

Charte LAN

Partie 2

Normes de commutation

Vers ion	Date	Auteur	Commentaires
3.1	20 août 2020	SI2B-DMOCSS- Réseaux MSNRL	Ajout Offre de service DGFIP de ToIP centralisée Mise à jour plan de nommage des vlan Mise à jour du lexique
3.0	11 juin 2018	SI2B PILSTRAT LAN-WAN MSNRL	Ajout de l'offre WIFI Complément sur la téléphonie Complément sur la supervision Complément sur le DHCP National Mise à jour maîtrise réseau LAN
2.0	Janvier 2012	SI2B/DRASSS MSNRL U.Virnot	Découpage de la Charte LAN en trois documents : <ul style="list-style-type: none"> - un guide de câblage (équipements passifs) incluant l'ex-CCTP Câblage, - un guide de normes de commutation (équipements actifs), - la Documentation de site et Annexes.
1.0	15/07/2010	SI2B/DRASSS MSNRL U.Virnot	

Sommaire

I. Introduction.....	5
I.1 OBJET DU DOCUMENT.....	5
I.1.1 Définition et périmètre.....	5
I.1.2 Destinataires et usages.....	5
I.2 ENJEUX POUR LES RÉSEAUX LAN DE LA DGFIP.....	5
I.2.1 Enjeux liés à l'hétérogénéité de l'existant.....	5
I.2.2 Enjeux économiques.....	6
I.2.3 Enjeux liés à l'arrivée des nouveaux services.....	6
I.2.4 Exigence de qualité.....	6
I.2.5 Enjeux organisationnels.....	6
I.3 INTERVENANTS ET RÔLES.....	7
I.4 PÉRIMÈTRE DE SITES.....	7
I.5 MARCHÉS D'ACQUISITION DU MINISTÈRE.....	8
I.6 ÉTUDE ET CONCEPTION DU SERVICE LAN.....	8
II. Équipements actifs.....	10
II.1 TYPOLOGIE DES ARCHITECTURES LAN.....	10
II.2 LES ÉLÉMENTS ACTIFS DES ARCHITECTURES LAN.....	11
II.2.1 Cœur de réseau.....	11
II.2.2 Commutateur d'accès.....	12
II.2.3 Le Wifi.....	12
II.2.4 La ToIP.....	19
II.3 RÈGLES GÉNÉRALES.....	23
II.3.1 Règles de configuration de base des équipements.....	23
II.3.2 Règles pour les « Piles de commutateurs ».....	25
II.3.3 Niveaux de chaînage des équipements.....	26
II.3.4 Activation des fonctionnalités de niveau 3.....	26
II.3.5 Raccordement des serveurs.....	26
II.3.6 Ports à réserver pour usages particuliers.....	27
II.3.7 Documents de référence et mises à jour de firmware.....	28
II.3.8 Sauvegarde de configurations et syslog.....	28
II.3.9 Constitution d'un stock d'équipements en Spare.....	28
II.3.10 Remplacement ou démontage d'un commutateur.....	28
II.3.11 Gestion de la haute disponibilité.....	29
II.4 ARCHITECTURES DE RÉFÉRENCE.....	30
II.4.1 Architecture d'un petit site.....	30
II.4.2 Architecture d'un site moyen.....	30
II.4.3 Architecture d'un grand site.....	31
II.4.4 Architecture complexe et redondance de cœur de réseau.....	33
II.5 CONFIGURATION ET ADMINISTRATION.....	34

<i>II.5.1 Acteurs.....</i>	<i>34</i>
<i>II.5.2 Règles de nommage des équipements.....</i>	<i>34</i>
<i>II.5.3 Règles d'administration.....</i>	<i>38</i>
<i>II.5.4 VLAN.....</i>	<i>40</i>
<i>II.5.5 Classification et priorisation des flux.....</i>	<i>46</i>
<i>II.5.6 Activation des fonctionnalités de niveau 3.....</i>	<i>47</i>
<i>II.5.7 Supervision des équipements.....</i>	<i>47</i>
<i>II.5.8 Suivi des changements et de la qualité de service.....</i>	<i>48</i>
<i>II.5.9 Gestion de la sécurité.....</i>	<i>49</i>
<i>II.5.10 DHCP (Dynamic Host Configuration Protocol).....</i>	<i>49</i>
III. Maîtrise des architectures réseaux LAN de la DGFIP.....	51
<i>III.1 LES CHANGEMENTS EN MODE PROJET.....</i>	<i>51</i>
<i>III.1.1 Les acteurs.....</i>	<i>51</i>
<i>III.1.2 La phase d'étude et de préparation.....</i>	<i>52</i>
<i>III.1.3 La phase de mise en œuvre et de support.....</i>	<i>52</i>
<i>III.1.4 La phase de reporting et de documentation.....</i>	<i>52</i>
<i>III.1.5 Les règles d'installation des équipements actifs.....</i>	<i>52</i>
<i>III.1.6 Les étapes de déploiement.....</i>	<i>53</i>
<i>III.2 LES CHANGEMENTS EN MODE CORRECTIF.....</i>	<i>57</i>
<i>III.2.1 Les fondamentaux.....</i>	<i>57</i>
<i>III.2.2 Anticiper les pannes.....</i>	<i>57</i>
<i>III.2.3 Outil de cartographie.....</i>	<i>58</i>
IV. Dépannage des réseaux LAN de la DGFIP.....	59
<i>IV.1 LES INFORMATIONS PRÉLIMINAIRES À COLLECTER :.....</i>	<i>59</i>
<i>IV.2 MÉTHODE POUR MISE EN CONDITION ET REPRODUCTION DE L'ANOMALIE :.....</i>	<i>59</i>
<i>IV.3 ÉLÉMENTS À ANALYSER :.....</i>	<i>60</i>
<i>IV.4 LA MÉTHODE D'ANALYSE :.....</i>	<i>60</i>
<i>IV.5 LES FICHES DE RÉOLUTION D'INCIDENTS.....</i>	<i>61</i>
V. Annexe 1- Circuit des commandes des directions sur le marché UGAP-LAN.....	63
VI. Annexe 2 - Circuit des commandes des directions sur le marché UGAP – Connectique.....	64
VII. Annexe 3 - Les fiches de résolution d'incidents.....	65
VIII. Annexe 4 - Présentation synthétique des actions à réaliser par chaque entité.....	73
IX. Lexique.....	74

I. Introduction

I.1 Objet du document

I.1.1 Définition et périmètre

La Charte LAN est l'ensemble des normes, méthodes, outils et procédures recommandés par la DGFIP pour la mise en service et le maintien en conditions opérationnelles des réseaux locaux des sites territoriaux de la DGFIP. Elle précise également l'organisation, les relations entre intervenants et la gestion des changements, des incidents et de la qualité de services. Elle rassemble et formalise les règles qui s'appliquent à l'ensemble des sites DGFIP et doit devenir un manuel de référence au quotidien pour l'ensemble des intervenants. Elle constitue une cible à atteindre à terme.

La Charte LAN est composée de trois parties :

- 1) Le Guide de câblage, incluant les normes associées aux éléments passifs (précâblage, locaux techniques...)
- 2) Les Normes de commutation, associées aux éléments actifs (commutateurs, routeurs, serveurs, systèmes de sauvegarde...)
- 3) La Documentation de site et les Annexes

Le présent document est la seconde partie de la Charte LAN.

I.1.2 Destinataires et usages

La Charte est organisée pour pouvoir être utilisée par :

- les décideurs :
 - o les directeurs et chefs d'établissements,
 - o les responsables logistiques, les acheteurs,
 - o la sous-direction SI2,
- les équipes techniques :
 - o le Support aux Infrastructures Locales (SIL),
 - o la Cellule Informatique Départementale (CID),
 - o la Mission de Support National des Réseaux Locaux (MSNRL)
- les installateurs et câbleurs titulaires d'un marché de travaux d'infrastructure de câblage.

L'objectif est d'apporter une aide à la décision et de fixer un cadre visant à assurer une homogénéité des solutions qui seule garantira la maîtrise de la qualité du service réseau. Cette qualité est nécessaire à la continuité du service réseau et à la satisfaction de ses utilisateurs.

I.2 Enjeux pour les réseaux LAN de la DGFIP

I.2.1 Enjeux liés à l'hétérogénéité de l'existant

L'état actuel des réseaux locaux de la DGFIP résulte de leur histoire. On y trouve une grande variété d'équipements, d'architectures de câblage, de typologies de composants, de contrats de maintenance, etc. Cette diversité se retrouve même au sein d'un site et elle est source de problèmes qui ne peuvent apparaître qu'avec le temps et la mise à disposition de nouveaux services applicatifs.

Le principal risque est de se rendre compte trop tard qu'un réseau qui semblait fonctionner parfaitement est devenu vétuste et ne permet plus d'assurer correctement le service attendu. Ce risque est amplifié par le fait que ce constat peut apparaître sur une multitude de sites simultanément et qu'il devient potentiellement impossible d'y faire face sans remettre en cause des déploiements d'applications.

I.2.2 Enjeux économiques

La politique budgétaire de l'État est de faire baisser la dépense publique. Cette politique se décline dans les Collectivités Locales détentrices des budgets d'acquisitions et de dépenses de fonctionnement des infrastructures informatiques des sites de la DGFIP.

Il n'est donc pas possible de lancer des travaux de grande envergure sans préparation. Ceux-ci nécessitent souvent une planification sur de nombreuses années, compatible avec une stabilité, voire une baisse régulière des dépenses. Il faut donc que les infrastructures soient suffisamment maîtrisées et à niveau pour pouvoir absorber sans difficulté les exigences des évolutions du métier sans provoquer d'à-coups dans les nécessaires mises à jour. Les économies sont fortement dépendantes de la réduction des interventions sur les réseaux, d'où l'intérêt de réaliser des mises en service pérennes s'appuyant sur des normes reconnues.

I.2.3 Enjeux liés à l'arrivée des nouveaux services

Ces dernières années ont vu de fortes mutations dans les architectures applicatives, avec un impact direct sur les infrastructures: la centralisation des exploitations, les interfaces Web. Dans la suite de ces mouvements, qui ne sont pas achevés, se profilent d'autres services comme la ToIP, la visioconférence, la formation à distance, l'interconnexion de centres d'appels virtuels, le Wifi, etc. Si tous ces services améliorent le confort des agents et leur productivité, ils sont aussi une source d'économie en termes de déplacements et apportent une grande souplesse dans le fonctionnement des services de l'Administration. En contre-partie ils requièrent une plus grande bande passante et un fonctionnement en temps réel. Ils nécessitent également une forte disponibilité du réseau, des mécanismes de redondance, du routage intelligent.

Pour faire face à ces exigences, les systèmes de câblage doivent être au niveau de l'état de l'art et les équipements réseau doivent être parfaitement interopérables pour former un ensemble cohérent.

I.2.4 Exigence de qualité

Ce qui importe vraiment aux décideurs, c'est de disposer de réseaux aptes à assurer en permanence le support des applications métier avec une qualité irréprochable dans le respect des contraintes budgétaires.

La maîtrise des réseaux nécessite que les équipements soient administrables et supervisés à distance pour prévenir de dysfonctionnements potentiels ou pour prévenir les administrateurs réseaux d'une défaillance du réseau grâce à un système d'alertes. Une documentation à jour et des outils associés réduiront sensiblement les délais de remise en service en cas d'incident, ainsi que les délais d'information sur les capacités d'extensions (déménagements, etc.).

I.2.5 Enjeux organisationnels

Comme on le voit dans la section I.3, les acteurs participant à la création et au maintien des réseaux locaux sont multiples. La maîtrise des réseaux ne peut se faire que si les différentes équipes impliquées collaborent, depuis la conception du câblage, où les responsables logistiques devront **faire intervenir les SIL très en amont des projets**, dès l'initiation des appels d'offres, jusqu'à la recette, la mise en service et l'exploitation des architectures techniques, où les équipes réseaux s'appuient sur les équipes informatiques de proximité et coordonnent les opérations de branchement physique des équipements.

I.3 Intervenants et rôles

La fusion de la Filière Fiscale et de la Filière Gestion Publique au sein de la DGFiP a conduit à une réorganisation des équipes de support et de leurs rôles.

Les structures informatiques territoriales sont les Directions des Services Informatiques (DISI) qui comportent plusieurs établissements régionaux, les Établissements de Services Informatiques (ESI).

Les intervenants dans la gestion des réseaux locaux sont :

- en interne (DGFiP) :
 - o au niveau national, pour la définition des normes et le support de niveau 3 :
 - la MSNRL,
 - le bureau SI2B-DMOCSS-Réseaux;
 - o au niveau régional (périmètre d'un ESI) :
 - le SIL a la responsabilité des réseaux (LAN et WAN), des serveurs et des locaux techniques;
 - o au niveau du département:
 - le service logistique engage les travaux liés à l'immobilier et au déplacement des agents, y compris les travaux de pré-câblage en collaboration avec les SIL ;
 - la CID a la responsabilité des stations et des imprimantes et le support à leurs utilisateurs;
 - o au niveau d'un site, pour réaliser des opérations ponctuelles sous le contrôle des SIL :
 - le RBL (Responsable Bureautique Local) est un agent administratif;
- en externe
 - o l'architecte ou le bureau d'études ,
 - o les entreprises retenues pour les travaux,
 - o éventuellement, l'organisme chargé du contrôle du câblage.
 - o

Les équipes sécurité et TVM du bureau SI2B ainsi que le bureau SI2A-DMT pour la partie ToIP sont également consultés avant toute validation.

Les SIL bénéficient de l'assistance d'outils remontant des informations sur la configuration et l'état des réseaux, qu'ils tiennent à jour et auxquels d'autres acteurs peuvent avoir accès en consultation.

I.4 Périmètre de sites

En complément de ce qui est indiqué au § I.1.1, la Charte LAN s'applique à l'ensemble des sites de la DGFiP, à l'exception des sites de production informatique (SPS de Bussy, plate-forme INTEX de Noisiel, site de Marcoussis). Concernant les ESI (ex-CSI et ex-DI) et le site de NDV, elle s'applique jusqu'à l'entrée des plateaux de production, limite d'intervention de la MSNRL. Cependant, dans la mesure du possible, les équipes responsables de ces sites et plateaux de production s'efforceront d'appliquer les normes et recommandations de la Charte LAN.

I.5 Marchés d'acquisition du Ministère

Afin de garantir l'interopérabilité des équipements et de faciliter leur administration, tout en maîtrisant les budgets, les directions de la DGFIP sont tenues de se reporter au cahier des charges de la consultation et au marché de référence (géré par l'UGAP) en vigueur pour toutes les prestations relatives au marché LAN

Ces marchés de référence comportent les engagements contractuels et de performance des équipements. Ils décrivent l'offre de services ainsi que les prestations associées.

La MSNRL assiste les différents acteurs dans le choix de leurs équipements.

 Voir le catalogue UGAP/LAN sur le site MSNRL rubrique « équipements d'interconnexion »

Seuls sont supportés par la MSNRL les équipements ayant été acquis dans le cadre du marché en cours UGAP/SCC avec les matériels HP et les deux marchés précédents (3Com et HP/H3C). Les équipements Enterasys et 3Com sont classés « Obsolètes ».

Les autres équipements sont considérés hors marché et candidats au remplacement. La MSNRL ne répondra à aucune question les concernant. Leur remplacement pourra s'effectuer progressivement en fonction des contraintes techniques et budgétaires.

Les procédures de gestion de la maintenance et de la garantie sont centralisées et gérées par la MSNRL exclusivement. Pour toute demande d'intervention, les équipes SIL doivent remplir le formulaire de panne sur le site MSNRL rubrique « équipements d'interconnexion » « maintenance ».

Le processus d'achat des équipements LAN est décrit à l'Annexe 1 et celui de la connectique à l'Annexe 2.

Le financement des équipements est porté par le Bureau SI2B pour les cœurs de réseau, y compris les équipements en SPARE : voir au §II.3.9

Le financement des autres équipements de commutation est à la charge des Directions Locales.

Recommandation 1

Marché public de référence

Afin de garantir l'interopérabilité des équipements et de faciliter leur administration, tout en maîtrisant les budgets, la DGFIP met à disposition un extrait du catalogue de matériels de commutation (Référencement LAN marché 612390_PRIX_DGFIP). La MSNRL assiste les différents acteurs dans le choix de leurs équipements.

L'utilisation exclusive de ces marchés d'acquisition est nécessaire et obligatoire, afin de garantir la qualité et l'interopérabilité des équipements en réponse aux enjeux mentionnés ci-dessus.

I.6 Étude et conception du service LAN

Ce chapitre a pour objet de décrire les recommandations en termes de règles d'ingénierie pour la phase d'étude et conception des architectures LAN des sites DGFIP.

Objectif :

- la conception et les spécifications techniques de l'architecture LAN des sites DGFIP (topologie, plan d'adressage, règles de commutation et de routage) ;
- les préconisations de configuration et d'installation des équipements LAN sur site ;
- les recommandations pour l'administration et la supervision des équipements LAN ;
- les recommandations pour l'exploitation et la gestion de la maintenance des équipements.

