ERICSSON

Network failover: Cellular strategies that protect against downtime

How to effectively integrate cellular broadband to build resilience and uptime in offices, stores, and other fixed locations

Image courtesy of Getty Images

Addressing critical risk points in fixed-site networks

No. 1

Add link diversity

Jump to page 3 →

No. 2

Ensure multi-carrier connectivity

Jump to page 4 →

No. 3

Add hardware redundancy

Jump to page 5 →

No. 4

Accomodate traffic spikes

Jump to page 6 →

No. 5

Troubleshoot networks remotely out of band

Jump to page 7 →

How much business can your organization conduct when your office or HQ network is down? Mission-critical and cloud-based applications have made reliable wide-area networks (WANs) essential for distributed sites such as stores and offices. Currently, most companies' workloads run or are stored in the cloud, and employees use an increasing number of cloud-based services every day for file sharing, collaboration, and communication tools.

Increasing the diversity of network components and connections reduces single points of failure that can significantly impact your operations. Wireless WAN (WWAN) links built on 5G and LTE technologies are powerful, flexible, and cost-effective additions to fixed-site operations. They improve network uptime, application performance, and business continuity — especially when integrated with software-defined WAN (SD-WAN) capabilities.

This resource outlines how hybrid Wireless WAN capabilities can boost the resilience of your business through five essential networking strategies:

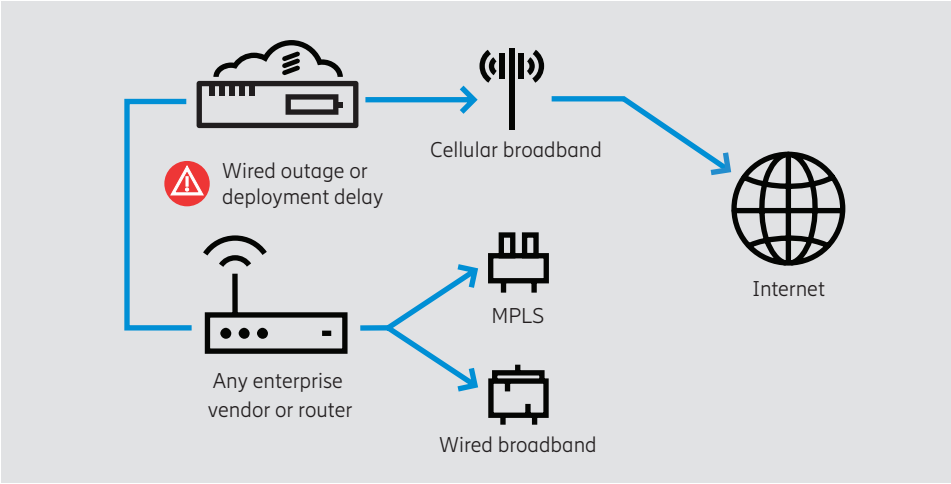
- No. 1: Add link diversity
- No. 2: Ensure multi-carrier connectivity
- No. 3: Add hardware redundancy
- No. 4: Accomodate traffic spikes
- No. 5: Troubleshoot networks remotely out of band

Image courtesy of Getty Images

No. 1 Add link diversity

In many cases, a fixed-site WAN connection depends on a single wire running to a chosen internet service provider (ISP). This thin link to the corporate network and cloud can be disabled in a variety of ways, including serious weather events, construction accidents, or human configuration errors.

A quick and easy way to reduce the risk of a disconnect is to add another WAN connection. A second wire is susceptible to the same risks as the first one, and the wait for installation may be lengthy. Adding a cellular or satellite wireless link provides both backup and diversity to the network. Rapid failover seamlessly switches from one link to another, minimizing network and service disruption.



Lower-bandwidth LTE connections may only carry critical traffic, as configured by WAN and traffic management policies. But higher-bandwidth links such as 5G can carry the full traffic load.

This wireless connection can also be a network and IT management lifeline, enabling you to remotely monitor, manage, and troubleshoot the router and other equipment over the air.

There are a couple of ways to add WWAN connections to your existing network, enabled connections to your existing network, enabled and enhanced by a cloudbased, centralized management service. Ericsson Cradlepoint 5G routers provide reliable connectivity, advanced management, and failover capabilities as well as Ethernet and Wi-Fi interfaces, making them a simple, drop-in addition at the branch. These sophisticated devices can be configured at scale using Ericsson Cradlepoint NetCloud Manager™, which offers a full range of SD-WAN, security, application quality of service (QoS), and management features that integrate into existing configurations with standards-based routing and support for zero trust architecture.

