Things to consider for **BETTER INTERNET FAILOVER**

Today, having failover coverage is crucial for any modern business that relies on the internet. There are many options and points to consider when creating the right failover setup for your business.

So how do you choose?

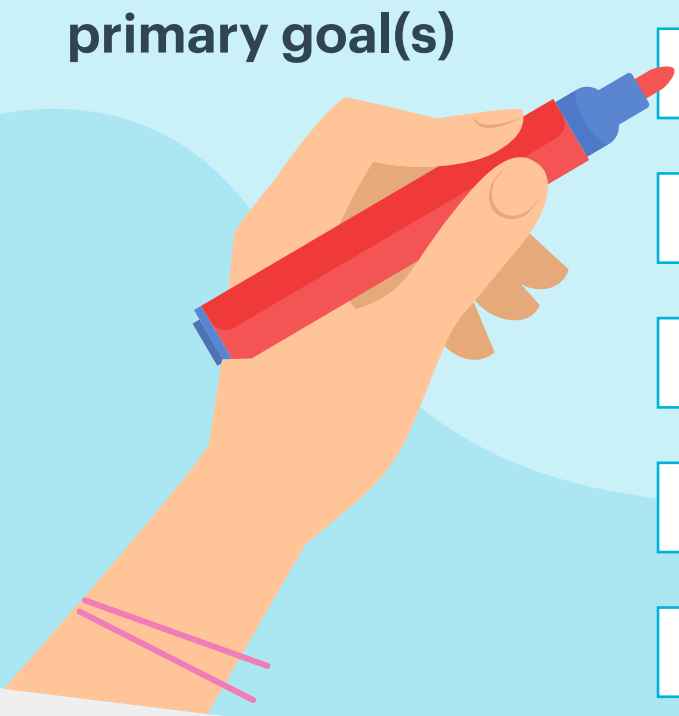
STEP 1

Understand the many ways that internet connections can fail

- ISP outage
- Latency spikes or packet loss
- Scheduled (or unscheduled) maintenance
- Natural disasters
- Hardware failure
- Power outage
- Physical cutting of the service line
- Human error
- DDoS or other cyber attacks

STEP 2

Identify your primary goal(s)



Rank the following from most to least important for your business:

- ☐ Get as much uptime as possible
- ☐ Resume business operations quickly following an outage, including those caused by a natural disaster
- ☐ Optimize cloud technology and application performance (video conferencing, VoIP calls, Microsoft 365, POS, CRM, ERP, etc.)
- ☐ Avoid interruptions when failing over from one internet connection to another
- ☐ Efficiently manage company IT resources, from budget to team staffing
- ☐ Other

STEP 3

Consider your organization's needs and check the items necessary to optimize your internet failover setup

☐ **ISP diversity**

Separate internet connections from different ISPs or carriers. This gives you a greater ability to mitigate problems and route around issues, like when an ISP's entire network goes down, because you're not reliant on one internet provider.

☐ **Last mile & connection type diversity**

Physical diversity in the "last mile" to your offices and sites consisting of multiple and different circuit types (i.e. a combination of fiber, enterprise fixed wireless, cable, copper, T1/T3, other fixed wireless, DSL, cellular, or satellite connections).

☐ **Same IP address failover**

A static public IP address that doesn't change when your traffic moves between ISP connections. This ensures that all your applications automatically stay up and running without any noticeable disruption, even when one of your circuits is experiencing an outage or performance issues.

☐ **Active-active or active-passive configuration**

An active-active configuration is where both (or all) of your internet connections are actively carrying some of your traffic at any given time. You can even have different types of traffic routed to the connection that's best suited for it. In an active-passive configuration, one line sits idle waiting for the primary line to completely fail before hopping into action.

☐ **Bi-directional QoS**

Bi-directional QoS allows you to prioritize important traffic, and even route upload and download traffic to specific circuits for maximum control; compared to traditional failover options that almost never give you control over your download traffic.

☐ **Automated, intelligently-powered software**

Software that automatically monitors your circuit performance, detects and classifies new technologies and traffic types on your network, and routes and reroutes your traffic to prevent disruptions – without the need for constant manual policy configuration, testing, debugging, and implementation.

STEP 4

Choose the best internet failover setup for your business

Internet failover isn't one-size-fits-all; what's right for one business may not make sense or be reliable enough for another. The main factors to consider are IT resources, budget, and how much the business relies on cloud- and internet-based applications.

If you're ready for effortless internet reliability and optimization, then we invite you to learn more about Bigleaf.

Your business depends on the internet.
Your internet depends on Bigleaf.

REQUEST A DEMO TODAY

bigleaf networks

www.bigleaf.net
888.244.3133
sales@bigleaf.net