Progress® WhatsUp® Gold

Network Path Analysis

See where network performance problems begin

DATA SHEET

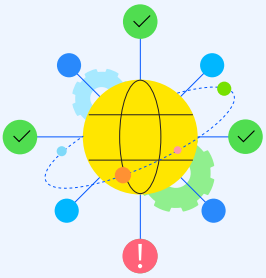
Troubleshoot Network Paths Without Guesswork

A slow application does not always point to a server problem. Performance can degrade across a WAN link, VPN gateway, ISP handoff, cloud route, or another segment outside your direct control.

WhatsUp Gold Network Path Analysis gives network teams a clearer view of the route traffic takes and how that route behaves over time.

Instead of relying on a single traceroute taken after the problem has passed, teams can review historical path information and compare what changed during the incident.

See the path. Find the point of degradation. Investigate with evidence.



Visualize the paths between users and critical services, track changes over time, and identify where latency, packet loss, or routing issues first appear.

Understand What Changed When Performance Dropped

Traditional traceroute provides a useful point-in-time view of a route. But intermittent network problems often disappear before an administrator has a chance to investigate them.

Continuous network path monitoring repeatedly measures the route between a defined source and destination, building a history of path and performance data. Administrators can compare normal and affected periods to see where latency increased, where packet loss appeared, or whether the observed route changed around the same time users experienced an issue.

What Network Path Analysis Means for Your Team

1. **Isolate Problem Areas Faster**

   Enterprise Plus consolidates infrastructure monitoring, cloud insights, wireless visibility, and virtualization intelligence into a single, interactive platform view—eliminating blind spots and tool sprawl.

2. **Investigate Intermittent Issues with Historical Data**

   Network problems do not always occur while someone is watching.

   Historical path information preserves what happened during the affected period, giving administrators a way to compare the normal route with the route and performance observed during an incident.

3. **Track Route Changes Over Time**

   Network paths can change because of routing policies, failover events, maintenance, SD-WAN decisions, or upstream traffic engineering.

   Path history helps administrators determine when those changes occurred and whether they coincided with changes in application or network performance.

4. **Build Better Evidence for Escalation**

   When degradation appears beyond infrastructure you control, path information provides a clearer technical reference for conversations with ISPs, cloud providers, application owners, or other infrastructure teams.

   Share the affected source and destination, incident timeframe, observed route, and point where degradation first became visible.

Visibility Across Distributed and Hybrid Environments

Application traffic increasingly crosses infrastructure managed by different teams and providers. Monitor network paths from locations that reflect how your users actually connect to important services.

Path monitoring can provide visibility across:

- Branch and remote office connections
- Data center and campus networks
- Cloud-hosted workloads
- SaaS application paths
- VPN and remote access connections
- ISP and transit segments
- Hybrid infrastructure

Monitoring from multiple locations can also reveal differences that a single central vantage point may miss. A service that performs normally from the data center, for example, may follow a different route for branch or remote users.

Move From a Complaint to a Focused Diagnosis

Without path history

- A user reports that an application was slow
- Device and server checks appear normal
- A traceroute taken later shows no obvious problem
- Administrators try to recreate an issue that has already disappeared

With continuous path monitoring

- Review the network path during the affected period
- Compare it with normal path behavior
- Identify route changes or sustained increases in latency and loss
- Focus investigation on the segment where performance changed

Path data does not automatically prove which provider or device caused an issue, but it gives teams a much more precise starting point for investigation.

Why Network Teams Use WhatsUp Gold for Path Analysis

See More Than the Symptom

A slow application tells you there is a problem. Network path analysis helps narrow down where that problem may have started by showing the route and its performance.

Keep the Evidence After the Incident

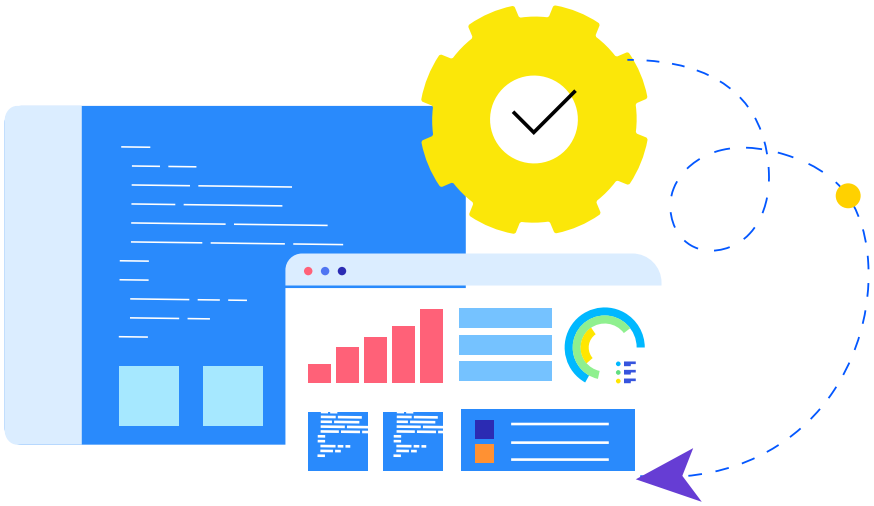
Continuous measurements provide historical context for problems that are difficult to reproduce after the fact.

Extend Visibility Beyond Your Own Infrastructure

Follow application delivery paths as they cross internal networks, ISPs, cloud environments, and SaaS infrastructure.

Give Other Teams Something They Can Investigate

Use path maps and historical performance data to provide a specific timeframe and affected network segment when escalating an issue.



Discover WhatsUp Gold
Contact your Progress representative today to future-proof your monitoring and strengthen your security posture with every renewal.

About Progress

Progress Software (Nasdaq: PRGS) empowers organizations to achieve transformational success in the face of disruptive change. Our software enables our customers to develop, deploy and manage responsible AI-powered applications and personalized digital experiences with agility and ease. Businesses of all sizes get a trusted provider in Progress, with the products, expertise and vision they need to turn AI disruption into a competitive advantage. Millions of developers and technologists at hundreds of thousands of organizations depend on Progress every day. Learn more at www.progress.com.

/progresssw
/progresssw
/progresssw
/progress-software
/progress_sw_

Progress