Les commutateurs installés sur un site peuvent remplir plusieurs rôles en général, dont :

- le raccordement des utilisateurs (commutateur d'accès) ;
- les interconnexions du local technique principal et du local technique secondaire (rôle cœur de réseau d'un côté et/ou commutateur d'accès de l'autre pour le raccordement des utilisateurs) ;
- le raccordement des serveurs d'applications au réseau local ;
- l'interconnexion entre le cœur de réseau et le routeur d'accès WAN qui assure le routage vers les sites.

La conception du service doit tenir compte a minima :

- du service à délivrer sur site (type d'application : data, ToIP, Visio-conférence, Wifi...) ;
- de la qualité du service souhaitée (performance, QoS, haute disponibilité ...)
- du nombre d'agents sur site (classification du site : petit, moyen, grand, important...) ;
- du nombre d'étages ou niveaux à interconnecter ;
- du nombre de locaux techniques à desservir ;
- de la mobilité souhaitée et des types de terminaux (solution filaire ou Wi-Fi...)
- de la sécurité souhaitée (cloisonnement de certains flux spécifiques avec des règles de routage) ;

Recommandation 2

Étude et conception du réseau LAN

Il est recommandé de s'appuyer sur les équipes SIL en charge du réseau LAN et WAN au sein de chaque direction pour la définition de l'architecture du LAN du site.

L'étude et la conception du service doivent respecter les préconisations du constructeur des équipements du marché en vigueur au regard des prérequis énoncés dans le cahier des charges.

II. Équipements actifs

II.1 Typologie des architectures LAN

Quatre catégories de sites peuvent être distinguées en fonction de la complexité présumée de l'architecture: petits sites, sites moyens, grands sites et sites importants. Les équipements peuvent être localisés dans une baie d'un local technique ou dans un coffret mural selon la typologie du site et les différentes contraintes techniques associées.

A cela peut s'ajouter le type de service LAN à déployer sur le site :

- ◆ LAN Data uniquement ;
- ◆ LAN Voix et data (inclus la ToIP) ;
- ◆ LAN avec un VLAN par service.

Les **petits sites** correspondent aux **trésoreries, SIP, SIE et annexes de petite taille** et sont caractérisés par :

- **le nombre d'agents inférieur à 20,**
- avec ou sans local technique,
- un unique équipement LAN

Les **sites moyens** correspondent aux **trésoreries, SIP, SIE, annexes...** Dans un même bâtiment, il n'y aura qu'une seule sortie WAN. Ils sont caractérisés par :

- **le nombre d'agents compris dans une fourchette de 20 à 50 environ,**
- un local technique spécifique (LTI),
- deux niveaux d'architecture (Cœur de réseau et accès)

Les **grands sites** correspondent aux **DRFiP, DDFiP, ESI...** Ils ont les caractéristiques suivantes :

- le nombre d'agents entre 50 et 150 environ,
- un local technique d'immeuble (LTI) et des locaux techniques d'étage (LTE),
- deux niveaux d'architecture (cœur de réseau et commutateurs d'accès)

Les **sites importants** correspondent aux cités administratives et à certaines **DRFiP, DDFiP, ESI** de très grande taille, souvent avec plusieurs bâtiments... Ils ont les caractéristiques suivantes :

- le nombre d'agents supérieur à 150,
- un local technique d'immeuble (LTI) par bâtiment et des locaux techniques d'étage (LTE),
- deux niveaux d'architecture par bâtiment (cœur de réseau et commutateurs d'accès).

Recommandation 3

Étude et conception du réseau LAN : services à déployer

Il est recommandé d'anticiper les fonctionnalités à déployer à court et à moyen terme pour une direction ou un site dès lors que les projets d'évolution sont connus. Pour exemple, les projets de convergence LAN voix et data avec l'intégration de la Téléphonie sur IP (ToIP). Il est préconisé que ces données soient prises en compte dès la phase de spécifications :

- LAN Data uniquement ;
- LAN Voix et data (inclus la ToIP) ;
- LAN avec un VLAN par service.

Il est également recommandé lors de la phase conception du service d'anticiper en prévoyant un nombre de ports suffisants (prévoir une marge de 5 à 10% en fonction) pour ce qui concerne les

commutateurs de cœur de réseau et d'accès.

II.2 Les éléments actifs des architectures LAN

L'architecture cible retient deux types logiques d'équipements :

- Le **cœur de réseau**, est le premier commutateur directement raccordé au routeur d'accès du réseau WAN (exemple RIE (Réseau Interministériel de l'État)). Il constitue en général le point central sur lequel sont raccordés les serveurs. S'il existe sur le site des besoins de communications entre plusieurs VLAN, les fonctionnalités de routage (Niveau 3) sont activées sur le cœur de réseau.
- L'**équipement d'accès** sert à connecter les équipements terminaux (PC, imprimantes ...). Il est obligatoirement raccordé à un cœur de réseau sur les sites moyens et grands. Les petits sites ne comportent qu'un commutateur d'accès directement raccordé au routeur WAN.

Le choix des équipements actifs dans le catalogue du Marché, en accord avec la MSNRL, se fera en fonction des besoins de connectivité, de puissance ou de Power Over Ethernet (PoE).



La technologie Power over Ethernet (PoE), norme IEEE 802.3af, permet d'alimenter les Postes IP et de transmettre les données via un seul et même câble, pour une puissance maximale de 15,4 W pour le PoE et de 25,5 W pour le PoE+.

Depuis le 01/01/2017, l'offre de service Wifi DGFIP est venue compléter cette architecture.

II.2.1 Cœur de réseau

Suivant la taille du site, le cœur de réseau ne réalise pas les mêmes fonctions :

- Sur un petit site, le commutateur est unique :
 - o commutateur avec fonction de routage (niveau 3) – 24 ports 10/100 Mb/s (ou 10/100/1000 Mb/s (Cu) avec PoE si nécessaire)
 - o niveau 3 activé
- Sur un site moyen,
 - o commutateur avec fonction de routage (niveau 3) – 24 ou 48 ports 10/100/1000 Mb/s (Fo ou Cu)
 - o niveau 3 activé
 - o pas de redondance d'équipements
- Sur un grand site et sites importants,
 - o commutateur avec fonction de routage (niveau 3) – 24 ou 48 ports 10/100/1000 Mb/s - empilable ou de type châssis (Fo ou Cu)
 - o niveau 3 activé
 - o mise en œuvre possible de la redondance interne par duplication de module (alim, CPU...)
 - o mise en œuvre possible de la haute disponibilité par duplication des cœurs de réseau (empilement).

Si le LTI dispose d'une double source d'énergie distincte et que l'alimentation du cœur de réseau est redondante, le cœur de réseau sera alimenté par chacune de ces deux sources d'énergie.

Pour les architectures LAN réparties sur plusieurs bâtiments distants et raccordés par des liaisons de type interlan loué ou propriétaire, l'équipement connecté à chaque extrémité des liaisons sera un commutateur cœur de réseau qui assurera le routage des VLAN du bâtiment qui l'héberge.

Sur les grands sites, **les piles de commutateurs sont à privilégier par rapport aux châssis** pour des raisons de coût et de facilité de maintenance (gestion du SPARE, contrats de maintenance), les principaux intérêts du châssis étant sa puissance de commutation et sa modularité.

II.2.2 Commutateur d'accès

Les commutateurs d'accès sont des équipements de type 24 ou 48 ports cuivres 10/100 Mb/s ou 24 ou 48 ports cuivres 10/100/1000 Mb/s, suivant les besoins. A terme, tous les commutateurs d'accès seront administrables et supporteront le protocole RSTP. En principe les commutateurs d'accès sont localisés dans les LTI ou LTE, ils permettent d'alimenter les points d'accès des équipements terminaux. Cependant, dans quelques cas spécifiques (salles de formation à haute densité de postes, par exemple), le commutateur d'accès pourra être déporté.

Les commutateurs d'accès peuvent être organisés en piles (cf §II.3.2). Celles-ci sont connectées directement sur le cœur de réseau via des rocares.

En cas de saturation des rocares, une solution sera envisagée en accord avec le bureau SI2B et la MSNRL.

Recommandation 4

Etude et conception du réseau LAN : choix des équipements

Il est recommandé d'adapter le choix du commutateur selon le catalogue du marché en vigueur, en fonction des besoins de connectivité (nombre d'équipements à raccorder, inclus les ports pour les routeurs d'accès WAN), de puissance, et du service à déployer (mode PoE pour la ToIP, visio)

II.2.3 Le Wifi

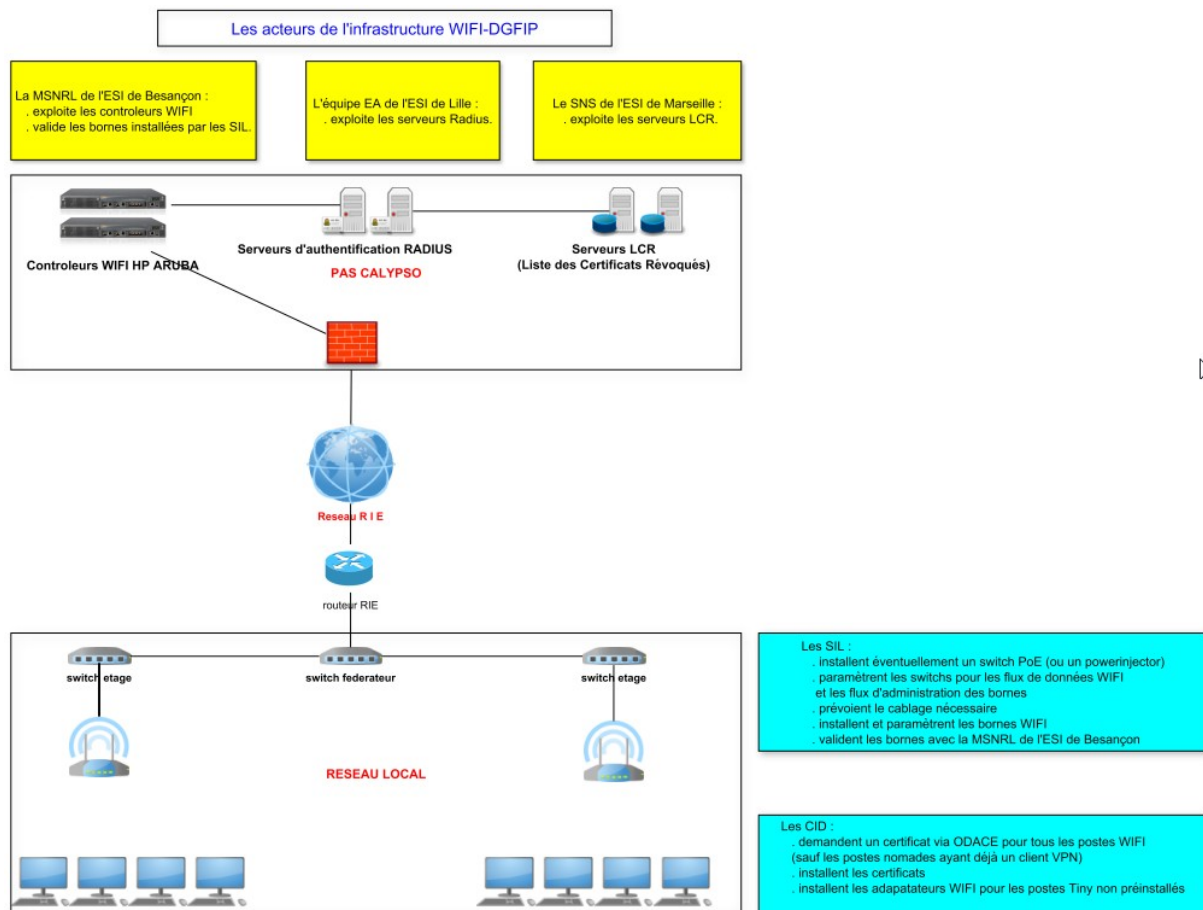
Dans la réflexion d'une offre de service de connexion au réseau de la DGFIP via une liaison sans fil WIFI, différents cas d'usages ont été identifiés :

- l'extension du réseau filaire DGFIP afin de traiter un axe de la mobilité des agents, à savoir, avoir un accès sans fil aux ressources internes pour les agents présents sur les sites DGFIP (exemple : salles de réunions, salles de formation...) ;
- l'alternative (coût d'installation moindre) à la mise en œuvre d'un câblage réseau pour des accès à partir de postes fixes (e.g : salles de formation) .

Afin de répondre à ces différents cas d'usage, une infrastructure composée de bornes Wifi installées sur les sites clients, et d'une paire de contrôleurs en haute disponibilité géographique rackés dans la PAS Calypso, a été mise en place.

Les contrôleurs gèrent l'ensemble du parc des bornes WIFI, maintiennent à jour les firmwares, poussent les configurations et politiques radio/sécurité...

Ils servent de point de management centralisé avec un tableau de bord et des indicateurs. Lors de la connexion du client, ils relaient les flux d'authentification nécessaires jusqu'aux serveurs Radius.



II.2.3.1 Pré-requis réseau à une installation WIFI

Un réseau WIFI a une bande passante partagée, contrairement au réseau cuivre qui bénéficie de la totalité de la bande passante de son câble pour chaque utilisateur.

Les échanges entre les équipements doivent donc être orchestrés et limités au minimum utile.

II.2.3.1.1 Implantation et nombre de bornes

1. Au niveau de la Direction

Une Direction souhaite faire une étude :

- l'extension pour savoir s'il est opportun de remplacer une installation filaire par du WIFI ;
- pour connaître le coût d'une installation.

2. Au niveau du SIL

Une étude sur plan doit impérativement être réalisée. Le plan à l'échelle devra :

- faire figurer les postes de travail, les LTE et le LTI ;
- préciser les matériaux utilisés et susceptibles d'être un frein à la propagation des ondes (cloisons épaisses, mobilier ou structure métallique, étagère d'archives papier, etc).

II.2.3.1.2 Conformité à la Charte LAN

L'architecture du réseau local et la configuration des commutateurs doivent respecter la charte LAN.

II.2.3.2 Architecture physique

II.2.3.2.1 État des lieux des locaux techniques

- Local Technique d'Immeuble (cf charte LAN) :
 - Vérifier la disponibilité de rocade si le projet d'installation WIFI implique l'utilisation d'une rocade supplémentaire.
- Local Technique d'Etage (cf charte LAN) :
 - Vérifier la disponibilité de liens capillaires si le projet d'installation WIFI implique l'utilisation de liens supplémentaires.
 - S'il y a lieu d'installer un switch POE (dégagement de chaleur conséquente) vérifier que le LTE soit suffisamment aéré ou ventilé.

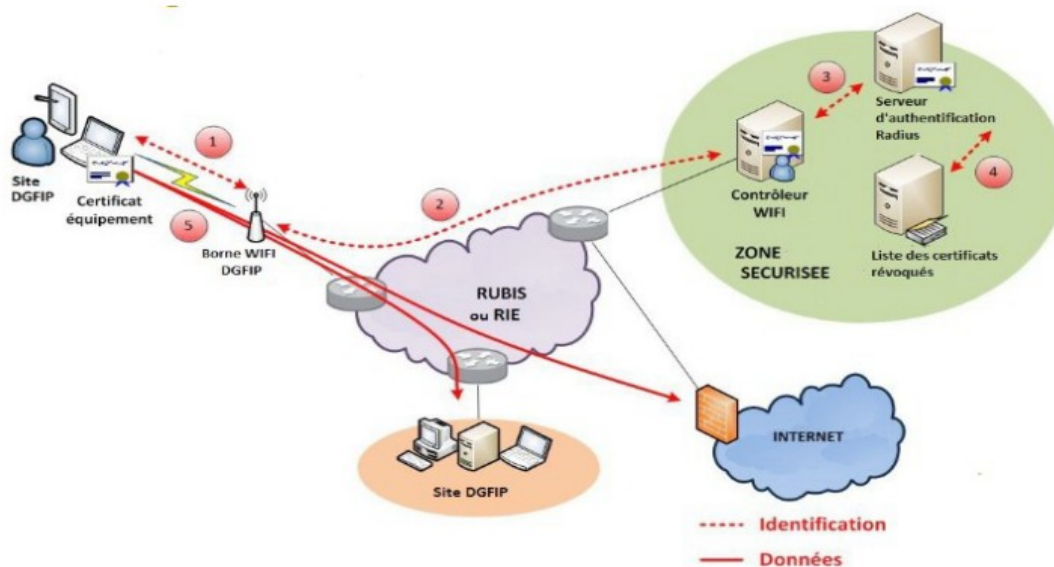
☞ **La connexion des bornes au réseau LAN nécessite un câblage de catégorie 6-6A et l'utilisation de ports gigabits.**

II.2.3.2.2 Le poste de travail :

Le poste de travail communique par WIFI avec une borne. La sécurité de la connexion est assurée par la mise en place d'un certificat sur le poste lui-même (authentification de la machine via le serveur radius). Les pré-requis :

- disposer d'un poste de travail avec le socle Windows ou Linux DGFIP
- disposer d'un certificat (fichier .p12) obtenu via l'application ODACE
- valider les tests d'authentification de la machine par le serveur radius,
- Vérifier la désactivation de tous les protocoles inutiles (IPV6, IPX, les protocoles multimédia...) afin d'optimiser les débits (cf fiche « optimisation réseau d'un poste » mise en ligne sur le portail SSI/SI2B/WIFI documentation pour la CID). Sachant que :
 - *Pour les postes W7 v4.6.3 et les versions supérieures, la désactivation des protocoles IPV6, LLNR, Ipx et SSDP doit être faite.*
 - *Concernant les postes Windows qui sont dans le domaine national, mise en place d'une GPO qui désactive IPV6, LLNR et SSDP.*
- Configurer l'adaptateur WIFI du poste de travail selon la fiche (mise en ligne sur le portail SSI/SI2B/WIFI documentation pour la CID).

