



WAN Monitoring Software Configuration Guide for Cisco 1000 Series Connected Grid Routers (Cisco IOS)

First Published: January 2014

Release: Cisco IOS Release 15.4(1)CG

OL-31242-01

This document describes the WAN Monitoring software module, WANMon, as implemented in Cisco IOS deployments. WANMon monitors the backhaul and initiates recovery actions on link failure.

This guide includes the following sections:

- [Information About WANMon, page 1](#)
- [Prerequisites, page 2](#)
- [Guidelines and Limitations, page 3](#)
- [Configuring WANMon, page 3](#)
- [Verifying WANMon Configuration, page 5](#)
- [Configuration Examples, page 5](#)
- [Feature History, page 6](#)
- [Related Documentation, page 6](#)

Information About WANMon

WANMon is a flexible solution to address the WAN link recovery requirements for the following products and interfaces:

- Physical networks: 3G GSM or CDMA, WiMAX, Ethernet (connected to a satellite modem).
- Virtual links: Non-crypto map based IPsec tunnels (either legacy or FlexVPN); that is, any IPsec tunnel you configure as an interface.



Note

Other link types are not supported.



Cisco Systems, Inc.
www.cisco.com

You enable WANMon to monitor your WAN links and initiate link recovery actions on receipt of link failure triggers.

Built-in Recovery Actions

The following are the three levels of built-in recovery processes specific to the link type:

Link Type	Recovery Actions		
	Level 0 (Immediate)	Level 1 (Active)	Level 2 (Last-Resort)
Cellular	Clear interface, and then shut/no-shut	Module reload	System reload
WiMAX	Clear interface	Module reload	System reload
Ethernet	Clear interface, and then shut/no-shut	No action taken	System reload
Tunnel	Shut/no-shut	No action taken	System reload

Each level has two time-based thresholds based on which built-in recovery actions are taken. The following are the default settings for each level:

- *threshold* is the wait time in minutes after receipt of a link failure trigger to initiate the recovery action as set in the specified level.
- *mintime* is the frequency to perform the recovery action if the link remains down.

The built-in values are:

Level	threshold	mintime	Description
Level 0	10 min	10 min	Triggers Level 0 actions 10 minutes after the link went down. Repeat no more than every 10 minutes.
Level 1	60 min	60 min	Triggers Level 1 actions 10 minutes after the link went down. Repeat no more than every 60 minutes.
Level 2	480 min	60 min	Triggers Level 2 actions 480 minutes after the link went down. Repeat no more than every 60 minutes.



Note

If threshold values are specified as 0, no recovery actions are taken for that level. You can use this to avoid system reload (the built-in Level 2 recovery action) on receipt of a link failure trigger where other WAN links may be operational.

Prerequisites

Ensure that the WANMon module is available. The WANMon module is included in the CGR image as the tm_wanmon.tcl policy file. Refer to [Feature History](#) for the minimum required software release.

Guidelines and Limitations

- WANMon automatically performs IP address checking (no user configuration) as required for the link type:
 - For cellular interfaces, WANMon performs IP address checking only for external dialer configurations, not for dial-on-demand configurations.
 - For WiMAX interfaces, WANMon always performs IP address checking.
 - For all other interfaces, WANMon never performs IP address checking.
- WANMon indirectly triggers user-specified actions by generating an application event that link resetter applets monitor.
- If your network is live, ensure that you understand the potential impact of any command.

Configuring WANMon

You can enable WANMon on the router and assign WANMon support to specific interfaces. Optionally, you can override the built-in recovery actions, define custom recovery links, and define an event manager environment policy to set the track object value and disable IP address checking. WANMon is disabled by default.

BEFORE YOU BEGIN

Ensure that the [Guidelines and Limitations](#) are met.

DETAILED STEPS

	Command	Purpose
Step 1	event manager policy tm_wanmon.tcl authorization bypass	Enables the WANMon link recovery module. Use authorization bypass to avoid authorization for CLIs invoked by this policy.
Step 2	event manager environment wanmon_if_list <instance> {interface name { ipsla <instance>}}	Configures WANMon for the interfaces in your WAN, and indicates that this is an interface configuration command. Note Any environment variable with the prefix <code>wanmon_if_list</code> constitutes an interface configuration. Multiple interfaces are allowed by specifying an instance. Be sure to specify the full interface name (for example, <code>cellular3/1</code>). You can set the IP SLA <code>icmp-echo</code> trigger, if desired. Multiple IP SLA triggers are allowed by specifying an instance. Note WANMon only looks at the status of the SLA ID. Even though <code>icmp-echo</code> is most common, if needed any other type of SLA probe (for example, <code>udp-echo</code>) can be used instead.

