Monitoring of Phantom Packets

Overview

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, punting the packets to UDP process is not required. This helps in reducing the performance issues.

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.

It is recommend that you configure the IP address and port ranges specific to the media IP addresses, even if you are using a single virtual IP address for media. 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.

Feature Information

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. 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	Baseline functionality	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).

Restrictions

- The authentication, authorization, and accounting (AAA) default port range of 21645–21844 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 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.

Configure 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* **port range** *starting-port-number ending-port-number*

5. **port-range** *starting-port-number ending-port-number*
6. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**voice service voip** **Example:** `Device(config)# voice service voip`	Specifies VoIP encapsulation and enters voice-service configuration mode.

Step 4	**media-address range** *starting-ip-address ending-ip-address* **port range** *starting-port-number ending-port-number*
	Example:
	Using IPv4 addresses:
	For single IP:
	`Device(conf-voi-serv)# media-address range 10.1.1.1 10.1.1.1`
	For a range of IPs:
	`Device(conf-voi-serv)# media-address range 10.1.1.1 10.1.1.254`
	Example:
	Using IPv6 addresses:
	For single IP:
	`Device(conf-voi-serv)# media-address range 2001:DB8:1::1 2001:DB8:1::1`
	For a range of IPs:
	`Device(conf-voi-serv)# media-address range 2001:DB8:1::1 2001:DB8:1::17`
	Example:
	Port range for media address.
	`Device(cfg-media-addr-range)# port-range 8000 48198`
		Configures an IPv4 or IPv6 media address range. And, creates a port range for the configured media addresses.
		Note If you do not configure any port range, the default port range is applied. The default port range is 8000-48198 for ASR and ISR G3 platforms.

Step 5	**port-range** *starting-port-number ending-port-number* **Example:**	Configures a port range. If you do not configure any port range nothing is applied.

	Command or Action	Purpose
	`Device(cfg-media-addr-range)# port-range 8000 48198`	**Note** Ensure that the port range is not greater than the port range (if configured) specified in the media-address range command.
Step 6	**end** **Example:** `Router(cfg-media-addr-range)# end`	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 8000 21643
Device(cfg-media-addr-range)# port-range 21846 48000
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 8000 21643
Device(cfg-media-addr-range)# port-range 21846 48000
Device(cfg-media-addr-range)# end
```

Note The ports 21643–21845 are not used by the RTP layer. They might be used by applications such as AAA/Radius. These ports are allowed to be punted to the control plane if needed.

Additional References for Configurable Pass-Through of SIP INVITE Parameters

Related Documents

Related Topic	Document Title
Voice commands	Cisco IOS Voice Command Reference
Cisco IOS commands	Cisco IOS Command List, All Releases
SIP configuration tasks	SIP Configuration Guide, Cisco IOS Release 15M&T

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. 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. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/support