# Überprüfung und Identifizierung von Paketverlusten im WAN für das SD-WAN

### Inhalt

Einleitung Voraussetzungen Anforderungen Verwendete Komponenten Hintergrund Fehlerbehebung Übersichtsprozess Markieren des gewünschten Datenverkehrs mit DSCP Erfassen Sie den Datenverkehr mit der integrierten Erfassung Analyse über Wireshark Filtern des gewünschten Datenverkehrs nach ESP-Sequenz Zugehörige Informationen

# Einleitung

In diesem Dokument wird beschrieben, wie Sie Daten identifizieren und erfassen, wenn der Datenverkehr im WAN verloren geht, am SD-WAN-Edge jedoch keine Datenverluste auftreten.

## Voraussetzungen

### Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Cisco Software-Defined Wide Area Network (SD-WAN)
- Integrierte Paketerfassung oder vManage-Paketerfassung
- Wireshark
- Microsoft Excel

### Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- C8000V Version 17.03.04
- vManage, Version 20.3.4
- Wireshark Version 2.6.3

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer

gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle verstehen.

# Hintergrund

Zur Unterstützung bei dieser Herausforderung wird in diesem Dokument beschrieben, wie Sie bestimmten Datenverkehr mit Differentiated Services Code Point (DSCP) markieren, um die gewünschten Pakete zu identifizieren. DSCP kann verwendet werden, um den Datenverkehr zu identifizieren, da dieser Wert vom inneren Paket-Header in den IPsec-Header kopiert wird. Sobald die gewünschten Pakete identifiziert wurden, wird gezeigt, wie der Datenverkehr über zwei WAN-Erfassungen abgeglichen werden kann, um sicherzustellen, dass der Datenverkehr von der Quelle bis zum Ziel übertragen wird.

Diese Fehlerbehebungstechnik wird an zwei Standorten mit einem Router demonstriert. In diesem Fall wird der ICMP-Datenverkehr zwischen 10.0.0.10 und 10.0.2.10 in Form von 100 Pings gesendet, wie im Bild gezeigt. In diesem Beispiel gibt es keinen Verlust, aber die gleiche Fehlerbehebungstechnik wird verwendet, wenn ein Verlust vorliegt, um ihn zu identifizieren.



# Fehlerbehebung

### Übersichtsprozess

- 1. Für den Datenverkehr, der über das WAN verfolgt wird, ist eine Zugriffsliste (ACL) (oder eine zentrale Richtlinie) erforderlich, um den Datenverkehr mit einem nicht verwendeten DSCP-Wert zu markieren. In diesem Beispiel wird DSCP 27 verwendet.
- 2. Sobald der Datenverkehr markiert ist, wird die integrierte Paketerfassung verwendet, um die Pakete an der Transportschnittstelle des Quell- und Zielrouters zu erfassen.

**Hinweis**: Die vManage-Paketerfassung kann ebenfalls verwendet werden, auch wenn die Laufzeit auf 5 MB an Daten oder 5 Minuten beschränkt ist.

- 1. Nachdem die Aufnahmen gemacht wurden, öffnen Sie sie in Wireshark, um sie anzuzeigen.
- 2. Der Filter wird in Wireshark angewendet, um anzuzeigen, welche Pakete erwünscht sind, und dann werden sie verglichen.
- 3. Microsoft Excel wird für große Aufnahmen verwendet, um die Genauigkeit zu gewährleisten.

### Markieren des gewünschten Datenverkehrs mit DSCP

Eine Zugriffsliste wie im Beispiel wird auf dem Quellrouter (in diesem Beispiel cEdge1) konfiguriert und auf die Schnittstelle im SD-WAN-Teil der Routerkonfiguration angewendet, wie dargestellt.

Ein optionaler Zähler wird angewendet, um zu überprüfen, ob der Datenverkehr die Richtlinie wie erwartet erreicht. Dies kann mithilfe des Befehls **show sdwan policy access-list-counters überprüft werden**.

```
policy
access-list mark_dscp_27
sequence 10
match
source-ip 10.0.0.10/32
destination-ip 10.0.2.10/32
!
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
```

#### Erfassen Sie den Datenverkehr mit der integrierten Erfassung

**Hinweis**: Konfigurieren einer integrierten Paketerfassung in Cisco IOS XE zur Erfassung der verschlüsselten Pakete, die das WAN durchlaufen; Navigieren Sie zu <u>Embedded Packet</u> <u>Capture für Cisco IOS und Cisco IOS XE - Konfigurationsbeispiel</u>

**Hinweis**: Eine ACL muss verwendet werden, um den EPC im WAN zu begrenzen, da der EPC eine Durchsatzrate von mehr als 1000 PPS haben könnte.

#### Beispiel

Auf cEdge1 und cEdge3 wird eine ACL konfiguriert, da der Datenverkehr in diesem Beispiel nur in der Richtung von Quelle zu Ziel überprüft wird.

**Hinweis**: Die WAN-IP-Adressen werden zum Filtern der Erfassung verwendet. Es gibt mehrere Ausgänge, die den Pfad für den Datenverkehr identifizieren können, sodass die richtigen WAN-IPs für den ACL-Filter identifiziert werden können. Die Befehle, die zum Generieren dieser Ausgabe verwendet werden können, sind **show sdwan app-fwd cflowd flows** und **show sdwan policy service path**. Bitte navigieren Sie zu <u>Conditional Packet Trace</u>, um die Fehlerbehebungsbedingung zu erhalten.

An diesem Punkt werden die Captures auf beiden Routern gestartet und 100 Pings über das Overlay gesendet.

