



IP Addressing: Fragmentation and Reassembly Configuration Guide, Cisco IOS XE Release 3S (Cisco ASR 1000)

Americas Headquarters

Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
<http://www.cisco.com>
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

© 2012 Cisco Systems, Inc. All rights reserved.



CONTENTS

| | |
|---|-----------|
| Virtual Fragmentation Reassembly | 1 |
| Finding Feature Information | 1 |
| Restrictions for Virtual Fragmentation Reassembly | 1 |
| Performance Impact | 1 |
| VFR Configuration Restriction | 2 |
| Information About Virtual Fragmentation Reassembly | 2 |
| VFR Detection of Fragment Attacks | 2 |
| VFR Enablement | 2 |
| VFR on Outbound Interfaces | 3 |
| How to Configure Virtual Fragmentation Reassembly | 3 |
| Configuring VFR | 3 |
| Enabling VFR Manually on Outbound Interface Traffic | 4 |
| Troubleshooting Tips | 6 |
| Configuration Examples for Fragmentation Reassembly | 6 |
| Example Configuring VFR on Outbound Interface Traffic | 6 |
| Additional References | 6 |
| Feature Information for Virtual Fragmentation Reassembly | 7 |
| IPv6 Virtual Fragmentation Reassembly | 9 |
| Finding Feature Information | 9 |
| Information About IPv6 Virtual Fragmentation Reassembly | 9 |
| IPv6 Virtual Fragmentation Reassembly | 9 |
| How to Implement IPv6 Virtual Fragmentation Reassembly | 9 |
| Configuring IPv6 Virtual Fragmentation Reassembly | 10 |
| Configuration Example for IPv6 Virtual Fragmentation Reassembly | 11 |
| Example: Configuring IPv6 Virtual Fragmentation Reassembly | 11 |
| Additional References | 12 |
| Feature Information for IPv6 Virtual Fragmentation Reassembly | 12 |
| GRE Fragment and Reassembly Performance Tuning | 15 |
| Finding Feature Information | 15 |

- Restrictions for GRE Fragment and Reassembly 15
- Information About GRE Fragment and Reassembly 15
 - Fragmentation and Reassembly 16
- How to Use GRE Fragment and Reassembly 16
 - Configuring GRE Fragment and Reassembly (GFR) 16
- Configuration Examples for GRE Fragment and Reassembly 18
 - Example: Configuring GFR 18
- Additional References for GRE Fragment and Reassembly 18
- Feature Information for GRE Fragment and Reassembly 19



Virtual Fragmentation Reassembly

Virtual fragmentation reassembly (VFR) enables the Cisco IOS Firewall to create the appropriate dynamic access control lists (ACLs) to protect the network from various fragmentation attacks.

Without VFR, the Cisco IOS Firewall--specifically Context-based Access Control (CBAC) and the Intrusion Detection System (IDS)--cannot identify the contents of the IP fragments nor can it gather port information from the fragment. These inabilities allow the fragments to pass through the network without being examined or without dynamic ACL creation.

- [Finding Feature Information, page 1](#)
- [Restrictions for Virtual Fragmentation Reassembly, page 1](#)
- [Information About Virtual Fragmentation Reassembly, page 2](#)
- [How to Configure Virtual Fragmentation Reassembly, page 3](#)
- [Configuration Examples for Fragmentation Reassembly, page 6](#)
- [Additional References, page 6](#)
- [Feature Information for Virtual Fragmentation Reassembly, page 7](#)

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see [Bug Search Tool](#) and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

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.

Restrictions for Virtual Fragmentation Reassembly

- [Performance Impact, page 1](#)
- [VFR Configuration Restriction, page 2](#)

Performance Impact

VFR causes a performance impact on the basis of functions such as packet copying, fragment validation, and fragment reorder. This performance impact varies depending on the number of concurrent IP datagrams that are being reassembled.

VFR Configuration Restriction

VFR should not be enabled on a router that is placed on an asymmetric path. The reassembly process requires all of the fragments within an IP datagram. Routers placed in the asymmetric path may not receive all of the fragments, so the fragment reassembly will fail.

