wire (1408 bits), 176 bytes captured (1408 bits)
> Ethernet II, Src: VMware_84:af:45 (00:50:56:84:af:45), Dst: VMware_84:e2:b7
> Internet Protocol Version 4, Src: 192.168.23.149, Dst: 192.168.28.240
> User Datagram Protocol, Src Port: 12386, Dst Port: 12407
UDP Encapsulation of IPsec Packets
> Encansulating Security Payload
ESP SPI: 0x040001dc (67109340)
ESP Sequence: 319
```

Open de doelopname, herhaal de stappen om te decoderen als **UDPENCAP**, en toon de ESP Sequence nummers in de pakketten.

Zodra de pakketten het ESP volgnummer weergeven, kan de ESP SPI van de eerste opname worden gebruikt als filter op de tweede opname om alleen het verkeer binnen die SPI weer te geven die overeenkomt met het gewenste verkeer.

Bericht dat de aantallen van de pakketopeenvolging die allebei aanpassen DSCP 27 duidelijk hebben.



Deze vergelijking kan handmatig worden uitgevoerd in Wireshark of Microsoft Excel kan worden gebruikt om deze vergelijking te doen.

Om Microsoft Excel te gebruiken om te vergelijken, is het noodzakelijk om beide opnamen te snijden om alleen pakketten te bevatten die in beide opnamen zijn.

In de bronopname heeft het eerste relevante pakket ESP-reeks 306 en die correspondeert met pakketnummer 451.

🚄 CAP.pcap						-		\times				
File Edit View Go Capture	Analyze Statistics Tele	ephony Wireless Tools	Help									
📶 🔳 🖉 💿 📙 🛅 🗙 😂 I	९ 🗢 🗢 🗟 🖗 🕹	💶 🖲 २, २, 🖽										
ip.dsfield.dscp == 27	ip.dsfield.dscp == 27											
No. Time	Source	Destination	Protocol	Length	ESP Sequence		Different					
451 55.441963	192.168.23.149	192.168.28.240	ESP	176	5	306	27					
452 55.445976	192.168.23.149	192.168.28.240	ESP	176	5	307	27					
453 55.448966	192.168.23.149	192.168.28.240	ESP	176	5	308	27					
454 55.450965	192.168.23.149	192.168.28.240	ESP	176	5	309	27					
455 55.452964	192.168.23.149	192.168.28.240	ESP	176	5	310	27					
456 55.454963	192.168.23.149	192.168.28.240	ESP	176	5	311	27					
457 55.455970	192.168.23.149	192.168.28.240	ESP	176	5	312	27					
458 55.456977	192.168.23.149	192.168.28.240	ESP	176	;	313	27					

Het laatste relevante pakket in de bronopname heeft ESP-reeks 405 en is pakketnummer 550.

			10111001101110		2.0	102 27	
	548 55.608962	192.168.23.149	192.168.28.240	ESP	176	403 27	
	549 55.609969	192.168.23.149	192.168.28.240	ESP	176	404 27	
	550 55.610960	192.168.23.149	192.168.28.240	ESP	176	405 27	
							×
<						>	

In de bestemmingsopname komt het eerste relevante pakket overeen met de bronopname met ESP-reeks 306, maar in deze opname is pakket 463.

461 60.522028 192.168.23.149	192.168.28.240	ESP	168	407 Class Se
462 60.715026 192.168.23.149 463 60.999008 192.168.23.149	192.168.28.240	ESP	175	408 Class Se 306 27
464 61.003006 192.168.23.149	192.168.28.240	ESP	176	307 27

Het laatste relevante pakket is ook aanwezig met ESP Sequence 405 en het is pakket 564.

560 61.165052	192.168.23.149	192.168.28.240	ESP	1/6	403 27
561 61.166043	192.168.23.149	192.168.28.240	ESP	176	404 27
562 61.166043	192.168.23.149	192.168.28.240	ESP	176	405 27
563 61.431029	192.168.23.149	192.168.28.240	ESP	168	409 Class Se
564 61.584021	192.168.23.149	192.168.28.240	ESP	175	410 Class Se

De eerste opname moet nu worden gesneden om alleen relevante pakketten te bevatten.

Navigeer naar Bestand > Packet Dissections exporteren > Als CSV...