Success rate is 100 percent (100/100), round-trip min/avg/max = 1/1/4 ms

Nachdem die Aufnahmen angehalten und von beiden Routern gesammelt wurden, müssen sie in Wireshark geöffnet werden, um sie anzuzeigen.

#### Analyse über Wireshark

Sobald die cEdge1-Erfassung in Wireshark geöffnet ist, wird deutlich, dass der gesamte Datenverkehr verschlüsselt ist und es nicht einfach ist, zu entschlüsseln, welche Pakete die Pings sind, die gesendet wurden.

kay fiter <ctrl-></ctrl->										 -
 Time	Source	Destination	Protocol Length	ESP Sequence	Differentiated Services Codepoint	Source Port	Destination Port	Sequence Number	Info	î
1 0,000000	192.168.23.149	192.168.28.240	UDP	175	Class Selector 6				12386 + 12407 Len=133	
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 11.416978	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	UDP	176	Default				12386 + 12407 Len=134	
35 14.175985	192.168.23.149	192.168.28.240	UDP	176	Default				12386 + 12407 Len=134	
36 14.176977	192.168.23.149	192.168.28.240	UDP	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	UDP	176	Default				12386 + 12407 Len=134	
20 11 100000			1100	1.04	P. C. 11					

Filtern Sie diese Erfassung mit einem Anzeigefilter **ip.dsfield.dscp == 27**, es wird deutlich, dass nur 100 Pakete am unteren Bildschirmrand angezeigt werden und dass der DSCP-Spaltenwert alle 27 anzeigt.

Time Source								CO
451 55 441963 102 168 23	Destination	Protocol Length	ESP Sequence	Differentiated Services Codepoint	Source Port Destination Port	Sequence Number	Info	
431 33.441303 191.100.113.	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	1		12386 → 12407 Len=134	
454 55.450965 192.168.23.	.149 192.168.28.240	UDP	176	27	1		12386 → 12407 Len=134	
455 55.452964 192.168.23.	.149 192.168.28.240	UDP	176	27	1		12386 → 12407 Len=134	
456 55.454963 192.168.23.	.149 192.168.28.240	UDP	176	27	1		12386 → 12407 Len=134	
457 55.455970 192.168.23.	.149 192.168.28.240	UDP	176	27	1		12386 → 12407 Len=134	
458 55.456977 192.168.23.	.149 192.168.28.240	UDP	176	27	1		12386 - 12407 Len=134	
459 55.457968 192.168.23.	.149 192.168.28.240	UDP	176	27	1		12386 + 12487 Len=134	
460 55.458975 192.168.23.	.149 192.168.28.240	UDP	176	27	1		12386 - 12407 Len=134	
461 55.461966 192.168.23.	.149 192.168.28.240	UDP	176	27	1		12386 + 12407 Len=134	
462 55.463965 192.168.23.	.149 192.168.28.240	UDP	176	27	1		12386 → 12407 Len=134	
463 55.465964 192.168.23.	149 192.168.28.240	UDP	176	27	1		12386 → 12407 Len=134	
464 55.466971 192.168.23.	.149 192.168.28.240	UDP	176	27	1		12386 - 12407 Len=134	
465 55.467962 192.168.23.	.149 192.168.28.240	UDP	176	27	1		12386 → 12407 Len=134	
466 55.469961 192.168.23.	.149 192.168.28.240	UDP	176	27	1		12386 → 12407 Len=134	
467 55.470968 192.168.23.	149 192.168.28.240	UDP	176	27	1		12386 + 12407 Len=134	
468 55.471975 192.168.23.	149 192.168.28.240	UDP	176	27	1		12386 - 12407 Len=134	
469 55.472967 192.168.23.	.149 192.168.28.240	UDP	176	27	1		12386 + 12407 Len=134	
478 55.474966 192.168.23.	149 192.168.28.240	UDP	176	27	1		12386 + 12407 Len=134	
471 55.475973 192.168.23.	.149 192.168.28.240	UDP	176	27	1		12386 + 12407 Len=134	
472 55.476965 192.168.23.	.149 192.168.28.240	UDP	176	27	1		12386 → 12407 Len=134	
473 55.478963 192.168.23.	149 192.168.28.240	UDP	176	27	1		12386 + 12407 Len=134	
474 55.480962 192.168.23.	149 192.168.28.240	UDP	176	27	1		12386 -+ 12407 Len=134	
475 55,481969 192,168,23,	149 192,168,28,240	UDP	176	27	1		12386 + 12407 Len=134	
476 55,484975 192,168,23,	149 192,168,28,240	UDP	176	27	1		12386 + 12407 Len=134	
477 55,485967 192,168,23,	149 192,168,28,240	UDP	176	27	1		12386 + 12407 Len=134	
478 55,487966 192,168,23,	149 192,168,28,240	LIDP	176	27	1		12386 + 12407 Len+134	
479 55.488973 192.168.23.	149 192,168,28,248	LIDP	176	27	1		12386 + 12407 Len=134	
488 55.491963 192.168.23	149 192,168,28,248	LIDP	176	27	1		12386 + 12407 Len+134	
481 55 508961 192 168 21	140 102 168 28 240	LINE	176	27	1		12386 a 12407 Lene134	
482 55 518050 102 168 23	140 102 168 28 240	100	176	27	1		12386 + 12407 Lene134	
483 55 511066 103 168 33	140 103 168 38 340	100	176	27	1		12386 - 12407 Len-134	
405 55.511900 192.100.25.	140 103 168 38 340	100	176	27	1		12300 - 12407 Len-134	
485 55 514073 103 148 33	140 103 168 38 340	100	176	27	1		13386 - 13407 Len-134	
405 55.514972 192.100.23.	149 192.100.20.240	000	176	27	1		12300 + 12407 Len+134	
400 33.3109/1 192.100.23.	140 103 160 20 240	100	176	27	1		12300 - 12407 Len-134	
407 55.517905 192.100.25.	149 192.100.20.240	009	176	27	1		12300 + 1240/ Len+134	
400 55.523739 192.100.23.	149 192.100.20.240	100	176	27	1		12300 = 12407 Len=134	
489 55.524966 192.168.23.	149 192.168.28.240	009	176	27			12380 + 12407 Len+134	

In einigen Fällen, in denen der DSCP-Wert im gesamten WAN beibehalten wird, kann derselbe Filter für die Zielerfassung verwendet werden.