Représentation schématique de l'établissement d'une connexion d'un poste à un LAN DGFIP via une borne WIFI



Légende des flux :

- 1) Le PC tente de se connecter au réseau sans fil (SSID) diffusé par la borne.
- 2) la demande d'authentification du PC est relayée au contrôleur WIFI par la borne.
- 3) le contrôleur WIFI demande au serveur radius d'authentifier le certificat du PC.
- 4) le serveur radius vérifie que le certificat ne figure pas dans la liste des certificats révoqués.
- 5) Si le certificat est reconnu valide, le PC est autorisé à se connecter au réseau DGFIP.

II.2.3.2.3 La borne WIFI

Règle d'acquisition des bornes : étant donné le coût d'une maintenance de 3 ans sur les bornes et le faible risque de panne matérielle, il est recommandé aux Directions de s'affranchir de cette maintenance.

En revanche, il est demandé aux SIL de prévoir une borne en Spare pour chaque Direction lors de la 1ere commande passée par celle-ci pour un de ses sites.

- Les bornes doivent être reliées soit au commutateur d'étage en utilisant le capillaire soit au cœur de réseau en utilisant des rocade cuivres (pré-requis : câblage catégorie 6-6A avec utilisation de ports gigabits).
- Il faut impérativement accrocher la borne sur son support (kit de montage) pour éviter une surchauffe.

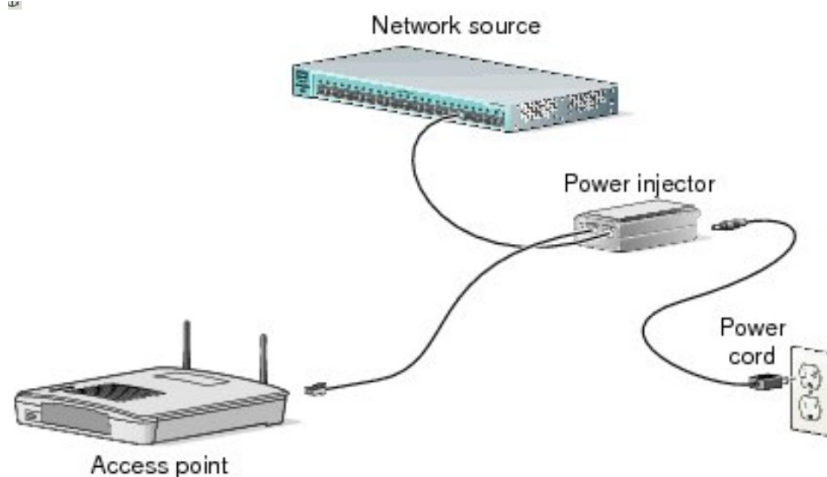
Les bornes Aruba sont construites pour dissiper la chaleur via les parties métalliques et non par ventilation d'air. La quantité de chaleur dissipée est équivalente mais contrairement au refroidissement par flux d'air, c'est l'équipement lui-même (ici la borne wifi) qui conduit cette chaleur vers l'extérieur d'où son échauffement en particulier --- par conception --- au niveau des parties métalliques. Il n'y a pas lieu de s'inquiéter de cet échauffement, qui est normal.

- L'alimentation électrique de la borne sera réalisée soit par :

- ⌘ l'activation de la PoE (Power On Ethernet) sur les commutateurs « PoE »
- ⌘ l'utilisation de Power Injector HP, qui est un injecteur de courant. Il convertit le courant alternatif 240V en courant continu de 48 v et le distribue à travers le câble Ethernet.

Dans le cadre d'une installation WIFI, les Power Injector sont adaptés pour les salles de réunion et les salles de formation nécessitant un seul point d'accès.

En revanche, l'installation de points d'accès WIFI pour remplacer le câblage de service(s) implique l'acquisition de switches PoE.



II.2.3.3 Gestion des VLAN, du SSID et des adresses IP

Les commutateurs d'extrémités doivent posséder une adresse IP et une IP route définies uniquement dans le vlan d'administration.

Les bornes posséderont une adresse IP attribuée en DHCP (adresse fixe dans GPAR) et une adresse IP de Gateway définies dans ce même vlan d'administration. L'attribution des adresses IP fixes se fera en commençant par la fin du sous-réseau IP.

Si les adresses disponibles dans le vlan admin (attribué au site) ne suffisent pas, un nouveau sous-réseau dans le vlan admin sera attribué (soit en continuité, soit de façon distincte).

Le port d'interconnexion entre la borne et le commutateur d'étage ou le cœur de réseau est un port trunk qui autorise le vlan d'admin et le (ou les) vlan data des utilisateurs mais interdit le vlan 1 (vlan par défaut). Les vlan utilisés par les utilisateurs WIFI seront les mêmes que les vlan des utilisateurs filaires. Le protocole STP devra être désactivé sur ce port.

Le SSID (Service Set Identifier) est le nom du réseau WIFI permettant de connecter un terminal à un point d'accès. A un SSID correspond un VLAN dans le contrôleur WIFI.

L'attribution d'adresses IP aux postes de travail se fait soit :

- par le service DHCP de la MMA,
- par le service DHCP des serveurs DHCP nationaux,
- manuellement pour les sites sans DHCP. Dans ce dernier cas, les utilisateurs sont

privés de mobilité.

Les imprimantes restent sur le réseau filaire et ont une adresse fixe.

Recommandation 5

Installation WIFI

Pré-requis :

- Les bornes seront impérativement connectées sur du câblage de catégorie 6-6A. Elles devront être accrochées sur leur support (kit de montage).
- L'installation de points d'accès WIFI pour remplacer le câblage de service(s) implique l'acquisition de switchs PoE et la vérification de l'aération ou de la ventilation des LTI/LTE.
- Si l'installation de plusieurs bornes est prévue dans le projet WIFI, il conviendra de vérifier la disponibilité de rocares ou de liens capillaires pour ces bornes avec les caractéristiques adéquates.

II.2.3.4 L'offre de service « WIFI-DGFiP » pour les directions

L'offre WIFI-DGFiP est une solution au remplacement du réseau câblé devenu obsolète pour un ou plusieurs étages d'un bâtiment et convient également dans le cas d'équipement WIFI d'une salle de réunion.

Le projet d'implantation d'un réseau WIFI est initié par une demande de devis formulée par la Direction puis adressée à la DiSI de rattachement. Cette demande permettra de recueillir les informations techniques, les éléments financiers et le calendrier de réalisation afin de décider de l'opportunité économique de cette installation.

Après l'avis du CHSCT local, la Direction indiquera à la DiSI la décision retenue et, si le projet d'implantation est confirmé, elle procédera aux commandes de matériels.

La phase d'étude préalable à la commande est composée de quatre étapes qui suivent la séquence suivante.

II.2.3.4.1 La Direction présente le projet d'implantation à la DiSI de rattachement

La Direction adresse à la DiSI de rattachement une demande de devis pour une implantation du WIFI-DGFiP en utilisant le fichier "**devis_installation_WIFI.ods**". Ce document permet d'identifier le bâtiment, les étages, les services et la date de mise en œuvre souhaitée.

L'ESI de la DiSI concernée effectue une demande d'étude à l'ESI de Besançon MSNRL pour une installation WIFI

Le bureau SI-2B met à disposition des SIL une interface web "EDWAR" permettant d'échanger de manière standardisée avec la MSNRL. Cet outil est présenté dans la fiche EDWAR pour les SIL en annexe 2. Elle indique, notamment, comment demander un identifiant de connexion à l'équipe TVM du bureau SI-2B.

EDWAR permet aux SIL de transmettre une demande d'étude pour une installation WIFI et de suivre le traitement de la demande. Deux fichiers seront impérativement joints, à défaut la demande sera rejetée :

- un plan à l'échelle avec le positionnement des postes de travail et la description des matériaux utilisés dans le bâtiment qui pourraient faire obstacle à la bonne diffusion des ondes;
- le fichier "devis_installation_WIFI.ods" transmis par la Direction et complété par le SIL (feuille "DEVIS établi par le SIL et la MSNRL") avec le nombre :

- d'adaptateurs WIFI;
- de switch POE;
- d'agents;
- d'imprimantes.

II.2.3.4.2 La DiSI transmet le devis complet à la Direction

En réponse à la demande d'étude, la MSNRL de l'ESI de Besançon complète les deux documents et les transmet au SIL de l'ESI demandeur à l'aide de l'outil EDWAR :

• Selon les spécificités du site il peut être nécessaire de faire réaliser une étude de couverture WIFI. Deux types de sites sont donc à considérer :

- des sites dits standards, n'ayant pas de particularité immobilière,
- des sites dits spécifiques, si on considère leur architecture ou leurs matériaux de construction (amphithéâtre avec hauts plafonds, bâtiments anciens aux murs épais, bâtiments ayant des structures métalliques, etc).

Dans la grande majorité des cas, les sites seront "standards" et cette prestation externe ne sera pas nécessaire. L'étude sur plan, réalisée par la MSNRL via une demande EDWAR, suffira pour savoir où et combien de points d'accès il faudra positionner.

Pour les sites qui seront jugés "spécifiques" par la MSNRL, une demande de prestation sera conseillée selon les termes suivants :

- cette étude peut être réalisée par :
 - un prestataire local, bien connu du SIL. Le coût de cette prestation sera à ajouter au devis établi par la MSNRL.
 - le prestataire titulaire du marché UGAP-LAN. Le coût de la prestation apparaîtra dans le devis établi par la MSNRL.
- Le SIL devra demander l'envoi du kit "étude couverture WIFI DGFIP" à la MSNRL, mais l'envoi et le retour sera pris en charge financièrement par la direction. Ce kit comprendra :
 - une ou plusieurs bornes du marché, elles seront utilisées en fonction de l'étude du site,
 - un injecteur PoE pour l'alimentation de la borne,
 - un câble eth long pour la connexion au réseau de la DGFIP.

Cette exigence se justifie par le souhait de faire des mesures au plus près des conditions réelles de fonctionnement (même sensibilité d'antenne et de réseau), même si les prestataires la jugeront inutile...

- Le prestataire devra réaliser son étude avec soit le logiciel EKAHAU soit le logiciel AIRMAGNET et **rendre un rapport de cette étude ainsi que les plans de couverture**. Ce rapport sera transmis par le SIL à la MSNRL, via EDWAR, pour examen.
- Le câblage des bornes est une prestation qui peut être commandée à SCC ou à son prestataire local. Cette prestation comprend la fixation des bornes.
- Le fichier "devis_installation_WIFI.ods" est complété :
 - du nombre de bornes y compris les licences, les kits de montage et les prises RJ45

nécessaires;

- du nombre éventuel de Power Injector ou de commutateur POE.

A réception de ces fichiers, l'ESI est en mesure de transmettre le devis complet à la DiSI pour communication à la Direction. L'ESI précisera à la direction qu'il s'agit d'une estimation financière, certes la plus fine possible, mais qu'une différence de coûts (très limitée) est toujours possible .

II.2.3.4.3 Le choix de la Direction

Les informations portées dans le devis permettent à la Direction :

- de ne pas engager l'installation; dans ce cas, le SIL signifie, à l'aide d'EDWAR, le refus de la Direction et la MSNRL clôture le ticket ouvert;
- d'accepter le projet d'installation. Trois actions sont à engager :
 1. la présentation du projet en CHSCT par la Direction, avec l'accompagnement d'un « représentant ou expert technique de l'ESI ». Un support, à demander auprès de l'équipe TVM, permet de préparer la présentation aux partenaires sociaux.
 2. la commande des matériels, des licences et éventuellement des prestations (de câblage, d'étude de couverture wifi) nécessaires par la Direction. Les bornes sont garanties 5 ans par le constructeur en tant que matériel.
 3. la notification à la MSNRL par le SIL avec l'outil EDWAR de l'autorisation de la Direction d'engager les opérations techniques (ouverture des flux entre les bornes et les contrôleurs, le provisionnement des bornes). Lorsque ces opérations sont réalisées, la MSNRL informe le SIL avec EDWAR.

Une chronologie de l'ensemble des étapes et des échanges à réaliser est présentée à l'annexe 4.



La documentation de l'offre de service WIFI-DGFIP est publiée dans l'intranet du bureau

SI-2B [<http://si.intranet.dgfip/si2b/wifi>].

II.2.4 La ToIP

Le déploiement d'une offre de service DGFIP de ToIP centralisée et entièrement sécurisée via deux datacenters impose des contraintes particulières sur les infrastructures réseaux.

Cette solution permet de mutualiser les ressources de téléphonie afin d'homogénéiser le parc de la DGFIP.

L'architecture est composée de multiples nœuds d'IPBX répartis sur 2 Datacenters du Ministère de la Justice et reliés avec des liens du RIE aux différents sites de la DGFIP.

Les téléphones IP raccordés sur l'infrastructure réseaux communiquent directement avec les IPBX centralisés. Ils sont branchés en « coupure » entre le PC utilisateur et le commutateur de distribution Power Over Ethernet (PoE).

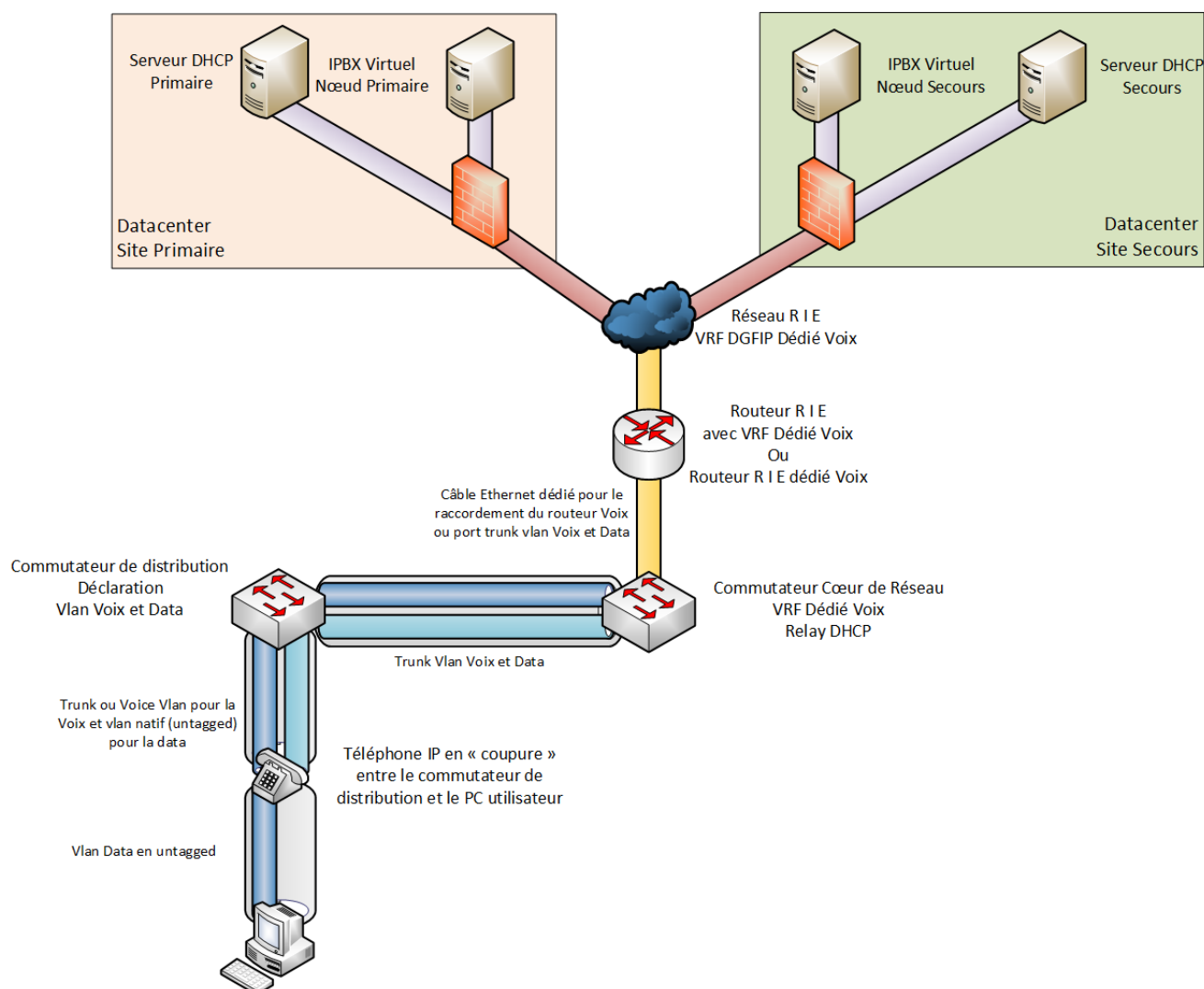


Schéma simplifié de l'infrastructure de ToIP Centralisée

II.2.4.1 Pré-requis réseau à une installation ToIP

II.2.4.1.1 Partie Opérateur

Le projet de téléphonie impose une **isolation de l'accès à la VRF Voix dédiée du RIE**.

