Increase the Stability of your Network

By Ivan Pepelnjak

1. 9. 2007

The introduction of real-time mission-critical applications (like voice-over-IP) into data networks has prompted many network designers to tune their routing protocols for faster convergence. The resulting network, while being able to quickly detect failures and reroute around them, usually becomes highly susceptible to repetitive failures (for example, a flapping interface), which can cause recurring instabilities in large parts of the network. A flapping interface can also cause significant data loss, as the data streams are constantly rerouted across the network following a routing protocol adjacency establishment and subsequent loss.

To address this issue, Cisco has introduced *IP Event Dampening*, an interface-level mechanism similar to BGP route dampening, in Cisco IOS release 12.3. In this article, you'll see how you can use the IP Event Dampening to increase the stability of your network, as well as how you can cope with scenarios that are beyond the scope of this feature.

Introduction to IP Event Dampening

The mathematical background used in the IP Event Dampening is identical to the one used in the BGP route dampening (described in RFC 2439, the interested reader can find all the details there):

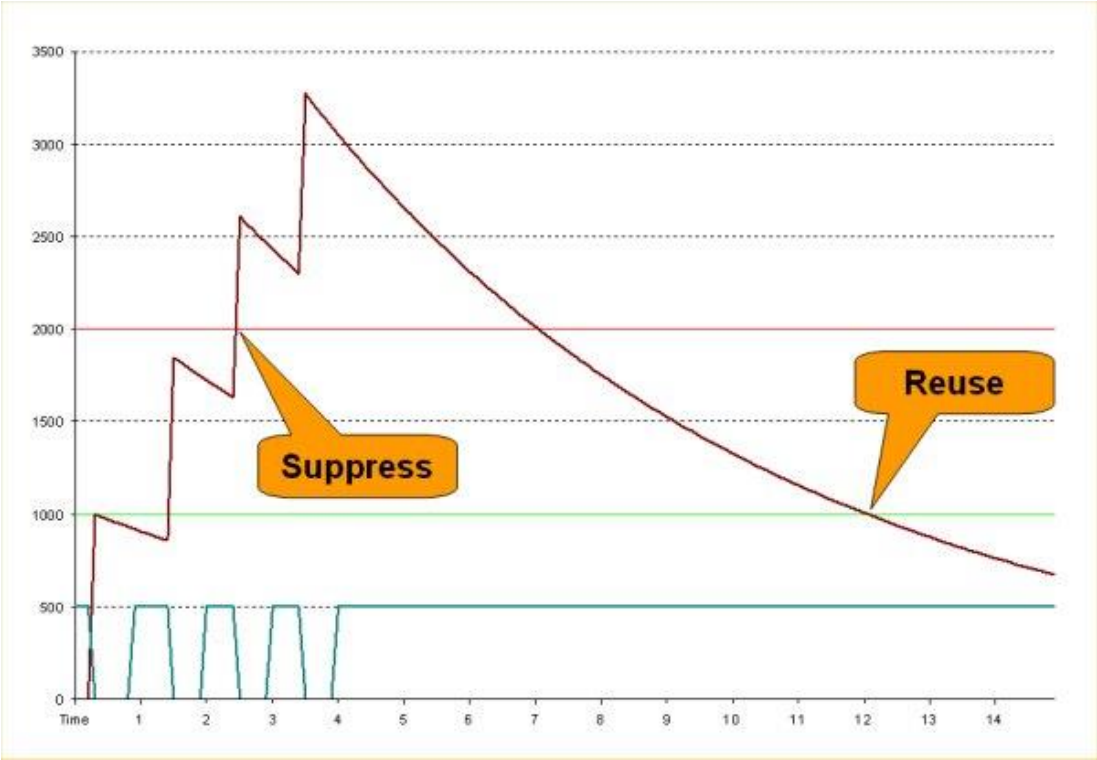
- Whenever an interface changes its state from *up* to *down*, a penalty is applied to the interface. In Cisco IOS, the per-flap penalty is fixed at 1000 points and cannot be changed.
  Note: You could also apply a penalty to interface restarts (for interfaces that differentiate restarts from carrier transitions).
- The accumulated penalty decays exponentially with configurable *half-time period* (the period in which the penalty is halved). The default half-time period for IP event dampening is five seconds.
  Example: The half-time period of 10 seconds would mean that the accumulated penalty of 1200 points would be 600 points after 10 seconds, 300 points after 20 seconds and 150 points after 30 seconds.
- If the accumulated penalty exceeds the *suppress threshold*, the interface is dampened (declared unreachable for the routing protocol purposes, regardless of the actual interface state). Default value in Cisco IOS is 2000 points.
- A dampened interface is made available when the accumulated penalty decays below the *reuse threshold.* Its default value is 1000 points.
  Note: The reuse threshold should be several times lower than the suppress threshold to ensure that the sporadic interface flaps don't cause flaps in the dampening algorithm.
- As a large number of interface flaps could cause the interface to be dampened for an exceedingly long time, there is an upper limit on the penalty an interface can accrue. In Cisco IOS, the upper limit is fixed at 20000 points, but could also be lower depending on the maximum suppress time you configure.