File	Edit View Go Ca	pture Analyze St	tatistic	s Telephony	Wireless	Tools Help	
	Open	Ctrl+O	1	5 🕹 📃 🔳	Θ Θ	9. 🎹	
	Open Recent	•					
	Merge			Destinatio	on	Protocol	Length E
	Import from Hex Dump.		149	192.16	3.28.240	ESP	176
	Close	Ctrl+W	149	192.16	3.28.240	ESP	176
	ciose	current	149	192.16	3.28.240	ESP	176
	Save	Ctrl+S	149	192.16	3.28.240	ESP	176
	Save As	Ctrl+Shift+S	149	192.16	3.28.240	ESP	176
	Save As	Carronners	149	192.16	3.28.240	ESP	176
	File Set	•	149	192.16	3.28.240	ESP	176
			149	192.16	3.28.240	ESP	176
	Export Specified Packets		149	192.16	3.28.240	ESP	176
	Export Packet Dissection	is 🕨		As Plain Text	. 240	ESP	176
	Export Packet Butes	Ctrl+Shift+X		As CSV	.240	ESP	176
	Export Packet bytes	Carronnerx		A3 C5V	.240	ESP	176
	Export PDUs to File			As "C" Arrays	.240	ESP	176
	Export TLS Session Keys.				.240	ESP	176
	Export Objects	•		AS POIVIL AIVIL	.240	ESP	176
				As PDML XML	.240	ESP	176
	Print	Ctrl+P		As JSON	.240	ESP	176
					.240	ESP	176
	Quit	Ctrl+Q	149	192.16	3.28.240	ESP	176
-	547 55.00	0902 192.100.20	.149	192.16	8.28.240	ESP	176
	548 55.60	8962 192.168.23	.149	192.16	3.28.240	ESP	176

Selecteer **Opgenomen** en **Bereik** en typ in het veld **Bereik** het bereik van het eerste relevante pakket tot het laatste relevante pakket.

Voer een bestandsnaam in het veld Bestandsnaam in en klik op Opslaan.

	Wireshark · Ex	port Packet	Dissections	
--	----------------	-------------	-------------	--

Save in:	Desktop			► 🔝 🏷	
Quick access	Name	^ No items mat	Status ch your search.	Date	nodified
Desktop					
Libraries					
This PC					
Setwork	<	CAP1 alian			>
	Save as type:	CSV (Comma Separated V	alues summary) (*.c	× III	Cancel
	Packet Range				Pack
			Captured	O Displayed	Pa
	○ All packets		880	100	
	O Selected pack	ket	1	1	Pa
	Marked packet Direct to look	ets 	0	0	F
	Range: 451	550	100	100	
	Remove Ignor	red packets	0	0	E

Herhaal hetzelfde proces bij opname 2 voor de desbetreffende pakketten.

Wireshark - Export Packet Dissections Save in: E Desktop 🗿 🎓 📂 🛄 🕶 \sim × Date modified Name Status No items match your search. Quick access Desktop Libraries This PC < > Network CAP2_slice ~ Save File name: CSV (Comma Separated Values summary) (".csr ~ Cancel Save as type: Help Packet Range Packe O Displayed Captured Pa Pa All packets 904 904 \mathbb{P} Selected packet 1 1 Pa Marked packets A) First to last marked Pa Range: 463-564 102 Ea Ea Remove Ignored packets

Open beide CSV-bestanden in Microsoft Excel.

Leg op de bron CSV vast, behalve als XLSX formaat.

Save As		
C Recent	↑ ▷ Desktop CAP1_slice	
Cisco	Excel Workbook (*.xlsx)	🖓 Save

Selecteer onder in het scherm het symbool + om een ander vel toe te voegen. Noem het CAP2_slice

j.	485	55.51497 192.168.23 192.168.28 ESP	176	340	27	ESP (SPI=0x040001dc)
•	486	55.51697 192.168.23 192.168.28 ESP	176	341	27	ESP (SPI=0x040001dc)
1	487	55.51796 192.168.2 192.168.2 ESP	176	342	27	ESP (SPI=0x040001dc)
4	•	CAP1_slice +				

Open het CAP2 CSV-bestand en druk op CTRL + a om alle bestanden te selecteren en op CTRL + c om het te kopiëren.