In anderen Fällen ist dies nicht möglich, z. B. wenn der DSCP-Wert über eine öffentlich-rechtliche Internetverbindung gelöscht wird.

### Filtern des gewünschten Datenverkehrs nach ESP-Sequenz

In beiden Fällen kann der Datenverkehr mit den ESP-Sequenznummern identifiziert werden.

Um die ESP-Sequenznummern im Paket anzuzeigen, klicken Sie mit der rechten Maustaste auf die Erfassung, und wählen Sie **Decode (Dekodieren), wie** dargestellt.

			12386
			12386
	Mark/Upmark Packet	Ctrl+M	12386
			12386
	Ignore/Unignore Packet	Ctrl+D	12386
	Set/Unset Time Reference	Ctrl+T	12386
	Time Shift	Ctrl+Shift+T	12386
	Packet Comments	•	12386
	i deket 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
	Follow		12386
	Copy	•	12386
	copy		12386
	Protocol Preferences	•	12386
	Decode As		12386
			12386
	Show Packet in New Window	N	12386

Wählen Sie das Dropdown-Menü **Aktuelles** Feld aus, und geben Sie in diesem Feld **UDPENCAP ein**, oder wählen Sie es aus dem Dropdown-Menü aus.



Nire	shark	· Dec	ode/	As
			ouc,	

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 (	2			Or I	Caus	Copyfrom	Canad	Hala
					UK	Save	Copy from	Cancel	нер

Wählen Sie nach Abschluss dieses Vorgangs OK aus.

<b>Wires</b>	Wireshark · Decode As ×											
_												
Field	Value	Туре	Default	Current								
UDP po	t 12386	Integer, base 10	(none)	UDPENCAP								
										- 1		
										- 1		
										- 1		
										- 1		
										- 1		
+ -	4	0										
					OK	Save	Copy from	Cancel	Help			

Erweitern Sie im Abschnitt "Wireshark Packet Details" den Encapsulating Security Payload-Teil des Pakets, um die ESP-Sequenz anzuzeigen.

×

	479 55 488973 192 168 23	149 1	192 168	28 240	FSP	176	
<							
>	Frame 464: 176 bytes on wire (1408 b	its), 176 b	ytes cap	otured (140	8 bits)		
>	Ethernet II, Src: VMware_84:af:45 (0	0:50:56:84:	af:45),	Dst: VMwar	e_84:e2:b7	(00:50:56:84:e2:b7)	
>	Internet Protocol Version 4, Src: 19	2.168.23.14	9, Dst:	192.168.28	.240		
>	User Datagram Protocol, Src Port: 12	386, Dst Po	ort: 1240	97			
	UDP Encapsulation of IPsec Packets	_					
	Encapsulating Security Payload						
•	ESP SP1: 0X0400010C (67109340)						
	ESP Sequence: 319						

Klicken Sie mit der rechten Maustaste auf **ESP Sequence (ESP-Sequenz)** und wählen Sie **Apply as column (Als Spalte anwenden)** aus, damit die ESP Sequence als Spalte im Abschnitt Packet List (Paketliste) im oberen Bereich des Wireshark-Bildschirms angezeigt wird.

	+J2J0+ 1J2.100.2J.14J	172.100.20.240	201
456 55.4	Expand Subtrees		ESP
457 55.4	c Expand Subtrees		ESP
458 55.4	Collapse Subtrees		ESP
459 55.4	Expand All		ESP
460 55.4	Collapse All		ESP
461 55.			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		,	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	Show Dacket Puter	Chilly Shifty, O	ESP
4/3 55.4	Show Packet bytes	Ctri+Shirt+O	ESP
4/4 55.4	Export Packet Bytes	Ctrl+Shift+X	ESP
	Wiki Protocol Page		
Frame 464: 176 byt	Wiki Plotocol Page		08 bits)
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	Show Link d Packet in New Wir	ndow	
ESP Sequence: 3	L		1

**Hinweis**: Der ESP-SPI für die Pakete auf cEdge1 ist **0x040001dc**. Dies wird für einen Filter für die Zielerfassung verwendet.

```
> 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
```

Öffnen Sie die Zielerfassung, wiederholen Sie die Schritte zur Dekodierung als **UDPENCAP**, und zeigen Sie die ESP-Sequenznummern in den Paketen an.

Sobald die Pakete die ESP-Sequenznummer anzeigen, kann der ESP-SPI aus der ersten Erfassung als Filter für die zweite Erfassung verwendet werden, um nur den Datenverkehr innerhalb dieses SPI anzuzeigen, der dem gewünschten Datenverkehr entspricht.

Beachten Sie, dass für die Paketsequenznummern, die mit beiden übereinstimmen, DSCP 27 markiert ist.