These concepts are best illustrated with a sample graph (Figure 1). The interface state (the green line at the bottom of the graph) changed every half second for four seconds, accumulating a total of 4000 penalty points.

As the penalty started to decay immediately, the second flap did not bring the interface into suppressed state (as the accumulated penalty has at that time decayed to approximately 850 points), but the third one did. The interface remained suppressed (for routing protocol purposes) until the accumulated penalty (close to 3300 after the fourth flap) decayed to 1000 points (almost nine seconds after the last flap).

Note: The sample scenario uses default values used by Cisco IOS. Obviously, these values are appropriate for high-speed interfaces; you should use significantly higher half-time periods for lower-speed serial interfaces.

Figure 1: Sample IP event dampening scenario



Configure and Monitor IP Event Dampening

The IP Event Dampening is configured with a single interface-level configuration command **dampening** [*half-time reuse-threshold suppress-threshold max-suppress-time* [**restart** *penalty*]]. The default values assumed by Cisco IOS are summarized in Table 1. You can change as many parameters as you wish; if you specify a different half-time period and don't specify the maximum suppress time, it's four times the half-time period.

Table 1: IP Event Dampening configuration commands

Parameter	Default value
half time	5 seconds
reuse threshold	1000
suppress threshold	2000
maximum suppress time	20 seconds

The **dampening** command can be applied only on physical interfaces, IP event dampening does not work on subinterfaces or virtual templates. The events triggering the dampening penalty include a change in interface state (loss of carrier) as well as the line protocol state; the easiest way to trigger interface flaps in a lab environment is thus with a script that changes line protocol on a serial interface between HDLC and PPP. A sample Tcl script that generates four flaps in approximately two seconds is included in Listing 1 (you should execute it on the router where the IP event dampening is enabled, as the quick changes between the layer-2 protocols will not be detected by the remote router).

Listing 1: Tcl script that flaps the interface

```
proc usage {} { puts "Syntax: tclsh ifchange.tcl interface";}
proc flapState { ifnum } {
  puts "... waiting ...";
  after 500;
  puts "... flap ...";
  ios_config"interface $ifnum" "encapsulation hdlc";
  after 50;
  ios_config "interface $ifnum" "encapsulation ppp";
}
set ifnum [lindex $argv 0]
if {[string equal $ifnum ""]} { usage; return; }
flapState $ifnum;
flapState $ifnum;
```

```
flapState $ifnum;

flapState $ifnum;
```

There are two confusingly similar commands that monitor the IP event dampening feature: the **show dampening interface** (Listing 2) displays an overview on the IP event dampening configuration and the **show interface dampening** (Listing 3) displays the actual status of every interface where the IP event dampening is configured.

