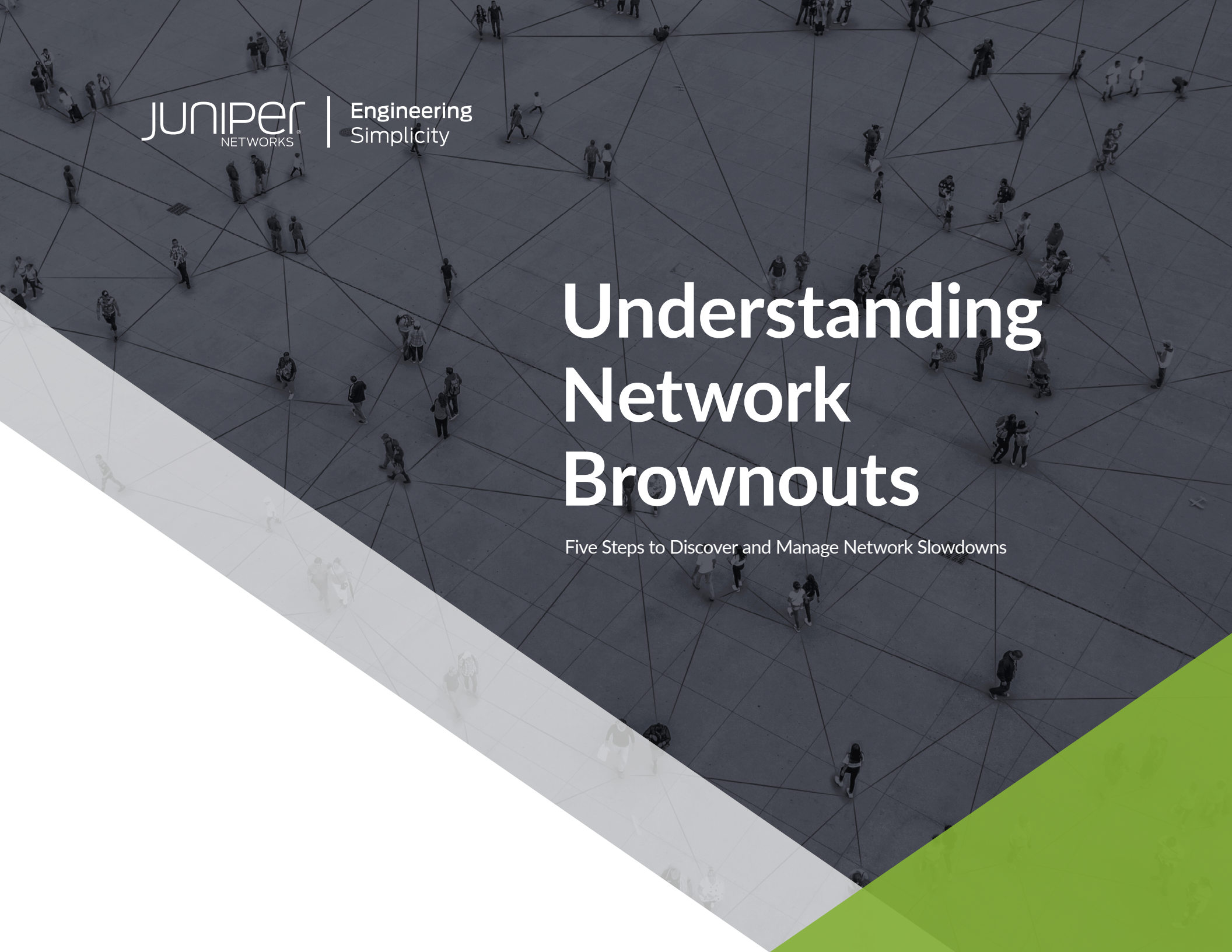


JUNIPER NETWORKS | Engineering Simplicity

Understanding Network Brownouts

Five Steps to Discover and Manage Network Slowdowns

Network Brownouts are First Discovered by IT Customers

Despite how critical network performance is, the 2019 Network Brownouts Survey found that IT organizations are blind to more than 60% of brownouts – or unexpected and unintentional drops in network quality. This is a vital blind spot, as 85% of respondents listed the network as relatively to critically important and identified reliability and availability as the most important aspects of the networking platform – more important than security, performance, or cost.