Dieser Vergleich kann manuell in Wireshark durchgeführt werden, oder Sie können diesen Vergleich mit Microsoft Excel durchführen.

Um Microsoft Excel zum Vergleichen zu verwenden, müssen beide Erfassungen so aufgeteilt werden, dass sie nur Pakete enthalten, die sich in beiden Erfassungen befinden.

Bei der Quellenerfassung weist das erste relevante Paket die ESP-Sequenz 306 auf, die der Paketnummer 451 entspricht.

CAP.pcap						_		$\times$
File Edit View Go Capture	Analyze Statistics Tel	ephony Wireless Tools	Help					
📶 🔳 🔬 💿 📙 🛅 🗙 🖸	९ 🗢 🗢 🗟 🚹 👃	🚽 📃 🔍 🔍 🔍 🖽						
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		306	27	
452 55.445976	192.168.23.149	192.168.28.240	ESP	176		307	27	
453 55.448966	192.168.23.149	192.168.28.240	ESP	176		308	27	
454 55.450965	192.168.23.149	192.168.28.240	ESP	176		309	27	
455 55.452964	192.168.23.149	192.168.28.240	ESP	176		310	27	
456 55.454963	192.168.23.149	192.168.28.240	ESP	176		311	27	
457 55.455970	192.168.23.149	192.168.28.240	ESP	176		312	27	
458 55.456977	192.168.23.149	192.168.28.240	ESP	176		313	27	

Das letzte relevante Paket in der Quellenerfassung hat die ESP-Sequenz 405 und ist die Paketnummer 550.

	548 55.608962 549 55.609969	192.168.23.149 192.168.23.149	192.168.28.240 192.168.28.240	ESP	176 176	403 27 404 27
	550 55.610960	192.168.23.149	192.168.28.240	ESP	176	405 27
۲						>

Bei der Zielerfassung entspricht das erste relevante Paket der Quellerfassung mit ESP-Sequenz 306, bei dieser Erfassung ist es jedoch Paket 463.

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

Das letzte relevante Paket ist ebenfalls mit der ESP-Sequenz 405 vorhanden und es ist das Paket 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	

Die erste Erfassung muss nun in Abschnitte aufgeteilt werden, sodass nur relevante Pakete enthalten sind.

Navigieren Sie zu Datei > Paketdissektionen exportieren > Als CSV...

|--|

File	Edit	View	Go	Capture	Analyze	Statisti	cs Telephony	Wirel	ess	Tools	Help			
	Open				Ctrl+0	E 3	§ 🕭 📃 🔳	⊕ (						
	Open R	lecent				• ⊨								Ē
	Merge						Destinati				Destand	Length		
	incige.	 					Destinat	on			Protocol	Length		2
	Import	from H	ex Du	mp		149	192.16	8.28.	240		ESP		176	
	Close				Ctrl+W	149	192.16	8.28.	240		ESP		176	
						149	192.16	8.28.	240		ESP		176	
	Save				Ctrl+S	149	192.16	8.28.	240		ESP		176	
	Save As	5			Ctrl+Shift+S	149	192.16	8.28.	240		ESP		176	
						149	192.16	8.28.	240		ESP		176	
	File Set				)	149	192.16	8.28.	240		ESP		176	
						- 149	192.16	8.28.	240		ESP		176	
	Export	Specifie	d Pac	kets		149	192.16	8.28.	240		ESP		176	
	Export	Packet (	Dissec	tions		•	As Plain Text	- 1-	240		ESP		176	
	Export	Dacket P	Ruter		Ctrl+Shift+X		Ac CSV	ŀ	240		ESP		176	
	export	Fackett	Jytes		Cur+Shirt+X		As Covin		240		ESP		176	
	Export	PDUs to	File				As "C" Arrays	- ŀ	240		ESP		176	
	Export	TLS Sess	sion K	eys				- I-	240		ESP		176	
	Export Objects						As PSML XML	- I-	240		ESP		176	
	Export Objects					_	As PDML XML	. I.	240		ESP		176	
	Drint		Ctrl+P		As ISON	- I.	240		ESP		176			
					curr			J.	240		ESP		176	
	Quit				Ctrl+Q	149	192.16	8.28.	240		ESP		176	
-		24	/ >>	000902	192.100.1	<del>cə.</del> 149	192.16	8.28.	240		ESP		176	
		54	8 55.	608962	192.168.2	23.149	192.16	8.28.	240		ESP		176	

Wählen Sie **Captured** (**Erfasst**) und **Range (Bereich)** aus, und geben Sie im Feld **Range (Bereich**) den Bereich vom ersten relevanten Paket bis zum letzten relevanten Paket ein.

Geben Sie einen Dateinamen in das Feld Dateiname ein, und klicken Sie auf Speichern.

	Wireshark ·	Export Packet	Dissections
--	-------------	---------------	-------------