Sur les petits sites, cela peut prendre la forme d'un deuxième routeur dédié Voix ou la mise en œuvre de la solution multi-VRF cuivre en cours d'étude.

Pour tous les sites, la VRF sera propagée directement sur le routeur RIE.

Les (ou le) routeurs seront raccordés au cœur de réseau via un vlan d'interconnexion spécifique avec comme identifiant de **vlan (VID) 913**.

Ils (ou il) seront branchés directement sur le cœur de réseau :

- soit en ajoutant de nouveaux câbles Ethernet de catégorie 6a ;

- soit en utilisant le câble actuel mais en configuration « port trunk » si le nombre de port réseau sur le routeur ne le permet pas.

Le routeur opérateur ne doit pas effacer le marquage en EF des trames pour ne pas perdre la qualité de service (QoS).

Le port sera en auto-négociation, vitesse auto et spanning-tree désactivés

II.2.4.1.2 Partie LAN locaux techniques et baies

En matière de climatisation, il est impératif de respecter les points de consignes de la Charte LAN.

A savoir températures mini 10° / maxi 40° ; hygrométrie mini 10 % / maxi 90 %

Le respect de cette température permettra d'augmenter la durée de vie des matériels.

Pour rappel, il est recommandé d'installer les équipements LAN dans les baies dédiées, ou coffret mural avec un dispositif de ventilation intégré.

Les commutateurs PoE dégageant une chaleur plus conséquente, il est impératif de vérifier que le LTE soit suffisamment aéré ou ventilé.

De plus, les dimensions de ces équipements au niveau profondeur peuvent être supérieures à celles des équipements standard (les baies réseau et mixte répondent à ce besoin).

Pour rappel, les bâti-racks sont à proscrire, car il n'y a pas de panneaux de protection pour les matériels et les flux d'aération ne sont pas gérés.

II.2.4.1.3 Partie LAN cœurs de réseau

Une VRF dédiée Voix doit être créée sur le cœur de réseau du site afin de gérer le routage des vlan ToIP. Elle isolera complètement la partie téléphonique pour la rendre étanche du réseau data et préserver l'intégrité de ce dernier. Celle-ci permet de créer une route par défaut vers la VRF opérateur RIE.

Un ou plusieurs vlan dédiés à la ToIP en /24 seront créés sur le cœur de réseau pour isoler les réseaux de la data (ou des autres services). Ils seront propagés en mode trunk vers les commutateurs d'extrémité via les liens déjà existants. Ces vlan auront les champs de QoS activés pour la téléphonie (voice vlan...).

Le cœur de réseau sera raccordé au(x) routeur(s) via un vlan d'interconnexion [supplémentaire et](#) spécifique avec comme identifiant de vlan (VID) 913.

Le **Relay DHCP** sera activé pour chaque vlan ToIP vers les deux serveurs DHCP hébergés sur la plateforme de ToIP centralisée.

La séparation de flux, en plus d'apporter de la sécurité, va permettre de faire de la QoS (Quality of Service).

Par défaut, les téléphones remplissent le champ CoS (Class of Service) pour donner une priorité élevée à la trame (6).

Au niveau du paquet IP, le marquage du champ DSCP (Differentiated Services Code Point) avec le point code EF (Expedited Forwarding) permettra de bénéficier du meilleur traitement disponible sur le réseau.

Le cœur de réseau ne doit pas effacer le marquage en EF des trames pour ne pas perdre la QoS.

Le port sera en auto-négociation et vitesse auto.

II.2.4.1.4 Partie LAN distribution

Afin d'alimenter électriquement les téléphones IP, les commutateurs d'extrémité seront PoE. Le budget de puissance maximal PoE, qui correspond à la quantité totale de puissance attendue par les équipements de la téléphonie (téléphone Alcatel) sera de maximum 5 watts (classe 2) par port. Pour les pieuvres de téléconférence, il sera de maximum 15 watts (classe 3).

Les vlan ToIP et Data seront propagés sur l'ensemble des ports de distribution. Ces vlan auront les champs de QoS activés pour la téléphonie (voice vlan...).

Le Link Layer Discovery Protocol (LLDP) et son extension LLDP-MED (Media Endpoint Discovery), seront activés afin d'indiquer aux téléphones IP le vlan ToIP.

II.2.4.1.5 Conformité à la Charte LAN

Quel que soit le projet, l'architecture du réseau local et la configuration des commutateurs doivent respecter la charte LAN de la DGFIP.

II.2.4.2 Architecture Physique

II.2.4.2.1 Le téléphone IP

Le téléphone IP est branché en « coupure » sur le réseau filaire entre le commutateur d'extrémité et le PC de l'utilisateur.

Il utilise la technologie PoE pour être alimenté électriquement via le câble Ethernet de catégorie 6a de type LSZH (Low Smoke Zero Halogène) avec un blindage '**U/FTP** ou **F/FTP**'. Ce procédé permet de ne pas encombrer le bureau d'un câble d'alimentation dédié.

Le commutateur propage en mode tagged le vlan voix, que le téléphone IP apprend à l'aide du protocole LLDP-MED, et en mode untagged le vlan data du poste de travail de l'utilisateur. Ce mode ne nécessite aucune modification de configuration réseau sur le poste de travail de l'utilisateur.

Pour obtenir une adresse IP, le téléphone IP fera une **requête DHCP sur le vlan Voix** qui sera relayée vers un serveur DHCP de la plateforme centralisée.

Le Téléphone IP communique avec la plateforme centralisée via le vlan ToIP en passant successivement par la VRF ToIP du cœur de réseau, puis la VRF DGFIP ToIP du routeur pour enfin accéder à l'IPBX en Datacenter.

Nota :

- Si deux téléphones IP internes (inter ou intra-site) veulent communiquer ensemble, le flux voix sera établi directement entre les deux équipements en mode Peer to Peer (P2P).
- Si un téléphone IP interne veut joindre « l'extérieur », il établira le flux voix vers la plateforme centralisée.
- S'il y a une rupture du lien WAN sur la VRF Voix ou du lien dédié Voix sur site, les téléphones IP ne vont plus pouvoir émettre et recevoir d'appel et cela même en interne.
- S'il y a une dégradation de qualité du lien WAN sur la VRF Voix ou du lien dédié Voix sur site, il y aura une dégradation de la qualité des appels téléphonique vers l'extérieur et vers les autres sites.

II.2.4.3 Normalisation des VLAN et des adresses IP

L'environnement technique vlan voix est abordé différemment en fonction de chaque constructeur. Selon les équipements, les administrateurs réseaux se reporteront aux guides de configuration à leur disposition pour implémenter la propagation du vlan ToIP pour les téléphones IP.

Le switch du téléphone IP ne propage pas vers le PC de l'utilisateur le vlan ToIP.

Tous les équipements des vlan Voix seront configurés en DHCP. Le serveur DHCP, hébergé sur la plate-forme de la Justice, sera dédié à la ToIP. Une configuration relay-DHCP vers ce serveur, qui attribuera les adresses IP des téléphones IP, sera nécessaire sur les cœurs de réseau.

La MSNRL définit la norme du plan d'adressage ToIP.

Elle collecte et centralise les données pour répondre aux objectifs définis dans la Charte LAN qui sont d'optimiser le plan d'adressage réseau à la DGFIP et ainsi, éviter une redondance des informations.

Elle est responsable de la surveillance de la normalisation réseau ToIP de la DGFIP et en assure le contrôle de conformité.

Par mesure de sécurité, les mécanismes de gestion du plan d'adressage ToIP et DATA seront indépendants.

II.3 Règles générales

II.3.1 Règles de configuration de base des équipements

Les spécifications en matière de configurations des équipements actifs à déployer sur site doivent être réalisées lors de la phase d'étude et conception du service.

Recommandation 6

Spécifications LAN : configuration de base des équipements

Il est recommandé d'intégrer au minimum les paramètres de configuration suivants dans les commutateurs :


- ◆ un nom d'équipement conforme à la Charte LAN définie au §II.5infra ;
- ◆ une adresse IP d'administration (cf §II.5.3.1) ;
- ◆ une adresse IP dans le vlan Opérateur 901 pour un équipement Cœur de Réseau;
- ◆ deux utilisateurs (admin et monitor) avec accès sécurisé SSH ;
 - le premier ayant accès en lecture/écriture,
 - le second en lecture seule ;
- ◆ configuration de la zone fuseau horaire : timezone=Paris (sauf pour les sites d'outre-mer) ;
- ◆ activation du service temps (NTP) pour mise à jour date et heure automatique. C'est les adresses des serveurs de temps (10.156.33.113 et 10.154.59.70) qui servent de référence ;
- ◆ activation de Spanning Tree (mode RSTP) sur l'ensemble des commutateurs avec :
 - priorité haute (0) pour un équipement cœur de Réseau,
 - priorité par défaut (32768) pour les autres équipements,
 - désactivation du Spanning Tree sur le lien du (ou des) routeur(s) WAN et du (ou des) borne(s) WIFI ;
- ◆ définir le server syslog de destination (serveur de supervision des SILs), le trap server de

destination ;

- ◆ définir les paramètres SNMP (location, contact, community name (lanread et SIL « dep ») ...).

Pour tout commutateur, chaque port sera configuré comme suit :

- ◆ gestion des VLAN :
 - pour les ports Access, configuration du vlan data en vlan natif et suppression systématique du VLAN 1 (vlan par défaut),
 - pour les ports Trunk, configuration des vlan (administration, data et voix) et suppression du VLAN 1 (vlan par défaut)
- ◆ configuration des ports Gigabits en auto-négociation, ceux-ci seront privilégiés pour les interconnexions de commutateurs,
- ◆ pour les ports limités au 10/100 Mbps :
 - configuration du (ou des) port(s) 1 (et 2) 100 Mbps full duplex pour les liens vers le (ou les) routeur WAN
 - configuration des ports d'interconnexions de commutateurs au débit fixe de 100 Mbps full duplex,
 - configuration des ports 3 et 4 en mode 'Trunk', uniquement sur les cœurs de réseau, avec tous les vlan du site, y compris admin et ToIP, pour pouvoir brancher un équipement d'audit ou un PC de l'administrateur ; ces ports devront être "Admin down" lorsqu'ils ne sont pas utilisés ;
 - configuration en auto-négociation pour les stations et imprimantes,
- ◆ désactivation (ADMIN DOWN) de tous les ports inutilisés : obligatoire sur le cœur de réseau et fortement recommandée sur les commutateurs d'accès ;
- ◆ **désactiver le serveur web de gestion du commutateur, que ce soit en version sécurisée (HTTPS) ou non (HTTP). En effet, la présence d'un serveur web augmente la surface d'attaque de l'équipement et peut nuire à ses performances.**
- ◆ activation de la fonction MDI/MDI-X de l'adaptation électrique (croisé/décroisé) des câbles

 Quelle que soit la liaison, les configurations speed et duplex doivent être strictement identiques de part et d'autre d'une liaison.

Recommandation 7

Spécifications LAN : configuration de base pour les sites équipés de la ToIP

Il est recommandé de configurer les paramètres suivants :

Sur le cœur de réseau, configuration d'une VRF (ToIP) pour isoler le trafic voix du trafic data, activation de la fonction Relay DHCP pour que les deux serveurs DHCP hébergés sur la plateforme de ToIP centralisée fournissent automatiquement une adresse IP aux téléphones dans le vlan voix et configuration du vlan voix avec un interface IP.

Sur les commutateurs d'extrémité, activation du LLDP et configuration du voice vlan

Les ports sur lesquels sont connectés l'ensemble des équipements téléphone/poste de travail doivent être configurés en mode 'Trunk'. Le « vlan data » sera configuré en vlan natif, le « vlan voix » sera configuré en 802.1Q (tagué) et le vlan 1 sera désactivé.

Cette configuration pourra être mise en œuvre en avance de phase sur le déploiement de la ToIP, puisqu'elle autorise le fonctionnement d'un poste de travail directement connecté au commutateur.

A l'installation d'un téléphone (IP-phone), celui-ci viendra s'intercaler entre le commutateur et le poste de travail PC.

Les autres paramètres dépendent de l'architecture et sont configurés au moment de la mise en service des équipements

II.3.2 Règles pour les « Piles de commutateurs »


Recommandation 8

Spécifications LAN : empilement des commutateurs

Les commutateurs (cœurs de réseau ou accès) peuvent être regroupés en piles. Ils sont considérés, du point de vue de l'architecture et l'administration du LAN, comme un unique commutateur avec une grande capacité et une performance accrue.

Il est recommandé de configurer les deux commutateurs d'une pile de manière identique, y compris pour la configuration des ports, de manière à pouvoir facilement déplacer une connexion de l'un à l'autre (redondance des ports).

La taille de la pile doit se limiter à 2 commutateurs pour des raisons de performances et de limitation des perturbations réseau.

 *Exceptionnellement, un troisième élément pourra être ajouté en cas de saturation de rocade. Le chaînage de deux commutateurs par des ports Ethernet (RJ45) n'est pas autorisé.*

L'empilement des commutateurs sera réalisé à partir des modules d'empilement spécifiques propres à chaque constructeur et à chaque modèle.

Il est autorisé d'empiler les commutateurs 48 ports mais nous attirons votre attention sur le fait qu'en cas de panne d'un élément de la pile le nombre de personnes impactées est deux fois plus élevé qu'avec

les 24 ports.

Sur les grands sites, les piles de commutateurs sont à privilégier par rapport aux châssis pour les raisons de facilité de maintenance (gestion du Spare, contrats de maintenance), les principaux intérêts du châssis étant sa puissance de commutation et sa modularité

Dans le cas de redondance des équipements 'cœur de réseau' (pile) ou des cartes d'entrée sortie d'un châssis, le double attachement avec les piles de commutateurs d'accès sera réparti sur chaque élément du cœur de réseau.

En ce qui concerne la redondance électrique, vous devez, lorsque cela est possible, brancher électriquement chaque élément de la pile sur un bandeau différent, voir une voie différente.

II.3.3 Niveaux de chaînage des équipements

Recommandation 9

Spécifications LAN : niveau de chaînage des équipements

Il n'est pas autorisé de cascader un commutateur d'accès sur un autre. Tout équipement d'accès doit être raccordé au cœur de réseau.

Le nombre d'équipements LAN à traverser d'un équipement terminal au routeur d'accès du site n'excédera pas deux, sauf si l'accès WAN dessert plusieurs bâtiments, auquel cas on pourra avoir un cœur de réseau de bâtiment à traverser, soit un niveau de plus.

🔧 *Afin de faciliter le repérage entre les commutateurs il est recommandé de connecter un cordon de brassage de couleur*

Les câbles de raccordement entre commutateurs sont des câbles droits. La fonction de détection automatique (MDI/MDI-X) sera activée systématiquement sur les équipements : elle se charge de l'adaptation des câbles.

II.3.4 Activation des fonctionnalités de niveau 3

Les fonctionnalités de niveau 3 ne sont activées dans le cœur de réseau que s'il est nécessaire d'établir des communications entre équipements terminaux et/ou serveurs appartenant à des VLAN différents dans un même site. Les critères d'activation du niveau 3 sont présentés au §II.5.6

II.3.5 Raccordement des serveurs

Les serveurs, regroupés dans le Local Technique de l'Immeuble (LTI) ou dans un local adjacent, seront de préférence tous raccordés directement au cœur de réseau (lien unique ou doubles liens agrégés).

Dans les grands sites, certains serveurs ayant besoin d'un surcroît de résilience pourront être raccordés par un double attachement.

Dans ce cas, si le cœur de réseau est redondé, chaque attachement sera raccordé à un cœur de réseau distinct. Un tel montage couvre le basculement du commutateur actif vers le commutateur de backup, mais pas la panne de la carte Ethernet du serveur. La résilience complète est obtenue en agrégeant les liens du serveur vers une pile de cœurs de réseau redondés.

Chaque serveur de domaine doit être isolé dans un vlan dédié constituant un sous-réseau IP distinct. Le système de sauvegarde associé doit être dans le même vlan pour favoriser les temps de traitement.

La numérotation, pour un site, de l'identifiant de VLAN (VID) associé est 3000 pour le premier serveur, 3001 pour le suivant... avec des sous-réseaux IP différents.

Recommandation 10

Spécifications LAN : raccordement des serveurs

Il est recommandé que les serveurs d'applications du site soient directement raccordés au cœur de réseau.

Chaque serveur sera isolé dans un vlan dédié. L'identifiant du VLAN (VID) débutera à 3000 pour le 1^{er} serveur du site, 3001 pour le deuxième serveur, etc ... avec des sous-réseaux différents.

II.3.6 Ports à réserver pour usages particuliers

Une normalisation en termes de raccordement de certains équipements est nécessaire pour une gestion et exploitation efficace :

- Sur les cœurs de réseau, les ports 1 et 2 seront réservés pour l'interconnexion des interfaces du (ou des) routeurs.
- Sur les équipements d'extrémité, les ports GigaBits seront privilégiés pour l'interconnexion avec le (ou les) cœurs de réseau.
- Les ports 3 et 4 devront être disponibles sur les cœurs de réseau pour des usages ponctuels, notamment en cas d'incident :
 - un port pour connecter un PC en console d'administration
 - un port pour connecter une sonde de mesure
- Un port, au minimum, devra rester libre quel que soit le type d'équipement. Dans la négative, une étude de l'architecture devra être effectuée par les responsables réseaux.