 \times

J77 \bullet : $\times \checkmark f_x$

1	А	В	С	D	E	F	G	Н	1	J	К	L	м
1	No.	Time	Source	Destinatio	Protocol	Length	ESP Seque	Differenti	Source Po	Destinatio	Info	Sequence	Number
2	463	60.99901	192.168.2	192.168.28	ESP	176	306	27			ESP (SPI=	0x040001dc	
3	464	61.00301	192.168.2	192.168.28	ESP	176	307	27			ESP (SPI=	0x040001dc	
4	465	61.00506	192.168.2	192.168.28	ESP	176	308	27			ESP (SPI=	0x040001dc	
5	466	61.00706	192.168.2	192.168.28	ESP	176	309	27			ESP (SPI=	0x040001dd)
6	467	61.00905	192.168.2	192.168.28	ESP	176	310	27			ESP (SPI=	0x040001dc)
7	468	61.01006	192.168.2	192.168.28	ESP	176	311	27			ESP (SPI=	0x040001dc	
8	469	61.01105	192.168.2	192.168.28	ESP	176	312	27			ESP (SPI=	0x040001dd)
9	470	61.01305	192.168.2	192.168.28	ESP	176	313	27			ESP (SPI=	0x040001do)
10	471	61.01406	192.168.2	192.168.28	ESP	176	314	27			ESP (SPI=	0x040001dc)
11	472	61.01606	192.168.2	192.168.28	ESP	176	315	27			ESP (SPI=	0x040001dc	
12	473	61.01806	192.168.2	192.168.28	ESP	176	316	27			ESP (SPI=	0x040001dc	
13	474	61.02106	192.168.2	192.168.28	ESP	176	317	27			ESP (SPI=	0x040001dc)
14	475	61.02205	192.168.2	192.168.28	ESP	176	318	27			ESP (SPI=	0x040001dd)
15	476	61.02306	192.168.2	192.168.28	ESP	176	319	27			ESP (SPI=	0x040001dc)
16	477	61.02506	192.168.2	192.168.28	ESP	176	320	27			ESP (SPI=	0x040001dc	
17	478	61.02605	192.168.2	192.168.28	ESP	176	321	27			ESP (SPI=	0x040001dc	

Navigeer naar het bestand CAP1_slice.xlsx en plak op het tweede tabblad voor CAP2_slice (CTRL + v) de gekopieerde informatie in de cel A1.

Auto	Save On O	R	9- 9				CAP	1_slice.xlsx	• Saved •				2
File	Home	Inse	rt Pag	e Layout	Formulas	Dat	a Review	View	Help				
ĥ	👗 Cut		Calibri		v 11 v /	A° Aĭ	= = =	89	🐉 Wrap Te	ect	Genera	I	~
Paste	Copy ~		BI		1. 0.	Α.	= = =		Merge /	R Center v	¢.,	% 9	€ <u>0</u> .00
*	ダ Format P	ainter	0.1		 -	- ·			Merge	a center -		/0 /	.00 -20
	Clipboard	13	ù l	Font	t	F2		Aligne	nent	5		Number	5
A1	Ŧ	: >	\sim	f _x									
	A	B	С	D	E	F	G	н	1	J	К	L	N
1													
3		_											_
4													
5													
6													
7													_
8													
10		_											
11													
12													
13													
14													_
15													_
17													
18													_
19													
20													
21													_
22													
23													_
25		_											_
26													
27													
28													
29							_						_
30													
32													
33													-
34													
35													
36													_
37							_						
38													
-	> (CAP1_sl	ice CA	P2_slice	(+)								

1	~				-	· · · · ·	•		· · · ·			IN I	-	
1	No.	Time	Source	Destinatio	Protocol	Length	ESP Seque	Differenti	Source Po	Destinatio	Info		Seque	nce N
2	463	60.99901	192.168.23	192.168.28	ESP	176	306	27			ESP	(SPI=0)x04000)1dc)
3	464	61.00301	192.168.23	192.168.28	ESP	176	307	27			ESP	(SPI=0)x04000)1dc)
4	465	61.00506	192.168.23	192.168.28	ESP	176	308	27			ESP	(SPI=0)x04000)1dc)
5	466	61.00706	192.168.23	192.168.28	ESP	176	309	27			ESP	(SPI=0)x04000)1dc)
6	467	61.00905	192.168.23	192.168.28	ESP	176	310	27			ESP	(SPI=0)x04000)1dc)