Another option is adding a wireless connection to an existing router using a 5G or LTE adapter, then relying on its SD-WAN and failover functionality. Best of all, you can deploy wireless failover much faster than waiting for a new wire. Both routers and adapters offer zero-touch deployment features, eliminating the need for an on-site visit.

"When we deployed Ericsson Cradlepoint solutions in our retail stores, the results were immediate. We experienced increased availability as we saw our network take over when the primary transport link went down."

T-Mobile Operations Department

Image courtesy of Getty Images

No. 2 Ensure multi-carrier connectivity

Relying on a single telecom carrier or internet provider is another risk point for branch continuity. Network congestion, routing and DNS issues, and core network outages are just some of the potential incidents that can disrupt business operations.

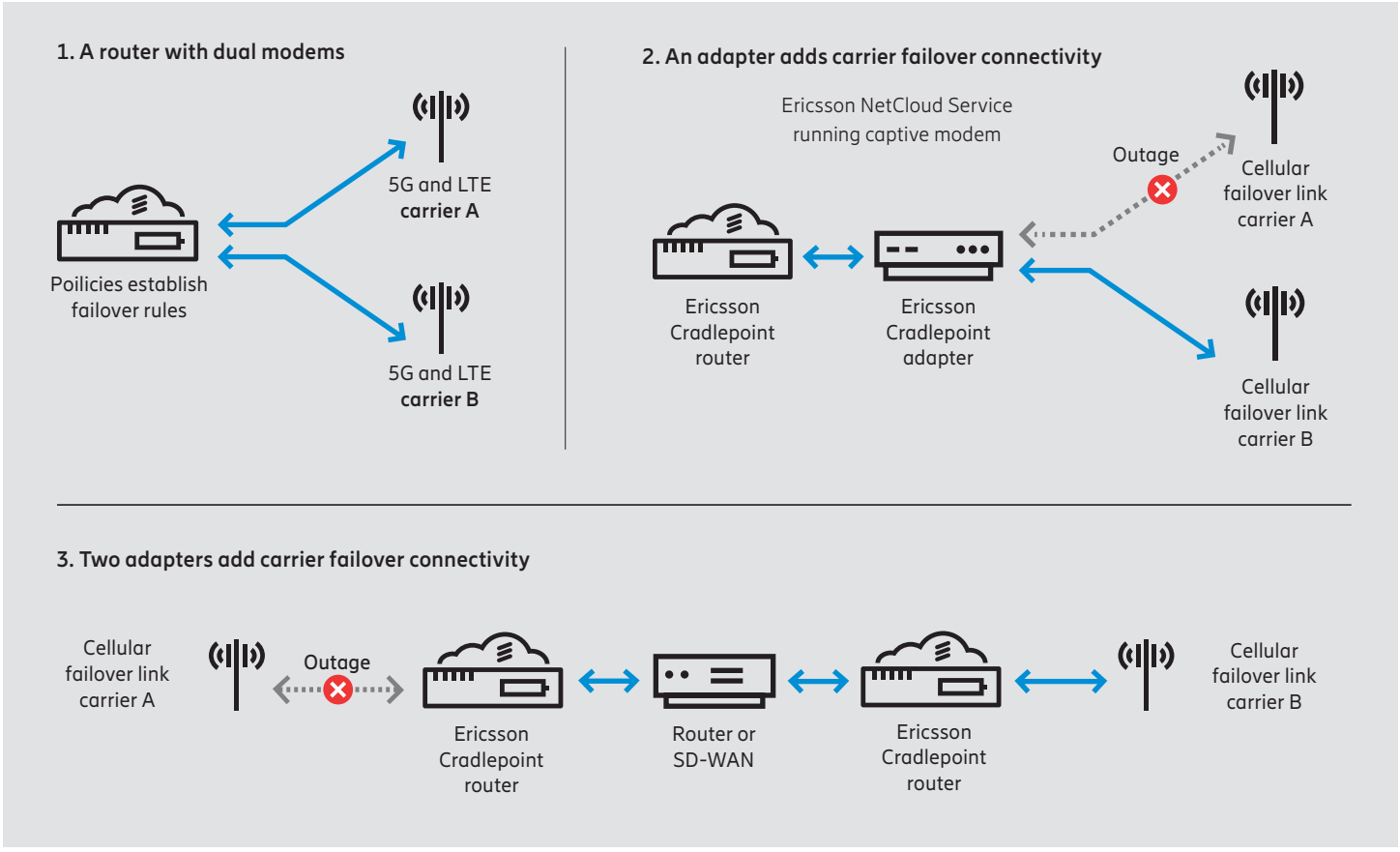
You can reduce the risk of carrier disruptions by using two links with different wireless carriers. The separate infrastructure adds network diversity, making it highly unlikely that both would be unavailable at the same time. You can establish policies to operate the two links as a primary and backup, or increase your bandwidth using intelligent link bonding.