A noter que le VLAN d'administration devra comporter obligatoirement une adresse IP pour la console d'administration ou matériel d'audit et une adresse IP pour une éventuelle sonde. Dans les ESI (des SIL), une adresse supplémentaire sera réservée pour le serveur de supervision OpManager.

Recommandation 11

Spécifications LAN : ports réservés pour usages particuliers

Il est recommandé de réserver les ports LAN suivants lors des spécifications de configurations des commutateurs :

- cœur de réseau :
 - ports 1 (et 2) pour le(s) routeur(s) d'accès WAN,
 - ports 3 et 4 pour la console d'administration et pour une sonde de mesure,
 - ports Gigabits pour l'interconnexion avec les équipements d'accès.
- équipements d'accès :
 - ports Gigabits pour l'interconnexion avec le cœur de réseau.

II.3.7 Documents de référence et mises à jour de firmware

Les guides de configuration des commutateurs (fonctionnalités de niveau 2 et de niveau 3 ainsi que les mises à jour de firmware sont disponibles sur le site de la MSNRL à l'adresse suivante :

<http://msnrl.intranet.dgfip/msnrl/missions/reseau/equipements.htm>

Les évolutions de version sont parfois rapides et il est impératif de s'assurer régulièrement que la dernière est en service.

Attention : sauf cas très particuliers, les évolutions de versions doivent toujours être réalisées dans le sens montant (upgrade). Les évolutions dans le sens descendant (downgrade) provoquent des blocages matériels.

La connexion à l'utilitaire réseau <http://utilitaires-reseau.appli.dgfip> onglet « MajCom » permet aux équipes SIL de mettre à jour les firmwares des commutateurs de façon plus rapide et plus sécurisée.

II.3.8 Sauvegarde de configurations et syslog

Une sauvegarde automatique ou à la demande sera réalisée et centralisée mensuellement ou lors de toute modification via l'utilitaire réseau.

La sauvegarde déportée, régulière et systématique des configurations est obligatoire à chaque nouvelle installation et à chaque changement de configuration (voir nom du fichier de sauvegarde dans 'nommage des fichiers de sauvegarde...' au §II.5.2.6). Elle est réalisée par le service TFTP sur le serveur dédié à cette tâche.

De même, les fichiers syslog, générés par les commutateurs en cas d'incident, seront sauvegardés sur le serveur de supervision du SIL.

II.3.9 Constitution d'un stock d'équipements en Spare

Le stock en SPARE permet de :

- réaliser des économies sur les contrats de maintenance
- réduire le temps de remplacement d'un commutateur

Le stock de SPARE est situé dans les ESI et géré par les SIL. Il ne sera utilisé que pour remplacer des équipements défectueux et en aucun cas pour réaliser des extensions ou remplacements de modèles obsolètes. En retour de réparation, les équipements remplacés sont remis dans le stock de SPARE.

Le SPARE comprend :

- un commutateur cœur de réseau de chaque type (hors châssis) par SIL. Le coût de ces commutateurs est à la charge du bureau SI2B.
- un commutateur d'extrémité de chaque type (en 24 ports ou 48 ports) par SIL. Le coût de ces commutateurs est à la charge des directions locales.

Tous les commutateurs destinés au stock de SPARE doivent être testés rapidement après la livraison, mis à jour du firmware en cours et stockés dans un endroit approprié.

L'affectation ou le remplacement d'un cœur de réseau est planifié en accord avec la MSNRL.

II.3.10 Remplacement ou démontage d'un commutateur

Lorsqu'un commutateur administrable quitte un site pour cause de remplacement par un autre commutateur ou parce qu'il n'est plus utile sur ce site, il retourne obligatoirement au stock des commutateurs en Spare, après avoir subi:

- Reconfiguration en configuration d'usine,
- Mise à jour du firmware avec la dernière version validée par la MSNRL.

La même politique sera appliquée sur un matériel en retour de réparation ou d'échange standard.

En aucun cas, un commutateur ne peut être réinstallé sur un autre site ou dans un autre local technique du même site sans avoir subi ces deux opérations.

II.3.11 Gestion de la haute disponibilité

La haute disponibilité est présentée dans le schéma du §II.4.4. On y observe une redondance des routeurs et des cœurs de réseau. Dans la plupart des cas, les cœurs de réseau redondés seront placés dans le même LTI. La redondance des arrivées d'énergie électrique est également fortement recommandée.

☞ Les liens entre le cœur de réseau redondé et les commutateurs d'accès seront doublés avec un lien sur chaque élément du cœur de réseau et l'activation du protocole « Spanning Tree » sur l'ensemble des équipements.

Sur le cœur de réseau redondé, la priorité haute (0) du « Spanning Tree » sera affectée au Master et une priorité inférieure (4096) sera affectée au Backup. Sur les équipements d'accès, la priorité restera par défaut 32768.

Les liens avec les équipements terminaux (serveurs, routeurs...) pourront être doublés ou non. S'ils sont doublés, le basculement vers le cœur de réseau Backup pourra être réalisé automatiquement ou manuellement. Dans ce cas, l'administrateur devra intervenir sur les câbles Ethernet.

La DGFIP recommande de créer une pile de commutateurs (ex: deux A5500 de HP/H3C), avec redondance des liens vers les commutateurs d'accès et si possible vers les serveurs. Cette configuration simplifie les problématiques de maintenance et de SPARE.

Certains sites sont équipés de châssis. Dans ce cas, la redondance (CPU et alimentation) est intrinsèque à l'équipement. La redondance des ports se fait en installant plusieurs cartes identiques et en connectant les équipements (commutateurs d'accès et serveurs) sur des ports de cartes distinctes.

☞ Compte tenu des coûts de maintenance, des éléments de Spare ont été livrés sur les sites disposant d'un châssis et les contrats de maintenance n'ont pas été reconduits. De même, le coût important des châssis conduit à ne pas recommander la redondance par doublement des châssis.

Dans le cas, de redondance par doublement des cœurs de réseau, les interfaces IP des VLAN (cf. §II.5.4.2) sont implantées dans l'un ou l'autre cœur. Il est alors nécessaire de configurer leur basculement automatique d'un cœur à l'autre en cas de panne, à l'aide du protocole VRRP (RFC 3768).

II.4 Architectures de référence

Les schémas d'architecture présentés dans ce chapitre sont simplifiés pour plus de clarté. Se référer à la Documentation de site pour plus de détails sur le contenu d'un schéma d'architecture logique.

II.4.1 Architecture d'un petit site

Dans le cas d'un petit site, le commutateur ne nécessite pas d'autre configuration que la configuration de base présentée au § II.3.1supra. Ces sites ne disposant généralement que d'un commutateur, le vlan d'admin sera remplacé par une loopback admin.

Exemple :

Interface loopback 0

ip address 10.dd.216.yyy 32 (32 correspond au masque de sous-réseau)

Un petit site n'est pas doté nécessairement d'un LTI. Cependant les équipements (routeur, commutateur et éventuellement panneau de brassage) ne doivent pas être posés sur une table, mais plutôt fixés sur une étagère murale ou mieux, un coffret mural 19 U à une hauteur de 1,40 m environ pour être accessible facilement.

Quel que soit le type d'architecture, les ports non utilisés devront être désactivés (shutdown).

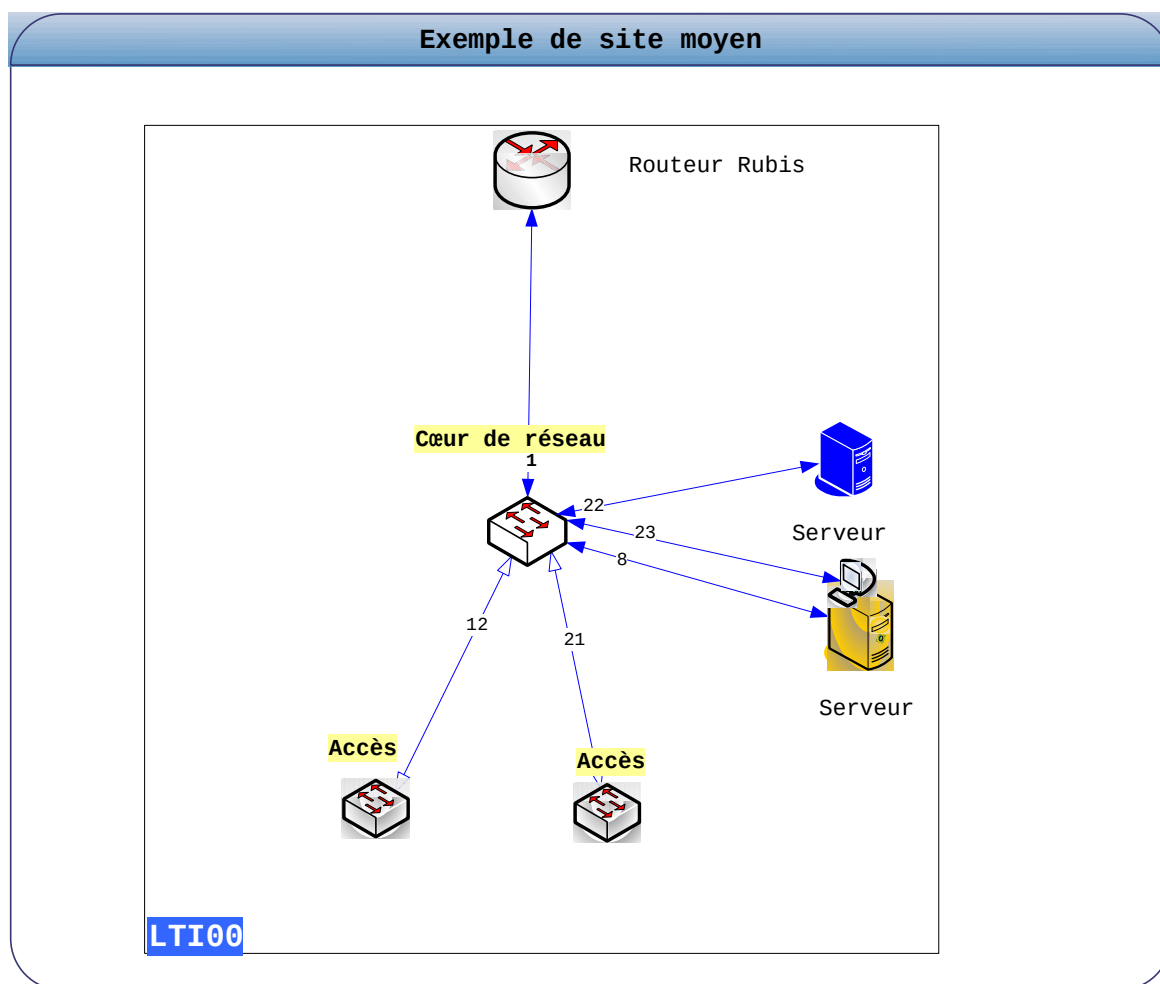
La mise en service du réseau LAN comprend les étapes suivantes :

- réalisation des branchements en respectant les normes,
- mise en service du commutateur pré-configuré,
- test de la connectique et du fonctionnement des différentes applications dans le site (intranet, messagerie, Wincom...)

II.4.2 Architecture d'un site moyen

Un site moyen (cf. II.1 ci-dessus) est doté d'un cœur de réseau et d'un ou plusieurs commutateurs d'accès. Ces équipements sont placés dans le LTI dans une baie réseau 19" (cf. normes des locaux techniques et des baies réseau dans la première partie de la Charte LAN (Guide de câblage)).

L'ensemble du pré-câblage est construit en étoile autour du LTI qui contient les armoires de brassage et les équipements.



Les accès aux équipements serveurs sont configurés de manière spécifique, ainsi que les liens trunk entre le cœur de réseau et les commutateurs d'accès (cf § II.5.4.2infra)

II.4.3 Architecture d'un grand site

Un grand site (cf. §II.1 ci-dessus) est doté d'un LTI et d'au moins un LTE par étage.

Le LTI est muni de baies réseau contenant le cœur de réseau LAN, il regroupe les serveurs et en général le routeur d'accès WAN (ex RIE).

Si le site ne contient pas de Data Center, les serveurs du site sont regroupés dans le LTI et directement raccordés au cœur de réseau.

Dans chaque LTE, les commutateurs d'accès employés seuls ou en piles seront raccordés sur le cœur de réseau en utilisant les rocade fibres ou cuivres. Dans le cas de piles, les liaisons pourront être doublées pour minimiser l'impact de la coupure réseau en cas de panne matérielle d'un élément de la pile.

Le schéma type d'une architecture de grand site est présenté dans la première partie de la Charte LAN (Guide de câblage au §II.2.1). Le chapitre III.2.2 de ce même document présente les normes de rackage : comment disposer les équipements réseaux dans des baies réseau avec panneaux de brassage.

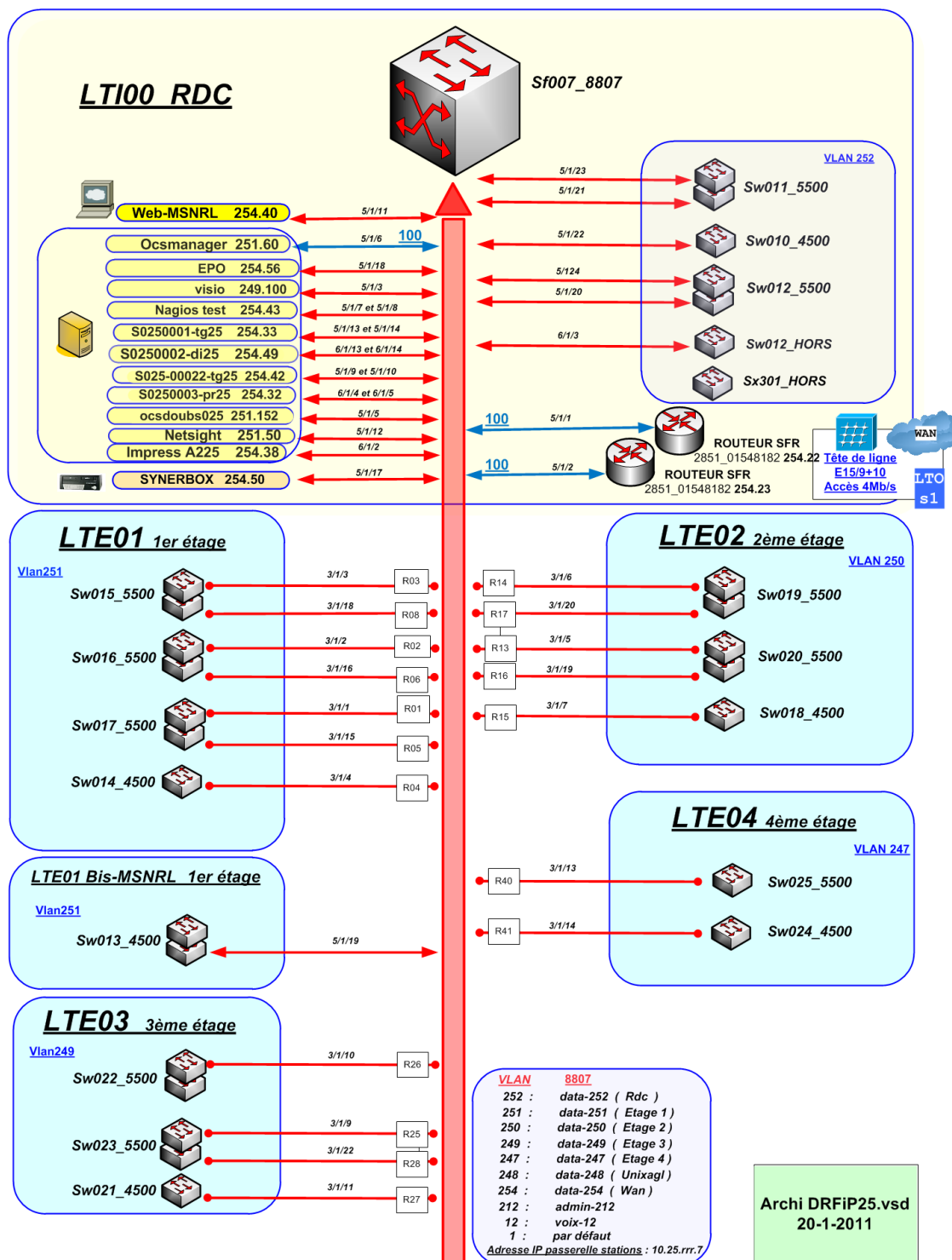
Le schéma ci-dessous montre une architecture de 2 bâtiments reliés par fibre optique, avec un cœur de réseau dans le LTI du bâtiment secondaire qui possède également 2 étages.

DRFIP BESANCON

Site : 0250000 - Master ID : 0000000001548182


Adresse : 63 Quai Veil Picard 25000 BESANCON

Vlan Admin : 10.25.212.0/27



II.4.4 Architecture complexe et redondance de cœur de réseau

Enfin, dans le cas des architectures complexes pour lesquelles existent de fortes contraintes de disponibilité, la redondance des cœurs de réseau pourra être envisagée et devra apparaître clairement décrite sur le synoptique.