7	468	61.01006	192.168.23	192.168.28	ESP	176	311	27			ESP	(SPI=0)x04000)1dc)
8	469	61.01105	192.168.23	192.168.28	ESP	176	312	27			ESP	(SPI=0)x04000)1dc)
9	470	61.01305	192.168.23	192.168.28	ESP	176	313	27			ESP	(SPI=0)x04000)1dc)
10	471	61.01406	192.168.23	192.168.28	ESP	176	314	27			ESP	(SPI=0)x04000)1dc)
11	472	61.01606	192.168.23	192.168.28	ESP	176	315	27			ESP	(SPI=0)x04000)1dc)
12	473	61.01806	192.168.23	192.168.28	ESP	176	316	27			ESP	(SPI=0)x04000)1dc)
13	474	61.02106	192.168.23	192.168.28	ESP	176	317	27			ESP	(SPI=0)x04000)1dc)
14	475	61.02205	192.168.23	192.168.28	ESP	176	318	27			ESP	(SPI=0)x04000)1dc)
15	476	61.02306	192.168.23	192.168.28	ESP	176	319	27			ESP	(SPI=0)x04000)1dc)
16	477	61.02506	192.168.23	192.168.28	ESP	176	320	27			ESP	(SPI=0)x04000)1dc)
17	478	61.02605	192.168.23	192.168.28	ESP	176	321	27			ESP	(SPI=0)x04000)1dc)
18	479	61.02805	192.168.23	192.168.28	ESP	176	322	27			ESP	(SPI=0)x04000)1dc)
19	480	61.02906	192.168.23	192.168.28	ESP	176	323	27			ESP	(SPI=0)x04000)1dc)
20	481	61.02906	192.168.23	192.168.28	ESP	176	324	27			ESP	(SPI=0)x04000)1dc)
21	482	61.03005	192.168.23	192.168.28	ESP	176	325	27			ESP	(SPI=0)x04000)1dc)
22	483	61.03206	192.168.23	192.168.28	ESP	176	326	27			ESP	(SPI=0)x04000)1dc)
23	484	61.03306	192.168.23	192.168.28	ESP	176	327	27			ESP	(SPI=0)x04000)1dc)
24	485	61.03505	192.168.23	192.168.28	ESP	176	328	27			ESP	(SPI=0)x04000)1dc)
25	486	61.03606	192.168.23	192.168.28	ESP	176	329	27			ESP	(SPI=0)x04000)1dc)
26	487	61.03905	192.168.23	192.168.28	ESP	176	330	27			ESP	(SPI=0)x04000)1dc)
27	488	61.04105	192.168.23	192.168.28	ESP	176	331	27			ESP	(SPI=0)x04000)1dc)
28	489	61.04206	192.168.23	192.168.28	ESP	176	332	27			ESP	(SPI=0)x04000)1dc)
29	490	61.04406	192.168.23	192.168.28	ESP	176	333	27			ESP	(SPI=0)x04000)1dc)
30	491	61.04606	192.168.23	192.168.28	ESP	176	334	27			ESP	(SPI=0)x04000)1dc)
31	492	61.06305	192.168.23	192.168.28	ESP	176	335	27			ESP	(SPI=0)x04000	01dc)
32	493	61.06505	192.168.23	192.168.28	ESP	176	336	27			ESP	(SPI=0)x04000)1dc)
33	494	61.06705	192.168.23	192.168.28	ESP	176	337	27			ESP	(SPI=0)x04000)1dc)
34	495	61.06905	192.168.23	192.168.28	ESP	176	338	27			ESP	(SPI=0	x04000	01dc)
35	496	61.07105	192.168.23	192.168.28	ESP	176	339	27			ESP	(SPI=0)x04000)1dc)
36	497	61.07105	192.168.23	192.168.28	ESP	176	340	27			ESP	(SPI=0	x04000)1dc)
7	400	£1 07005	100 160 00	100 160 00	F60	176	241	77			CCD.	(001-0	00000	

Navigeer terug naar CAP1_slice sheet en maak een nieuwe kolom genaamd Compare_ESP_SEQUENCE.

1		A	в	С	D	E	F	G	н	1	J	к	L	м	N	0	Р	Q	R
1	No.		Time	Source	Destinatio	Protocol	Length	ESP Seque	Differenti	Source Po	Destinatio	Info	Sequence	Number		COMPARE	ESP_SEQ	UENCE	
2		451	55.44196	192.168.2	192.168.28	ESP	176	306	27			ESP (SPI=	0x040001d	c)					
3		452	55.44598	192.168.2	192.168.28	ESP	176	307	27			ESP (SPI=	0x040001d	c)					
		450	EE 44007	100 160 0	103 160 30	ren	176	200	27			ren (eni-	0-040001d	-1					

Aangezien het ESP-volgnummer in kolom G staat, stel een VLOOKUP-opdracht samen zoals getoond om de twee bladen te vergelijken om ervoor te zorgen dat alles in kolom G op de bron in kolom G op de bestemming is.