Listing 2: Display a summary of the IP event dampening configuration

```
router#show dampening interface

2 interfaces are configured with dampening.

1 interface is being suppressed.

Features that are using interface dampening:

  IP Routing

  HSRP
```

```
Listing 3

Per-interface status of the IP event dampening

router#show interfaces dampening

Serial0/0/0

  Flaps Penalty  Supp ReuseTm HalfL ReuseV SuppV MaxSTm MaxP Restart

      0       0 FALSE       0    20   1000  2000    80  16000       0

Serial0/1/0

  Flaps Penalty  Supp ReuseTm HalfL ReuseV SuppV MaxSTm MaxP Restart

      0    2245  TRUE      33    15    500  2000    60   8000     500
```

The IP Event Dampening feature generates no logging messages; the only means to detect when an interface has been suppressed and later unsuppressed is through the **debug dampening interface** command.

*Note: You cannot use the event tracking feature of Cisco IOS, as the **track interface ip routing** command does not consider the dampening status of the interface and reports it as up even when it's dampened.*

Dampen Other Instabilities

The external BGP routes and physical interface flaps are the only network instabilities that can be dampened using standard Cisco IOS features. To dampen any other instabilities in your network (for example, reloading routers, lost neighbors on LAN interfaces or flapping Frame Relay subinterfaces), you have to write your own Embedded Event Manager (EEM) applets or Tcl scripts. The EEM applets are usually applied as a temporary fix, as you cannot extract the interface name or OSPF neighbor's IP address in them, and thus have to configure a separate applet for each interface or neighbor router. Using Tcl scripts registered as EEM policies give you greater flexibility (you could even implement exponential decay dampening using Tcl), but is well beyond the scope of this article; if you need a network-wide solution, contact our Professional Services team.

The best method to detect network instability is to monitor the *syslog* messages generated by the router (for example, the *OSPF-5-ADJCHG* messages) and trigger an action if the same message is generated too often in a certain time frame. For example, you could trigger an EEM applet if the OSPF neighbor on interface **Serial0/1/0** is lost more than three times in a minute (Listing 4).

Listing 4: Detect repeated OSPF neighbor loss on a serial interface

```
event manager applet OSPF_Down_Serial0/1/0

 event syslog occurs 3 pattern "OSPF-5-
ADJCHG.*Serial0/1/0.*to DOWN" period 60
```

Once the network instability is detected, you might want to take proactive steps to reduce its impacts. For example, if an OSPF adjacency is constantly failing on an interface, you could make that interface passive (Listing 5).

Note: When taking such a radical step, you might want to notify the network administrator with an e-mail (potentially forwarded as an SMS message to a mobile phone). The ***action mail*** *EEM configuration command allows you to send e-mails from an EEM applet.*

Listing 5: Caption

```
event manager applet OSPF_Down_Serial0/1/0
```

```
 event syslog occurs 3 pattern "OSPF-5-
ADJCHG.*Serial0/1/0.*to DOWN" period 60
 action 1.0 cli command "enable"
 action 2.0 cli command "configure terminal"
 action 2.1 cli command "router ospf 1"
 action 2.2 cli command "passive-interface serial 0/1/0"
 action 3.0 syslog msg "OSPF disabled on Serial0/1/0"
```

You could decide that the router will just disable a discovered network instability and inform the network administrator, or you could trigger a reverse configuration change after a period of time. To do that, you have to define another EEM applet with reverse effects (Listing 6) and trigger that applet with a countdown timer (Listing 7).

