L'ATELIER DE BDSN

Souveraineté · Doctrine · Transformation

Je suis passé à une offre à 8 Gb/s et voici comment j'ai repris tout mon réseau

Un réseau domestique se migre comme une infrastructure de production : préparation isolée, bascule contrôlée, validation mesurée, retour arrière possible à tout instant.

Par **Bruno DE SAN NICOLAS**

1er août 2026 — bdsn.eu — Rubrique Technologie

8 Gb/s. C'est le débit que mon opérateur me vend désormais. C'est aussi la vitesse à laquelle j'ai réalisé que mon réseau de 2018 était devenu le goulot d'étranglement de la maison. Vendredi soir : la nouvelle box est annoncée pour le lendemain. Samedi matin : le routeur Wi-Fi 7 est configuré à blanc, hors ligne, sur un coin de bureau. Samedi soir : 25 clients ont basculé sans qu'aucun membre de la famille ne s'en aperçoive.

Ce n'est pas de la chance. C'est de la méthode. La voici, du déballage du carton au dernier ping.

Le point de départ

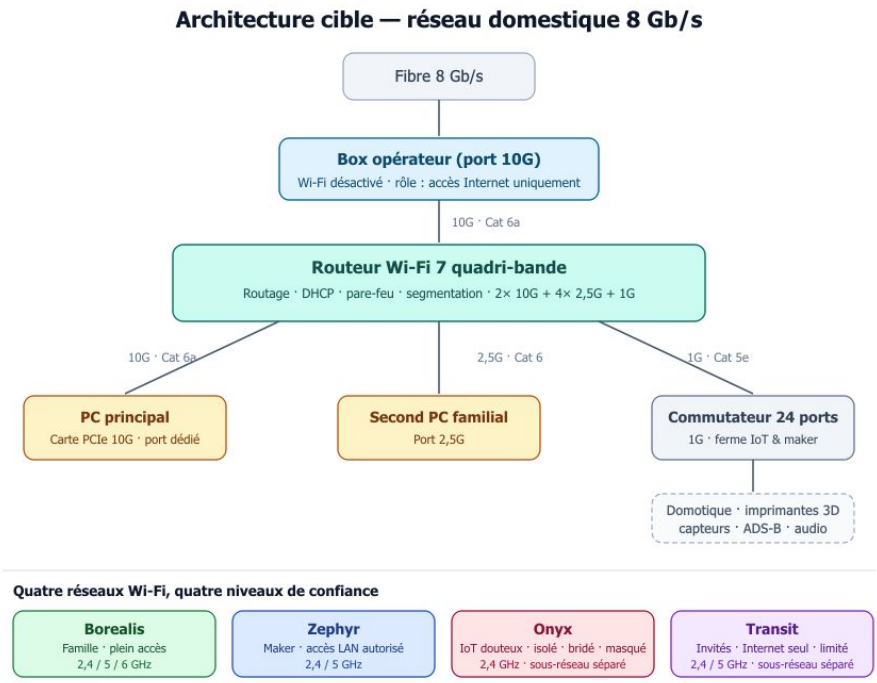
L'existant datait d'une autre époque du très haut débit :

- une box opérateur de génération précédente, plafonnée à 1 Gb/s sur ses ports ;
- un routeur Wi-Fi de 2018 (Wi-Fi 5), vaillant mais dépassé ;
- deux répéteurs Wi-Fi qui multipliaient la latence plus que la couverture ;
- un commutateur 24 ports Gigabit hébergeant la ferme maker : domotique, imprimantes 3D, récepteur ADS-B, station météo, amplificateur réseau ;
- 25 clients au total, dont une majorité entassée sur la bande 2,4 GHz ;
- et deux caméras IP d'entrée de gamme, conception chinoise, dont le trafic part par défaut vers des serveurs hors Union européenne. On y reviendra.

Le tout fonctionnait. C'est précisément le piège : un réseau qui fonctionne n'incite jamais à être repensé. L'arrivée d'une offre à 8 Gb/s a fourni le prétexte — et l'obligation, puisque la nouvelle box impose un port 10 Gb/s que rien dans l'existant ne savait exploiter.