=IF(ISNA(VLOOKUP(G2,CAP2_slice!G:G,1,FALSE)),"ONTBREEKT","AANWEZIG")

•	\times	\checkmark	f_x	=1F	(ISNA(VLO	OKUP(G2,	CAP2_slice	G:G,1,FAL	SE)), "MISS	ING","PRE	SENT")														
в		с		D	E	F	G	н	1	J	к	L	м	N	0	Р	Q	R	s	т	U	v	w	1	x
'ime	So	ource	De	stinatio	Protocol	Length	ESP Seque	Differenti	Source Po	Destinatio	Info	Sequence	Number		COMPA -	ESP_SEQU	IENCE								
55.441	96 19	2.168.2	192	.168.2	ESP	176	306	27			ESP (SPI=	0x040001dc)		=IF(ISNA(VLOOKUP(2,CAP2_9	slice!G:G,1,	FALSE)),"M	MISSING","	PRESENT")				
55.445	98 19	2.168.2	192	.168.2	ESP	176	307	27			ESP (SPI=	0x040001dc)												

Nadat ENTER is geselecteerd wordt het woord PRESENT weergegeven. Dit betekent dat het pakket met ESP Sequence **306** in het tweede blad aanwezig is. Dit is belangrijk omdat het

betekent dat het pakket het van de bron naar de bestemming maakte.

	Α		в	с	D	E	F	G	н	1	J	к	L	м	N	0	Р	Q	R	
1 N	lo.		Time	Source	Destinatio	Protocol	Length	ESP Seque	Differenti	Source Po	Destinatio	Info	Sequence	Number		COMPA -	ESP_SEQ	JENCE		
2		451	55.44196	192.168.23	192.168.28	ESP	176	306	27			ESP (SPI=	0x040001dd	:)		PRESENT				
3		452	55.44598	192.168.23	192.168.28	ESP	176	307	27			ESP (SPI=	0x040001dd	:)						

Selecteer Kolom O Rij 2 en zweef rechtsonder in het groene vak rond die cel.



Selecteer en houd de muis ingedrukt om deze formule naar de onderkant van de cellen met waarden te kopiëren.

	B	С	D	E	F	G	н	1.1	J.	ĸ	L	M	N	0	P	Q	R	S	т	U	V	W
	Time	Source	Destinat	ic Protocol	Length	ESP Seque	Differenti	Source Po	Destinatio	Info	Sequence	Number		COMPARE	_ESP_SEC	UENCE						
51	55.44196	5 192.168.2	192.168.	28 ESP	176	306	27			ESP (SP	1=0x040001dc)		PRESENT								
52	55.44598	3 192.168.2	192.168.	28 ESP	176	307	27			ESP (SP	1=0x040001dc)										
53	55.44897	192.168.2	192.168.	28 ESP	176	308	27			ESP (SP	1=0x040001dc)										
54	55.45097	192.168.2	192.168.	28 ESP	176	309	27			ESP (SP	1=0x040001dc)		_								
55	55.45296	5 192.168.2	192.168.	28 ESP	176	310	27			ESP (SP	1=0x040001dc)										
56	55.45496	5 192.168.2	192.168.	28 ESP	176	311	27			ESP (SP	1=0x040001dc)										
57	55.45597	192.168.2	192.168.	28 ESP	176	312	27			ESP (SP	1=0x040001dc)										
58	55.45698	3 192.168.2	3 192.168.	28 ESP	176	313	27			ESP (SP	1=0x040001dc)										
59	55.45797	192.168.2	192.168.	ZEESP	176	314	27			ESP (SP	1=0x040001dc)										
50	55.45898	3 192.168.2	192.168.	28 ESP	176	315	27			ESP (SP	1=0x040001dc)										
21	55,46207	192.108.2	192.108.	20 559	170	310	27			ESP (SP	1=0x040001dc)										
22	55 46596	192.100.2	192.100.	20 550	170	31/	27			ESP (SP	1=0x040001dc)										
10	55,46697	192.108.2	192.108.	25 ESD	176	319	27			ESP (SP	1=0x040001dc)										
55	55.46796	192.168.2	192.168	25 ESP	176	320	27			ESP (SP	1=0x040001dc)										