Information About Virtual Fragmentation Reassembly

- [VFR Detection of Fragment Attacks, page 2](#)
- [VFR Enablement, page 2](#)
- [VFR on Outbound Interfaces, page 3](#)

VFR Detection of Fragment Attacks

VFR is responsible for detecting and preventing the following types of fragment attacks:

- **Tiny fragment attack**--In this type of attack, the attacker makes the fragment size small enough to force Layer 4 (TCP and UDP) header fields into the second fragment. Thus, the ACL rules that have been configured for those fields will not match.

VFR drops all tiny fragments, and an alert message such as “VFR-3-TINY_FRAGMENTS” is logged to the syslog server.

- **Overlapping fragment attack**--In this type of attack, the attacker can overwrite the fragment offset in the noninitial IP fragment packets. When the firewall reassembles the IP fragments, it might create wrong IP packets, causing the memory to overflow or the system to reload.

VFR drops all fragments within a fragment chain if an overlap fragment is detected.

- **Buffer overflow attack**--In this type of denial-of-service (DoS) attack, the attacker can continuously send a large number of incomplete IP fragments, causing the firewall to lose time and memory while trying to reassemble the fake packets.

To avoid buffer overflow and control memory use, configure a maximum threshold for the number of IP datagrams that are being reassembled and the number of fragments per datagram. You can use the **ip virtual-reassembly** command or the **ip virtual-reassembly-out** command to specify these parameters.

When the maximum number of datagrams that can be reassembled at any given time is reached, all subsequent fragments are dropped, and the global statistics item “ReassDrop” is incremented by one.

When the maximum number of fragments per datagram is reached, subsequent fragments are dropped, and the global statistics item “ReassTooManyFrag” is incremented by one. .

In addition to the maximum threshold values being configured, each IP datagram is associated with a managed timer. If the IP datagram does not receive all of the fragments within the specified time, the timer expires and the IP datagram and all of its fragments are dropped.

VFR Enablement

VFR is designed to work with any feature that requires fragment reassembly (such as Cisco IOS Firewall and NAT). By default, NAT enables and disables VFR internally; that is, when NAT is enabled on an interface, VFR is automatically enabled on that interface.

If more than one feature attempts to automatically enable VFR on an interface, VFR will maintain a reference count to keep track of the number of features that have enabled VFR. When the reference count is reduced to zero, VFR is automatically disabled.

VFR on Outbound Interfaces

In Cisco IOS Release XE 3.2S and later releases, you can use the **ip virtual-reassembly-out** command to manually enable or disable VFR on outbound interface traffic.

How to Configure Virtual Fragmentation Reassembly

- [Configuring VFR, page 3](#)
- [Enabling VFR Manually on Outbound Interface Traffic, page 4](#)

Configuring VFR

Perform this task to enable VFR on an interface, specify maximum threshold values to combat buffer overflow and control memory usage, and verify any VFR configurations.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ip virtual-reassembly** [max-reassemblies number] [max-fragments number] [timeout seconds] [drop-fragments]
5. **exit**
6. **exit**
7. **show ip virtual-reassembly** [interface type]

DETAILED STEPS

| | Command or Action | Purpose |
|--------|--|--|
| Step 1 | enable Example: Router> enable | Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted. |
| Step 2 | configure terminal Example: Router# configure terminal | Enters global configuration mode. |

| Command or Action | Purpose |
|---|--|
| Step 3 <code>interface type number</code> Example: <pre>Router(config)# interface GigabitEthernet0/0/1</pre> | Configures an interface type and enters interface configuration mode. |
| Step 4 <code>ip virtual-reassembly [max-reassemblies number] [max-fragments number] [timeout seconds] [drop-fragments]</code> Example: <pre>Router(config-if)# ip virtual-reassembly max-reassemblies 64 max-fragments 16 timeout 5</pre> | Enables VFR on the interface and specifies the maximum threshold values. |
| Step 5 <code>exit</code> Example: <pre>Router(config-if)# exit</pre> | Exits interface configuration mode. |
| Step 6 <code>exit</code> Example: <pre>Router(config)# exit</pre> | Exits global configuration mode. |
| Step 7 <code>show ip virtual-reassembly [interface type]</code> Example: <pre>Router# show ip virtual-reassembly GigabitEthernet0/0/1</pre> | Displays the configuration and statistical information of the VFR. <ul style="list-style-type: none"> If an interface is not specified, VFR information is shown for all configured interfaces. |

Enabling VFR Manually on Outbound Interface Traffic

Perform this task to enable VFR manually on outbound interface traffic. You can use this procedure to reenable VFR on outbound interface traffic if it is disabled, for example, by the **no ip virtual-reassembly** command.