La cible

L'architecture visée tient en quatre étages :



Architecture cible — réseau domestique 8 Gb/s

La box opérateur descend d'un cran dans la hiérarchie : Wi-Fi désactivé, rôle réduit au strict accès Internet. Le routeur Wi-Fi 7 devient le cerveau — routage, DHCP, pare-feu, segmentation. En dessous, trois branches filaires : le PC principal en 10G, le second PC familial en 2,5G, et le commutateur 24 ports en 1G qui dessert la ferme IoT et maker.

> Principe directeur : **chaque équipement au niveau de débit qu'il sait réellement consommer**. Le commutateur 1G reste en 1G — ses clients plafonnent à quelques dizaines de Mb/s chacun, lui offrir une liaison montante 10G serait payer une Ferrari pour livrer des baguettes. À l'inverse, le PC principal reçoit une carte 10G : c'est lui qui bénéficiera des transferts massifs, aujourd'hui vers Internet, demain vers un NAS.

Le matériel

RÔLE	ÉQUIPEMENT	POURQUOI CELUI-LÀ
Accès fibre 8 Gb/s	Box opérateur dernière génération (port 10G)	Imposée par l'offre — et c'est très bien ainsi
Routeur principal	ASUS ROG Rapture GT-BE98 (Wi-Fi 7 quadri-bande, 2 ports 10G, 4 ports 2,5G)	Le vrai cerveau du réseau : segmentation avancée, pare-feu, QoS
Commutateur ferme maker	TP-Link TL-SG1024DE (24 ports 1G)	Déjà en place, parfaitement dimensionné pour de l'IoT
	TP-Link TX401 (PCIe 10G)	

Carte réseau PC principal		Négociation multi-débits, firmware maintenu, câble Cat 6a fourni
Câblage	Cat 6a S/FTP pour les liaisons 10G, Cat 8 pour la plus longue traversée (34 m)	Le cuivre est intransigeant : 100 % cuivre, blindage double, jamais d'aluminium cuivré

Coût total hors box : environ 800 €, dont l'essentiel pour le routeur. C'est le prix d'une infrastructure qui tiendra dix ans.

Étape 1 — Préparer hors ligne, toujours

La règle d'or de toute migration : **ne jamais configurer un équipement neuf sur un réseau en production**. Le nouveau routeur a donc vécu sa première journée en bulle isolée — alimentation seule, un PC portable en Ethernet direct, aucun lien avec le réseau familial qui continuait de tourner normalement.

Dans cette bulle, tout se prépare :

1. **Réinitialisation d'usine** — partir d'un état connu, même sur du matériel neuf.
2. **Vérification du firmware** — et prudence : la toute dernière version venait d'être retirée par le constructeur pour cause de bugs sur les ports Ethernet. La version stable précédente était la bonne cible. Vérifier les forums spécialisés avant de flasher n'est pas de la paranoïa, c'est de l'hygiène.
3. **Compte administrateur dédié** — identifiant personnalisé (jamais `admin`), mot de passe long généré par gestionnaire.
4. **Plan d'adressage** — reprendre le sous-réseau historique du LAN (disons `192.168.10.0/24`) pour que les réservations DHCP existantes survivent à la migration. Un équipement domotique qui change d'adresse, ce sont des scénarios qui cassent en silence.
5. **Réservations DHCP** — ressaisir les adresses fixes des équipements critiques : domotique, récepteur ADS-B, imprimantes. Quinze minutes de saisie qui économisent des heures de diagnostic.
6. **Réseaux Wi-Fi** — tout créer à l'avance (voir étape 3), puis **couper les radios** : le routeur est prêt, mais silencieux. Personne ne doit se connecter à un réseau qui n'a pas encore d'accès Internet.

À la fin de cette journée, le routeur est un clone froid de la cible. Il ne reste qu'à le brancher.

