

Switch-Konfiguration für passive VoIP-Aufzeichnung



Administrationsanleitung für Systembetreiber

08.09.2021

Originalanleitung

Produktlinie neo, Version 6.x

Die beschriebenen Funktionen können mit folgenden ASC-Produkten verwendet werden:

EVOIPneo

Im Partnerbereich unserer Webseite <http://www.asctechnologies.com> finden Sie immer die aktuellsten technischen Dokumente und Produktaktualisierungen.

Copyright © 2021 ASC Technologies AG. Alle Rechte vorbehalten.

Windows ist ein eingetragenes Markenzeichen der Microsoft Corporation. VMware® ist ein eingetragenes Markenzeichen von VMware, Inc. Alle anderen hier erwähnten Marken und Produktnamen sind das Eigentum ihrer jeweiligen Inhaber.

Inhaltsverzeichnis

| | | |
|----------|---|-----------|
| 1 | Allgemeine Hinweise | 4 |
| 2 | Einleitung | 5 |
| 3 | Konfiguration..... | 6 |
| 3.1 | Anzahl der zu überwachenden Geräte..... | 6 |
| 3.1.1 | Überwachung eines Quellports | 6 |
| 3.1.2 | Überwachung mehrerer Quellports | 6 |
| 3.2 | Konfiguration mit einem Switch | 7 |
| 3.2.1 | Beispielkonfiguration: Cisco Catalyst | 7 |
| 3.3 | Konfiguration mit mehreren Switchen | 8 |
| 3.3.1 | Cisco Catalyst | 8 |
| 3.4 | Netzwerkkarte | 9 |
| 3.4.1 | Verwendung mehrerer Netzwerkkarten | 9 |
| 3.5 | Device Filter/Filter Presets | 9 |
| | Abbildungsverzeichnis | 11 |
| | Tabellenverzeichnis | 12 |
| | Glossar | 13 |

Allgemeine Hinweise

ASC steht im Kontext dieses Dokuments für die ASC Technologies AG, deren Tochtergesellschaften, Niederlassungen und Vertriebsbüros. Deren aktuelle Übersicht kann auf der Webseite unter <https://www.asctechnologies.com> eingesehen werden.

ASC übernimmt keinerlei Gewähr für die Aktualität, Korrektheit, Vollständigkeit oder Qualität der in den Anleitungen bereitgestellten Informationen.

ASC kontrolliert regelmäßig den Inhalt der veröffentlichten Anleitungen auf Übereinstimmung mit der beschriebenen Hard- und Software. Dennoch können Abweichungen nicht ausgeschlossen werden. Notwendige Korrekturen sind in den nachfolgenden Auflagen enthalten.

Einige Aspekte der ASC-Technologie werden in allgemeiner Form beschrieben, um das Eigentum und die vertraulichen Informationen und/oder Geschäftsgeheimnisse von ASC zu schützen.

Die Softwareprogramme und Anleitungen von ASC sind urheberrechtlich geschützt. Alle Rechte an den Anleitungen sind vorbehalten, auch die der Reproduktion und/oder Vervielfältigung in jeglicher Form, sei es fotomechanisch, drucktechnisch oder auf digitalen Datenträgern. Dies gilt auch für Übersetzungen. Nachdruck der Anleitungen, vollständig oder auszugsweise, ist nur mit schriftlicher Genehmigung von ASC gestattet.

Maßgebend ist, soweit nicht anders angegeben, der technische Stand zum Zeitpunkt der Auslieferung von Software, Geräten und Anleitungen durch ASC. Technische Änderungen ohne gesonderte Ankündigung bleiben vorbehalten. Bisherige Anleitungen verlieren ihre Gültigkeit.

Es gelten die Allgemeinen Verkaufs- und Lieferbedingungen von ASC in ihrer jeweils gültigen Fassung.

Die EVOIP_{neo} passive-Software stellt eine passive Lösung zur Aufzeichnung von VoIP-Gesprächen dar. Um Audiodaten empfangen zu können, muss lediglich ein Rechner mit EVOIP_{neo} passive-Software an das gewünschte Netzwerk angeschlossen werden. Dies ist die einfachste Möglichkeit der Gesprächsaufzeichnung.

Der Anschluss des EVOIP_{neo}-Aufzeichnungssystems kann über unterschiedlichste Geräte und in den verschiedensten Netzwerkarchitekturen erfolgen. Neben allgemeinen Informationen enthält das Dokument kurze Beschreibungen der gängigsten Netzwerkgeräte und deren unterschiedliche Netzwerkkonfigurationen.

