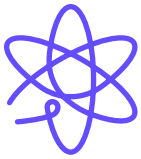
Increase resilience of critical infrastructure

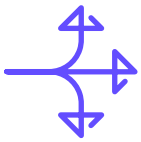
When's the last time you had a network outage?

Maybe things are so good that you can't even remember the last time. (If so, congratulations.) Or maybe your last outage happened more recently than you care to remember. Maybe that outage was only the latest in a string of incidents stretching over the past week, month, or quarter. Maybe those outages are becoming more frequent, and lasting longer.

Fragile networks are easy to spot. Here are some of the most common symptoms:



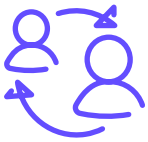
Decentralized Siloed operations are a telltale sign of a fragile network. When everyone's responsible for their own little fiefdom, they tend to charge forward without understanding the consequences. This often leads to conflicts and misconfigurations which spiral out of control.



Complex On a fragile network, everything runs through a dizzying array of configurations and processes - so many, in fact, that nobody really understands how they all work together. One missed connection is all it takes to bring the whole system to a halt.

Unpredictable When nobody knows how changes will impact the network, that's a clear indicator of fragility. If you're scared to tackle strategic initiatives or roll out new systems, something's seriously wrong.

Manual If the network team is spending most of its time simply managing back-end configurations, you're probably dealing with a fragile network. When any workload change seems unmanageable, it's a sign that scaling up is out of the question.



Compartmentalized Fragile networks can't operate without the knowledge of a few people (or a single person). If you're aligning change windows around vacations of certain people, that's an indicator that your network isn't resilient enough to operate without them.

The first step in dealing with network fragility is acknowledging that you have a problem.

With apologies to Hemmingway, networks become fragile gradually, then suddenly. When outages become all too frequent, it's usually the result of infrastructure problems that developed over months or years. Every IT manager reaches a point where the network they built simply can't deliver the performance everyone expects.

Maybe it's a major outage that threatens the business. Maybe it's a steady drip of incidents that suddenly become noticeable to internal users or customers.

BLUECAT™

If any of this sounds familiar, you probably know where we're going to point the finger. It's not at the network team - they're just trying to stay afloat. It's not your end-users or executives - they just want a network that delivers.

The problem is your DNS, DHCP, and IPAM (DDI).

When it functions well, you're not supposed to even notice DDI. It just blends into the background. You can take it for granted.

When your DDI is complex, your network is inherently fragile. That fragile network drives up back-end operational costs, increases risk, and prevents you from meeting basic service expectations. You've probably got compliance issues, too.

It's an even bigger problem if you're trying to move to the cloud, implementing automation, or operating a complex global enterprise. (And who isn't doing one or all of those things?)

Your DDI should be:

Dynamic DDI should provide visibility and insight into the state of users, devices and applications across hybrid environments

Open DDI systems should integrate seamlessly with hybrid cloud and other mission-critical IT systems, using open APIs and built code.

Secure DDI should act as an intelligent control plane for rapid threat detection and response on both internal and external pathways.

Scalable DDI systems should be easy to deploy whenever and wherever you want them to be.

Automated DDI should implement smart security policies, remediate threats, and analyze data at machine speed.

BLUECAT™

In a nutshell, that's BlueCat's vision for your network. We call it Adaptive DNS.

Of course, there's a lot more to it than that. We can talk your ear off about high availability, IPv6, GSS-TSIG, direct internet access, and all the other nitty-gritty technical details. But all the bits and bytes really point to one thing: DDI that you can take for granted. DDI that doesn't crash your network.

Isn't that what you want, after all?

But seriously, though, here's where we get into the weeds.

Learn more about BlueCat's DDI solutions

bluecatnetworks.com