Wireless WANs also bring greater agility to many locations, making it easier to open new locations or move existing ones. You decide when and where to set up, making wireless even more important for short-term or temporary locations. Larger organizations may find it cheaper and easier to negotiate and operate two national wireless contracts, instead of a varied mix of internet service providers.

The simplest way to employ two wireless carriers is to use a 5G or LTE router that supports two modems. Most Ericsson Cradlepoint routers have this capability, making deployment as easy as adding a second modem and SIM card to the device. SD-WAN capabilities and smart routing policies manage the different links, from seamless failover to burst capacity in peak periods. You can identify and route traffic independently, sending specified devices or applications on different paths for security or performance reasons.

It is also possible to use two carriers by adding two wireless adapters to an existing router, but this configuration lacks the advanced network awareness and routing capabilities of an integrated solution.

Dual-carrier connectivity three ways

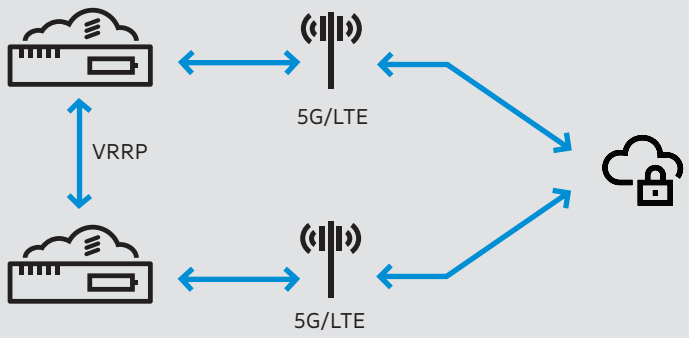


No. 3 Add hardware redundancy

A single branch router can go offline for several reasons, from configuration errors and software update failures to security attacks and even cable issues. These often require a site visit to fix, leaving the location isolated until tech support arrives.

Business functions that rely on 24/7 network uptime can be adversely impacted by service disruptions. Redundant or mirrored routers are an effective protection against router downtime from maintenance or failure. The routers monitor each other, and the backup automatically takes over if the primary router or WAN link fails, and then switches back when the primary is restored. With a primary and backup router, you can safely stage updates, configuration changes, and other periodic maintenance without risking business critical communications.

Adding different WAN links or carriers to each router provides additional protection from common business continuity risks. Configuring both routers with the same security capabilities ensures that operations continue without additional risk. If the backup router has a lower bandwidth connection, traffic policies ensure essential traffic is prioritized.



As shown, up to four carriers could be connected with dual-modem routers. Ericsson Cradlepoint routers can also mirror already installed VRRP-capable routers.

Ericsson Cradlepoint routers for sites use Virtual Router Redundancy Protocol (VRRP) to configure and coordinate router failover. The routers are linked together via direct cable or through an Ethernet switch. NetCloud configuration parameters identify the primary and backup router as well as the desired timing and conditions for determining WAN link failure. Both routers share a virtual gateway address and DHCP table, so other devices on the network continue as if nothing has changed.