 **Il est fortement recommandé de privilégier l'architecture IRF (mise en pile des équipements) pour une gestion plus rapide et plus sécurisée.**

Le schéma montre l'interconnexion des différents éléments avec les 2 commutateurs cœur de réseau : le "master" et le "backup". Les deux commutateurs sont reliés au moyen d'une agrégation de liens qui supporte le protocole 802.1q pour le transport des vlan. Un échange permanent d'informations a lieu entre les deux équipements.

Il faut noter que les liens entre le cœur de réseau et les commutateurs d'accès sont doublés. La gestion des boucles et de la double connexion des équipements terminaux est réalisée de la même façon. (voir [§ II.3.11](#))

La configuration retenue est la suivante :

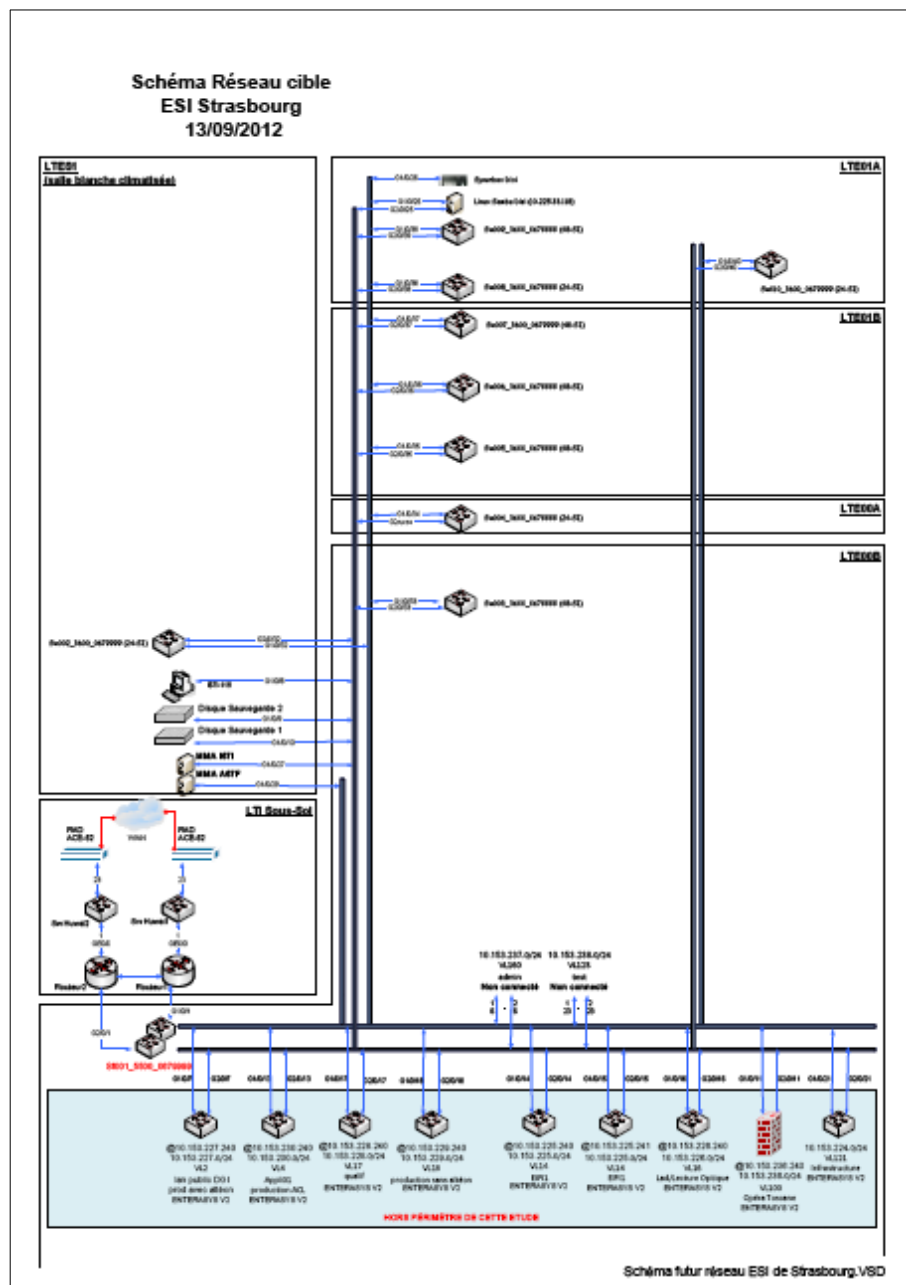
- configuration spécifique des liens pour le ou les serveurs (agrégat),
- configuration spécifique des liens d'interconnexion (trunk). Ces liens pourront être doublés pour assurer une redondance (agrégat),
- configuration spécifique des liens entre le cœur de réseau master et le cœur de réseau backup (VRRP) ou IRF.
- mise en place des vlan : voir § II.5.4
- le cœur de réseau assurera le routage entre les Vlan ; une adresse IP sera configurée sur chaque vlan-interface ; cette adresse IP servira de passerelle pour les serveurs, stations et imprimantes ;
- autant que possible, on se rapprochera de configurations identiques sur les deux cœurs de réseau (même configuration matérielle, utilisation des mêmes ports pour les mêmes usages)

Recommandation 12

Architecture de référence : règles spécifiques

- Configuration spécifique des liens pour le ou les serveurs (agrégat),
- Configuration spécifique des liens d'interconnexion (trunk). Ces liens pourront être doublés pour assurer une redondance (agrégat),
- Mise en place des vlan,
- Le cœur de réseau assurera le routage entre les Vlan.

Pour l'ensemble des architectures DGFIP, sauf les petits sites, le cœur de réseau (fédérateur) est un équipement empilable dont l'ensemble des ports sont Gigabits, de type 24 et/ou 48 ports cuivres et/ou 24 ports SFP (fibres optiques).



II.5 Configuration et administration

II.5.1 Acteurs

Les SIL sont pleinement responsables de la mise en service et de l'exploitation des équipements de réseau, ce qui inclut l'application des architectures définies par le bureau SI2B, l'installation, la configuration, le branchement, la documentation, l'administration, la gestion des incidents, l'audit de site et la gestion des changements sur ces équipements.

L'organisation est décrite au §I.3.

II.5.2 Règles de nommage des équipements

Les règles de nommage interviennent dans :

- ◆ l'élaboration des schémas d'architecture ;
- ◆ le prompt en mode administration des équipements ;
- ◆ l'étiquetage des équipements ;
- ◆ le nommage des fichiers de sauvegarde des configurations et des fichiers logs d'événements ;
- ◆ la constitution d'un référentiel du parc des commutateurs au niveau du SIL, qui sera consolidé au niveau national.

Afin de pouvoir localiser et identifier précisément les équipements, leur nom comprend:

- ◆ le type de commutateur ;
- ◆ le 4e octet de l'adresse IP d'administration (ou le N° de séquence pour les équipements non administrables) ;
- ◆ le type d'équipement (ou 'Hors' pour les équipements achetés hors marché) ;
- ◆ le code site.

Recommandation 13

Spécifications LAN : règles de nommage des équipements

Il est recommandé d'identifier par un nom tous les équipements qui seront déployés sur un site donné.

L'ensemble des règles de nommage détaillé ci-après doit suivre les règles énoncées ci-dessus et dans la suite de ce paragraphe.

Document support	Type	Adresse admin / N° séquence	Code modèle	Ident. site	Date	Exemples
NbCar	2car	3car	4car	5 car	8car	NBcar = nbre de caractères
Rackage	x	x	x			Sf001_4500
Inventaire	x	x	x			Sf001_4500
Schéma	x	x	x	x		Sf001_4500
Prompt	x	x	x	x		Sw005_4500_0920009
Etiquette	x	x	x	x		Sw005_4500_0920009
Fichier config	x	x	x	x	x	Sf001_4500_0920009_aaaa mmjj.txt

II.5.2.1 Clé d'identification dans le site

Le besoin exprimé de faire porter le maximum d'informations dans les schémas d'architecture a conduit à y faire figurer un élément permettant de retrouver l'adresse d'administration des équipements. Comme indiqué au §II.5.3infra, chaque site est doté d'une plage d'adresses d'administration. Le numéro unique d'un équipement administrable dans un site est le dernier octet de son adresse d'administration. Pour un équipement non administrable, on utilisera un numéro d'ordre à partir de 300.

Ainsi, l'identifiant unique d'un équipement dans un site est composé de :

- ◆ préfixe « Sf » pour un cœur de réseau, « Sw » pour un commutateur administrable ou Sx pour un équipement non administrable,
- ◆ dernier octet de son adresse d'administration sur 3 chiffres (pour un équipement administrable

Sf ou Sw) ou N° d'ordre du commutateur à partir de 300 (pour un équipement non administrable Sx)

Exemples: **Sw005** commutateur administrable dont l'adresse d'administration se termine par .5

Sx300 commutateur non administrable (1^{er} de la liste)

Cet identifiant unique sera accompagné d'un suffixe informatif en fonction de l'usage, comme indiqué ci-dessous.

Note : un équipement acquis hors marché (ex : DLINK ou SMC) peut être administrable, mais non administré (la config par défaut n'a pas été modifiée). Dans ce cas, il pourra être considéré comme un équipement non administrable (préfixe Sx).

II.5.2.2 Nommage dans les schémas d'architecture

Le titre du schéma contient obligatoirement l'identifiant du site (7 caractères) et la plage d'adresses d'administration des équipements du site sous la forme 10.x.y.z/l (où l est la longueur du masque de sous-réseau).

Chaque équipement **administrable** est nommé comme suit :

- Identifiant tel que décrit au §II.5.2.1supra
- Modèle de l'équipement sur 4 caractères, précédé d'un '_' , selon le tableau du §II.5.2.8

Chaque équipement **non administrable** est nommé comme suit :

- Identifiant tel que décrit au §II.5.2.1supra
- Modèle de l'équipement remplacé par 'xxxx' précédé d'un '_'

Exemples: **Sw005_3600** pour un commutateur HP3600 administrable dont l'adresse d'administration se termine par .5

Sx301_hors pour un commutateur non administrable (ou un hub) ou administrable hors marché

II.5.2.3 Nommage du prompt d'administration

En cas d'ouverture simultanée de fenêtres d'administration sur les commutateurs de plusieurs sites, il est important de pouvoir distinguer sur quel site on travaille afin d'éviter les erreurs.

Le prompt contient :

- Identifiant tel que décrit au §II.5.2.1supra
- Modèle de l'équipement sur 4 caractères, précédé d'un '_' , selon le tableau du §II.5.2.8
- un '_' suivi du code site d'installation (identifiant de site conforme à la définition de la Documentation de site)

Exemple : **Sw005_3600_0920009** pour l'équipement de l'exemple précédent, situé sur le site 0920009.

II.5.2.4 Règles de nommage des bornes

Les bornes ou AP (Access Point) seront nommées selon la règle suivante :

- ✓ AP : 2 car
- ✓ Dernier octet de son adresse IP d'administration : 3 car
_ (underscore)ET : 3 car
- ✓ N° d'étage d'installation de la borne : 2 car
_ (underscore) : 1 car
- ✓ code site du référentiel GPAR : 7 car

soit 18 caractères

Exemple : la borne de l'étage 5, dont l'adresse IP se termine par 019, du site codifié 0341000 dans GPAR (on ne retient pas les "_") de la DRFIP34 aura pour nom **AP019_ET05_0341000**

Ce nom normalisé de borne sera repris comme nom d'objet dans la demande d'ouverture de flux.

Le SSID (Service Set Identifier) est le nom du réseau WIFI permettant de connecter un terminal à un point d'accès (mode infrastructure). Dans les sites DGFIP, il a été convenu de nommer le SSID : « agentsN°VLANdata ».

Exemple : dans un site où les datas du poste de travail circulent dans le vlan data N°80, le SSID sera identifié « **agents80** »

- Le vlan attribué au réseau WIFI sera le même que le vlan data attribué au réseau filaire.
- à un SSID correspond un VLAN dans le contrôleur WIFI.

II.5.2.5 Nommage des étiquettes collées sur les commutateurs

Il peut être utile de connaître la provenance d'un commutateur si celui-ci est amené à sortir du site.

Pour un commutateur administrable, l'étiquette est identique au prompt (§II.5.2.3).

Pour un commutateur non administrable, l'étiquette est construite de la même façon, mais le modèle de l'équipement est toujours 'xxxx'. Exemple : "Sx300_xxxx_0920009"

II.5.2.6 Nommage des fichiers de sauvegarde des configurations et des fichiers syslog

Les configurations des équipements sont sauvegardées dans un serveur (emplacement à définir) sous forme de fichiers nommés comme suit:

- Identifiant tel que décrit au §II.5.2.1supra
- Modèle de l'équipement sur 4 caractères, précédé d'un '_', selon le tableau du §II.5.2.8
- un '_' suivi du code site d'installation (identifiant de site conforme à la définition de la Documentation de site),
- un '_' suivi de la date de sauvegarde sous la forme 'aaaammjj' (aaaa = année, mm = mois, jj = jour),
- avec l'extension '.txt'

Si un problème de taille des noms de fichiers apparaît, il sera possible de créer des noms de fichiers sans l'information de code site et de sauvegarder ensuite ces fichiers dans un répertoire dont le nom contient le code site.

II.5.2.7 Nommage dans le référentiel parc des équipements

Le référentiel des équipements est défini dans la Documentation de site. Il est composé d'un ensemble de colonnes, dont l'une contient l'identifiant du site (conforme à la définition de la Documentation de site) et une autre contient l'identifiant de l'équipement comme suit :

- Identifiant tel que décrit au §II.5.2.1supra
- Modèle de l'équipement sur 4 caractères, précédé d'un '_', selon le tableau du §II.5.2.8

II.5.2.8 Liste des codes de modèles d'équipements

Ces codes de modèles d'équipements figurent dans les noms des commutateurs, afin de rappeler rapidement leurs principales caractéristiques (fonctionnalités, interface de configuration).

Nom complet de l'équipement	Type 4 carac t	Exemple schéma architecture « 001 ou 002 » 4è octet @IP	Exemple Hotsname « 001 ou 002 » 4è octet @IP ; code site =0250000
HP A7506	7506	Sf001_7506	Sf001_7506_0250000
HP A5500	5500	Sf002_5500	Sf002_5500_0250000
HP-5510-HI	5510	Sf003_5510	Sf003_5510_0250000
HP-5130	5130	Sw004_5130	Sw004_5130_0250000
HP A3600	3600	Sw005_3600	Sw005_3600_0250000
HP A3100	3100	Sw006_3100	Sw006_3100_0250000
Modèles administrés hors marché	hors	Sw001_hors	Sw001_hors_0250000
Non administrable ou non administré	hors	Sx001_hors	Sx301_hors_0250000

II.5.3 Règles d'administration

II.5.3.1 Adressage des commutateurs

Recommandation 14

Spécifications LAN : règles pour l'administration des commutateurs

Il est recommandé de mettre en place un VLAN d'administration sur tous les commutateurs des sites territoriaux de la DGFIP afin :

- d'isoler le flux d'administration des autres flux (voix/data),
- de permettre la gestion à distance de ces équipements par les équipes supports et les équipes SIL,
- d'envoyer les traps SNMP et données syslog vers les serveurs dédiés.

La mise en place d'un vlan d'administration pour les équipements d'interconnexion a pour objectifs :

- isoler le trafic d'administration par rapport au trafic de données et de voix et assurer, à terme, une QoS minimum pour garantir l'administration des équipements, y compris en cas de congestion du réseau,
- associer au vlan d'administration des sous-réseaux IP spécifiques,
- activer toutes les fonctions d'alertes SNMP et syslog qui vont permettre d'envoyer à un serveur SNMP et/ou un serveur syslog :
 - o les Traces de toutes les tentatives réussies ou non d'accès administrateurs (logs des noms d'administrateur et adresses IP source),
 - o les Traces de toutes les commandes tapées (liste de toutes les commandes envoyées par un

- administrateur),
 - o les Traces de toutes modifications de configuration, de système d'exploitation ou hardware.
- ☞ le VLAN d'administration doit obligatoirement comporter une adresse pour une console d'administration et une adresse pour une éventuelle sonde (sauf pour les sites équipés d'un seul commutateur).

Dans le cas de redondance d'équipements « cœur de réseau » ou cartes d'entrée sortie, le double attachement des piles de commutateurs d'accès devra être réparti sur les deux entités ([cf §II.3.2](#))

Le VLAN admin, utilisé pour l'administration des commutateurs, sera également dédié aux bornes. L'utilisation du vlan admin se fera en commençant par la fin([cf §II.2.3.3](#)).

Si les adresses disponibles dans le vlan admin (attribué au site) ne suffisent pas, un nouveau sous-réseau dans le vlan admin sera attribué par la MSNRL (soit en continuité, soit de façon distincte)([cf §II.2.3.3](#)).

Tous les équipements de ce VLAN d'administration seront joignables par une console de gestion de configuration SSH et à terme par :

- Un serveur de supervision SNMP (OpManager),
- Un serveur de surveillance temps réel Syslog,
- Un serveur d'archivage des configurations. (Ftp, Tftp).