56	55.46996	192.168.2	192.168.	28 ESP	176	321	27			ESP (SP	1=0x040001dc)										
57	55,47097	192.168.2	192.168.	2EESP	176	322	27			ESP (SP	1=0x040001dc)										
	JS9 JJ	.00257 1	92.100.2	: 172.100.	ZCEOP		1/0	324	4	/		ED	- (321-0	x040001u	cj.		PR	OCINI				
	540 55	.60496 1	92.168.2	192.168.	28 ESP		176	395	2	7		ES	P (SPI=0	x040001d	c)		PR	ESENT				
	541 55	.60596 1	92.168.2	192.168.	28 ESP		176	396	2	7		ES	P (SPI=0	x040001d	c)		PR	ESENT				
	542 55	.60696 1	92.168.2	192.168.	28 ESP		176	397	2	7		ES	P (SPI=0	x040001d	c)		PR	ESENT				
	543 55	.60696 1	92.168.2	192,168.	28 ESP	_	176	398	2	7		ES	P (SPI=0	x040001d	c)		PR	ESENT				
	544 55	60696 1	92.168.2	192,168	2EESP		176	399	2	7		ES	P (SPI=0	x040001d	c)		PR	ESENT				
	545 55	.60796 1	92.168.2	192,168.	28 ESP	_	176	400	2	7		ES	P (SPI=0	x040001d	c)		PR	ESENT				
	546 55	60796 1	92 168 2	192 168	25 ESD		176	401	2	7		ES	D (SDI-0	v040001d	c)		DR	ESENT				-
	540 33	60006 1	02 160 2	102.100.	20 550	-	176	401	2	,		5	P (SPI-0	w040001d			P D	CONT				-
	547 55	.00030 1	92.100.2	192.100.			170	402	2	-		ES	P (3PI=0	X0400010			PR	COENT				
	548 55	.00896 1	92.168.2	: 192.168.	ZEESP	_	1/6	403	2	/		ES	P (SPI=0	x040001d			PR	ESENT			-	
	549 55	.60997 1	92.168.2	3 192.168.	28 ESP		176	404	2	/		ES	P (SPI=0	x040001d	c)		PR	ESENT				_
	550 55	.61096 1	92.168.2	\$ 192.168.	28 ESP		176	405	2	7		ES	P (SPI=0	x040001d	c)		PR	ESENT				

Scroll terug naar de bovenkant van het blad en klik op **Compare_ESP_SEQUENCE**. Selecteer vervolgens **Sorteren en filteren**.

onal Format as ng v Table v	Normal Neutral	Bad Calculation	Good Check C	cell v	Insert	Delete Fo	rmat ✓	AutoSum] Fill ~ ? Clear ~	Sort & F	nd &
	P C	R	S	т	U	V	w	x	Y	

Kies Filter in het uitrolmenu.



Er verschijnt een vervolgkeuzemenu in de kolom Compare_ESP_SEQUENCE.

M	N	0	Р								
lumber		COMPA 👻	ESP_SEQ	JEN							
		PRESENT									
		PRESENT									
		PRESENT									

Klik op het vervolgkeuzemenu in de kop **VERGELIJKEN_ESP_SEQUENCE**. Merk op dat in dit voorbeeld, de enige getoonde waarde **AANWEZIG** is. Dit betekent dat alle pakketten aanwezig zijn in beide opnamen.

к	L	м	N	0	
c Info	Sequence	Number		COMPA -	ESI
ES ^A _Z ↓	Sort A to Z				
ES ZI	Cost 7 to A				
ES A↓	3 <u>o</u> rt Z to A				
ES S	or <u>t</u> by Color			>	
ES S	heet <u>V</u> iew			>	
ES		1001404			
ES 1×	Clear Filter Fro	om "COMPA	KE_ESP_SEQ	UENCE.	
ES F	ilter by Color			>	
ES T	ext <u>F</u> ilters			>	
ES	an ch			0	
ES	earch			~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~	
ES	✓ (Select A	AII) -			
ES	PRESEN	I			
ES					
EC					

Om een problematisch voorbeeld te creëren, verwijder 10 pakketten van de CAP2_slice, om aan te tonen hoe dit zou werken in een test waar sommige gemiste pakketten ontbreken.