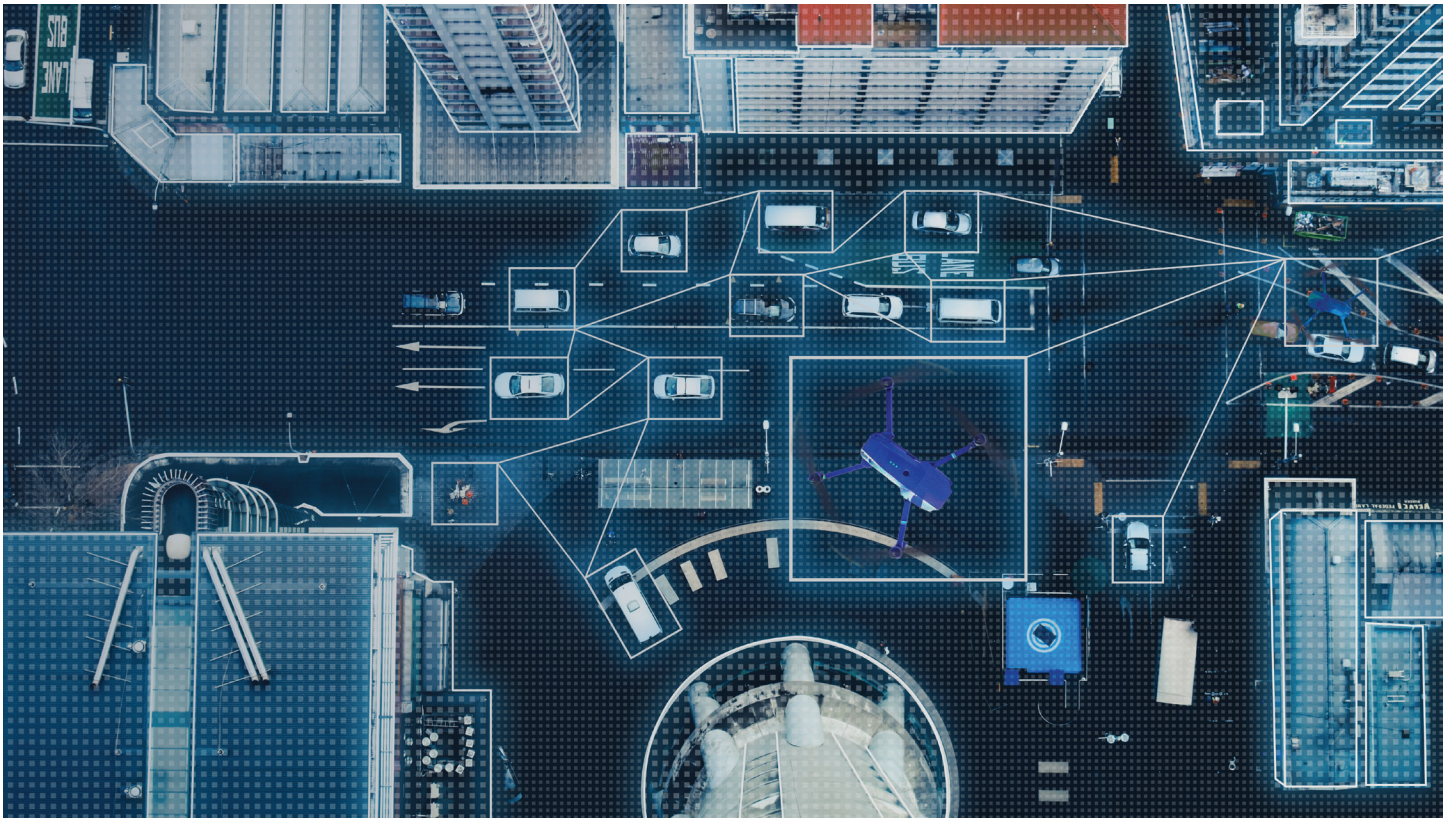
During the failover state, the former primary router continues checking its WAN connection and automatically signals to the backup that it is time to switch back when service has been restored.this configuration lacks the advanced network awareness and routing capabilities of an integrated solution.

No. 4 Accommodate traffic spikes

Sometimes everything is working fine, but the amount of traffic is just too much for the available bandwidth, causing some or all applications to slow down. Increasing use of video is a leading cause, but file-sharing apps, software updates, and the rising number of connected devices are also likely contributors to traffic spikes and network congestion.

One simple solution to traffic congestion is to use the backup wireless link to augment or off load the primary connection. As traffic builds, the secondary link is activated, and traffic is dynamically routed to the best available path. Once the spike has passed, the wireless connection is released. All of this is fully automatic and completely invisible to staff. You can also use the secondary link to regularly augment the network during peak periods or reserve it for specific applications or devices.

Ericsson Cradlepoint routers with NetCloud SD-WAN capabilities are optimized for cellular and can easily handle these scenarios. There are many ways to configure this function, based on WAN conditions, specific applications, or security considerations, among other criteria. Policies can be built to define the necessary conditions for using the alternate wireless link, with full awareness of your wireless services and any restrictions or caps. Advanced SD-WAN capabilities can separate applications or devices and assign them to a specific link. For example, IT teams may want to keep business-critical financial or database applications separate from generic web traffic and guest networks.