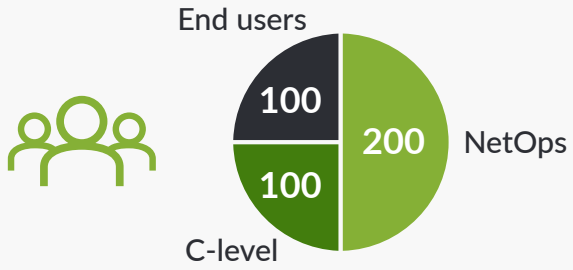
In an increasingly connected world, connectivity and network reliability matter more than ever. Companies rely on the network to communicate, iterate, and distribute their products. Consumers connect to purchase, consume, or engage with brands and services online. Employees increasingly rely on remote connections to accomplish their tasks and remain productive. Any degradation or outage significantly impacts the global marketplace.

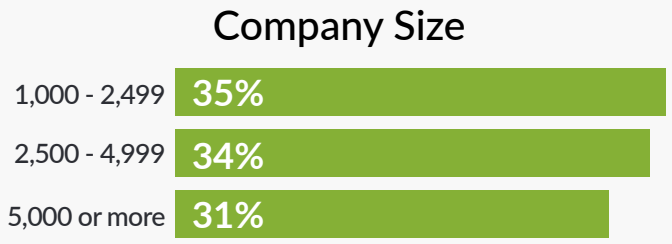
What are Network Brownouts?

Network brownouts are defined as unintentional or unexpected drops in network service quality.

METHODOLOGY
2019 Network Brownout Survey

Juniper Networks surveyed 400 companies across North America to find out how they were dealing with brownouts.





Five Critical Costs of Brownouts

Missing or mismanaging brownouts can be costly for an organization.
The survey found the following key costs of brownouts:

Lost Productivity

First, brownouts have a large impact on an organization's productivity.
Survey respondents state that organizations are 30% less productive as a result of brownouts. Brownouts can ruin the ability to communicate with remote team members, achieve tasks that require network connectivity, or consistently engage with customers. A brownout can cause nearly as much productivity damage as an outage.

Lost Revenue

Second, the survey found that typical organizations lost more than $420,000 over the past two years to brownouts. This revenue loss affected all sizes of organizations: from the Amazons of the world to smaller e-commerce retailers.

Mitigation Costs

Next, organizations often undertake mitigation in order to placate displeased or inconvenienced customers. From product discounts to free credit checks in the event of more serious network issues, these costs add up and hurt in the bottom line.

Monetary Damages

Further, brownouts can render the organization vulnerable to lawsuits, fines, and other monetary damages. From violating SLAs to breaching regulatory protocols, a mishandled brownout can hurt the organization in both the near and long term.

Damaged Reputation

Finally, repeated network degradation can erode customers' faith in the organization. Survey respondents reported experiencing 5 to 9 brownouts within the past two years, with a third experiencing 10 or more. Further, these brownouts were reported to last 3 to 4 hours with 19 percent lasting 7 or more hours.

Top Costs of Brownouts

Companies Are Currently Mishandling Brownouts

Compounding the problem – traditional assurance tools are not enough to discover and manage brownouts.

POOR DETECTION AND RESPONSE

Network operators only discover 39 percent of brownouts – the rest are reported by employees or customers, or are simply never discovered. Additionally, less than half of organizations identify brownouts as serious and add budget to mitigate. Further, the survey found that nearly a third of end users are upset, annoyed and frustrated by brownouts with nearly one in ten leaving the office to work elsewhere as a result.

LACK OF MONITORING

Most of the reported causes of brownouts require active monitoring in order to detect. In fact, five of the top six reasons brownouts occur can only be detected with active monitoring: congestion, missing or misconfigured QoS, problematic in-line devices, external network issues, and poor planning or design of Wi-Fi. Further, organizations which rarely ran activation tests had 10 percent higher costs than those who did.

TOP TIER VS BOTTOM TIER

The survey found that there was a big spread amongst respondents in terms of how well they actively monitored in preventative measures for brownouts. To better understand this, Juniper separated the survey data into three tiers.

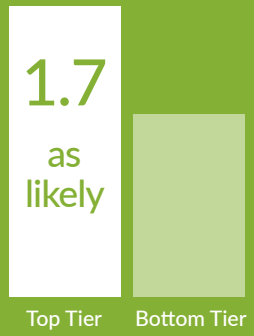
Bottom-tier companies are experiencing more frequent and longer-lasting brownouts than the top tier. As a result, the bottom-tier companies are experiencing significantly higher brownout costs. Additionally, because the top-tier organizations employ more activation tests and have active monitoring in place, they are more frequently discover brownouts earlier.