Étape 2 — La bascule

Le jour J, l'ordre des opérations compte plus que la vitesse d'exécution :

1. **Câbler la box au routeur** — port 10G de la box vers le port WAN 10G du routeur, en Cat 6a.
2. **Vérifier que le routeur obtient une adresse** côté box, et que l'accès Internet fonctionne depuis un poste de test.
3. **Réactiver les radios Wi-Fi** du routeur — les réseaux préparés se mettent à émettre.

4. **Désactiver le Wi-Fi de la box** — un seul émetteur dans la maison. La box devient un simple modem-passerelle.
5. **Rebrancher les clients filaires un par un** : PC principal sur le port 10G, second PC sur un port 2,5G, commutateur maker sur le port 1G. À chaque branchement, vérifier la vitesse négociée dans le système — c'est le moment où l'on découvre les câbles fatigués.
6. **Basculer les clients Wi-Fi** — les smartphones et tablettes rejoignent le nouveau réseau principal.
7. **Valider** : test de débit, ping vers chaque équipement critique de la ferme maker, vérification que les réservations DHCP ont bien pris.

L'ancien routeur reste branché électriquement mais radios coupées, prêt à reprendre du service en deux minutes si tout part en vrille. Il ne sera définitivement débranché qu'après 48 heures de stabilité. Le retour arrière n'est pas un aveu de faiblesse, c'est une capacité qu'on s'offre.

Étape 3 — Segmenter : quatre réseaux, quatre niveaux de confiance

C'est le vrai gain de la migration, bien plus que le débit. Le Wi-Fi 7 moderne permet de créer plusieurs réseaux avec des politiques distinctes. J'en ai défini quatre (les noms sont fictifs, faites de même chez vous — un SSID ne doit jamais rien révéler de son propriétaire) :

RÉSEAU	BANDES	CLIENTS	POLITIQUE
Borealis	2,4 / 5 / 6 GHz	Famille : PC, smartphones, tablettes	Plein accès
Zephyr	2,4 / 5 GHz	Maker : domotique, imprimantes 3D, capteurs	Même sous-réseau que le principal, accès LAN autorisé
Onyx	2,4 GHz uniquement	Caméras et IoT de conception douteuse	Sous-réseau séparé, SSID masqué, isolation totale, débit bridé
Transit	2,4 / 5 GHz	Invités	Sous-réseau séparé, Internet seul, débit limité

La logique : **le niveau d'isolation suit le niveau de confiance**. Les équipements maker que je maîtrise gardent l'accès au LAN — mon PC doit pouvoir parler aux imprimantes 3D. Les invités et les objets douteux, eux, sont dans des bulles étanches : ils voient Internet, rien d'autre, et ne se voient pas entre eux.

Étape 4 — Durcir

Une fois le réseau debout, trente minutes de fermeture de portes :

- **WPS désactivé** — le bouton d'appairage magique est une vulnérabilité documentée depuis quinze ans. Personne n'en a besoin en 2026.

- **UPnP désactivé** — aucun objet connecté ne doit pouvoir ouvrir des ports sur le pare-feu sans mon consentement explicite. Les rares services qui en auraient besoin obtiendront une redirection manuelle, unitaire, documentée.
- **Administration en HTTPS uniquement** — le mot de passe du routeur ne circule pas en clair sur le LAN, même « de confiance ».
- **Aucun accès d'administration depuis Internet** — ni web, ni SSH, ni Telnet. Zéro.
- **Protection réseau activée** — le moteur de sécurité intégré du routeur (blocage de sites malveillants, détection d'intrusion, quarantaine des équipements compromis) est gratuit à vie chez ce constructeur. Il serait absurde de s'en priver.

Le diagnostic de sécurité intégré du routeur donne à l'arrivée un tableau entièrement vert. C'est un indicateur, pas une garantie — mais c'est le bon point de départ.

Étape 5 — Le cas des caméras chinoises

Les deux caméras IP d'entrée de gamme méritent mieux qu'un paragraphe : elles méritent une doctrine.