Note

If VFR is enabled on both inbound and outbound interface traffic, you can use the **no ip virtual-reassembly-out** command to disable it on only the outbound interface traffic.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ip virtual-reassembly** [max-reassemblies number] [max-fragments number] [timeout seconds] [drop-fragments]
5. **exit**

DETAILED STEPS

| Command or Action | Purpose |
|--|--|
| Step 1 enable Example: <pre>Router> enable</pre> | Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted. |
| Step 2 configure terminal Example: <pre>Router# configure terminal</pre> | Enters global configuration mode. |
| Step 3 interface <i>type number</i> Example: <pre>Router(config)# interface GigabitEthernet0/0/1</pre> | Configures an interface type and enters interface configuration mode. |
| Step 4 ip virtual-reassembly [max-reassemblies number] [max-fragments number] [timeout seconds] [drop-fragments] Example: <pre>Router(config-if)# ip virtual-reassembly max-reassemblies 64 max-fragments 16 timeout 5</pre> | Enables VFR on the interface and specifies the maximum threshold values. |
| Step 5 exit Example: <pre>Router(config-if)# exit</pre> | Exits interface configuration mode. |

- [Troubleshooting Tips, page 6](#)

Troubleshooting Tips

To display debugging messages related to the VFR subsystem, use the **debug ip virtual-reassembly** command.

Configuration Examples for Fragmentation Reassembly

- [Example Configuring VFR on Outbound Interface Traffic, page 6](#)

Example Configuring VFR on Outbound Interface Traffic

The following example shows how to manually enable VFR on outbound traffic on interfaces GigabitEthernet0/0/1, GigabitEthernet0/0/0.773, and Serial 3/0:

```
interface Loopback 0
ip address 10.0.1.1 255.255.255.255
!
interface GigabitEthernet0/0/1
description LAN1
ip address 10.4.0.2 255.255.255.0
ip virtual-reassembly-out
!
interface GigabitEthernet0/0/0.773
encapsulation dot1Q 773
description LAN2
ip address 10.15.0.2 255.255.255.0
ip virtual-reassembly-out
!
interface Serial 3/0
description Internet
ip unnumbered Loopback0
encapsulation ppp
ip virtual-reassembly-out
serial restart-delay 0
```

Additional References

Related Documents

| Related Topic | Document Title |
|--------------------|--|
| Cisco IOS commands | Cisco IOS Master Commands List, All Releases |
| Security commands | <i>Cisco IOS Security Command Reference</i> |
| Dynamic IDS | Cisco IOS Intrusion Prevention System |
| CBAC | "Configuring Context-Based Access Control" |

Standards

| Standards | Title |
|-----------|-------|
| None | -- |

MIBs

| MIB | MIBs Link |
|------|---|
| None | To locate and download MIBs for selected platforms, Cisco software releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs |

RFCs

| RFCs | Title |
|----------|--|
| RFC 791 | <i>Internet Protocol</i> |
| RFC 1858 | <i>Security Considerations for IP Fragment Filtering</i> |

Technical Assistance

| Description | Link |
|---|---|
| The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password. | http://www.cisco.com/cisco/web/support/index.html |

Feature Information for Virtual Fragmentation Reassembly

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 Virtual Fragmentation Reassembly**

| Feature Name | Releases | Feature Information |
|----------------------------------|---------------------------|---|
| Virtual Fragmentation Reassembly | Cisco IOS XE Release 3.2S | <p>VFR enables the Cisco IOS Firewall to create the appropriate dynamic ACLs to protect the network from various fragmentation attacks.</p> <p>In Cisco IOS Release XE 3.2S, functionality to manually configure VFR for outbound or inbound interface traffic was added.</p> <p>The following commands were introduced or modified: ip virtual-reassembly-out, show ip virtual-reassembly.</p> |

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.



IPv6 Virtual Fragmentation Reassembly

- [Finding Feature Information, page 9](#)
- [Information About IPv6 Virtual Fragmentation Reassembly, page 9](#)
- [How to Implement IPv6 Virtual Fragmentation Reassembly, page 9](#)
- [Configuration Example for IPv6 Virtual Fragmentation Reassembly, page 11](#)
- [Additional References, page 12](#)
- [Feature Information for IPv6 Virtual Fragmentation Reassembly, page 12](#)

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see [Bug Search Tool](#) and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

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.