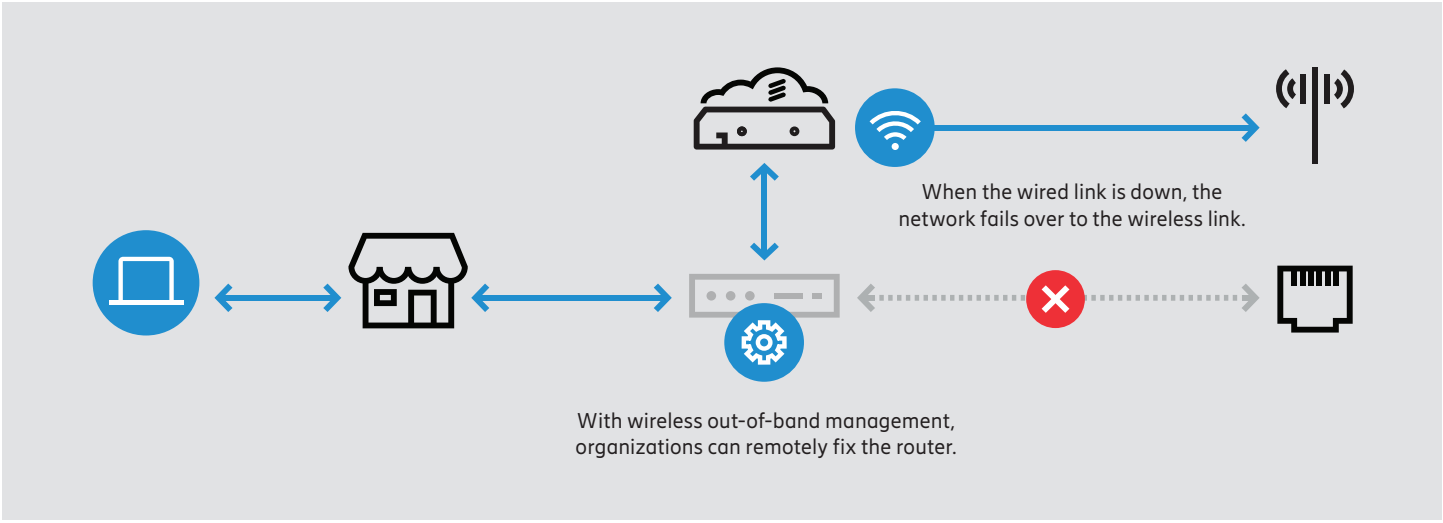


No. 5 Troubleshoot networks remotely out of band

When a fixed-site loses connection to the corporate network or the cloud for whatever reason, you also lose visibility of and access to all of the branch devices. Network management becomes much more difficult, often requiring a site visit or painstakingly walking a local employee through the troubleshooting process.

Wireless links provide an alternative network management option when the primary link or endpoint device is unreachable. You can easily add Out-of-Band Management (OOBM) capabilities to your network with an Ericsson Cradlepoint wireless router, or by connecting a wireless adapter directly to the console port of your primary router. Wireless connectivity gives network managers easy and secure access to the device, enabling them to diagnose and fix problems over the air.

You can also get to the LAN and any other important business devices on the local network with in-band management services. Ericsson Cradlepoint routers and NetCloud services make LAN devices accessible and manageable from anywhere. As a device joins the network, its IP address and host name appear in NetCloud Manager. With Remote Connect, the IT team can make it cloudmanaged with one click.



Greater resilience at the network edge

Network uptime is vital to the business, and WWAN links are critical for business continuity. Cloud services, IoT devices, and greater mobility are pushing businesses beyond the architectural constraints of wired networks and driving the need for greater diversity and resilience.

Establishing network redundancy and resilience does not have to be expensive or complicated. Cloud management, network and data plan monitoring, and zero-touch deployment make implementation and operations quick and easy. Advanced wireless capabilities understand what, when, and how to connect to cellular networks, with enhanced link reliability to get and stay connected. Cellular-optimized SD-WAN capabilities allow organizations to build and apply traffic policies based on multiple criteria, including WAN performance, application needs, and security. WWAN solves multiple problems for business networks, creates new opportunities, and lays the foundation for further transformation and innovation.

Learn more at cradlepoint.com

Image courtesy of Getty Images