SOLARWINDS WHITEPAPER

Network Route Monitoring

Author: Brad Hale

Share:

solarwinds
Unexpected Simplicity™

As today's dynamic networks grow in size and complexity, the number of active routing topology states grows exponentially. Advanced routing protocols such as OSPF and BGP, designed to automatically identify and dynamically update the optimal traffic route or path for network traffic based on the current state of your network devices and routing configuration. These protocols, as well as network problems caused by misconfigurations, hardware failures, and software bugs, make it increasingly difficult for the network professional to keep up with the state and topology of network routes. Network failures are characterized by a variety of different symptoms (loss of connectivity, inability to reach a destination, or a slow network) resulting from a variety of root causes (configuration errors, missing routes in a routing table, or route flapping).

Troubleshooting the Manual Way

Most network professionals will tell you that the best way to troubleshoot a network issue is to use the OSI model and go layer-by-layer. Read this article for an overview of How to use the OSI Model to Troubleshoot Networks. For the purposes of this paper, we will assume that you have verified a functional layer 1 and layer 2 and focus on troubleshooting a network route using layer 3.

In order for one network to communicate with another network, there needs to be either a static or dynamic route configured. The first step is to **`ping`** routers closest to you in the path between you and the destination.

If you know that there are multiple routers in the path, then you should try **`traceroute`** to discover the routes that packets actually take when travelling to their destination. Once you identify the hop or the router where you receive a timeout message, you can begin to run tests to determine the problem.

Once you have identified a suspect router, you will need to determine if there is a configured route. First, view the content of the routers routing table or route information base (RIB) by means of the **`show ip route`** command:

```
Router# show ip route
```

The output will look something like this and will tell you all of the networks the router can reach, how to get there, and the routers metric (preference for which is the best route):

```
Codes: I - IGRP derived, R - RIP derived, O - OSPF derived,
       C - connected, S - static, E - EGP derived, B - BGP derived,
       * - candidate default route, IA - OSPF inter area route,
       i - IS-IS derived, ia - IS-IS, U - per-user static route,
       o - on-demand routing, M - mobile, P - periodic downloaded static
route,
       D - EIGRP, EX - EIGRP external, E1 - OSPF external type 1 route,
       E2 - OSPF external type 2 route, N1 - OSPF NSSA external type 1
route,
       N2 - OSPF NSSA external type 2 route

Gateway of last resort is 10.119.254.240 to network 10.140.0.0
```

```
O E2 172.150.0.0 [160/5] via 10.119.254.6, 0:01:00, Ethernet2
B    172.17.10.0 [200/128] via 10.119.254.244, 0:02:22, Ethernet2
O E2 172.70.132.0 [160/5] via 10.119.254.6, 0:00:59, Ethernet2
O E2 10.130.0.0 [160/5] via 10.119.254.6, 0:00:59, Ethernet2
B    172.30.0.0 [200/128] via 10.119.254.244, 0:02:22, Ethernet2
B    10.129.0.0 [200/129] via 10.119.254.240, 0:02:22, Ethernet2
B    172.80.129.0 [200/128] via 10.119.254.244, 0:02:22, Ethernet2
B    10.10.0.0 [200/128] via 10.119.254.244, 0:02:22, Ethernet2
B    172.60.139.0 [200/129] via 10.119.254.240, 0:02:23, Ethernet2
B    172.90.208.0 [200/128] via 10.119.254.244, 0:02:22, Ethernet2
B    192.84.148.0 [200/129] via 10.119.254.240, 0:02:23, Ethernet2
B    192.168.223.0 [200/128] via 10.119.254.244, 0:02:22, Ethernet2
B    192.44.236.0 [200/129] via 10.119.254.240, 0:02:23, Ethernet2
B    10.141.0.0 [200/129] via 10.119.254.240, 0:02:22, Ethernet2
B    141.140.0.0 [200/129] via 10.119.254.240, 0:02:23, Ethernet2
```

Let's look at a single entry and see what it tells us:

```
B    172.17.10.0 [200/128] via 10.119.254.244, 0:02:22, Ethernet2
```

First is the route code which tells us the specific routing protocol. In this case, the B indicates that it is BGP derived.

Next is the route itself. In this example, the route is to the subnet 172.17.10.0. After that, the two numbers in brackets indicate the administrative distance and the metric for the route. The metric is determined by the routing protocol (in this case BGP).

The next piece of information is the next hop the router needs to send packets to in order to reach this subnet. In this case, **`via 10.119.254.244`** tells us the packets destined for the subnet 172.17.10.0 should be forwarded to the IP address 10.119.254.244.

Finally, you have the age of the route (**`0:02:22`**), followed by the interface out which the router will forward the packet (**`Ethernet 2`**).

As you can see, this manual method will become quite unmanageable in large, dynamic networks. Traceroute and Ping are fine for small static networks but if you need to solve problems in larger environments, you will quickly find a need to understand real-time topology without running CLI commands on every single router. This is where automated network monitoring tools come in handy.

Troubleshooting the Automated Way

Automated network tools can range from free basic network monitoring tools to highly advanced, very expensive analytics tools. For network route monitoring, the traditional use of SNMP to monitor, detect and troubleshoot network problems will not provide the detail required to detect changes in routing and traffic. This is where you need a tool that has the intelligence to analyze and monitor network routes and changes to those routes.

If you need to manage multiple routers you should consider a monitoring tool that will keep you informed about two things: the HW status of devices, their interfaces, and their physical connectivity; as well as the ability to quickly access routing data and analytic information like flapping routes, configuration status, and physical status. Ideally this information will be presented side-by-side.

As opposed to manually retrieving routing table information from each router in your network using CLI commands, automated tools can display routing tables that include destination network, next hop, interface, metric, and protocol and provide dynamic updates as your routes change. Additionally, by placing the route information side-by-side with status and performance statistics, you can get a real-time visual indication of your route status.

Monitoring and troubleshooting flapping routes manually can consume significant time. Automated tools can display both historical and real-time data on flapping routes, greatly simplifying your troubleshooting and reducing your time to resolution.

And lastly, automated tools can show related routing neighbors and topology maps as well as provide a historical view of route changes.

How SolarWinds® Can Help

By combining real-time network route information alongside device status and performance statistics, SolarWinds Network Performance Monitor (NPM) gives you the ability to monitor network route information and receive alerts when issues arise. You can view routing tables, changes in default routes, BGP transitions, and flapping routes in a fully customizable Web based interface.

Additionally, NPM gives you a visual network topology representation, provides visual alert indicators and audible alarms, and includes more than sixteen built-in network alert delivery methods and responses, including email, pages, SNMP traps, text-to-speech, syslog messages, and the launching of an external application.

See how SolarWinds Network Performance Monitor can help you monitor and troubleshoot network route issues, by downloading a free, fully functional 30-day trial at www.solarwinds.com.