Name Status Date modified   No items match your search. No items match your search. Date modified   Desktop Image: Carcel Image: Carcel   Desktop Image: Carcel Image: Carcel   Network Image: Carcel Image: Carcel   Packet Range Image: Carcel Image: Carcel   Packet Range Image: Carcel Image: Carcel   Image: Carcel Image: Carcel <	Save in:	Desktop			⊳ 🔝	
Desktop   Libraries   This PC   Network   File name:   CAP1_slice   Save as type:   CSV (Comma Separated Values summary) (*.cs)   Cancel   Help   Packet Range   Packet Range   O All packets   Selected packet   1   Marked packets   0   First to last marked   0   0   Range:   451-550   100   Brange:   451-550   0   0	Quick access	Name	^ No items match	Status h your search.	Date n	nodified
Libraries   This PC   Image: CAP1_slice   Save as type: CSV (Comma Separated Values summary) (*.cs)   Save as type: CSV (Comma Separated Values summary) (*.cs)   Packet Range   Packet Range   Image: Packets   Im	Desktop					
This PC   Image: This PC   Image: CAP1_slice   File name: CAP1_slice   Save   Save as type: CSV (Comma Separated Values summary) (*.csr v   Cancel   Help   Packet Range   Image: Packets   Image: All packets	Libraries					
Network        Save         File name:       CAP1_slice       Save         Save as type:       CSV (Comma Separated Values summary) (*.cs)       Cancel         Help       Help         Packet Range       © Captured Obsplayed         All packets       880       100         Selected packet       1       1         Marked packets       0       0         First to last marked       0       0         Range:       [451-550]       100       100         Remove Ignored packets       0       0       File	This PC					
Nie name: CAP I_slice   Save as type: CSV (Comma Separated Values summary) (*.cs)   Cancel   Help   Packet Range   Packet Range   O All packets   Selected packet   1   Marked packets   0   First to last marked   0   Range:   451-550   100   Remove Ignored packets	Setwork	<	CAP1 stor			>
Packet Range       Packet         ○ All packets       880       100         ○ Selected packet       1       1         ○ Marked packets       0       0         ○ First to last marked       0       0         ● Range:       451-550       100       100         ● Remove Ignored packets       0       0       1		Save as type:	CSV (Comma Separated Val	ues summary) (*.c	S1 ~	Cancel Help
Image: Captured       Displayed         All packets       880       100         Selected packet       1       1         Marked packets       0       0         First to last marked       0       0         Range:       451-550       100       100         Remove Ignored packets       0       0       1		Packet Range				Pack
○ All packets       880       100       [         ○ Selected packet       1       1       [         ○ Marked packets       0       0       [         ○ First to last marked       0       0       [         ● Range:       451-550       100       100       [         ■ Remove Ignored packets       0       0       [       [				Captured	O Displayed	Pa
○ Selected packet       1       1       I		○ All packets		880	100	
Marked packets       0       0       0         First to last marked       0       0       0         Range:       451-550       100       100       F         Remove Ignored packets       0       0       E		O Selected pack	ket	1	1	Pa
First to last marked     0     0     1 <ul> <li>Range:</li> <li>451-550</li> <li>100</li> <li>100</li> <li>F</li> <li>Remove Ignored packets</li> <li>0             <li>0</li> </li></ul> Image: Ima		Marked packet	ets	0	0	1
Range:   451-550   100   100   100     Remove Ignored packets   0   0   Image:		First to last ma	irked	0	0	
		Remove Ignor	red packets	0	0	E

Wiederholen Sie den gleichen Prozess bei Erfassung 2 für die relevanten Pakete.

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: Cancel CSV (Comma Separated Values summary) (".csi ~ Save as type: Help Packet Range Packe O Displayed Captured Pa Pa All packets 904 904  $\mathbb{P}$  Selected packet 1 1 Pa Pa Marked packets A ) First to last marked Pa Range: 463-564 102 Ea Ea Remove Ignored packets

Öffnen Sie beide CSV-Dateien in Microsoft Excel.

Speichern Sie das CSV für die Quellaufzeichnung als XLSX-Format.

Save As		
L Recent	↑ ▷ Desktop CAP1_slice	
Cisco	Excel Workbook (*.xlsx)	🕞 Save

Wählen Sie am unteren Bildschirmrand das +-Symbol aus, um ein weiteres Blatt hinzuzufügen. Nennen Sie es CAP2\_slice.

j	485	55.51497 192.168.2	192.168.28	ESP 176	340	27	ESP (SPI=0x040001dc)	
·	486	55.51697 192.168.2	192.168.28	ESP 176	341	27	ESP (SPI=0x040001dc)	
3	487	55.51796 192.168.2	192.168.28	ESP 176	342	27	ESP (SPI=0x040001dc)	
4	•	CAP1_slice	•					

Öffnen Sie die CSV-Datei CAP2 und drücken Sie STRG + a, um alle auszuwählen, und STRG + c, um sie zu kopieren.

 $\times$ 

J77  $\checkmark$  :  $\times \checkmark f_x$ 

1	А	В	С	D	E	F	G	Н	1	J	K	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=	0x040001dd	)
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	

Navigieren Sie zur Datei **CAP1\_slice.xlsx**, und fügen Sie auf der zweiten Registerkarte für CAP2\_slice (**STRG + v**) die kopierten Informationen in die Zelle **A1 ein**.

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.	A .	= = =		Merge /	R Center v	¢.,	%	€ <u>0</u> .00
*	ダ Format P	ainter	0.1		<del></del> -	- ·			Merge	a center -		/0 /	.00 -20
	Clipboard	13	ù l	Font	t	F2		Aligne	nent	5		Number	5
A1	Ŧ	: >	$\sim$	f <sub>x</sub>									
	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	(+)								

- All 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	01dc)
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	61 07005	100 160 00	100 160 00	F60	176	241	77			CCD.	(001-0	00000	

Navigieren Sie zurück zum Blatt **CAP1\_slice**, und erstellen Sie eine neue Spalte mit dem Namen **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	JENCE	
2		451	55.44196	192.168.2	192.168.28	ESP	176	306	27			ESP (SPI=	0x040001dd	:)					
3		452	55.44598	192.168.2	192.168.28	ESP	176	307	27			ESP (SPI=	0x040001dd	:)					
		450	EE 44007	102 160 2	103 169 30	ren	176	200	27			ren (eni-	0.040001d	4					

Da sich die ESP-Sequenznummer in Spalte G befindet, erstellen Sie einen VLOOKUP-Befehl, um die beiden Blätter zu vergleichen und sicherzustellen, dass alles in Spalte G der Quelle in Spalte G des Ziels enthalten ist.