Posons le fait, sans procès d'intention. Leur fonctionnement nominal — pas un bug, pas un dysfonctionnement, leur **conception** — consiste à envoyer leurs flux vidéo vers les serveurs cloud de leur fabricant, hors Union européenne. L'application mobile qui les pilote passe par les mêmes serveurs, même quand vous êtes dans la pièce d'à côté. Ces caméras à bas coût embarquent par ailleurs des kits de développement pair-à-pair partagés entre des dizaines de marques — la classe de composants visée par l'alerte CISA de 2021 sur le SDK ThroughTek Kalay (CVE-2021-28372, criticité 9,8/10, plus de 80 millions d'appareils actifs concernés, accès possible aux flux audio et vidéo). Autrement dit : vous avez installé chez vous un capteur audio et vidéo dont vous ne contrôlez ni le firmware, ni la destination des flux, ni le calendrier de correction des failles.

Trois options s'offrent alors, par ordre de radicalité croissante :

1. **Ne rien faire** — le choix par défaut de l'immense majorité des foyers, et de bien trop d'entreprises. C'est un risque subi, invisible jusqu'au jour où il ne l'est plus.
2. **Jeter et remplacer** — par des caméras à flux local (ONVIF/RTSP, cloud désactivable). Propre, mais 150 à 300 € pour remplacer du matériel qui fonctionne.
3. **Contenir** — garder le matériel, mais l'enfermer dans une bulle dont on définit soi-même les parois.

J'ai choisi le confinement. Voici les parois de la bulle :

- **réseau dédié** (Onyx), sur un sous-réseau séparé du reste de la maison — même si une caméra est compromise, elle n'a physiquement aucune route vers mes PC, ma domotique ou mes données ;
- **SSID masqué** — le réseau des caméras n'apparaît pas dans les scans Wi-Fi du voisinage ; un attaquant ne peut pas cibler ce qu'il ne voit pas listé ;
- **isolation entre clients** — les caméras ne se voient pas entre elles ; une caméra compromise ne peut pas pivoter vers sa voisine ;
- **débit bridé** à quelques Mb/s — leur usage légitime tient dans ce budget ; toute tentative d'exfiltration massive est mécaniquement étranglée ;

- prochaine étape planifiée : un **filtrage DNS local** pour ne laisser passer que les domaines strictement nécessaires au fonctionnement, et couper la télémétrie de confort.

Le test de vérité viendra avec ce filtrage DNS : observer pendant 48 heures la liste des domaines que ces caméras tentent de joindre. L'exercice est systématiquement édifiant — et je vous le recommande sur n'importe quel objet connecté de votre foyer.

> Une dernière remarque, qui dépasse le cadre domestique. Ce confinement m'a coûté vingt minutes de configuration sur un routeur grand public. Vingt minutes. Combien d'organisations — entreprises, collectivités, administrations — hébergent aujourd'hui des dizaines de caméras, capteurs et objets connectés de même provenance, branchés à plat sur le réseau de production, sans segmentation, sans bridage, sans inventaire ? Une caméra à 30 € reste une caméra à 30 €. Mais une caméra à 30 € enfermée dans une bulle étanche est un risque géré. La même caméra posée sur le LAN de production est une dette de sécurité qui court silencieusement. La différence entre les deux n'est pas budgétaire. Elle est doctrinale.

Les pièges rencontrés (pour vous les épargner)

Le port 10G squatté. Dans l'élan du câblage, le commutateur 1G s'est retrouvé branché sur le port 10G « gaming » du routeur. Aucun bénéfice — sa liaison montante plafonne physiquement à 1 Gb/s — et un port stratégique gaspillé. Chaque câble à sa place : le plan de câblage s'écrit avant, sur papier.

Les adresses MAC fantômes. Trois entrées différentes pour le même smartphone dans la table DHCP : les téléphones récents randomisent leur adresse MAC par défaut, réseau par réseau. Pour des réservations DHCP stables, il faut désactiver la MAC privée sur le réseau domestique, appareil par appareil, avant la migration.

Le câble de 34 mètres. La liaison la plus longue de la maison négociait péniblement. Le test de câble intégré au commutateur (une fonction méconnue des modèles administrables, même d'entrée de gamme) a permis de mesurer la longueur, de détecter deux câbles morts oubliés dans les murs, et de cibler le remplacement : Cat 8 blindé, 100 % cuivre. À cette distance, la catégorie du câble n'est plus un détail.