Listing 6: Re-enable OSPF on a serial interface

```
event manager applet OSPF_Enable_Serial0/1/0
 event none
 action 1.0 cli command "enable"
 action 2.0 cli command "configure terminal"
 action 2.1 cli command "router ospf 1"
 action 2.2 cli command "no passive-interface serial 0/1/0"
 action 3.0 syslog msg "OSPF enabled on Serial0/1/0"
```

Listing 7: Trigger the complementary EEM applet in 60 seconds

```
event manager applet OSPF_Down_Serial0/1/0
 action 4.0 cli command "event manager applet OSPF_Enable_Serial0/1/0"
 action 4.1 cli command "event timer countdown name OSPF_Enable_Serial0/1/0
time 60"
```

The complete EEM applet configuration is included in Listing 8 and a sample scenario where three interface flaps have been generated far enough apart that the IP Event Dampening did not detect them but EEM detected OSPF instability is included in Listing 9.

Listing 8: Complete EEM configuration to detect OSPF instabilities on Serial0/1/0

```
event manager applet OSPF_Down_Serial0/1/0
```

```
 event syslog occurs 3 pattern "OSPF-5-
ADJCHG.*Serial0/1/0.*to DOWN" period 60

 action 1.0 cli command "enable"

 action 2.0 cli command "configure terminal"

 action 2.1 cli command "router ospf 1"

 action 2.2 cli command "passive-interface serial 0/1/0"

 action 3.0 syslog msg "OSPF disabled on Serial0/1/0"

 action 4.0 cli command "event manager applet OSPF_Enable_Serial0/1/0"

 action 4.1 cli command "event timer countdown name OSPF_Enable_Serial0/1/0
time 60"

event manager applet OSPF_Enable_Serial0/1/0

 event timer countdown name OSPF_Enable_Serial0/1/0 time 60

 action 1.0 cli command "enable"

 action 2.0 cli command "configure terminal"

 action 2.1 cli command "router ospf 1"

 action 2.2 cli command "no passive-interface serial 0/1/0"

 action 3.0 syslog msg "OSPF enabled on Serial0/1/0"
```

Listing 9: EEM applet disables OSPF on a serial interface

```
Aug 14 11:02:15: %LINK-3-
UPDOWN: Interface Serial0/1/0, changed state to down

Aug 14 11:02:15: %OSPF-5-
ADJCHG: Process 1, Nbr 172.16.0.12 on Serial0/1/0 from FULL to DOWN,
Neighbor Down: Interface down or detached

Aug 14 11:02:21: %LINK-3-UPDOWN: Interface Serial0/1/0, changed state to up

Aug 14 11:02:27: %LINK-3-
UPDOWN: Interface Serial0/1/0, changed state to down

Aug 14 11:02:27: %OSPF-5-
ADJCHG: Process 1, Nbr 172.16.0.12 on Serial0/1/0 from INIT to DOWN,
Neighbor Down: Interface down or detached

Aug 14 11:02:33: %LINK-3-UPDOWN: Interface Serial0/1/0, changed state to up

Aug 14 11:02:34: %LINEPROTO-5-
UPDOWN: Line protocol on Interface Serial0/1/0, changed state to up

Aug 14 11:02:40: %LINK-3-
UPDOWN: Interface Serial0/1/0, changed state to down
```

```
Aug 14 11:02:40: %OSPF-5-
ADJCHG: Process 1, Nbr 172.16.0.12 on Serial0/1/0 from INIT to DOWN,
Neighbor Down: Interface down or detached

Aug 14 11:02:40: %HA_EM-6-
LOG: OSPF_Down_Serial0/1/0: OSPF disabled on Serial0/1/0

Aug 14 11:02:40: %SYS-5-CONFIG_I: Configured from console by vty0

Aug 14 11:02:46: %LINK-3-UPDOWN: Interface Serial0/1/0, changed state to up

Aug 14 11:03:40: %HA_EM-6-
LOG: OSPF_Enable_Serial0/1/0: OSPF enabled on Serial0/1/0

Aug 14 11:03:40: %SYS-5-CONFIG_I: Configured from console by vty0

Aug 14 11:03:46: %OSPF-5-
ADJCHG: Process 1, Nbr 172.16.0.12 on Serial0/1/0 from LOADING to FULL, Load
ing Done
```

Summary

In this article, you've seen how you can reduce the impact of interface flaps on the stability of your network. The IP Event Dampening feature provides a mechanism by which Cisco IOS detects highly repetitive interface flaps and temporarily disables IP routing on the interface (suppresses the interface). The suppressed interface is not available to any IP routing activity; the routing protocols stop sending Hello packets over the interface and the static routes pointing to the suppressed interface (or next-hops reachable through it) are removed from the IP routing table while the interface is not operational.