=IF(ISNA(VLOOKUP(G2,CAP2\_slice!G:G,1,FALSE)),"MISSING","PRESENT")

•	$\times$	$\checkmark$	$f_x$	=1F	(ISNA(VLO	OKUP(G2,	CAP2_slice	G:G,1,FAL	SE) <b>),</b> "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_5	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	)												

Nachdem die Eingabetaste ausgewählt wurde, wird das Wort PRESENT angezeigt. Dies bedeutet, dass das Paket mit ESP-Sequenz **306** im zweiten Blatt vorhanden ist. Dies ist von

Bedeutung, da es bedeutet, dass das Paket von der Quelle bis zum Ziel übertragen wurde.

	А		В	С	D	E	F	G	н	1	J	к	L	м	N	0	Р	Q	R	
1 1	No.		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	:)						

Wählen Sie Spalte O Zeile 2 aus, und bewegen Sie den Mauszeiger über die untere rechte Ecke des grünen Felds um diese Zelle.

N	0	Р	Q	R	S						
	COMPARE										
	3 10	3 0									

Halten Sie die Maustaste gedrückt, und ziehen Sie die Maus nach unten, um diese Formel an das Ende der Zellen zu kopieren, die Werte haben.

i	· ·	XV	f <sub>x</sub> =	=IF(ISNA(VLO	OKUP(G2,	,CAP2_slice	2!G:G,1,FA	ALSE)),"MI	SSING","PRE	SENT")						1			-			
	B	C	D	E	F	G	H	1	J	K	L	M	N	0	P	Q	R	S	T	U	V	W
	Time	Source	Destina	tic Protocol	Length	ESP Sequ	e Differen	nti Source I	Po Destinati	c Info	Sequence N	lumber		COMPARE	ESP_SEC	UENCE						
21	55.441	90 192.108.	2: 192.108	20550	170	6 207	2 2	27		ESP (SP	I=0x040001dc)			PRESENT								
12	55 448	7 192 168	2:192.108	25 ESD	170	5 309	2 2	27		ESP (SP	1=0x040001dc)											
54	55.450	97 192.168.	2: 192.168	28 ESP	170	5 309	2	27		ESP (SP	I=0x040001dc)											
55	55,452	96 192.168.	2:192.168	28 ESP	170	5 310	2	27		ESP (SP	I=0x040001dc)											
56	55.454	96 192.168.	2:192.168	.2EESP	170	5 311	2	27		ESP (SP	I=0x040001dc)											
57	55.455	97 192.168.	2:192.168	.2EESP	170	5 312	2 2	27		ESP (SP	I=0x040001dc)											
58	55.456	98 192.168.	2:192.168	.28 ESP	170	5 313	3 2	27		ESP (SP	I=0x040001dc)											
59	55.457	97 192.168.	2:192.168	.28 ESP	170	5 314	2	27		ESP (SP	I=0x040001dc)											
50	55.458	98 192.168.	2:192.168	.28 ESP	170	6 315	5 2	27		ESP (SP	I=0x040001dc)											
51	55.461	97 192.168.	2:192.168	.28 ESP	170	5 316	5 2	27		ESP (SP	l=0x040001dc)											
52	55.463	97 192.168.	2:192.168	.28 ESP	170	5 317	/ 2	27		ESP (SP	I=0x040001dc)											
53	55.465	96 192.168.	2:192.168	.28 ESP	170	5 318	3 2	27		ESP (SP	I=0x040001dc)											
54	55.466	97 192.168.	2:192.168	.28 ESP	176	5 319	2	27		ESP (SP	I=0x040001dc)											
55	55.467	96 192.168.	2:192.168	.28 ESP	170	5 320	) 2	27		ESP (SP	I=0x040001dc)											
56	55.469	96 192.168.	2:192.168	.28 ESP	170	6 321	1 2	27		ESP (SP	I=0x040001dc)											
57	55.470	97 192.168.	2:192.168	.2EESP	170	5 322	2 2	27		ESP (SP	I=0x040001dc)											
	J22 J	5.00257	172.100.	2: 172.100.	20 EOP		170	374	• 2	/		CON	r (3MI-0	X0400010	u)		Pho	DEINI				
	540 5	5.60496	192.168.2	2:192.168.	28 ESP		176	395	5 2	7		ESP	P (SPI=0	x040001d	c)		PRE	SENT				
	541 5	5.60596	192.168.2	2: 192.168.:	28 ESP		176	396	5 2	7		ESF	o (SPI=0	x040001d	c)		PRE	SENT				
	542 5	5.60696	192.168.2	2: 192.168.	28 ESP		176	397	7 2	7		ESP	(SPI=0	x040001d	c)		PRE	SENT				
	543 5	5.60696	192.168.2	2: 192.168.	28 ESP		176	398	3 2	7		ESF	P (SPI=0	x040001d	c)		PRE	SENT				
	544 5	5.60696	192.168.2	2: 192.168.	28 ESP		176	399	) 2	7		ESP	(SPI=0	x040001d	c)		PRE	SENT				
	545 5	5.60796	192.168.2	2: 192.168.	28 ESP		176	400	) 2	7		ESP	P (SPI=0	x040001d	c)		PRE	SENT				
	546 5	5.60796	192.168.	2: 192.168.	28 ESP		176	401	L 2	7		ESF	(SPI=0	x040001d	c)		PRE	SENT				
	547 5	5.60896	192.168.2	2: 192.168.	28 ESP		176	402	2 2	7		ESP	(SPI=0	x040001d	c)		PRE	SENT				
	548 5	5.60896	192.168.2	2: 192.168.	28 ESP		176	403	3 2	7		ESP	P (SPI=0	x040001d	c)		PRE	SENT				-
	549 5	5.60997	192.168.	2: 192.168.	28 ESP		176	404	1 2	7		ESF	P (SPI=0	x040001d	c)		PRE	SENT			-	-
	550 5	5.61096	192.168.2	2:192.168.	28 ESP		176	405	5 2	7		ESP	P (SPI=0	x040001d	c)		PRE	SENT				
							_//	100					10.100						-			

