Preventing and Diagnosing EIGRP Stuck-in-Active Issues with Route Explorer
# Table of Contents

Introduction .................................................................................................................................................. 3
Technical Overview ........................................................................................................................................... 3
  EIGRP Operation ........................................................................................................................................ 3
  Stuck in Active State .................................................................................................................................. 4
  SIA Behavior in pre-12.1 IOS ....................................................................................................................... 4
  SIA Behavior in IOS 12.1 (4.4) E and Later ................................................................................................. 5
  SIA Troubleshooting and its Limitations ...................................................................................................... 5
    Troubleshooting In Progress SIAs .............................................................................................................. 5
    Discovering the Root Cause of the Lack of Response to Active Queries .................................................... 6
    Discovering Why the Route Went Active .................................................................................................. 6
Route Explorer Solution Overview .................................................................................................................. 6
  Route Explorer for EIGRP Networks ........................................................................................................... 6
  Using Route Explorer to Prevent and Troubleshoot Stuck-in-Active Issues .............................................. 7
  Historical Forensic Analysis ....................................................................................................................... 8
  SIA Probing and Analysis ............................................................................................................................ 10
Conclusion ..................................................................................................................................................... 11
Resources .................................................................................................................................................... 12
  EIGRP and SIA Resources .......................................................................................................................... 12
  Route Explorer Resources ......................................................................................................................... 12
Introduction

The distributed intelligence of IP routing is a key advantage of IP networks, offering greater scalability, cost-effectiveness and superior resilience than statically configured networks. However, this same dynamic, distributed architecture presents significant management challenges to network administrators and engineers responsible for assuring service availability, reliability and predictability. While various router configurations can influence how packets will be forwarded, it is essentially the routing algorithms and routing protocol communications that determine the operational behavior of the network at any moment. Despite the critical nature of routing, there have been very few tools available to simplify and automate the monitoring, analysis and troubleshooting of routing in an IP network. The result is that network engineers have found themselves ill equipped to tackle the complex routing issues that cause 59% of network downtime\(^1\).

This application note explores the specific phenomenon of “Stuck in Active” (SIA) errors in networks utilizing Cisco\(^2\)’s Enhanced Interior Gateway Routing Protocol (EIGRP). The first section provides a technical overview of EIGRP operation including the details behind SIA errors, describes the challenges of how network administrators have traditionally performed troubleshooting on SIA errors, and illustrates the need for a much more effective approach to dealing with routing-related issues. The second section provides an overview of Route Analysis technology, and explains how Route Explorer specifically equips network engineers to more effectively prevent and rapidly troubleshoot EIGRP SIA issues.

Technical Overview

Cisco’s EIGRP routing protocol is an enhanced distance-vector protocol used in many large enterprise networks due to its scalability and quick convergence time. EIGRP implements a number of enhancements over earlier distance-vector protocols that make EIGRP a bandwidth-efficient routing protocol useful for deployment in large networks:

- Incremental route updates based on topology changes that are not locally resolvable
- Updates are only sent to relevant neighbor routers rather than to all routers
- Finite time windows within which protocol messages must be received

EIGRP Operation

When a router advertises a route, it includes the total calculated metric for the entire path to that destination network. Each router establishes a feasible distance for each route by calculating the lowest total metric based on the reported distances (RD) it has received from its neighbors and the metric to reach each of the advertising routers. The neighbor router that is calculated to have the lowest feasible distance to a route is established as the successor for that route and is placed in the routing table. As route advertisements are received for particular networks, their RD is compared to the feasible distance of the successor. If (and only if) a route is advertised with an RD lower than the successor’s feasible distance, the advertising router is recorded in the routing table as a feasible successor.

---

\(^1\) Study by University of Michigan and Sprint

\(^2\) Cisco\® is a registered trademark of Cisco Systems, Inc
When the network is in steady state and the successors for each network are known, each network listed in the routing table is said to be in the passive state. The list of feasible successors for a particular route will be reassessed locally if there are any changes to the cost of the links, a change of state or if update, query or reply packets are received. It could be that a feasible distance changes, or that a feasible successor takes over from the existing successor. Provided that a new successor is found, this is advertised via updates while remaining in passive state. Thus, if a topology change occurs, the router can quickly find an alternate route without having to recompute the route.