Für den Anschluss des EVOIP_{neo}-Aufzeichnungssystems eignen sich nur Switches, welche die Funktionen Portspiegelung, **SPAN** (Switched Port Analyzing) oder **RSPAN** (Remote SPAN) unterstützen. Durch die Aktivierung einer dieser Funktionen kann der Datenstrom einer oder mehrerer Ports auf einen speziellen Port kopiert werden. An diesem Port ist der EVOIP_{neo}-Server angeschlossen.

Die Praxis hält jedoch kompliziertere Netzwerkstrukturen bereit, in denen z. B. verschiedene Switches miteinander verbunden sind.

Die folgenden Abschnitte enthalten die verschiedenen Switches, die mit dem EVOIP_{neo}-Aufzeichnungssystem betrieben werden können, sowie deren typische Konfigurationen und Einstellungen.

Unterstützung der **SPAN**-Funktion

So gut wie alle Cisco Catalyst Switches unterstützen die **SPAN**-Funktion. Beispielsweise unterstützt der Catalyst 6500 sowohl **RSPAN** als auch **SPAN**.



Einzelheiten zu eventuellen Einschränkungen der SPAN- und RSPAN-Eigenschaften finden Sie in den Benutzerhandbüchern der jeweiligen Switches.

Funktionsmerkmale Catalyst 6500

- RSPAN- oder SPAN-Sessions möglich
- Überwachung des gesamten VLAN, mehrere Ports
- Ausschließliche Überwachung des RX-Datenstroms eines gesamten VLAN
- Überwachung der RX- und TX-Datenströme nur eines Ports



Diese Switches eignen sich sehr gut für die passive Gesprächsaufzeichnung mit EVOIP_{neo}-Aufzeichnungssystemen. Es stehen viele Konfigurationsmöglichkeiten zur Verfügung, mit denen ein breites Spektrum von Netzwerkarchitekturen abgedeckt wird.



Weitere Informationen zur Switch-Konfiguration finden Sie in der Installationsanleitung *Konfiguration Virtualisierung*.

3 Konfiguration

3.1 Anzahl der zu überwachenden Geräte

Abhängig von der Anzahl der Quellports, die überwacht werden sollen, sind unterschiedliche Konfigurationseinstellungen notwendig.

3.1.1 Überwachung eines Quellports

Wird nur ein Quellport für das Sammeln von Daten verwendet, so handelt es sich um eine gatewayseitige Aufzeichnung aller externen Gespräche. In diesem Fall ist das Gateway an Ihren Quellport anzuschließen. Darüber hinaus besteht auch die Möglichkeit, ein einziges IP-Telefon an den Quellport anzuschließen, der aufgezeichnet werden soll.

Um alle Daten aufzuzeichnen, muss der Quellport so konfiguriert werden, dass beide Datenrichtungen des Quellports, d. h. sowohl die **RX**- als auch die **TX**-Richtung, aufgezeichnet werden. Ansonsten wird nur eine Gesprächsrichtung aufgenommen.

Bei der EVOIP_{neo}-Konfiguration ist unbedingt darauf zu achten, Gateways als *Non Phone IPs* zu definieren.

Beispiel:

Ein VoIP-Gateway ist an den Port 23 mit der IP-Adresse 192.168.1.15 angeschlossen. Der EVOIP_{neo}-Server ist an die Ports 10 und 11 angeschlossen. Die Überwachung soll über die Netzwerkkarte erfolgen, die an den Port 10 angeschlossen ist.

- Einstellungen am Switch
Überwachung des Ports 23 RX und TX
Zielport 10
- Einstellungen am EVOIP_{neo}-Aufzeichnungssystem
Non Phone IP: 192.168.1.15
Aktivierung der Netzwerkkarte, die an den Port 10 für die Datenüberwachung angeschlossen ist.

3.1.2 Überwachung mehrerer Quellports

Wird ein VLAN als Quelle verwendet, so stehen im Allgemeinen mehrere Quellports zur Verfügung.

Wenn mehrere Quellports eingesetzt werden, um die Audiodaten verschiedener IP-Telefone aufzuzeichnen, ist der Switch folgendermaßen zu konfigurieren.

Um das Duplizieren von Paketen zu vermeiden, ist die Konfiguration des Quellports so vorzunehmen, dass nur die Daten einer Richtung an den Zielport oder das RSPAN-VLAN kopiert werden. Dabei handelt es sich normalerweise um die Empfangsrichtung (**RX**) jedes Quellports.