Information About IPv6 Virtual Fragmentation Reassembly

- [IPv6 Virtual Fragmentation Reassembly, page 9](#)

IPv6 Virtual Fragmentation Reassembly

Fragmentation is a process of breaking down an IP datagram into smaller packets to be transmitted over different types of network media. Non-initial fragments of a fragmented IPv6 packet is used to pass through IPsec and NAT64 without any examination due to the lack of the L4 header, which usually is only available on the initial fragment. The IPv6 Virtual Fragmentation Reassembly (VFR) feature provides the ability to collect the fragments and provide L4 info for all fragments for IPsec and NAT64 features.

How to Implement IPv6 Virtual Fragmentation Reassembly

- [Configuring IPv6 Virtual Fragmentation Reassembly, page 10](#)

Configuring IPv6 Virtual Fragmentation Reassembly

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ipv6 virtual-reassembly** [**in** | **out**] [**max-reassemblies** *maxreassemblies*] [**max-fragments** *max-fragments*] [**timeout** *seconds*] [**drop-fragments**]
5. **exit**
6. **show ipv6 virtual-reassembly interface** *interface-type*
7. **show ipv6 virtual-reassembly features interface** *interface-type*

DETAILED STEPS

| Command or Action | Purpose |
|--|---|
| <p>Step 1 enable</p> <p>Example:</p> <pre>Router> enable</pre> | <p>Enables privileged EXEC mode.</p> <ul style="list-style-type: none"> • Enter your password if prompted. |
| <p>Step 2 configure terminal</p> <p>Example:</p> <pre>Router# configure terminal</pre> | <p>Enters global configuration mode.</p> |
| <p>Step 3 interface <i>type number</i></p> <p>Example:</p> <pre>Router(config)# interface gigabitethernet 3/1/1</pre> | <p>Specifies an interface type and number, and places the router in interface configuration mode.</p> |
| <p>Step 4 ipv6 virtual-reassembly [in out] [max-reassemblies <i>maxreassemblies</i>] [max-fragments <i>max-fragments</i>] [timeout <i>seconds</i>] [drop-fragments]</p> <p>Example:</p> <pre>Router(config-if)# ipv6 virtual-reassembly max-reassemblies 32 max-fragments 4 timeout 7</pre> | <p>Enables VFR on an interface.</p> |

| Command or Action | Purpose |
|---|---|
| <p>Step 5 <code>exit</code></p> <p>Example:</p> <pre>Router(config-if)# exit</pre> | <p>Exits interface configuration mode and places the router in global configuration mode.</p> <ul style="list-style-type: none"> Enter this command twice to reach privileged EXEC mode. |
| <p>Step 6 <code>show ipv6 virtual-reassembly interface <i>interface-type</i></code></p> <p>Example:</p> <pre>Router# show ipv6 virtual-reassembly interface e1/1/1</pre> | <p>Displays VRF configuration and statistical information on a specific interface.</p> |
| <p>Step 7 <code>show ipv6 virtual-reassembly features interface <i>interface-type</i></code></p> <p>Example:</p> <pre>Router# show ipv6 virtual-reassembly features</pre> | <p>Displays VFR information on all interfaces or on a specified interface.</p> |

Configuration Example for IPv6 Virtual Fragmentation Reassembly

- [Example: Configuring IPv6 Virtual Fragmentation Reassembly, page 11](#)

Example: Configuring IPv6 Virtual Fragmentation Reassembly

```
Router# show ipv6 virtual-reassembly interface gigabitethernet1/1/1
GigabitEthernet1/1/1:
IPv6 Virtual Fragment Reassembly (VFR) is ENABLED(in)
Concurrent reassemblies (max-reassemblies): 64
Fragments per reassembly (max-fragments): 16
Reassembly timeout (timeout): 3 seconds
Drop fragments: OFF
Current reassembly count: 0
Current fragment count: 0
Total reassembly count: 6950
Total reassembly timeout count: 9
GigabitEthernet1/1/1:
IPv6 Virtual Fragment Reassembly (VFR) is ENABLED(out)
Concurrent reassemblies (max-reassemblies): 64
Fragments per reassembly (max-fragments): 16
Reassembly timeout (timeout): 3 seconds
Drop fragments: OFF
Current reassembly count: 0
Current fragment count: 0
Total reassembly count: 0
Total reassembly timeout count: 0
```