However, if the network changes and a feasible successor is not found for a given route, then the local router goes into active state, and queries its neighbors for routing information to the desired network. The local router sets a Reply Status flag to track all the queries to its neighbor routers. If a neighbor has feasible successors, it will recalculate its own local distance to the network and send this back as an RD. If a neighbor does not have a feasible successor, then it will itself move into active state and query its neighbors.

Stuck in Active State

In essence, SIA is the state that occurs when a feasible successor cannot be found for a route due to lack of response from a neighbor. The reason for lack of response from a neighbor is typically the result of unrelated causes, but the effect is that the adjacency to that neighbor is dropped after a timeout occurs. There are two ways that an SIA condition can behave in an EIGRP network, depending on the version of IOS running. These two behaviors are explained below.

SIA Behavior in pre-12.1 IOS

As noted above, when a route goes into the active state, the router queries its neighbors to find a path to the pertinent network. At this point, the router starts a three minute active timer by which time it must receive replies from all queried neighbors. If a neighbor has feasible successors for the route, it will recalculate its own local distance to the network and report this back. However, if a neighbor does not have a feasible successor, it also goes into active state. In some cases, multiple routers along multiple query paths will go into active state as routers continue to query for the desired route. In most cases, this process will yield responses from all queried routers and the sought after route will transition back into the passive state within the three minute SIA query timer. In the case that none of the queried routers can provide a feasible successor, the route is cleared.

In some cases, a response is not received between two neighbor routers because of link failures, congestion or some other adverse condition in either the network or on the queried router, and the three minute active timer expires on the router originating the query. When this happens, the querying router that did not receive a response logs a “DUAL-3-SIA” or “stuck-in-active” error for the route and then drops and restarts its adjacency with the non-responding router. This has the effect of causing more routers to go into the “active” state. Furthermore, more routers in the active query path may also exceed their three minute active timer while waiting for neighbors to respond, and log additional DUAL-3-SIA errors. In many cases, multiple routers may drop adjacencies, causing a large-scale network reconvergence process to occur, during which time

---

3 All descriptions of Cisco EIGRP behavior are derived from Cisco documentation referenced in this paper.
EIGRP Stuck-In-Active Technical Brief

Traffic may be seriously disrupted. The overhead traffic from so many routes going into an active state and the resulting queries may cause congestion on some links, which may further induce additional SIA errors, dropped adjacencies, etc.

SIA Behavior in IOS 12.1 (4.4) E and Later

In order to mitigate the possible cascading effect of SIA errors, Cisco released a bug fix (Cisco Bug ID CSCdp33034) effective with Cisco IOS Software Release 12.1(4.4)E. In this, and later versions of IOS, separate SIA query messages are periodically sent by the router that originated the active query to its neighbor routers who received queries. This allows the neighbor routers to respond that they are still waiting on responses from yet other routers that they have queried. The effect of this enhancement is to create a trail of SIA queries across multiple router hops towards the router that isn’t responding and is the cause of the SIA condition. It also means that if SIA queries are in effect across multiple hops, then only the last SIA querying router (the penultimate router before the non-responsive neighbor) will reset the neighbor adjacency. While this cuts down on the overhead traffic from dropped adjacencies when compared to pre-12.1 IOS, even the single dropped adjacency will likely trigger additional active routes that can impact service and cloud the troubleshooting process.

SIA Troubleshooting and its Limitations

In order to stave off a broad network reconvergence or, at a minimum, a reset adjacency that can cause costly downtime, network administrators must try to find the router that is not responding to the active route query before the active timer has expired. Once the timer has expired, it becomes virtually impossible to identify the router(s) that was responsible for the stuck-in-active condition.

Troubleshooting In Progress SIAs

The typical procedure for determining the cause of a stuck-in-active route is a manual process that also requires some fortunate timing. Assuming that the network engineer becomes aware of an active route in progress, they can attempt to trace the source of the stuck route as follows:

1. Log into the active router and run the show ip eigrp topology active command
2. Sort through the routes that are active and aging to see which neighbor routers have not responded
3. Log into each neighbor router that was queried and repeat the above process until you find the router or routers that were queried, but are not active and are not responding to the query – this is the source of the SIA error
4. Determine why the stuck router(s) are not responding to the active query