Chaque site est doté d'un VLAN d'administration avec un sous-réseau IP de la forme :

10.	<dept>.	Vlan d'admin.	sous-réseau
-----	---------	---------------	-------------

- Le champ <dept> prend pour valeur le 'N° de département' du site (ou 'N° de département'+158, afin de doubler le nombre de plages d'adresses disponibles pour l'administration)
- Le champ 'Vlan d'admin' a la valeur 212, 213, 214, 215 ou 216 en fonction du type de site (sauf si ces adresses sont non disponibles sur le site)

Type de site	Sous-réseaux masque	Numéro vlan	Nombre de sites par département	Nombre d'équipements administrables par site
Site important : nbre users > 150	10."dept".212.0/27	212	16	28*
Grand site : 50 < nbre users > 150	10."dept".213.0/28	213	32	12*
Moyen site : 20 <nbre users > 50	10."dept".214.0/29	214 ou 215	128	4*
	10."dept".215.0/29			
Petit site : nbre users <20	10."dept".216.0/32	216	253	1
RESERVE	10.158.212-214-215-216			

(*) 2 adresses sont réservées (pour une sonde et une console de management)

Tout commutateur administrable doit être doté d'une adresse IP d'administration dans ce sous-réseau.

Processus d'affectation des Vlan d'admin

- ✓ Les équipes SIL chargées de la gestion du LAN doivent impérativement faire une demande auprès de la MSNRL (cf formulaire demande de vlan sur le site MSNRL : <http://msnrl.intranet.dgfip/msnrl/missions/reseau/formulaire-demande-vlan.htm>)
- ✓ La MSNRL traite la demande en attribuant un sous-réseau d'administration et retourne la réponse au SIL.

- ✓ La demande de changement dans l'extranet SFR est réalisée par l'équipe SIL chargée de la gestion du LAN qui informe la MSNRL de la réalisation du changement par l'opérateur.
- ✓ Les changements sont consultables dans l'application GPAR
<http://gpar.appli.dgfip/login>

II.5.3.2 Accès en administration aux commutateurs

Les règles d'accès aux équipements doivent être définies durant la phase de spécifications techniques.

Comme indiqué au §II.3.1, 2 utilisateurs sont paramétrés sur chaque commutateur, l'un avec accès en lecture seule (CID), l'autre avec accès en lecture/écriture (SIL). Par mesure de sécurité un serveur Radius a été mis en place pour la gestion individualisée des habilitations d'accès aux commutateurs. Il permet en outre d'assurer la traçabilité des actions effectuées par l'un ou l'autre des administrateurs habilités.

Recommandation 15

Spécifications LAN : accès aux équipements à distance

Par mesure de sécurité et de simplification, il est obligatoire de configurer sur chaque commutateur la procédure d'authentification via le serveur « Radius » pour la gestion individualisée d'accès aux commutateurs.

II.5.4 VLAN

II.5.4.1 Usages et nomenclature

La définition des VLAN doit être élaborée durant la phase de spécifications techniques. Certains VLAN ID pourront être normalisés par les directions du ministère selon le besoin pour faciliter l'exploitabilité des réseaux locaux.

Recommandation 16

Spécifications LAN : usage et Nomenclature des VLAN

Pour améliorer la sécurité en séparant les domaines fonctionnels ou pour accroître la performance en limitant la taille des domaines de broadcast, Il est recommandé de créer plusieurs réseaux locaux indépendants les uns des autres dans un même site.

Afin de limiter le nombre de commutateurs et la complexité du câblage, on mutualise ces LAN sur une même infrastructure physique en créant des LAN virtuels ou VLAN. Au niveau 2 (Ethernet), ces VLAN sont étanches car ils ne peuvent pas communiquer entre eux.

Chaque VLAN constitue un sous-réseau IP distinct. Les plages d'adresses affectées aux VLAN sont définies soit en /22 (1024 adresses IP, si le VLAN héberge encore une MMA) soit en /24 (256 adresses IP). La définition d'une "secondary address" est à proscrire.

La norme pour la création de nouveaux sous-réseaux est en /24 (256 adresses disponibles) maximum.

A chaque VLAN est associé un identifiant de VLAN (VID numéroté de 1 à 4094) qui reste local au site et n'est pas transmis par routage vers les réseaux longue distance (ex : RIE).

☞ Au-delà de la normalisation de la majorité des VID, certains VID pourront être définis au cas par cas pour les besoins spécifiques de chaque site (sous réserve d'une acceptation de la MSNRL). Le tableau suivant répertorie les identifiants de VLAN connus et leur actuel usage à la DGFIP.

Plusieurs types de vlan sont répertoriés sur les architectures DGFIP :

- le vlan d'interconnexion (/29) qui sert à relier le (ou les) routeur (s) avec le cœur de réseau,
- le vlan admin sert à l'administration des commutateurs (cf §II.5.3)
- le ou les vlan voix contiennent tous les postes, passerelle et serveurs de la téléphonie IP (en règle générale, l'autocom est dans un vlan différent des postes téléphoniques pour éviter d'être pollué par les broadcast),
- les vlan data correspondent aux vlan internes DGFIP. La numérotation prise en compte correspond au 3^{ème} octet du sous-réseau IP quel que soit le masque de sous-réseau (/22 ou /24).
- le vlan visio (/28) qui sert à relier au LAN les équipements de visio-conférence,
- le vlan externe (/28) qui permet de relier au LAN des équipements spécifiques (PLSU, SEP, machine à affranchir de type Néopost, Gestionnaire de file d'attente (GFA)...),
- le (ou les) vlan serveur (s) (/28) qui sert à relier au LAN les serveurs (bureautique, les futures MMA...).

☞ La création d'un vlan serveur est **obligatoire** pour chaque installation d'un nouveau serveur. Celui-ci ne devra contenir que le serveur et son système de sauvegarde.

Une liste, très restrictive, de vlan spécifiques a été élaborée. L'utilisation de ces vlan est réservée aux sites existants qui ne peuvent intégrer la norme ci-dessous.

Le tableau suivant résume ces règles et donne la liste des VLAN spécifiques :

VRF Data					
VLAN	Type	ID VLAN	Sous-réseau associé	Name	Description
Vlan VISIBY	visiby	2218	22.18.dept.0 à 254/29	visiby-« vid »	<ul style="list-style-type: none"> La 1^{ère} @IP est réservée à l'adresse de l'interface sur le cœur
Vlan d'administration	admin	212 -216	212 – 216	admin-« vid »	obligatoire
Vlan interne DGFIP	data	3 ^{ème} octet du sous-réseau IP <u>cas particuliers :</u> <ul style="list-style-type: none"> 260 ⇒ ⇒ 261 ⇒ ⇒ 270 à 299 	<ul style="list-style-type: none"> 2-211 et 217-254 sous-réseau 0 sous-réseau 1 sans sous-réseau IP 	data-« vid »	localisation
Doublons ID Vlan		600+3 ^{ème} octet du sous réseau IP	<ul style="list-style-type: none"> 600-855 	Identique à la règle initiale	<ul style="list-style-type: none"> La 1^{ère} @IP est réservée à l'adresse de l'interface sur le cœur
Vlan opérateur *	data	900 – 999 901 902	<ul style="list-style-type: none"> Interconnexion Wan diagonal serveur 	oper-« vid »	<ul style="list-style-type: none"> La 1^{ère} @IP est réservée à l'adresse de l'interface sur le cœur La dernière @IP est réservée à l'HSRP (et au routeur 1 si un seul routeur)
Vlan serveur ***	data	3000-3999 le 1 ^{er} vlan serveur VID=3000 le suivant VID=3001,...	<ul style="list-style-type: none"> Vlan serveur en /28 	serv-« vid »	<ul style="list-style-type: none"> La 1^{ère} @IP est réservée à l'adresse de l'interface sur le cœur
Vlan Externe	externe	301	<ul style="list-style-type: none"> 10.dept.x.x en /28 	ext-301	SEP-DRH3 <ul style="list-style-type: none"> La dernière @IP est réservée à l'adresse de l'interface sur le cœur
	externe	302	<ul style="list-style-type: none"> 10.dept.x.x en /28 	ext-302	PLSU <ul style="list-style-type: none"> La dernière @IP est réservée à l'adresse de l'interface sur le cœur
	externe	304	<ul style="list-style-type: none"> 10.dept.x.x en /28 	ext-304	Matériels divers non conformes <ul style="list-style-type: none"> La dernière @IP est réservée à l'adresse de l'interface sur le cœur
(gestionnaire file d'attente et distributeurs de ticket)	externe	306	<ul style="list-style-type: none"> 10.dept.x.x en /28 	ext-306	GFA <ul style="list-style-type: none"> La dernière @IP est réservée à l'adresse de l'interface sur le cœur

Projet ToIP (VRF dédiée)					
VLAN	Type	ID VLAN	Sous-réseau associé	Name	Description
Vlan opérateur	ToIP	913	13.dept.x.y (en adéquation avec le vlan 901)	operToIP-«vid»	<ul style="list-style-type: none"> La 1^{ère} @IP est réservée à l'adresse de l'interface sur le cœur La dernière @IP est réservée à l'HSRP (et au routeur 1 si un seul routeur)
Vlan ToIP	ToIP	1300 1301, 1302...	13.dept.xxx.0 à 254/24	ToIP-« vid »	<ul style="list-style-type: none"> La 1^{ère} @IP est réservée à l'adresse de l'interface sur le cœur
Vlan PRA ToIP (PCS – autocom de secours (T2 de secours)/site critique)	ToIP	1600	13.254.xxx.0 à 254/24	praToIP-« vid »	<ul style="list-style-type: none"> La 1^{ère} @IP est réservée à l'adresse de l'interface sur le cœur
Projet RPV Tunnel GRE					
VLAN	Type	ID VLAN	Sous-réseau associé	Name	Description
RPV-Transport (Sous réseau réservé au fonctionnement des tunnels ; 1 par site maximum)	externe	399	10.159.1dept.x en /30 (201 pour 971, 202 pour 972, 203 pour 973, 205 pour 974, 205 pour 975 et 214 pour 984, 216 pour 986, 217 pour 987 et 218 pour 988)	ext-399	Existe de façon identique dans chaque VRF. La 1^{ère} @IP est configurée en local et la seconde sur les MSR4000
Tunnel GRE 1 (RPV-TPE)	externe	307	<ul style="list-style-type: none"> 10.162.1dept.x en /29 ou 10.162.dept.x en /29 (201 pour 971, 202 pour 972, 203 pour 973, 205 pour 974, 205 pour 975 et 214 pour 984, 216 pour 986, 217 pour 987 et 218 pour 988)	ext-307	RPV-TPE <ul style="list-style-type: none"> La 1^{ère} @IP @IP est réservée à l'adresse de l'interface sur le cœur
Tunnel GRE 2 (alarme TELSUD + vidéosurveillance à destination de TELSUD ; contrôle d'accès) (RPV-Alarme)	externe	308	<ul style="list-style-type: none"> 10.164.1dept.x en /29 ou 10.164.dept.x en /29 (201 pour 971, 202 pour 972, 203 pour 973, 205 pour 974, 205 pour 975 et 214 pour 984, 216 pour 986, 217 pour 987 et 218 pour 988)	ext-308	RPV-ALARME La 1^{ère} @IP est réservée à l'adresse de l'interface sur le cœur
Tunnel GRE 3 Machines à affranchir (RPV-Affranchissement)	externe	309	<ul style="list-style-type: none"> 10.166.1dept.x en /28 ou 10.166.dept.x en /28 (201 pour 971, 202 pour 972, 203 pour 973, 205 pour 974, 205 pour 975 et 214 pour 984, 216 pour 986, 217 pour 987 et 218 pour 988)	ext-309	RPV-AFFRANCHISSEMENT <ul style="list-style-type: none"> La 1^{ère} @IP est réservée à l'adresse de l'interface sur le cœur

II.5.4.2 Configuration des VLAN

Recommandation 17

Spécifications LAN : règles de configuration des VLAN

Il est recommandé de configurer des VLAN statiques de niveau 1 (VLAN par port) :

- les ports associés à des terminaux sont configurés en mode 'Access' avec un unique VID (identificateur de VLAN),
- les ports associés à un couplage téléphones / terminaux sont configurés en mode "Trunk" avec 2 VID autorisés (vlan voix et vlan data),
- les ports servant à l'interconnexion des commutateurs sont configurés en mode "Trunk", avec une liste de VID autorisés (vlan voix, vlan(s) data et vlan admin).

II.5.4.3 VLAN d'interconnexion Wan – Lan

Pour tous les sites comportant un cœur de réseau réalisant un routage de niveau 3, la mise en place d'une politique de sécurité, permettant d'isoler le trafic du réseau LAN de celui du réseau WAN, impose la création d'un vlan dédié entre le routeur et le cœur de réseau.

La mise en place du vlan associé, vlan 901 (vlan opérateur), a été généralisée sur l'ensemble des sites de la DGFIP.

Le sous-réseau correspondant est défini en /29. En l'absence de redondance de l'accès WAN, seules les interfaces du routeur (loopback DGFIP) et l'interface du commutateur cœur de réseau (ou fédérateur) seront affectées à ce vlan. En partage de charge des accès WAN et de redondance des cœurs de réseau, il comportera 6 adresses : 2 pour les routeurs + la VRRP (ou HSRP) et 2 pour les cœurs de réseau + la VRRP.

Par ailleurs, le vlan d'interconnexion permettra, si nécessaire, la mise en place facile de filtrage, de boîtier d'accélération ou de chiffrement.

Recommandation 18

Spécifications LAN : VLAN d'interconnexion WAN-LAN

Il est recommandé de configurer un VLAN dédié entre le routeur WAN et le commutateur cœur de réseau, ce qui permet d'isoler le trafic du réseau LAN de celui du réseau WAN pour des raisons de sécurité.

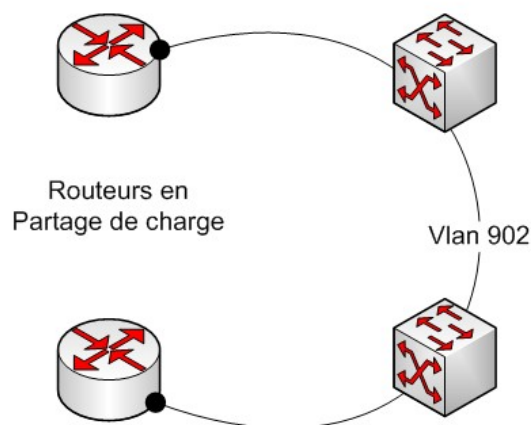
	Règles d'attribution		
VLAN d'interconnexion « n°ID 901 »	Cas 1 2 Cœurs de réseau 2 routeurs	Cas 2 1 Cœur de réseau 2 routeurs	Cas 3 1 Cœur de réseau 1 routeur
	Valeur à ajouter au 4 ^{ème} octet du sous-réseau		
Cœur de réseau 1	adresse du sous-réseau +2	adresse du sous-réseau +1	adresse du sous-réseau +1

Cœur de réseau 2	adresse du sous-réseau +3		
HSRP/VRRP Cœur de réseau	adresse du sous-réseau +1		
Routeur 1	adresse du sous-réseau +4	adresse du sous-réseau +4	adresse du sous-réseau +6
Routeur 2	adresse du sous-réseau +5	adresse du sous-réseau +5	
HSRP/VRRP routeurs	adresse du sous-réseau +6	adresse du sous-réseau +6	

II.5.4.4 Le Vlan diagonal (lien back to back)

Sur les sites disposant de 2 routeurs configurés en 'partage de charge' et non 'Actif / Backup', les routeurs ont besoin d'une interface de niveau 2 en commun. Deux cas de figures peuvent se présenter.

- Les routeurs sont co-localisés : un lien direct sera réalisé entre les 2 routeurs (Fast Ethernet 2)
- Les routeurs sont distants : un vlan 902 sera créé sur le LAN pour permettre la communication des 2 routeurs. Seuls ces routeurs auront une adresse IP dans le vlan 902



II.5.4.5 Coexistence de plusieurs entités/applications dans un même site

Le regroupement de plusieurs entités sur un même site sera géré au niveau du cœur de réseau par la création de plusieurs interfaces IP. Il est recommandé de n'utiliser qu'une interface sur le routeur pour faire la liaison (vlan 901, §II.5.4.3) avec un commutateur cœur de réseau. Tous les VLAN sont concentrés sur le cœur de réseau, qui assure le rôle de passerelle (Gateway).

Recommandation 19

Spécifications LAN : coexistence de plusieurs entités/applications sur un même site

Il est recommandé de n'utiliser plus qu'une interface sur le routeur pour faire la liaison (vlan 901, §II.5.4.3) avec un commutateur cœur de réseau.

L'activation de la deuxième interface LAN du routeur interne ou WAN est à proscrire pour séparer les deux entités ou applications.

II.5.4.6 Cas particulier de la ToIP

Le déploiement de la ToIP sur les sites de la DGFIP est une évolution de l'architecture de la téléphonie. Ce paragraphe définit les recommandations à appliquer dans le cadre des projets de transformations de la téléphonie traditionnelle vers la solution de téléphonie sur IP.

Recommandation 20

Spécifications LAN : cas de raccordement de la ToIP

Il est recommandé d'associer sur un même port du commutateur LAN, un poste téléphonique IP et un poste informatique.

L'ensemble des recommandations ci-dessous doivent être appliquées a minima pour garantir la sécurité des équipements.