Le faux coupable. Au lendemain de la bascule, le VPN professionnel refusait de monter. Réflexe naturel : accuser le nouveau routeur. Diagnostic méthodique : test en contournant le routeur (échec aussi), test avec un autre VPN à travers le routeur (succès). Verdict : panne côté serveur distant, rien à voir avec la migration. **Trois tests, une conclusion, zéro bricolage inutile.** La moitié des « pannes réseau » post-migration n'en sont pas.

Bilan

- **Débit** : la maison exploite enfin son abonnement, et le LAN interne est prêt pour un NAS 10G.
- **Couverture** : le Wi-Fi 7 quadri-bande a rendu les deux répéteurs inutiles — débranchés, recyclés.
- **Sécurité** : quatre zones de confiance, des objets douteux en quarantaine, une surface d'attaque réduite au strict nécessaire.

- **Réversibilité** : à chaque étape, un chemin de retour existait. Il n'a jamais servi. C'est exactement pour ça qu'il faut le prévoir.
- **Temps total** : une journée de préparation hors ligne, une heure de bascule, deux jours d'observation.

La méthode tient en une phrase : **préparer à froid, basculer dans l'ordre, valider en mesurant, durcir sans attendre, et documenter chaque choix** — dans dix-huit mois, celui qui rouvrira le capot vous remerciera. Ce sera probablement vous.

La checklist de migration

À imprimer, à cocher, à adapter. Trois phases, aucun raccourci.

Avant le jour J (préparation à froid)

✔	ACTION
☐	Inventorier tous les clients du réseau : nom, adresse MAC, adresse IP, port ou SSID
☐	Identifier les équipements à adresse fixe (domotique, capteurs, imprimantes) et noter leurs réservations DHCP
☐	Désactiver la MAC privée (adresse aléatoire) sur les smartphones et tablettes du foyer
☐	Tester les câbles en place (fonction test du commutateur) ; remplacer les douteux, retirer les morts
☐	Vérifier la version de firmware cible du nouveau routeur — forums spécialisés inclus, une version fraîchement retirée est un signal
☐	Configurer le nouveau routeur **hors ligne** : réinitialisation d'usine, compte admin dédié, plan d'adressage, réservations DHCP, réseaux Wi-Fi
☐	Couper les radios Wi-Fi du routeur préparé jusqu'à la bascule
☐	Écrire le plan de câblage : quel équipement sur quel port, à quelle vitesse attendue

Le jour J (bascule ordonnée)

✔	ACTION
☐	Câbler box → routeur (port 10G, Cat 6a minimum)
☐	Vérifier l'obtention d'adresse WAN et l'accès Internet depuis un poste de test
☐	Réactiver les radios Wi-Fi du routeur
☐	Désactiver le Wi-Fi de la box — un seul émetteur dans la maison
☐	Rebrancher les clients filaires un par un, en vérifiant la vitesse négociée à chaque branchement
☐	Basculer les clients Wi-Fi sur les nouveaux réseaux, par niveau de confiance
☐	Valider : test de débit, ping de chaque équipement critique, réservations DHCP effectives
☐	Conserver l'ancien routeur sous tension, radios coupées — c'est votre chemin de retour

Après (durcissement et observation)

✔	ACTION
☐	Désactiver WPS
☐	Désactiver UPnP
☐	Passer l'administration en HTTPS uniquement ; aucun accès admin depuis Internet
☐	Activer la protection réseau intégrée (blocage de sites malveillants, détection d'intrusion)
☐	Isoler les objets connectés douteux : sous-réseau dédié, SSID masqué, isolation client, débit bridé
☐	Lancer le diagnostic de sécurité intégré et corriger tout voyant orange
☐	Observer 48 heures avant de débrancher définitivement l'ancien matériel
☐	Photographier le câblage final, étiqueter les câbles, documenter le plan d'adressage

Huit cases par phase. Une journée de travail. Dix ans de tranquillité.