	Command	Purpose
Step 3	event manager environment wanmon_if_listx { <i>interface name</i> { recovery <i>Level0</i> { <i>Level1</i> } <i>Level2</i> }}	(Optional) Overrides the built-in thresholds.
Step 4	publish-event sub-system 798 type 2000 arg1 < <i>interface name</i> > arg2 < <i>level</i> >	(Optional) Configures custom recovery actions using link resetter applets. < <i>interface</i> > is the full interface name (for example, cellular3/1). < <i>level</i> > is 0, 1, or 2 to match the desired link recovery action.
Step 5	{stub < <i>track-stub-id</i> >	(Optional) Allows an event manager environment policy to set the track object value. WANMon can set a track-stub-object value to reflect the link state so that an external applet can track the stub object.
Step 6	event manager environment wanmon_if_listx {< <i>interface name</i> > { checkip < <i>instance</i> >}}	(Optional) Disables IP address checking.

EXAMPLES

```
event manager policy tm_wanmon.tcl authorization bypass
```

The following examples are Event Manager commands to configure cellular and Ethernet interfaces:

```
event manager environment wanmon_if_list1 {cellular3/1 {ipsla 1}}
```

```
event manager environment wanmon_if_list2 {eth2/2 {ipsla 2}}
```

This example sets custom recovery thresholds:

```
event manager environment wanmon_if_list {cellular3/1 {recovery 20 {90 75} 600}}}
```

where:

- The Level 0 threshold is set to 20 minutes after the link failure trigger. Level 0 recovery actions are performed for the cellular interface. Repeats indefinitely, no more than every 10 minutes (default).
- Level 1 threshold is set to 90 minutes. Level 1 recovery actions are performed for the cellular interface. Repeats no more frequently than every 75 minutes.
- The Level 2 threshold is set to 600 minutes (10 hours).

The following sets the track-stub-object value to 21:

```
conf t
track 21 stub-object
event manager environment wanmon_if_list {cellular3/1 {ipsla 1} {stub 21}}}
```

This example disables IP address checking on the wimax4/1 interface:

```
event manager environment wanmon_if_list1 {wimax4/1 {checkip 0}}}
```

Verifying WANMon Configuration

Use the following steps to verify your WANMon configuraion.

DETAILED STEPS

	Command	Purpose
Step 1	show event manager policy registered	Displays the WAN monitoring policy.
Step 2	show event manager environment	Displays the interface environment variables set during interface configuration.

EXAMPLE

```
show event manager policy registered
1 script system multiple Off Thu Jan 16 18:44:29 2014 tm_wanmon.tcl
show event manager environment
1 wanmon_if_list {cell13/1 {ipsla 1}}
```

Configuration Examples

The following examples are provided:

- [WANMon Cellular Interface Configuration Example, page 5](#)
- [Multiple WAN Link Monitoring Example, page 5](#)

WANMon Cellular Interface Configuration Example

```
track 1 ip sla 1
ip sla 1
 icmp-echo 172.27.166.250
 timeout 6000
 frequency 300
ip sla schedule 1 life forever start-time now

event manager environment wanmon_if_list {cellular3/1 {ipsla 1}}
event manager policy tm_wanmon.tcl authorization bypass
```

Multiple WAN Link Monitoring Example

```
track 1 ip sla 1
track 21 stub-object
ip sla 1
 icmp-echo 172.27.166.250
 timeout 6000
 frequency 300
ip sla schedule 1 life forever start-time now

track 2 ip sla 2
track 22 stub-object
ip sla 2
 icmp-echo 10.27.16.25
```

```

timeout 6000
frequency 300
ip sla schedule 2 life forever start-time now

event manager environment wanmon_if_list1 {cellular3/1 {ipsla 1} {stub 21}}
event manager environment wanmon_if_list2 {dot16Radio4/1 {ipsla 1} {stub 22}}
event manager policy tm_wanmon.tcl authorization bypass

```

Feature History

Feature	Release	Feature Information
WANMon software module	Cisco IOS Release 15.4(1)CG	Initial support of the feature on CGR 1000 Series Routers.

Related Documentation

[Configuring WAN Backhaul Redundancy](#)

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, using the Cisco Bug Search Tool (BST), submitting a service request, and gathering additional information, see *What's New in Cisco Product Documentation* at: <http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html>.

Subscribe to *What's New in Cisco Product Documentation*, which lists all new and revised Cisco technical documentation, as an RSS feed and deliver content directly to your desktop using a reader application. The RSS feeds are a free service.

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.

© 2014 Cisco Systems, Inc. All rights reserved.