Blättern Sie zurück zum Anfang der Tabelle, und klicken Sie auf **COMPARE\_ESP\_SEQUENCE**. Wählen Sie dann **Sortieren & Filtern**.

) onal ng ~	Format as Table ~	Normal Neutral	Ba Ca Styles	d Iculation	Good Check C	Cell -	insert	Delete For Cells	mat γ	AutoSum Fill ~ Clear ~	× AZZ , Sort & F Filter × So	nd 8 lect 1
V	O COMPAF	P RE_ESP_SEC		R	S	Т	U	V	W	x	Y	

Wählen Sie Filter aus dem Dropdown-Menü aus.



In der Spalte COMPARE\_ESP\_SEQUENCE wird ein Dropdown-Menü angezeigt.

М	N	0	Р	
lumber		COMPA 💌	ESP_SEQ	JEN
		PRESENT		
		PRESENT		
		PRESENT		

Klicken Sie auf das Dropdown-Menü in der Überschrift **COMPARE\_ESP\_SEQUENCE**. Beachten Sie, dass in diesem Beispiel nur der Wert **PRESENT** angezeigt wird. Dies bedeutet, dass alle Pakete in beiden Erfassungen vorhanden sind.

	к	L	м	N	0	
c Inf	0	Sequence	Number		COMPA -	ESI
ES	2↓ s	ort A to Z				
ES ES	Z↓ S	ort Z to A				
ES	Sor	<u>t</u> by Color			>	
ES	She	eet <u>V</u> iew			>	
ES ES		lear Filter Fro	om "COMPA	RE_ESP_SEQ	UENCE"	
ES	Filt	er by Color			>	
ES	Tex	t <u>F</u> ilters			>	_
ES ES	Se	arch			Q	
ES		- ✓ (Select A	AII) T			
ES		PKESEN				
ES						
ES						
ES						
ES						
FS						

Um ein problematisches Beispiel zu erstellen, löschen Sie 10 Pakete aus dem CAP2\_slice, um zu zeigen, wie dies in einem Test funktionieren würde, bei dem einige verpasste Pakete fehlen.

11	4/2	01.01000 192.108.2: 192.108.28 F2h	1/0	315	27	ESP (SPI=0X0400010C)	
12	473	61.01806 192.168.23 192.168.28 ESP	176	316	27	ESP (SPI=0x040001dc)	
13	474	61.02106 192.168.23 192.168.28 ESP	176	317	27	ESP (SPI=0x040001dc)	
14	475	61.02205 192.168.23 192.168.28 ESP	176	318	27	ESP (SPI=0x040001dc)	
15	476	61.02306 192.168.23 192.168.28 ESP	176	319	27	ESP (SPI=0x040001dc)	
16	477	61.02506 192.168.23 192.168.28 ESP	176	320	27	ESP (SPI=0x040001dc)	
17	478	61.02605 192.168.23 192.168.28 ESP	176	321	27	ESP (SPI=0x040001dc)	
18	479	61.02805 192.168.23 192.168.28 ESP	176	322	27	ESP (SPI=0x040001dc)	
19	480	61.02906 192.168.23 192.168.28 ESP	176	323	27	ESP (SPI=0x040001dc)	
20	481	61.02906 192.168.23 192.168.28 ESP	176	324	27	ESP (SPI=0x040001dc)	
21	482	61.03005 192.168.23 192.168.28 ESP	176	325	27	ESP (SPI=0x040001dc)	
22	483	61.03206 192.168.23 192.168.28 ESP	176	326	27	ESP (SPI=0x040001dc)	
23	484	61.03306 192.168.23 192.168.28 ESP	176	327	27	ESP (SPI=0x040001dc)	
24	485	61.03505 192.168.23 192.168.28 ESP	176	328	27	ESP (SPI=0x040001dc)	
25	486	61.03606 192.168.23 192.168.28 ESP	176	329	27	ESP (SPI=0x040001dc)	
26	487	61.03905 192.168.23 192.168.28 ESP	176	330	27	ESP (SPI=0x040001dc)	
27	488	61.04105 192.168.23 192.168.28 ESP	176	331	27	ESP (SPI=0x040001dc)	
28	489	61.04206 192.168.23 192.168.28 ESP	176	332	27	ESP (SPI=0x040001dc)	
29	490	61.04406 192.168.23 192.168.28 ESP	176	333	27	ESP (SPI=0x040001dc)	
30	491	61.04606 192.168.23 192.168.28 ESP	176	334	27	ESP (SPI=0x040001dc)	
31	492	61.06305 192.168.23 192.168.28 ESP	176	335	27	ESP (SPI=0x040001dc)	
32	493	61.06505 192.168.23 192.168.28 ESP	176	336	27	ESP (SPI=0x040001dc)	
33	494	61.06705 192.168.23 192.168.28 ESP	176	337	27	ESP (SPI=0x040001dc)	
34	495	61.06905 192.168.23 192.168.28 ESP	176	338	27	ESP (SPI=0x040001dc)	
35	496	61.07105 192.168.23 192.168.28 ESP	176	339	27	ESP (SPI=0x040001dc)	
36	497	61.07105 192.168.23 192.168.28 ESP	176	340	27	ESP (SPI=0x040001dc)	
37	498	61.07205 192.168.23 192.168.28 ESP	176	341	27	ESP (SPI=0x040001dc)	
38	499	61.07605 192.168.23 192.168.28 ESP	176	342	27	ESP (SPI=0x040001dc)	
4	Þ	CAP1_slice CAP2_slice (+)					