You can monitor the IP event dampening status with the **show dampening interface** and the **show interface dampening** commands, but you cannot track it in real-time, as the object tracking feature of Cisco IOS does not take the interface suppression status into account when tracking the IP routing status of an interface (a workaround might be to configure a bogus static route pointing to the interface and track its presence).

Cisco IOS (as of release 12.4(15)T) cannot track any other network instabilities (for example, unstable routing protocol adjacency), but you can write Embedded Event Manager applets to track the status of a particular object (interface or routing protocol neighbor) or you could use EEM Tcl policy to implement a more generic solution.

NIL – More Than Just a Training Company

NIL Learning delivers the leading-edge Cisco training to IT professionals and companies around the globe. Through field-proven experts — each both active engineer and instructor — NIL Learning enhances the standard learning curriculum with real-life experience and helps clients to maximize their training investment.

NIL Learning is part of NIL, a leading global IT solutions provider. Since 1992, NIL has been at the forefront of advanced contributors to strategic partner Cisco's technologies, learning curriculum and value-added solutions deployed to clients around the globe. Today, NIL has earned the highest certifications offered by Cisco, VMware, EMC, HP, IBM, Microsoft, F5, Jive, MobileIron, RSA, VCE and others. Their portfolio of solutions consists of managed services, professional services and learning services.

NIL is headquartered in Slovenia, with regional offices in Croatia, Serbia, Saudi Arabia, the U.S., Turkey, South Africa, Morocco, Nigeria, Kenya and Botswana.

Why learn at NIL LEARNING?

- All NIL LEARNING instructors are **field-proven experts** - each both active engineer and instructor.
- **75% of NIL LEARNING engineers hold CCSI** certifica- tions, and **18 have already achieved the respected CCIE rank.**
- NIL LEARNING **enhances the standard learning curriculum** with real-life experience and helps clients to maximize their training investment.
- NIL has been a Cisco Training Partner for many years; it became a **Cisco Learning Partner in 1993**, and has been a **Cisco Gold Partner since 1995.**
- NIL was awarded the **Cisco Most Business Relevant Learning Partner in MEA in 2010 and the most innova- tive learning partner in MEA.**

- NIL received the **Innovation Award for its Technology Led Training and its extensive contribution to Cisco learning solutions** at the Cisco EMEAR Learning Partner Summit in 2012.
- NIL received the **Innovation Award for its Technology Led Training and Advanced Engineer Program** at the Cisco Global Learning Partner Summit in 2013.
- NIL LEARNING runs a **centralized training schedule across the whole EMEAR region.**

More Info

Slovenia

T: +386 1 4746 500

E: sales-support@nil.com

Botswana

T: +267 318 1684

E: training@it-iq.bw

Croatia

T: +385 (0)51 583 255

E: info-nilcroatia@nil.com

Kenya

T: +27 (0)11 575 4637

E: mea_sales@nil.com

Morocco

T: +212(0) 660 808 394

E: info-nilmorocco@nil.com

Nigeria

T: +27 (0)11 575 4637

E: mea_sales@nil.com

Saudi Arabia

T: +966 1 465 4641

E: info.nilme@nil.com

Serbia

T: +381 11 2282 818

E: info-nilserbia@nil.co.rs

South Africa

T: +27 (0)11 575 4637

E: mea_sales@nil.com

Turkey

T: +902 123 81 8639

E: info-nilturkey@nil.com

E: info-nilusa@nil.com

USA

T: +1 612 886 3900

www.learning.nil.com