In most cases, it is uncommon for an administrator to notice an SIA event and be able to react in time to find the source of the problem before adjacencies are reset. Unfortunately, once adjacencies are reset, active timers are cleared on the routers, so that the forensic audit trail in the network is effectively erased. This leaves the network engineer in the unenviable position of not having any clear idea of what actually happened, let alone why.
Discovering the Root Cause of the Lack of Response to Active Queries

Whether or not the SIA issue is caught and remedied before adjacencies are reset, it is critically important to discover why the router did not respond to the active queries by capturing the statistics on the adjacency that was reset, ideally right before the SIA event occurred. This can be very challenging particularly in pre-12.1 IOS implementations, since syslogs are typically the only available source of information on the adjacency status and they may only be triggered upon the adjacency dropping. After the adjacency is reset, the adjacency statistics are also reset, erasing any useful history. Even in the case of post-12.1 IOS, this is problematic and leaves essential troubleshooting information unrecorded.

Discovering Why the Route Went Active

Finally, it is also important to discover why the original route(s) went active. Common causes are link flapping and overloaded routers, as well as failure to configure route summarization on remote access routers, which can cause what looks like a flood of flapping links due to dynamic, PPP-assigned host routes being announced and withdrawn rapidly. The manual process for detecting and diagnosing problematic links or remote access routers is time consuming and does not necessarily correlate to any particular SIA event. Furthermore, in a large network where multiple administrators and engineers are affecting change on a continuous basis, configuration errors can rapidly introduce and re-introduce conditions that can precipitate further SIA events. Without real-time, network-wide visibility into the state of routing in the network, it is easy to miss these common configuration errors. In fact, 31% of network downtime is attributable to routing operation errors.4

Route Explorer Solution Overview

The Route Explorer family is the industry’s first Route Analysis solution offering an accurate and complete, real-time and historical view of network-wide IP routing. A single Route Explorer appliance provides network-wide IP route (Layer 3) visualization, monitoring, analysis and diagnostic capabilities by leveraging the information in the network’s routing protocols and applying patent-pending route processing algorithms. Route Explorer enables network engineers to easily verify, monitor and optimize network operations, as well as detect, diagnose and resolve IP network problems faster than has been possible till now. Route Explorer supports an integrated view of routing operations across multiple areas and Autonomous Systems with support for EIGRP, OSPF, IS-IS, and BGP.

Route Explorer for EIGRP Networks

Route Explorer’s EIGRP Routing Analysis software discovers and monitors multi-domain enterprise EIGRP networks from a single appliance. The network topology map (see Figure 1) shows all EIGRP ASes clearly and distinctly using different colors for each area. Route prefixes are listed by the AS they belong to, making it easy to trouble-shoot problems. Additional

4 U Mich/Sprint
EIGRP Stuck-In-Active Technical Brief

information about the network such as router platform and the IOS version running on it is also displayed.

A complete prefix advertisement history from the EIGRP update packets is maintained for the entire network, providing an audit trail that includes prefix type, AS of origin, metrics, etc. These events are then resolved by Route Explorer’s analysis into the link state change events that caused the EIGRP updates. Stepping through the event history greatly aids the network engineer in performing forensic analysis.

Tuning of link metrics or simulating down links and routers for impact analysis simplifies network planning and allows preventive actions to be taken. Alerts and reports can be generated on flapping routes or prefixes, excessive network churn, and other events that indicate potential service outages.


Using Route Explorer to Prevent and Troubleshoot Stuck-in-Active Issues

Route Explorer provides a real-time, network-wide topology map, allowing network engineers to proactively monitor for incorrect routing behavior that may be caused by configuration errors or
other problems. For example, Route Explorer makes it easy to verify that all remote access routers have been configured with route summarization to prevent rapidly changing route advertisements from precipitating SIA events in the broader network. Misconfigured routing redundancy can be readily caught before it causes routers to go active on important routes due to a lack of feasible successors.

Route Explorer is the only solution that provides the network administrator with visibility into the real-time routing status of an EIGRP network, as well as an historical perspective on steady state conditions and previous problem points. Route Explorer’s what-if analysis tools let the administrator analyze the impact of various events by showing how the network would respond if various links or routers were down, using the actual state of the network rather than an outdated or inaccurate simulation model. Since Route Explorer records the complete historical state of the network, it makes tracking and verifying changes easy, showing for example the actual network behavior resulting from a configuration change. This audit trail is an invaluable tool when other teams need to be involved in troubleshooting, simplifying and providing context for escalation processes.