Additional References

Related Documents

| Related Topic | Document Title |
|----------------------------------|--|
| IPv6 addressing and connectivity | <i>IPv6 Configuration Guide</i> |
| Cisco IOS commands | Master Commands List, All Releases |
| IPv6 commands | IPv6 Command Reference |
| Cisco IOS IPv6 features | IPv6 Feature Mapping |

Standards and RFCs

| Standard/RFC | Title |
|---------------|---------------------------|
| RFCs for IPv6 | IPv6 RFCs |

Technical Assistance

| Description | Link |
|---|---|
| The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password. | http://www.cisco.com/cisco/web/support/index.html |

Feature Information for IPv6 Virtual Fragmentation Reassembly

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 2 **Feature Information for IPv6 Virtual Fragmentation Reassembly**

| Feature Name | Releases | Feature Information |
|---------------------------------------|---------------------------|--|
| IPv6 Virtual Fragmentation Reassembly | Cisco IOS XE Release 3.4S | The IPv6 VFR feature provides the ability to collect the fragments and provide L4 info for all fragments for IPsec and NAT64 features. |

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.



GRE Fragment and Reassembly Performance Tuning

The GRE Fragment and Reassembly Performance Tuning feature enables you to customize reassembly resources. Reassembly resources are equally allocated to each interface to prevent fragment-related attack. However, in some generic routing encapsulation (GRE) tunnel deployments, fragments are reassembled in specific interfaces. This feature also allows you to adjust the reassembly timer to free up incomplete fragment sessions quickly and reserve the reassembly resources for high priority packets.

- [Finding Feature Information, page 15](#)
- [Restrictions for GRE Fragment and Reassembly, page 15](#)
- [Information About GRE Fragment and Reassembly, page 15](#)
- [How to Use GRE Fragment and Reassembly, page 16](#)
- [Configuration Examples for GRE Fragment and Reassembly, page 18](#)
- [Additional References for GRE Fragment and Reassembly, page 18](#)
- [Feature Information for GRE Fragment and Reassembly, page 19](#)

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see [Bug Search Tool](#) and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

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.

Restrictions for GRE Fragment and Reassembly

- The IPv4 or IPv6 protocol must be enabled on an interface.
- This feature supports manually created tunnel interfaces or physical interfaces (virtual template is not officially supported).

Information About GRE Fragment and Reassembly

- [Fragmentation and Reassembly, page 16](#)

Fragmentation and Reassembly

In Cisco software, packets may be dropped due to nonavailability of reassembly resources of an interface when fragments arrive concurrently on an interface, though, other interfaces have the resources to reassemble fragments. In some cases, some interfaces need additional resources, such as generic routing encapsulation (GRE) tunnel deployment, and resources are freed only when fragments are reassembled. Therefore, if all fragments are not received, the reassembly resources are not freed.

The GRE Fragment and Reassembly Performance Tuning feature improves reassembly performance by reassembling high priority fragments first so that these fragments are not dropped when low priority fragments occupy the reassembly resources.

How to Use GRE Fragment and Reassembly

- [Configuring GRE Fragment and Reassembly \(GFR\), page 16](#)

Configuring GRE Fragment and Reassembly (GFR)

Perform this task to do the following:

- Enable generic routing encapsulation (GRE) Fragment and Reassembly (GFR) on an interface
- Specify maximum threshold values to combat buffer overflow and control memory usage
- Verify GFR configurations

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. Enter one of the following:
 - **ip reassembly** [**max-reassemblies** *number*] [**timeout** *milliseconds*] [**percentage** *percent* {**dscp** *dscp-value* | **precedence** *precedence-value*}]
 - **ipv6 reassembly** [**max-reassemblies** *number*] [**timeout** *milliseconds*] [**percentage** *percent* {**dscp** *dscp-value* | **precedence** *precedence-value*}]
5. **end**
6. Enter one of the following:
 - **show ip reassembly interface** *type number*
 - **show ipv6 reassembly interface** *type number*