Navigieren Sie zurück zum Blatt CAP1\_slice, und jetzt sehen Sie, dass 10 Pakete fehlen.

	33.43737 132.100		110	314	21	2011		I NEGERI	
460	55.45898 192.168	.2: 192.168.28 ESP	176	315	27	ESP (	SPI=0x040001dc)	PRESENT	
461	55.46197 192.168	.2: 192.168.28 ESP	176	316	27	ESP (	SPI=0x040001dc)	PRESENT	
462	55.46397 192.168	.2: 192.168.28 ESP	176	317	27	ESP (	SPI=0x040001dc)	PRESENT	
463	55.46596 192.168	.2: 192.168.28 ESP	176	318	27	ESP (	SPI=0x040001dc)	MISSING	
464	55.46697 192.168	.2: 192.168.28 ESP	176	319	27	ESP (	SPI=0x040001dc)	MISSING	
465	55.46796 192.168	.2: 192.168.28 ESP	176	320	27	ESP (	SPI=0x040001dc)	MISSING	
466	55.46996 192.168	.2: 192.168.28 ESP	176	321	27	ESP (	SPI=0x040001dc)	MISSING	
467	55.47097 192.168	.2: 192.168.28 ESP	176	322	27	ESP (	SPI=0x040001dc)	MISSING	
468	55.47198 192.168	.2: 192.168.28 ESP	176	323	27	ESP (	SPI=0x040001dc)	MISSING	
469	55.47297 192.168	.2: 192.168.28 ESP	176	324	27	ESP (	SPI=0x040001dc)	MISSING	
470	55.47497 192.168	.2: 192.168.28 ESP	176	325	27	ESP (	SPI=0x040001dc)	MISSING	
471	55.47597 192.168	.2: 192.168.28 ESP	176	326	27	ESP (	SPI=0x040001dc)	MISSING	
472	55.47697 192.168	.2: 192.168.28 ESP	176	327	27	ESP (	SPI=0x040001dc)	MISSING	
473	55.47896 192.168	.2: 192.168.28 ESP	176	328	27	ESP (	SPI=0x040001dc)	PRESENT	
474	55.48096 192.168	.2: 192.168.28 ESP	176	329	27	ESP (	SPI=0x040001dc)	PRESENT	

Wenn das Dropdown-Menü in der Spalte **COMPARE\_ESP\_SEQUENCE** ausgewählt wird, werden auch **FEHLENDE** Pakete angezeigt. Sie können diese Einstellung aktivieren, um nur die **FEHLENDEN** Pakete anzuzeigen.

	ĸ	L	M	N	0
nfe	0	Sequence	Number		
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		lear Filter Fro	m "COMPA	RE_ESP_SEQ	UENCE"
s	Filt	er by Color			>
S	Tex	t <u>F</u> ilters			>
S	Sea	arch			2
		(Select A I MISSING I PRESENT	<b>III)</b> F		
5			0	K	Cancel .:



Jetzt werden nur noch die fehlenden Pakete in der Excel-Tabelle angezeigt.

	Α	В	С	D	E	F	G	н		J	K	L	M	N	0	P
	No.	Time	Source	Destinati	c Protocol	Length	ESP Seque	Different	Source Po	Destinatio	Info	Sequence	Number		COMPA J	_ESP_SEQ
4	463	55.46596	192.168.23	192.168.2	ESP .	176	318	27			ESP (SPI:	=0x040001dc	)		MISSING	
5	464	55.46697	192.168.23	192.168.2	ESP .	176	319	27			ESP (SPI:	=0x040001dc	)		MISSING	
6	465	55.46796	192.168.23	192.168.2	ESP	176	320	27			ESP (SPI:	=0x040001dc	)		MISSING	
7	466	55.46996	192.168.23	192.168.2	ESP .	176	321	27			ESP (SPI:	=0x040001dc	)		MISSING	
8	467	55.47097	192.168.23	192.168.2	ESP .	176	322	27			ESP (SPI:	=0x040001dc	)		MISSING	
9	468	55.47198	192.168.23	192.168.2	8 ESP	176	323	27			ESP (SPI:	=0x040001dc	)		MISSING	
0	469	55.47297	192.168.23	192.168.2	ESP	176	324	27			ESP (SPI:	=0x040001dc	)		MISSING	
1	470	55.47497	192.168.23	192.168.2	ESP 8	176	325	27			ESP (SPI:	=0x040001dc	)		MISSING	
2	471	55.47597	192.168.23	192.168.2	ESP .	176	326	27			ESP (SPI:	=0x040001dc	)		MISSING	
3	472	55.47697	192.168.23	192.168.2	ESP	176	327	27			ESP (SPI:	=0x040001dc	)		MISSING	
)2																
)3																

# Zugehörige Informationen

- Integrierte Paketerfassung von Cisco
- Technischer Support und Dokumentation für Cisco Systeme

#### Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.