Historical Forensic Analysis

Route Explorer’s History Navigator provides the ability to review and replay past routing events. Users can view a histogram of routing activity over time, which enables easy identification of when significant events took place. Start and stop times can be selected around activity of interest and the full list of detailed events during that period can be displayed. These capabilities allow for effective forensic analysis of SIA events. Like a VCR for network-wide routing updates, the History Navigator allows engineers to “rewind” to the time when the SIA event occurred and then step through the events to determine the root cause.
Upon becoming aware of an SIA event (either from Syslog or other means), the network engineer can isolate the problem router/link by pointing the History Navigator to the approximate timeframe of the SIA event and proceeding as follows:

1. Look for any sequence of EIGRP update events (active queries are recorded as routing updates) that Route Explorer has seen. This will give the most direct indicators of the originator and the sequence of other routers involved in the active/SIA query chain.
2. Look for a routing update that is followed roughly three to six minutes later by further route updates. This may indicate the original update that triggered the SIA, and the route updates precipitated by further routes gone active due to reset adjacencies.
3. For pre-12.1 IOS deployments, there may be a sequence of route updates from a number of routers. When a cascade of SIA-related dropped adjacencies occurs, the aggregate of route updates will show a tree of routes, with their root at one particular router. This is the penultimate hop that did not receive the active query reply. The originator of the active queries should be one of the first recorded routers to send route updates, and the penultimate hop router should be one of the last. Look for the most common routes occurring across multiple routers’ updates, and this will indicate the routes owned by the ultimate hop.

![History Navigator with Five EIGRP AS Tabs](image)
4. In post-12.1 IOS deployments, further correlation can be performed by looking at the Syslog of the dropped adjacency, which will directly indicate the problematic link. Unfortunately, as noted above, this Syslog will still not tell what the link status was before the adjacency was reset. However, using a historical recording of the routing updates, a reasonably full analysis can be performed to determine what happened.

SIA Probing and Analysis

As of release 3.0, Route Explorer provides an additional SIA detection capability that augments its forensic analysis capabilities. During its normal process to maintain an accurate, real-time topology of the network, Route Explorer examines relevant parts of the topology to verify the root cause of routing updates. If Route Explorer discovers an active route, it will monitor the status of the route to see if it returns to passive state. If the route continues to age, Route Explorer will probe possible active/SIA query paths to determine if there is an SIA condition on one of the query paths. If a pair of routers is found where one router has an active route and the neighbor has the same route but is not active, Route Explorer has found the two routers that are causing the SIA problem and the connection between them that is at fault.

Route Explorer will continue to monitor the link until either the route is resolved or the adjacency is reset. If the adjacency is reset, adjacency status including the interface ID captured during the probing is recorded for forensic analysis, and Route Explorer records an SIA event. By looking at the adjacency statistics captured by Route Explorer and the interface statistics on the router that correspond to the interface ID captured by Route Explorer, the administrator can assemble a full set of forensic data which will greatly speed the process of diagnosis and troubleshooting.
EIGRP Stuck-In-Active Technical Brief

While the nature of distance vector protocols prevents a guarantee of finding all SIA events, by peering Route Explorer with routers that have many neighbor adjacencies, network operators greatly increase the incidence of capturing the information needed to fully troubleshoot SIA conditions that emerge in their networks.

Conclusion

EIGRP Route Analysis greatly enhances network administrators' visibility, preventative and forensic analysis capabilities. Using a combination of Route Explorer tools along with other common administrative tools, network administrators and engineers can prevent many SIA errors and more rapidly detect and diagnose the cause of many more SIA events when they happen. The result is a reduction of costly network downtime, and freeing of resources to focus on proactive service availability improvements.
Resources

EIGRP and SIA Resources

Cisco EIGRP White Paper:
Cisco SIA Tech Note:
Cisco Product Documentation:

Route Explorer Resources

To learn more about Packet Design and Route Explorer, please:
- Email us at info@packetdesign.com
- Visit Packet Design’s web site at http://www.packetdesign.com
- Call us at 408.490.1000

Corporate Headquarters
Packet Design
7801 North Capital of Texas Hwy
Austin, TX 78731
Phone: 408.490.1000
Fax: 408.562.0080
http://www.packetdesign.com