11	4/2	01.01000 192.108.2: 192.108.2	ESP 1/	0 312	27	ESP (SPI=0X0400010	C)
12	473	61.01806 192.168.2 192.168.2	ESP 17	6 316	27	ESP (SPI=0x040001d	c)
13	474	61.02106 192.168.2 192.168.2	ESP 17	6 317	27	ESP (SPI=0x040001d	c)
14	475	61.02205 192.168.2 192.168.2	ESP 17	6 318	27	ESP (SPI=0x040001d	c)
15	476	61.02306 192.168.23 192.168.23	ESP 17	6 319	27	ESP (SPI=0x040001d	c)
16	477	61.02506 192.168.2 192.168.2	ESP 17	6 320	27	ESP (SPI=0x040001d	c)
17	478	61.02605 192.168.2 192.168.2	ESP 17	6 321	27	ESP (SPI=0x040001d	c)
18	479	61.02805 192.168.2 192.168.2	ESP 17	6 322	27	ESP (SPI=0x040001d	c)
19	480	61.02906 192.168.2 192.168.2	ESP 17	6 323	27	ESP (SPI=0x040001d	c)
20	481	61.02906 192.168.2 192.168.2	ESP 17	6 324	27	ESP (SPI=0x040001d	c)
21	482	61.03005 192.168.2 192.168.2	ESP 17	6 325	27	ESP (SPI=0x040001d	c)
22	483	61.03206 192.168.2 192.168.2	ESP 17	6 326	27	ESP (SPI=0x040001d	c)
23	484	61.03306 192.168.2 192.168.2	ESP 17	6 327	27	ESP (SPI=0x040001d	c)
24	485	61.03505 192.168.2 192.168.2	ESP 17	6 328	27	ESP (SPI=0x040001d	c)
25	486	61.03606 192.168.2 192.168.2	ESP 17	6 329	27	ESP (SPI=0x040001d	c)
26	487	61.03905 192.168.2 192.168.2	ESP 17	6 330	27	ESP (SPI=0x040001d	c)
27	488	61.04105 192.168.23 192.168.23	ESP 17	6 331	27	ESP (SPI=0x040001d	c)
28	489	61.04206 192.168.2 192.168.2	ESP 17	6 332	27	ESP (SPI=0x040001d	c)
29	490	61.04406 192.168.2 192.168.2	ESP 17	6 333	27	ESP (SPI=0x040001d	c)
30	491	61.04606 192.168.2 192.168.2	ESP 17	6 334	27	ESP (SPI=0x040001d	c)
31	492	61.06305 192.168.23 192.168.23	ESP 17	6 335	27	ESP (SPI=0x040001d	c)
32	493	61.06505 192.168.23 192.168.23	ESP 17	6 336	27	ESP (SPI=0x040001d	c)
33	494	61.06705 192.168.23 192.168.23	ESP 17	6 337	27	ESP (SPI=0x040001d	c)
34	495	61.06905 192.168.23 192.168.23	ESP 17	6 338	27	ESP (SPI=0x040001d	c)
35	496	61.07105 192.168.23 192.168.23	ESP 17	6 339	27	ESP (SPI=0x040001d	c)
36	497	61.07105 192.168.2 192.168.2	ESP 17	6 340	27	ESP (SPI=0x040001d	c)
37	498	61.07205 192.168.2 192.168.2	ESP 17	6 341	27	ESP (SPI=0x040001d	c)
38	499	61.07605 192.168.23 192.168.23	ESP 17	6 342	27	ESP (SPI=0x040001d	c)
-	->	CAP1_slice CAP2_slice	+				

Navigeer terug naar CAP1_slice sheet en nu wordt gezien dat er 10 pakketten ontbreken.

