



## Monitoring of Phantom Packets

---

The Monitoring of Phantom Packets feature allows you to configure port ranges specific to the VoIP Real-Time Transport Protocol (RTP) layer. This allows the VoIP RTP layer to safely drop packets without proper sessions (phantom packets) received on these ports of the Cisco Unified Border Element (CUBE) or Voice time-division multiplexing (TDM) gateways. Because the ports are configured specifically for the VoIP RTP layer, there is no need to punt the packets to the RP (control plane) in case the packets were intended for some other application, thus reducing performance issues.

- [Restrictions of Monitoring of Phantom Packets, page 1](#)
- [Information About Monitoring of Phantom Packets, page 2](#)
- [How to Configure Monitoring of Phantom Packets, page 2](#)
- [Configuration Examples For Monitoring of Phantom Packets, page 3](#)
- [Additional References for Configurable Pass-Through of SIP INVITE Parameters, page 4](#)
- [Feature Information for Monitoring of Phantom Packets, page 4](#)

## Restrictions of Monitoring of Phantom Packets

- The authentication, authorization, and accounting (AAA) default port range of 21645 to 21844 must not be configured.
- Up to ten port range entries can be defined under a single media-address range.
- The minimum port must be numerically lower than the maximum port.
- Port ranges should not overlap.
- Address ranges should not overlap.
- Address ranges and single addresses should not overlap
- Where a range of addresses are defined in a single command, they will share any port ranges assigned. If there is a requirement to have different port ranges for different media addresses, then the addresses must be configured separately.
- The interface used for media and signaling should be different.

- The media address and the signaling address should not be identical. If the media address and the signaling address are identical, and the Cisco IOS XE based router platform (Cisco ASR 1000 Series Aggregation Services Router, Cisco 4000 Series Integrated Services Routers, or Cisco Cloud Services Router 1000V Series) selects an ephemeral port to send out signaling packets, the port may overlap with the port range of the media address. As a result, the signaling packets do not get punted up to the RP, and get dropped by the media packet filter. This may result in events such as incomplete TCP handshakes during the second leg of a call through CUBE or Voice Gateways.

## Information About Monitoring of Phantom Packets

### Monitoring of Phantom Packets

The Monitoring of Phantom Packets feature allows you to configure port ranges specific to the VoIP Real-Time Transport Protocol (RTP) layer. This configuration allows the VoIP RTP layer to safely drop packets without proper sessions (phantom packets) received on the ports of the Cisco Unified Border Element (CUBE) or Voice time-division multiplexing (TDM) gateways. Because the ports are configured specifically for the VoIP RTP layer, there is no need to punt the packets to the UDP process in case the packets were intended for some other application, thus reducing performance issues.

A phantom packet is a valid RTP packet meant for the CUBE or Voice TDM gateway without an existing session on the respective gateways. When a phantom packet is received by the VoIP RTP layers of the gateways, the packet is punted to the UDP process to check if it is required by any other applications causing performance issues, especially when a large number of such packets are received. A malicious attacker can also send a large number of phantom packets. The packet is punted to the UDP process because UDP port ranges are shared by many applications other than VoIP RTP and the VoIP RTP layer cannot drop the packet assuming the packet is for itself.

This feature allows you to configure port ranges specific to the VoIP RTP layer. If a phantom packet is received on the configured port, the VoIP RTP layer can safely drop the packet. If a phantom packet is received on any other port, the VoIP RTP layer punts the packet to the UDP process.

## How to Configure Monitoring of Phantom Packets

### Configuring Monitoring of Phantom Packets

#### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **voice service voip**
4. **media-address range** *starting-ip-address ending-ip-address*
5. **port-range** *starting-port-number ending-port-number*
6. **end**

## DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>enable</b>  <b>Example:</b> Device> <b>enable</b>	Enables privileged EXEC mode.
Step 2	<b>configure terminal</b>  <b>Example:</b> Device# <b>configure terminal</b>	Enters global configuration mode.
Step 3	<b>voice service voip</b>  <b>Example:</b> Device(config)# <b>voice service voip</b>	Specifies VoIP encapsulation and enters voice-service configuration mode.
Step 4	<b>media-address range</b> <i>starting-ip-address ending-ip-address</i>  <b>Example:</b> Using IPv4 addresses: Device(conf-voi-serv)# <b>media-address range</b> 10.1.1.1 10.1.1.254  <b>Example:</b> Using IPv6 addresses: Device(conf-voi-serv)# <b>media-address range</b> 2001:DB8:1::1 2001:DB8:1::17	Configures an IPv4 or IPv6 media address range.
Step 5	<b>port-range</b> <i>starting-port-number ending-port-number</i>  <b>Example:</b> Device(cfg-media-addr-range)# <b>port-range</b> 32766 32768	Configures a port range.
Step 6	<b>end</b>  <b>Example:</b> Router(cfg-media-addr-range)# <b>end</b>	Exits voice-service configuration mode and returns to privileged EXEC mode.

## Configuration Examples For Monitoring of Phantom Packets

```
Device(config)# voice service voip
Device(conf-voi-serv)# media-address range 10.1.1.1 10.1.1.254
Device(cfg-media-addr-range)# port-range 32766 32768
Device(cfg-media-addr-range)# port-range 16384 16386
Device(cfg-media-addr-range)# exit
```

```
Device(conf-voi-serv)# media-address range 2001:DB8:1::1 2001:DB8:1::17
Device(cfg-media-addr-range)# port-range 32766 32768
Device(cfg-media-addr-range)# port-range 16384 16386
Device(cfg-media-addr-range)# end
```

# Additional References for Configurable Pass-Through of SIP INVITE Parameters

## Related Documents

Related Topic	Document Title
Voice commands	<a href="#">Cisco IOS Voice Command Reference</a>
Cisco IOS commands	<a href="#">Cisco IOS Master Command List, All Releases</a>
SIP configuration tasks	<a href="#">SIP Configuration Guide, Cisco IOS Release 15M&amp;T</a>

## Technical Assistance

Description	Link
<p>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.</p> <p>To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds.</p> <p>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</p>	<a href="http://www.cisco.com/support">http://www.cisco.com/support</a>

## Feature Information for Monitoring of Phantom Packets

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to [www.cisco.com/go/cfn](http://www.cisco.com/go/cfn). An account on Cisco.com is not required.

**Table 1: Feature Information for Monitoring of Phantom Packets**

Feature Name	Releases	Feature Information
Monitoring of Phantom Packets	Cisco IOS XE Release 3.9S 15.4(1)T	<p>This feature allows you to configure port ranges specific to the VoIP Real-Time Transport Protocol (RTP) layer and drop phantom RTP packets (RTP packets that are configured in valid port range but for which there is no matching call or session).</p> <p>The following commands were introduced: <b>port-range</b>, <b>media-address range</b>.</p>