Die Richtungen verschiedener Quellports dürfen nicht gemischt werden.

Um Gespräche mit beiden Gesprächsrichtungen aufzuzeichnen, müssen die folgenden Geräte als Quellports oder innerhalb des Quell-VLANs verwendet werden:

- Ports, an die IP-Telefone angeschlossen sind, die aufgezeichnet werden sollen
- Ports, an die IP-Telefone angeschlossen sind, die nicht aufgezeichnet werden sollen, die jedoch mit Geräten kommunizieren könnten, die aufgezeichnet werden sollen (ist dies nicht gewährleistet, so wird bei Verbindungen zwischen einem IP-Telefon, das von einem Switch überwacht wird, und einem IP-Telefon, das nicht überwacht wird, nur eine Gesprächsrichtung aufgezeichnet. Der Gesprächsteil des nicht überwachten Geräts wird nicht aufgezeichnet.)
- Ports, an die ein VoIP-Gateway angeschlossen ist, um externe Gespräche zu erhalten

- Ports, an die eine Conference Bridge (bei Cisco im Allgemeinen der CCM) angeschlossen ist

Die folgenden Ports sollten nicht als Quellports konfiguriert werden, auch nicht im zu überwachenden Quell-VLAN:

- Ports, die andere Switches verbinden, wenn der andere Switch über ein eigenes SPAN (Trunks) verfügt
- Ports, an die keine IP-Telefone angeschlossen sind (diese Ports sollten aus dem VLAN ausgeschlossen werden, das als Quelle für die Überwachung konfiguriert ist)

3.2 Konfiguration mit einem Switch

Dieses Beispiel beschreibt die Konfiguration eines Switches mit verschiedenen VLANs. VLAN 1 und VLAN 3 enthalten ausschließlich IP-Telefone. VLAN 2 ist ein reines Datennetzwerk für PCs. Das EVOIP_{neo}-Aufzeichnungssystem ist mit mindestens zwei Netzwerkkarten (NICs) bestückt. Die erste Netzwerkkarte wird für die Aufzeichnung von Audiodaten verwendet (die Aufzeichnungs-NIC), und die zweite dient der Erreichbarkeit des EVOIP_{neo}-Aufzeichnungssystems über das Netzwerk - z. B. für Administrationszwecke oder für Wiedergabeapplikationen wie *PO-WERplay* Web. Diese separate Netzwerkkarte ist erforderlich, da der für die Gesprächsaufzeichnung konfigurierte Switch-Port keinen allgemeinen Netzzugang zur Verfügung stellt.

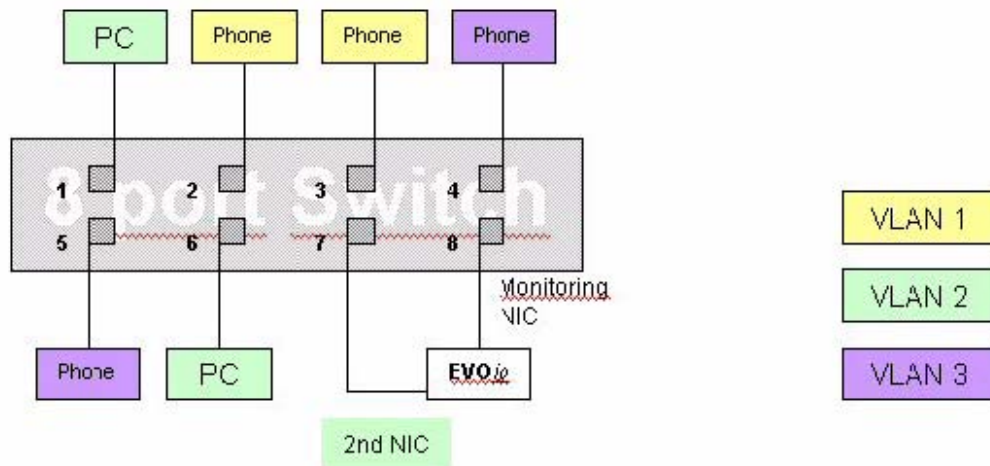


Abb. 1: Anschlussbeispiel

Für die Aufzeichnung spezieller IP-Telefone aus VLAN 1 und VLAN 3 müssen die Überwachungsports folgendermaßen konfiguriert werden:

3.2.1 Beispielkonfiguration: Cisco Catalyst

Möglichkeiten der Konfiguration:

- VSPAN-Session:
 - Überwachung von VLAN1 und VLAN 3 nur RX
 - Zielport 8
- SPAN-Session:
 - Portüberwachung – Quellports : 2, 3, 4, 5 alle nur RX
 - Zielport 8

3.3 Konfiguration mit mehreren Switchen

Sind in Ihrem Unternehmen mehrere Switches vorhanden, an denen zu überwachende Geräte angeschlossen sind, so können Sie entweder die im vorhergehenden Abschnitt beschriebene Konfiguration für einen Switch verwenden, wenn Sie für jeden Switch eine separate Überwachungsnetzwerkkarte einbauen, oder Sie können die einzelnen Switches so konfigurieren, dass sie zusammenarbeiten.

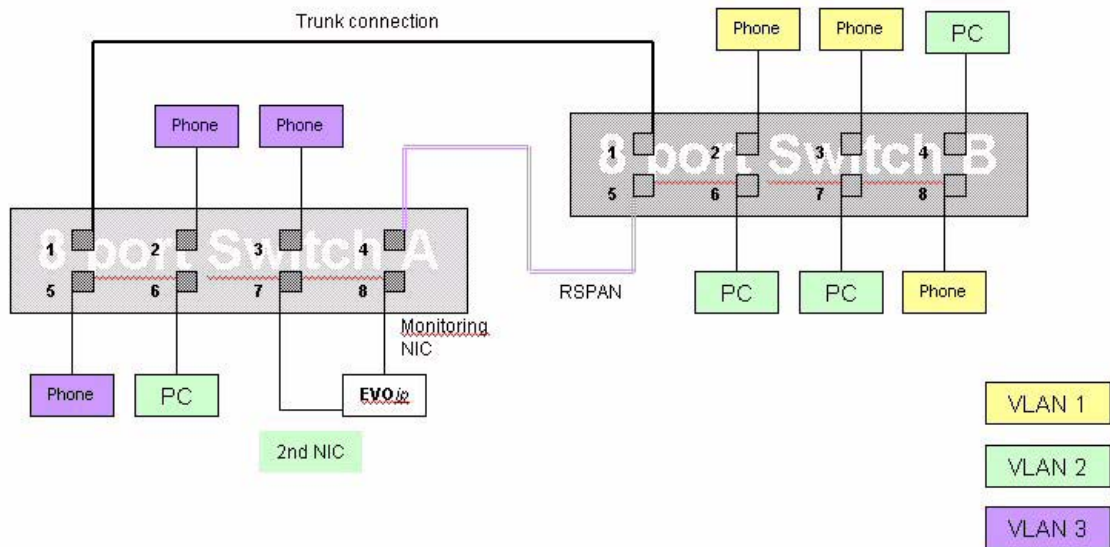


Abb. 2: Anschlusskonfiguration mit mehreren Switchen

3.3.1 Cisco Catalyst

RSPAN

Switch A ist an das EVOIPneo-Aufzeichnungssystem angeschlossen. Die IP-Telefone, deren Gespräche mit dem EVOIPneo-Aufzeichnungssystem aufgezeichnet werden sollen, sind sowohl an Switch A als auch an Switch B angeschlossen. Um die Gespräche aller IP-Telefone aufzeichnen zu können, müssen die relevanten Daten von Switch B nach Switch A übertragen werden. Dies wird über eine RSPAN-Session erreicht. Eine RSPAN-Session kann so konfiguriert werden, dass entweder einzelne Ports oder gesamte VLANs überwacht werden.

Es ist nicht möglich, ein gesamtes VLAN als Quelle für eine RSPAN-Session auszuwählen, da es aufgrund der Trunk-Leitung zu gedoppelten Paketen kommen würde. Vielmehr muss jeder einzelne Port separat als Quelle ausgewählt werden.