	JJ. 4 J/J/ 1J2.		10	514	£1	Loi (011-0x04000100)	1 HEVEN I
460	55.45898 192.1	168.23192.168.2	ESP 176	315	27	ESP (SPI=0x040001dc)	PRESENT
461	55.46197 192.3	168.23 192.168.2	ESP 176	316	27	ESP (SPI=0x040001dc)	PRESENT
462	55.46397 192.3	168.2: 192.168.2	ESP 176	317	27	ESP (SPI=0x040001dc)	PRESENT
463	55.46596 192.3	168.2: 192.168.2	ESP 176	318	27	ESP (SPI=0x040001dc)	MISSING
464	55.46697 192.3	168.2: 192.168.2	ESP 176	319	27	ESP (SPI=0x040001dc)	MISSING
465	55.46796 192.1	168.2: 192.168.2	ESP 176	320	27	ESP (SPI=0x040001dc)	MISSING
466	55.46996 192.1	168.2: 192.168.2	ESP 176	321	27	ESP (SPI=0x040001dc)	MISSING
467	55.47097 192.1	168.2: 192.168.2	ESP 176	322	27	ESP (SPI=0x040001dc)	MISSING
468	55.47198 192.1	168.2: 192.168.2	ESP 176	323	27	ESP (SPI=0x040001dc)	MISSING
469	55.47297 192.1	168.2: 192.168.2	ESP 176	324	27	ESP (SPI=0x040001dc)	MISSING
470	55.47497 192.1	168.2: 192.168.2	ESP 176	325	27	ESP (SPI=0x040001dc)	MISSING
471	55.47597 192.1	168.2: 192.168.2	ESP 176	326	27	ESP (SPI=0x040001dc)	MISSING
472	55.47697 192.3	168.2: 192.168.2	ESP 176	327	27	ESP (SPI=0x040001dc)	MISSING
473	55.47896 192.1	168.2: 192.168.2	ESP 176	328	27	ESP (SPI=0x040001dc)	PRESENT
474	55.48096 192.1	168.2: 192.168.2	ESP 176	329	27	ESP (SPI=0x040001dc)	PRESENT

Wanneer het dropdown menu is geselecteerd in de kolom **Compare_ESP_SEQUENCE**, zien we nu dat er ook **ONTBREKENDE** pakketten zijn. Dit kan worden omgeschakeld om alleen de **ONTBREKENDE** pakketten te bekijken.

	ĸ	L	M	N	0
nf	0	Sequence	Number		COMPA
S	<mark>2</mark> ↓ <u>s</u> o	ort A to Z			
S	Z↓ So	ort Z to A			-
S	Sor	<u>t</u> by Color			>
S	She	et <u>V</u> iew			>
S		ear Filter Fro	m "COMPA	RE_ESP_SEQ	JENCE"
s	Filte	er by Color			>
S	Tex	t <u>F</u> ilters			>
S	Sea	arch			Q
1 24 24 24 24 24 24 24 24 24 24		(Select A I MISSING I PRESENT	III) F		
5 5			0	K	Cancel .:



Nu worden alleen de ontbrekende pakketten getoond in het Excel-blad.

A	В	C	D	E	F	G	н		J	K	L	M	N	0	P
No.	Time	Source	Destinati	c Protocol	Length	ESP Seque	Differenti	Source Po	Destinati	Info	Sequence	Number		COMPA J	_ESP_SEQ
4 4	55.4659	5 192.168.2	192.168.2	ESP .	176	318	27			ESP (SPI	=0x040001dc)		MISSING	
5 4	55.4669	7 192.168.2	192.168.2	ESP .	176	319	27			ESP (SPI	=0x040001dc)		MISSING	
6 4	65 55.4679	5 192.168.2	192.168.2	ESP	176	320	27			ESP (SPI	=0x040001dc)		MISSING	
7 4	55.4699	5 192.168.2	192.168.2	ESP 8	176	321	27			ESP (SPI	=0x040001dc)		MISSING	
8 4	55.4709	7 192.168.2	192.168.2	ESP .	176	322	27			ESP (SPI	=0x040001dc)		MISSING	
9 4	55.4719	3 192.168.2	192.168.2	8 ESP	176	323	27			ESP (SPI	=0x040001dc)		MISSING	
0 4	55.4729	7 192.168.2	192.168.2	ESP	176	324	27			ESP (SPI	=0x040001dc)		MISSING	
1 4	70 55.4749	7 192.168.2	192.168.2	ESP	176	325	27			ESP (SPI	=0x040001dc)		MISSING	
2 4	71 55.4759	7 192.168.2	192.168.2	ESP .	176	326	27			ESP (SPI	=0x040001dc)		MISSING	
3 4	72 55.4769	7 192.168.2	192.168.2	ESP	176	327	27			ESP (SPI	=0x040001dc)		MISSING	
)2															
)3															

Gerelateerde informatie

- <u>Cisco ingesloten pakketvastlegging</u>
- Technische ondersteuning en documentatie Cisco Systems

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.