TOP & BOTTOM TIER?

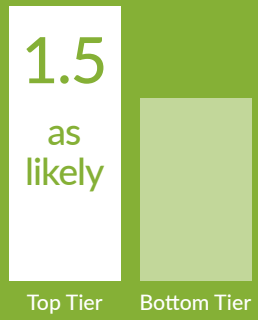
We scored each respondent on each response having to do with how they discover and manage/troubleshoot brownouts. Those whose aggregate score was in the top 33 percent we call "Top Tier" and those in the bottom 33 percent we call the "Bottom Tier."

The top tier more often apply activation tests before giving users access to a new service or network. They also set up a specific monitor for services after launch or configuration, such as continuously monitoring one-way delay to a cloud server. These are two best practices to improve network quality.

Set-up specific monitor for services

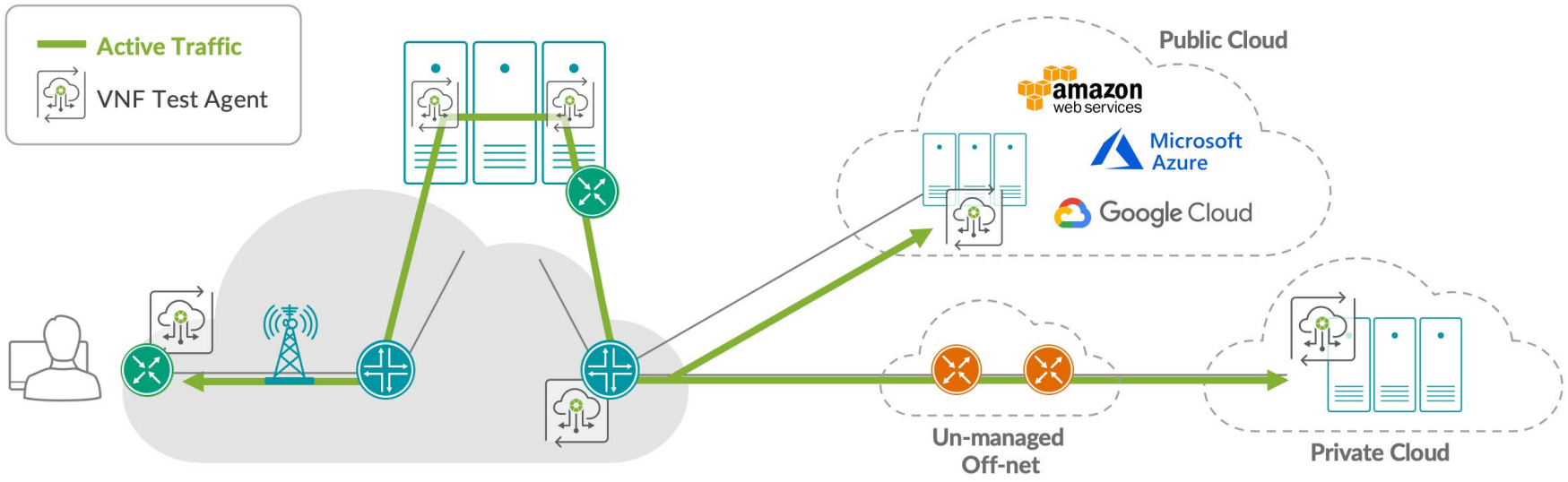


Run activation tests



How to Reduce Brownout Impacts?

Brownouts are common, and currently severe network slowdowns are reported by end users and customers – not by existing monitoring solutions. This can lead to customer attrition and reduced employee productivity. As traditional monitoring solutions focus on device health, they cannot detect complex network service issues affecting your customers and end users. Therefore, it is critical to evaluate solutions that are easy to deploy and use to simulate end-user behavior from the right locations for the relevant network services. When organizations augment their traditional monitoring solutions with active (synthetic) testing and monitoring of network services, they can more frequently catch and mitigate network slowdowns.



Actively inject real network traffic on the data plane - like an end user

Recommendations

1 **REALIZE THAT THE PROBLEM IS VERY COMMON.**
Severe network brownouts are in a majority of cases reported by end users and customers – and not by your existing monitoring solution.