DETAILED STEPS

| Command or Action | Purpose |
|---|---|
| <p>Step 1 <code>enable</code></p> <p>Example: Device> enable</p> | <p>Enables privileged EXEC mode.</p> <ul style="list-style-type: none"> • Enter your password if prompted. |
| <p>Step 2 <code>configure terminal</code></p> <p>Example: Device# configure terminal</p> | <p>Enters global configuration mode.</p> |
| <p>Step 3 <code>interface type number</code></p> <p>Example: Device(config)# interface GigabitEthernet 0/0/0</p> | <p>Configures an interface type and enters interface configuration mode.</p> |
| <p>Step 4 Enter one of the following:</p> <ul style="list-style-type: none"> • <code>ip reassembly [max-reassemblies number] [timeout milliseconds] [percentage percent {dscp dscp-value precedence precedence-value}]</code> • <code>ipv6 reassembly [max-reassemblies number] [timeout milliseconds] [percentage percent {dscp dscp-value precedence precedence-value}]</code> <p>Example: Device(config-if)# ip reassembly max-reassemblies 1024 timeout 1000 percentage 50 precedence critical routine</p> <p>Example: Device(config-if)# ipv6 reassembly max-reassemblies 1024 timeout 1000 percentage 50 precedence critical routine</p> | <p>Enables GFR on an IPv4 or IPv6 interface, as appropriate.</p> |
| <p>Step 5 <code>end</code></p> <p>Example: Device(config-if)# end</p> | <p>Exits interface configuration mode and returns to privileged EXEC mode.</p> |

| Command or Action | Purpose |
|---|---|
| <p>Step 6 Enter one of the following:</p> <ul style="list-style-type: none"> • <code>show ip reassembly interface type number</code> • <code>show ipv6 reassembly interface type number</code> <p>Example: Device# show ip reassembly GigabitEthernet 0/0/0</p> <p>Example: Device# show ipv6 reassembly GigabitEthernet 0/0/0</p> | Displays statistical information of the GFR configured about the interface. |

Configuration Examples for GRE Fragment and Reassembly

- [Example: Configuring GFR, page 18](#)

Example: Configuring GFR

The following example shows how to configure GFR on a Gigabit Ethernet interface and specify the maximum reassembly and timeout settings:

```
interface GigabitEthernet 0/0/0
ip address 10.10.10.1 255.255.255.0
ipv6 address 2001:DB8:1::1
ip reassembly max-reassemblies 1024 timeout 1 percentage 50 dscp ef
ipv6 reassembly max-reassemblies 1024 timeout 1 percentage 50 dscp ef
ip virtual-reassembly max-reassemblies 1024 timeout 1 percentage 10 dscp af41
ipv6 reassembly out max-reassemblies 1024 timeout 1 percentage 50 precedence cs1
```

Additional References for GRE Fragment and Reassembly

Related Documents

| Related Topic | Document Title |
|--------------------|--|
| Cisco IOS commands | <i>Cisco IOS Master Command List, All Releases</i> |

| Related Topic | Document Title |
|--------------------------------------|--|
| Security commands | <ul style="list-style-type: none"> • <i>Cisco IOS Security Command Reference Commands A to C</i> • <i>Cisco IOS Security Command Reference Commands D to L</i> • <i>Cisco IOS Security Command Reference Commands M to R</i> • <i>Cisco IOS Security Command Reference Commands S to Z</i> |
| Virtual Fragmentation and Reassembly | <i>Virtual Fragmentation and Reassembly</i> |

Technical Assistance

| Description | Link |
|---|---|
| The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password. | http://www.cisco.com/cisco/web/support/index.html |

Feature Information for GRE Fragment and Reassembly

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 3 **Feature Information for GRE Fragment and Reassembly**

| Feature Name | Releases | Feature Information |
|--|---------------------------|--|
| GRE Fragment and Reassembly Performance Tuning | Cisco IOS XE Release 3.8S | <p>The GRE Fragment and Reassembly Performance Tuning feature enables you to customize reassembly resources. Reassembly resources are equally allocated to each interface to prevent fragment-related attack. However, in some generic routing encapsulation (GRE) tunnel deployments, fragments are reassembled in specific interfaces. This feature also allows you to adjust the reassembly timer to free up incomplete fragment sessions quickly and reserve the reassembly resources for high priority packets.</p> <p>The following commands were introduced or modified: ip reassembly, show ip reassembly.</p> |

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.