

Configura convalida porta di origine RTP

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Premesse](#)

[Controllo configurazione:](#)

[Procedura di configurazione](#)

[Verifica](#)

[Risoluzione dei problemi](#)

[Ulteriori riferimenti](#)

Introduzione

In questo documento viene descritto come abilitare la convalida della porta di origine del protocollo RTP (Real Time Protocol) per evitare problemi di qualità vocale come i crosstalk.

Prerequisiti

Requisiti

IOS versione 12.4(6)T o successive.

Componenti usati

Il documento può essere consultato per tutte le versioni software o hardware.

Attenzione: le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Premesse

I chiamanti PSTN (Public Switch Telephone Network) hanno flussi di chiamate interstallate o miste:

Telefoni IP — Cisco Unified Communications Manager (CUCM) — Session Initiation Protocol (SIP) IOS Gateway — PSTN

Questo problema può verificarsi quando il gateway riceve un flusso RTP non valido destinato allo stesso indirizzo IP e alla stessa porta di una chiamata attiva.

Il flusso non valido ha una porta e un indirizzo IP di origine diversi da quelli negoziati tramite il protocollo SDP (SIP Session Description Protocol).

Controllo configurazione:

Verifica se:

a) Viene utilizzato il getto a forello:

```
dial-peer voice x voip
session protocol multicast
```

[Definizione CLI](#)

Questo comando viene utilizzato per le configurazioni delle conferenze vocali in un'implementazione di rete hoot and holler. Questo comando consente a più di due porte di accedere contemporaneamente alla stessa sessione.

b) Se il SIP è configurato:

```
dial-peer voice x voip
session protocol sipv2
```

[Definizione CLI](#)

Procedura di configurazione

Configurare i seguenti comandi:

```
voice service voip
sip
source filter
```

Questo comando elimina il rischio di crosstalk poiché il gateway blocca tutto l'audio non autorizzato da un'origine sconosciuta.

Nota: il comando precedente funziona solo per SIP, quindi H323, Media Gateway Control Protocol (MGCP) e Skinny Client Control Protocol (SCCP) sono ancora influenzati.

Esempio di configurazione:

```
voice service voip
```

```
allow-connections sip to sip
sip
bind control source-interface loopback0
bind media source-interface loopback0
source filter
```

```
dial-peer voice 2001 voip
destination-pattern 79...
session protocol sipv2
session target ipv4:172.16.32.21
incoming called-number .
voice-class codec 1
dtmf-relay rtp-nte
```

Verifica

Attualmente non è disponibile una procedura di verifica per questa configurazione.

Risoluzione dei problemi

Al momento non sono disponibili informazioni specifiche per la risoluzione dei problemi di questa configurazione.

[Ulteriori riferimenti](#)