2 **QUANTIFY THE IMPACT FOR YOUR BUSINESS.**
Recognize that the consequence of not detecting network brownouts proactively is lost customers and greatly reduced employee productivity.

3 **ANALYZE GAPS IN YOUR CURRENT SERVICE ASSURANCE SOLUTION.**
Accept that classical monitoring solutions focus on device health and cannot detect complex network service issues affecting your customers and end users.

4 **RESEARCH INNOVATIVE SOLUTIONS.**
There is a missing component in the assurance / monitoring stack that simulates end-user behavior from the right locations for the relevant network services. Evaluate solutions that are easy to deploy and use.

5 **AUGMENT YOUR CURRENT SOLUTIONS WITH AUTOMATED, ACTIVE ASSURANCE.**
Introduce active synthetic monitoring of network services to complement your existing monitoring solution. This will measure in the same way as your customers and end users consume the network and will help detect the majority of issues you are missing today.

CUSTOMER EXPERIENCE:

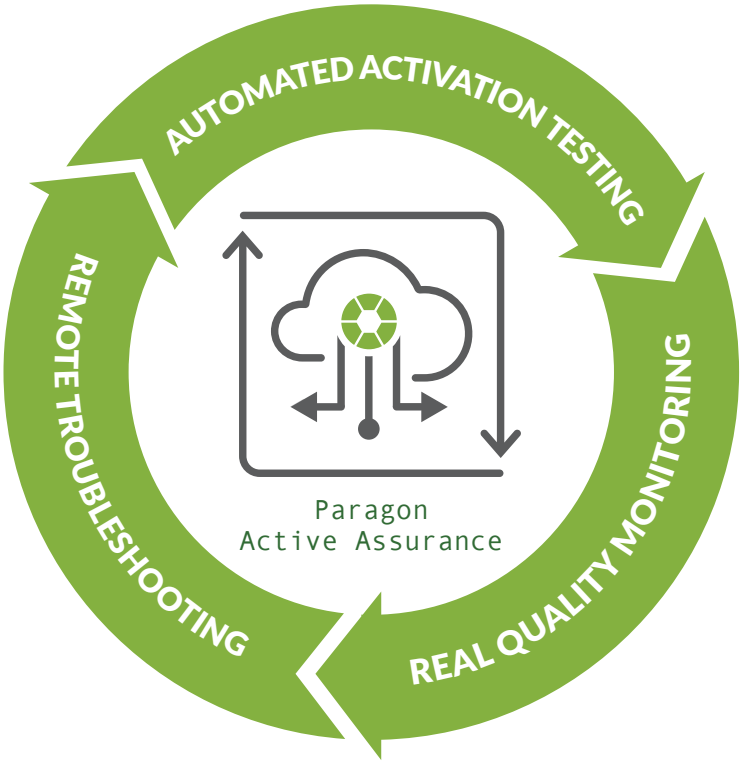
If you can't measure it, you can't manage it.

Conclusion

More than 60% of network brownouts go undiscovered by IT operations and their costs add up, causing an average of $420k of lost revenue for companies. With the adoption of disruptive technologies such as hybrid clouds, SD-WAN and network virtualization, the cost of brownouts will continue to increase.

The main reason for the high costs of brownouts is that many IT organizations are failing to resolve the problems fast enough. Top-performing companies solve more than half of their problems in less than four hours, whereas bottom-tier companies only manage to solve every sixth problem within the same time frame.

The most successful organizations employ active monitoring to quickly detect and resolve brownouts and maintain revenue. Companies prioritizing investments in these solutions will enjoy reduced financial damage and can embrace their digital transformation journey with peace of mind.



To learn more about Juniper in order to help you resolve and prevent brownouts while reducing costs with an active testing and monitoring solution, visit www.juniper.net/paragon-active-assurance or access our Paragon Active Assurance Datasheet.

Contact us to learn more about how we can help you

Corporate and Sales Headquarters

Juniper Networks, Inc.

1133 Innovation Way

Sunnyvale, CA 94089 USA

Phone: 888.JUNIPER (888.586.4737)

or +1.408.745.2000

Fax: +1.408.745.2100

www.juniper.net

APAC and EMEA Headquarters

Juniper Networks International B.V.

Boeing Avenue 240

1119 PZ Schiphol-Rijk

Amsterdam, The Netherlands

Fax: +31.0.207.125.701

PN2000759-001-EN

JUNIPER NETWORKS