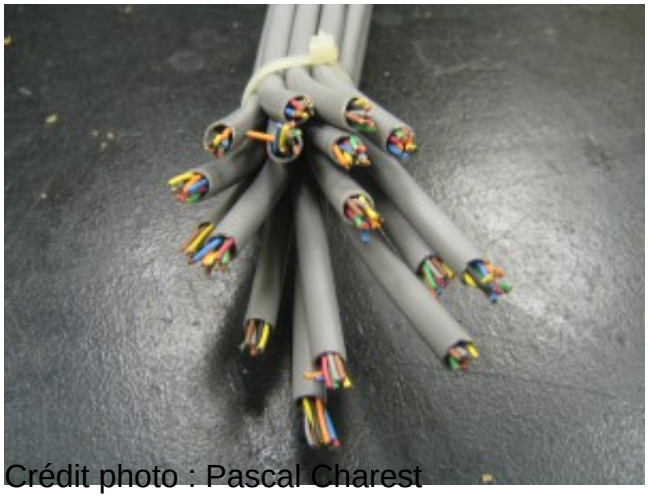
Fabriquer son internet (6)



Crédit photo : Pascal Charest

Après une petite incartade au pays du chiffrement et des e-monnaies, retour aux fondamentaux. Dans les épisodes précédents, on a à peu près fait le tour des choses minimales à traiter pour monter un petit fournisseur d'accès. Place maintenant à un peu d'envers du décor. Abordons ce qu'il convient de faire pour assurer ses arrières quand on bosse sur un réseau qui n'est plus local. Attention, chacun a ses méthodes préférées, je n'ai pas la prétention de les lister toutes, juste de vous présenter ce avec quoi j'ai, moi, l'habitude de travailler.

Le maître mot est l'accès aux équipements. Quand on construit un réseau, si l'équipement d'un client est en panne, c'est pas la mer à boire. Par contre, si c'est un bout ou la totalité du coeur de réseau qui part en sucette, c'est plus enquiquinant, vu que tout ou partie des utilisateurs se retrouvent dans le noir.

Il existe pour moi deux grandes familles de solutions qui se complètent très bien :

Le réseau d'administration

L'idée est de séparer, si possible physiquement, sinon logiquement, le morceau de réseau qui sert à administrer les équipements de celui qui sert à transporter les données des utilisateurs. Plusieurs avantages :

- les flux de données sont totalement séparés, ce qui rend donc beaucoup plus difficile pour un attaquant de s'en prendre à vos équipements puisqu'ils ne sont pas publiquement accessibles
- Corollaire, puisqu'ils ne sont pas publiquement accessibles, vous gagnez de précieuses adresses IP en les numérotant avec des IP privées (sauf si, bien entendu, vos équipements sont assez récents pour supporter l'adressage d'administration en IPv6)
- La topologie de votre réseau administratif peut être différente de celle du réseau client

On va surtout s'intéresser à ce dernier avantage. Lorsqu'on parle d'un réseau de fourniture d'accès, surtout dans le cas où celui-ci met en jeu des liens ADSL en cours de route, il peut être pratique de segmenter le réseau. Exemple concret, sur un réseau wireless, vous avez un point haut qui est capable de desservir deux villes, l'une va être sur un VLAN dédié, l'autre sur un second, ce qui permettra facilement de les relier à deux ADSL distincts et de basculer des utilisateurs de l'un à l'autre, le tout sur un même réseau physique.

Mais pour l'administration, on préférera souvent limiter au maximum les dispositifs de routage qui peuvent être plus capricieux que le reste. On aura donc un seul et unique VLAN d'administration qui sera global à toute l'infrastructure.

Là où ça se corse, c'est si votre réseau devient très étendu et dispose de chemins multiples. La boucle ethernet vous guette du coin de l'oeil et vous tombera sur le dos un jour ou l'autre. Pour adresser ce problème, on se tournera vers une autre solution :

Les accès « out of band »

L'idée est de se ménager des accès au réseau d'administration depuis d'autres réseaux. Idéalement, un par site physique distinct, pour pouvoir reprendre la main sur les équipements en cas de problème.

Concrètement, ça passe par exemple par la souscription d'une ligne ADSL chez Orange livrée au pied d'un pylône important de l'infrastructure si on sait que le gros de celle-ci repose sur des liaisons ADSL SFR. Ainsi, en cas de chute globale ou localisée de SFR, il est toujours possible de prendre la main sur le pylône via l'ADSL Orange et, si on se débrouille bien, de rétablir l'accès en trafiquant les configuration.

Dans le prochain épisode, on reparlera transport de données et montée en débit, parce que l'ADSL ça va bien 5 minutes.