Um den gesamten Datenverkehr der Gesprächs-VLANs 1 und 3 über die Überwachungs-NIC des EVOIPneo-Aufzeichnungssystems zu leiten, müssen die Switches folgendermaßen konfiguriert werden:

Switch A

RSPAN-Session

- Portüberwachung – RSPAN Quellports: 2, 3, 4, 5 alle nur RX, dem RSPAN VLAN 300 hinzugefügt
- Festlegen des Zielports für RSPAN VLAN 300, im obigen Beispiel Port 8

Switch B

RSPAN-Session

- Konfiguration eines neuen VLAN für RSPAN – z. B. VLAN 300

- Portüberwachung – RSPAN Quellports für das gewählte VLAN: 2, 3, 8 **alle nur RX** des Switches B
- Festlegen des RSPAN-Zielports, im obigen Beispiel Port 5

3.4 Netzwerkkarte

3.4.1 Verwendung mehrerer Netzwerkkarten



Wenn im System eine Netzwerkkarte als Sniffer Device konfiguriert wird, an der kein Netzkabel angeschlossen ist, bleibt das "EVOIP_{neo} passive"-Modul nach einer Änderung der "EVOIP_{neo} passive"-Konfiguration inaktiv.

Alle Netzwerkkarten, die für die Aufzeichnung von Audiodaten verwendet werden sollen, müssen in einem noch nicht existierenden Subnetz betrieben werden. Anderenfalls kann es zu Problemen kommen, wenn auf den EVOIP_{neo}-Server zu Administrationszwecken oder zur Gesprächswiedergabe zugegriffen wird.

Beispiel für eine Konfiguration:

Das Unternehmen verwendet die folgenden Netzwerkadressen:

192.168.1.0 bis 192.168.1.255 und

192.168.50.0 bis 192.168.50.255

Der EVOIP_{neo}-Server mit drei Netzwerkkarten soll den Datenverkehr beider Subnetze überwachen. Damit die Überwachungsnetzwerkkarten alle erforderlichen Daten erhalten, können diese auf jede IP-Adresse eingestellt werden, ohne dabei ein Standard-Gateway zu verwenden.

NIC1 (Überwachungsnetzwerkkarte):

IP-Adresse: 1.1.1.1 oder jede andere, abgesehen von den bereits vorhandenen Subnetzen 192.168.1.x und 192.168.50.x

Subnetz: 255.255.255.0

Standard-Gateway: keins

NIC2 (Überwachungsnetzwerkkarte):

IP-Adresse: 1.1.1.2 oder jede andere, abgesehen von den bereits vorhandenen Subnetzen 192.168.1.x und 192.168.50.x

Subnetz: 255.255.255.0

Standard-Gateway: keins

NIC3 (für den Datenaustausch):

IP-Adresse: 192.168.1.73 oder jede beliebige IP-Adresse im bestehenden Netzwerk

Subnetz: 255.255.255.0, abhängig von den Netzwerkadressen, die in diesem Subnetz verwendet werden

Standard-Gateway: 192.168.1.254, das Gateway, über welches das andere Subnetz erreicht werden kann

Achten Sie darauf, dass keine andere Netzwerkkarte das gleiche Standard-Gateway benutzt, da sonst keine spezielle NIC für das Senden von Daten definiert ist.

3.5 Device Filter/Filter Presets

Diese Werte müssen normalerweise nicht geändert werden. In manchen Fällen ist es jedoch notwendig, einige Werte hinzuzufügen, um Fehler oder falsche Aufzeichnungen zu vermeiden.

Verwendung von NORTEL IP-Telefonen

Um zu verhindern, dass interne Meldungen als Gespräche interpretiert werden, ist der Filter String für Ihre Netzwerkkarten folgendermaßen zu ändern:

(ip and udp and !(port 16550)) oder

(vlan and ip and udp and !(port 16550))

Abbildungsverzeichnis

| | | |
|--------|--|---|
| Abb. 1 | Anschlussbeispiel..... | 7 |
| Abb. 2 | Anschlusskonfiguration mit mehreren Switchen | 8 |

Tabellenverzeichnis

Glossar

NIC

Network Interface Card

RSPAN

Remote Switched Port Analyzing

RX

Receiver, Empfänger, RX ist die Bezeichnung für einen Empfänger bzw. für das Empfangen einer Funksendung im Funkverkehr oder von Computer-Daten (Herunterladen); Rx steht für den englischsprachigen Begriff Receiver, wobei das x als „Kürzel“ für die Buchstaben nach dem R anzusehen ist

SPAN

Switched Port Analyzing

TX

Transmitter, Sender, TX ist die Bezeichnung für einen Sender bzw. für das Senden einer Funksendung im Funkverkehr oder von Computer-Daten; Tx steht für den englischsprachigen Begriff Transmitter wobei das x als „Kürzel“ für die Buchstaben nach dem T anzusehen ist

VSPAN

VLAN Virtual Local Area Network; SPAN Switched Port Analyzing