



Secours de lien : actif/passif, actif/actif, bascule automatique — les architectures

Avant, une coupure internet laissait le téléphone en vie, et inversement : les réseaux étaient distincts. Après le cuivre, **un seul accès porte tout** — internet, téléphonie, paiement, alarmes, cloud. La question n'est donc plus « aurai-je une panne ? » (oui, un jour) mais « que se passe-t-il pendant ? ». La réponse s'appelle le secours de lien, et elle se décline en trois architectures aux comportements très différents. Les voici, du plus simple au plus exigeant — avec ce que chacune coûte et ce qu'elle garantit vraiment.

La règle d'or avant l'architecture : un secours de nature différente

Un secours ne vaut que s'il ne tombe pas avec le lien principal. Deux fibres du même opérateur passant par le même fourreau tombent ensemble au premier coup de pelleteuse. La redondance utile croise les **natures** : fibre + 4G/5G (le duo standard, détaillé dans [résilience et secours mobile](#)), fibre + satellite pour les sites isolés, ou deux fibres à **cheminements réellement distincts** — ce qui se vérifie, ne se suppose pas. Et le secours inclut l'électricité : un routeur de secours sans onduleur ne secourt rien du tout, comme le rappelle [la résilience de la voix sur IP](#).

Architecture 1 : le secours froid — présent, mais éteint

Le secours « froid » est l'assurance minimale : une clé ou box 4G dans un tiroir, un abonnement dormant, une procédure. En cas de panne, quelqu'un branche, reconfigure, redémarre. Coût quasi nul — mais **délai de rétablissement en heures**, dépendant de la présence de la bonne personne, et l'expérience montre que le matériel du tiroir n'a souvent jamais été testé. Acceptable pour un site secondaire sans usage critique ; insuffisant dès qu'un paiement, un accueil téléphonique ou une alarme dépendent du lien.

Architecture 2 : l'actif/passif — la bascule automatique

Le standard professionnel : le lien de secours (typiquement 4G/5G) est **raccordé en permanence au routeur**, qui surveille le lien principal et bascule seul en cas de défaillance — en quelques secondes à une minute. Retour automatique quand le principal revient. Trois points font la différence entre une bascule propre et un secours de papier : la **détection** (tester la connectivité réelle, pas seulement l'état du port), la **priorisation** en mode secours (le débit 4G étant partagé, la voix et le paiement passent avant la vidéo et les sauvegardes), et le **changement d'adresse IP** lors de la bascule — anodin pour la navigation, structurant pour la téléphonie et les accès distants, qui doivent être configurés pour y survivre. C'est l'architecture recommandée pour la grande majorité des sites professionnels.

Architecture 3 : l'actif/actif — les deux liens travaillent

Ici, les deux liens portent du trafic en permanence : les flux sont répartis (la voix sur le lien garanti, la masse sur le mutualisé), et la défaillance de l'un reroute instantanément vers l'autre — **sans délai de bascule perceptible**, puisque le second lien est déjà en service et déjà supervisé. C'est le domaine naturel du [SD-WAN](#), qui mesure la qualité des deux chemins en continu et peut même basculer un appel en cours. Contreparties : deux abonnements pleinement utilisés, un équipement plus capable, et une conception réseau sérieuse. À réserver aux sites où l'interruption, même d'une minute, coûte — accueil intensif, production, santé.

Choisir : la criticité décide, pas le catalogue

- **Site secondaire, usages non critiques** : secours froid documenté et testé deux fois par an — au minimum.
- **Site professionnel courant** (commerce, agence, cabinet, mairie) : actif/passif automatique avec priorisation voix/paiement — le standard raisonnable.
- **Site critique** : actif/actif — souvent fibre garantie ([GTR](#)) + second lien de nature différente, sous pilotage SD-WAN.

Et dans tous les cas, une règle que les plans oublient : **un secours non testé n'existe pas**. La bascule se teste à la mise en service, puis périodiquement, en conditions réelles — débrancher le lien principal un mardi matin et vérifier que le téléphone sonne encore. Ce test, et le dimensionnement du lien de secours (débit, enveloppe data), feront l'objet d'articles dédiés de ce dossier résilience.

En synthèse

- Après le cuivre, un seul accès porte tout : **le secours de lien est l'assurance-vie du site**.
- Règle d'or : un secours de **nature différente** (fibre + 4G/5G) et alimenté électriquement.
- **Froid** = heures d'interruption ; **actif/passif** = secondes, le standard pro ; **actif/actif** = continuité totale, pour les sites critiques.
- Détection réelle, priorisation des flux, survie au changement d'IP, tests périodiques : les quatre détails qui font un vrai secours.

Cet article décrit des architectures types à visée d'information ; le dimensionnement réel dépend des usages, de la couverture mobile locale et des équipements. Il se valide sur étude et se vérifie par des tests.

Pour aller plus loin

- [Résilience et secours mobile : assurer la continuité de service](#)
- [Résilience de la voix sur IP : que se passe-t-il en cas de coupure ?](#)
- [SD-WAN vs MPLS : le match de l'interconnexion multisite](#)
- [Comprendre la GTR \(Garantie de Temps de Rétablissement\)](#)

Combien coûterait une journée sans lien sur votre site ?

AILERYS Conseil dimensionne votre secours — architecture, priorisation, tests — au juste niveau de votre criticité, en toute indépendance.

Échanger avec un expert : <https://finducuire.info/contact/>

À lire aussi dans ce dossier

- [NIS2 et résilience télécom : quelles exigences après le cuivre ?](#)
- [Box 4G/5G fixe : quand est-ce une vraie alternative à la fibre ?](#)
- [Le coût d'une coupure non anticipée : le risque de l'attentisme](#)
- [QoS et qualité de la voix sur IP : les prérequis réseau à vérifier](#)

Article révisé le 21 septembre 2026 par FinduCuivre.info

<https://finducuivre.info/secours-lien-actif-passif-bascule-automatique/>