En définissant ce type d'architecture, le poste téléphonique est configuré sur un VLAN dédié commun à tous les équipements de téléphonie sur IP (y compris une éventuelle Media Gateway permettant d'interconnecter le site avec les réseaux téléphoniques publics).

Chacun des ports utilisateurs du commutateur d'accès est donc configuré en mode 'Trunk' dès qu'un équipement téléphonique y est raccordé.

On retient les choix d'architecture suivants :

- le VLAN ToIP est routé par le cœur de réseau avec une configuration spécifique à prévoir,
- La Qos (Qualité de services) doit impérativement être activée sur les routeurs CE et sur les routeurs PE.

Ces choix seront précisés lors de l'étude préalable au projet de déploiement de la ToIP.

II.5.5 Classification et priorisation des flux

La priorisation des flux se fait selon les protocoles 802.1Q et 802.1p qui définissent huit files de priorité (priority queuing).

Recommandation 21

Spécifications LAN : Classification et priorisation des flux

La perspective DGFIP à l'étude est la suivante :

- le VLAN d'administration est 'marqué' en priorité haute (7), car en cas d'engorgement du trafic, les équipements réseau doivent être visibles de l'extérieur tant que la saturation complète du réseau LAN n'est pas avérée
- le VLAN voix (ToIP) est 'marqué' en priorité juste inférieure (6)
- les autres VLAN (data) ont la priorité par défaut (0 = Best Effort).

Aucune priorisation de flux n'est configurée actuellement sur les architectures LAN de la DGFIP.

II.5.6 Activation des fonctionnalités de niveau 3

Le niveau 2 du modèle OSI ne permet pas de passer la frontière d'un VLAN. C'est pourquoi les fonctionnalités de niveau 3 seront activées dans le cœur de réseau. Le niveau 3 permettra d'établir les communications entre équipements terminaux et/ou serveurs appartenant à des VLAN différents sur un même site.

Recommandation 22

Spécifications LAN : routage

Il est impératif que la fonctionnalité de routage soit réalisée par le cœur de réseau du site de la DGFIP doté des fonctionnalités de niveau 3.

La configuration de routes statiques est nécessaire sur les routeurs WAN (ex RIE).

II.5.7 Supervision des équipements

La supervision des équipements permet d'anticiper et de détecter tous les types d'événements qui vont impacter un équipement LAN installé sur un site (traps SNMP). Elle consiste à configurer sur les commutateurs les adresses IP des différents serveurs de supervision.

La supervision offre une vue temps réel sur les équipements, leur configuration et leur fonctionnement. Elle inclut la gestion d'alarmes déclenchées sur des événements tels que l'impossibilité de joindre un équipement ou la détection d'un dépassement de seuil. Elle nécessite le plus souvent que des agents soient affectées en permanence à la surveillance de ces alarmes.

L'administration d'un réseau est la partie opérationnelle d'un réseau.

L'objectif de la supervision est d'assister les équipes du support réseau :

- en fournissant des alertes proactives pour anticiper les incidents ;
- en aidant à la résolution des incidents ;
- en indiquant la charge des réseaux.

L'administrateur réseau en charge de la supervision pourra ainsi agir sur les trois domaines fonctionnels suivants :

1 - La gestion des pannes grâce à :

- la détection des pannes,
- la localisation des pannes,
- la résolution des pannes,

afin de revenir au plus vite à une situation normale.

2 - La gestion des configurations qui permet d'identifier et de paramétrer les différents objets.

Les procédures requises pour gérer une configuration sont :

- la collecte d'informations ;
- le contrôle de l'état du système,
- la sauvegarde de l'état dans un historique.

3 - L'audit des performances

Il permet d'évaluer les performances et l'efficacité des systèmes et des réseaux grâce aux quatre paramètres suivants :

- le temps de réponse ;
- le débit,
- le taux d'erreur par bit ("Bit Error Rate"),
- la disponibilité.

La supervision des équipements porte sur 3 périmètres :

- Les routeurs WAN (ex RIE)
- Les cœurs de réseau LAN
- Les interconnexions entre le cœur de réseau et les commutateurs d'extrémités.

La supervision des routeurs WAN (exemple RIE) est réalisée à travers :

- l'extranet RIE ;

URL : https://noc-rie.infra.dgfip/access_list.php

Le portail extranet du Réseau Interministériel de l'État est un service ouvert aux chaînes de support ministérielles, qui leur permet de vérifier l'état de fonctionnement des sites raccordés au RIE et sous leur responsabilité.

L'infrastructure et les services du RIE sont exploités par le NOC RIE (centre d'exploitation et de supervision du SCN RIE) qui fonctionne 24h/24 et 7j/7.

Un accès à la supervision est mis à disposition de l'ensemble des équipes réseau.

- OpManager

Au sein de la DGFIP, la supervision des équipements du LAN est faite par les équipes SIL grâce à l'application OpManager. Pour réaliser cette mission, un serveur a été mis en place dans chaque structure d'équipe SIL.

ManageEngine OpManager est un logiciel complet de surveillance de réseau qui offre une surveillance combinée d'applications, du réseau à grande échelle et des serveurs avec des fonctionnalités intégrées de service d'assistance, d'administration et d'analyse du trafic sur le réseau. OpManager automatise plusieurs tâches de surveillance du réseau et élimine la complexité associée à l'administration réseau.

Il simplifie la gestion d'un réseau en alertant les administrateurs réseaux des dégradations de service et de performance.

OpManager apporte aux administrateurs :

- une meilleure visibilité des infrastructures,
- une présentation du réseau : classement automatique des routeurs, serveurs, commutateurs...,
- une visualisation organisationnelle : classement par systèmes, applications afin de mieux les gérer (classement géographique, etc.),
- une vue globale du réseau à partir d'un seul point centralisé
 - Infrastructure Wan (interconnexions, routeurs)
 - Infrastructure Lan (Commutateurs, Imprimantes et ordinateurs portables)
 - Serveurs (http, Mail, FTP, LDAP, Dns...)
 - Applications (Postfix, Oracle, MySQL...)

II.5.8 Suivi des changements et de la qualité de service

Sachant d'une part que la plupart des incidents résultent d'une modification mal maîtrisée dans un branchement ou une configuration et d'autre part qu'il n'est pas toujours possible pour les équipes réseau qui travaillent à distance de maîtriser toutes les modifications intentionnelles ou accidentelles

réalisées sur les sites, un outil d'historisation des changements est une aide supplémentaire pour diagnostiquer les incidents.

Afin d'éviter que cet outil ne représente une charge supplémentaire pour les équipes réseau, il doit être alimenté automatiquement, directement à partir des changements qu'il détecte sur les équipements. Il peut interagir avec la supervision et/ou avec la gestion de parc afin d'offrir un maximum d'informations.

L'outil de suivi des changements peut également assister les équipes réseau pour la découverte du réseau et la réalisation des schémas d'architecture. Il peut aussi permettre de suivre la qualité de service en historisant les heures de début et de fin d'incidents.

II.5.9 Gestion de la sécurité

II.5.9.1 Activation des ports LAN

Par défaut, tout port inutilisé sur un commutateur doit être mis dans l'état 'Admin DOWN' et n'être repositionné en 'UP' que lors d'une opération de mise en service d'une prise d'accès, à la demande de la CID, avec un utilisateur clairement identifié. La responsabilité du changement d'état est du ressort du SIL.

II.5.9.2 Filtrage des flux

En dehors des centres de production informatique, la DGFIP n'installe pas de pare-feu (Firewall) et aucun filtrage de flux n'est mis en œuvre dans les routeurs WAN (ex RIE).

II.5.9.3 Gestion des habilitations (802.1x)

La gestion des habilitations 802.1x pour l'accès aux LAN n'est pas mise en œuvre à ce jour. Un projet est lancé depuis 2011 à ce sujet.

II.5.10 DHCP (Dynamic Host Configuration Protocol)

Plusieurs projets ont participé à la mise en place du DHCP

1. la centralisation des bases des MMA (machines multi-applicatives) SPF en 2016,
2. le remplacement des MMA DIR par des serveurs d'infrastructure basés sur un socle Linux en 2017,
3. la centralisation des bases des MMA SIE/SIP en 2018...

Le service DHCP n'étant plus fourni par les MMA, le bureau SI2B a décidé de mettre en œuvre un serveur DHCP dit « National ». La cible à atteindre représente potentiellement plus de 150.000 matériels à adresser.

Le DHCP (Dynamic Host Configuration Protocol) est un protocole réseau. Il a pour objectif de délivrer tout ou partie d'une configuration IP à tout élément le demandant (station de travail, tablette multimédia, téléphone...).

Actuellement, le serveur DHCP National fournit automatiquement aux utilisateurs de la DGFIP une adresse IP et tous les éléments nécessaires au bon fonctionnement des postes de travail à savoir :

- le masque de sous-réseau
- la passerelle
- le DNS
- le WINS
- ...

Ce service a comme objectifs :

- L'attribution de configurations réseaux dont les adresses IP seront principalement distribuées de façon dynamique
- L'optimisation du plan d'adressage de la DGFIP selon les préconisations de la Charte LAN.

La solution de serveur DHCP National devant être sécurisée, un certain nombre d'éléments spécifiques ont été mis en œuvre afin d'éviter une rupture de service.

- 2 serveurs sont utilisés. Ils fonctionnent sur un mode actif / passif. En cas de défaillance de l'un des serveurs, le second prend le relais.
- Une partie des coeurs de réseau ne peuvent désigner qu'un seul serveur DHCP afin de réaliser du DHCP Relay. La nécessaire redondance entre le serveur Maître et le serveur Backup implique donc d'utiliser un outil permettant de gérer la bascule des serveurs en cas de dysfonctionnement tout en évitant de fastidieuses reconfigurations des coeurs de réseau.

Keepalived, implémentation du protocole VRRP, permet de créer une adresse virtuelle visible de l'extérieur tout en basculant sur l'une ou l'autre des adresses physiques de façon quasi transparente en cas de dysfonctionnement.

Les coeurs de réseau utilisent l'adresse virtuelle et keepalived assure la disponibilité du service DHCP en basculant les adresses entre le Maître et le Backup selon des règles bien établies.

- DRBD permet de réaliser une réplication en temps quasi réel de deux partitions. Il peut fonctionner en mode actif / actif.
- Les serveurs DHCP récupèrent leur configuration auprès de GPAR (Gestion Plan d'adressage Réseau) et l'intègre dans leur environnement local. Ainsi, en cas de rupture de service de GPAR, le DHCP n'est pas impacté dans son fonctionnement ; cependant les modifications d'adressage ne seront prises en compte qu'au retour au mode nominal.
- Les équipes SIL réaliseront la mise à jour de la configuration réseau du DHCP sur GPAR (adresses fixes uniquement : imprimantes, badgeuses et PC en Full internet). Au préalable, ils devront ajouter le ou les nouveaux sous-réseaux DHCP.

III. Maîtrise des architectures réseaux LAN de la DGFIP

On distingue deux contextes d'application de maîtrise d'un réseau LAN :

- Les changements d'architecture d'envergure gérés en **mode projet**, car ils nécessitent la refonte complète du réseau avec le remplacement de tout ou partie du réseau (cœur de réseau, commutateur d'accès...)
- Les changements correctifs gérés par les équipes SIL suite à des incidents.

III.1 Les changements en mode projet

Ces projets peuvent selon le cas avoir une envergure locale/régionale (un ou plusieurs sites à restructurer dans une même structure régionale) ou nationale (un changement sur une structure centrale ou un déploiement d'envergure nationale sur une catégorie de sites).

Il est toutefois possible de définir les différentes tâches liées à la Gestion des Changements, les rôles correspondants et les compétences nécessaires pour assurer ces rôles.

La gestion des changements fait l'objet d'un ensemble de processus incluant :

- La constitution d'un dossier d'étude des changements avec, suivant le cas :
 - o Études d'opportunité, de faisabilité et de risque
 - o Études de coût (et éventuellement étude de ROI (Retour sur investissement))
 - o Déroulement des opérations, acteurs, planning
 - o Maquettage
- le passage en comités de validation
- la communication vers les acteurs, les exploitants et les utilisateurs
- la réalisation des changements / tests et recette
- la mise à jour des documentations et historisation

III.1.1 Les acteurs

Les rôles identifiés à ce jour dans les processus de gestion des LAN sont :

- le bureau SI2B : définition des architectures, définition et mise en œuvre des marchés d'acquisition, gestion des projets d'envergure nationale.
- Mission de support national (MSNRL) : support LAN et WAN de Niveau 3, définition des configurations des équipements, formation des équipes réseau opérationnelles.
- Équipes SIL : définition des architectures réseau de sites, mise en œuvre, maintien en conditions opérationnelles, accompagnement des équipes micro, audit, documentation.
- Équipes CID : mise en service et maintien en conditions opérationnelles des postes de travail et des imprimantes, collaborations ponctuelles avec les équipes réseaux et serveurs.

III.1.2 La phase d'étude et de préparation

Tâches	Rôles	Compétences
Constitution d'un dossier d'étude de changements avec, suivant le cas : <ul style="list-style-type: none"> Études d'opportunité, de faisabilité et de risque Études de coût (et éventuellement étude de ROI) Déroulement des opérations, acteurs, planning Maquettage 	Projets locaux : équipe réseaux régionale avec l'appui de la MSNRL et de la Centrale SI2. Projets nationaux : équipe d'architectes du bureau avec l'appui de la MSNRL	Architecte réseaux LAN+WAN, Architecte sécurité
Passage en comités de validation	Les mêmes + leur responsable hiérarchique + une expertise sécurité + une instance budgétaire	Architectes, Compétences budgétaires

III.1.3 La phase de mise en œuvre et de support

Tâches	Rôles	Compétences
Gestion de projet	Projet local : équipe réseaux locale, Projet national : le bureau SI2	
Communication vers les acteurs, les exploitants et les utilisateurs	Les mêmes	
Réalisation des changements / tests et recette	Équipe(s) réseaux locale(s)	

III.1.4 La phase de reporting et de documentation

Tâches	Rôles	Compétences
Mise à jour des documentations et historisation	Équipe(s) réseaux locale(s)	

III.1.5 Les règles d'installation des équipements actifs

III.1.5.1.1 Préconisations et règles

Les spécifications techniques, définies lors de la phase étude et conception, doivent intégrer les règles d'installation des équipements sur site.

Ces règles doivent préciser :

- Les prérequis (baie d'accueil, alimentation, câbles, règles de brassage, ventilation...) ;
- Les règles de nommage et d'étiquetage des équipements LAN ;
- La procédure de configuration des équipements ;
- La procédure d'installation et migration LAN
- Les procédures de recette d'installation incluant la phase transfert en exploitation.

III.1.5.1.2 Locaux et baies d'accueil des équipements

Les équipes en charge du déploiement doivent intégrer l'ensemble des prérequis avant tout

déploiement d'équipement.

Recommandation 23

Déploiement du LAN : Local et baie d'accueil

Il est recommandé d'installer les équipements LAN dans des locaux techniques en fonction de la taille et de la configuration du site.

Il est recommandé d'installer les équipements LAN dans les baies dédiées, ou coffret mural avec un dispositif de ventilation intégrée.

III.1.6 Les étapes de déploiement

Les étapes d'un projet de déploiement du LAN doivent respecter un processus qui comprend les étapes suivantes :

- L'étude et la conception qui est réalisée en amont ;
- La maquette (optionnelle);
- Le pilote (optionnelle);
- Le déploiement généralisé.

III.1.6.1 Spécifications techniques

La phase étude et conception est l'étape préparatoire avant le déploiement des équipements et des services associés. Cela comprend la définition de l'architecture cible en fonction de l'expression de besoins du site ou de la direction du ministère. Elle intègre en priorité un état des lieux avec une analyse de l'existant en termes d'infrastructure LAN physique, locaux techniques, baies, équipements d'énergie, etc., pour accueillir les équipements LAN.

L'état des lieux sur site a pour objectif de réaliser une collecte de données et d'informations nécessaires pour une installation optimale des équipements et la réalisation de la migration de ces derniers pour le site concerné. Cette collecte de données peut être réalisée dans le cadre d'une prestation d'audit sur site, en fonction de la complexité de ce dernier (taille, nombre d'agents, nombre de bâtiments, de niveau/d'étage, technologie LAN à déployer...)

Les directions doivent mettre à disposition du prestataire l'ensemble des informations utiles à la bonne réalisation des installations par un tiers.

Cette collecte doit être réalisée auprès des différents acteurs en charge du projet du côté des directions du ministère.

La collecte permet de :

- Définir la typologie du site ;
- Évaluer les données et équipements d'accueil manquants ;

Les opérations à réaliser pour mettre aux normes le site avant le déploiement du LAN actif.

Recommandation 24

Etat des lieux : l'audit LAN

Document permettant de guider les équipes SIL sur tous les éléments techniques (infrastructure de câblage) à vérifier afin de se conformer aux préconisations de la Charte LAN.

➤ **Recommandations aux équipes SIL**

Il leur est recommandé de se déplacer sur site afin de :

- vérifier la capacité du site à accueillir le projet : conformité des locaux techniques (nombre, alimentation électrique, rocade, accès...), capacités des baies dédiées aux équipements réseaux ou coffret mural, câblage (rocades horizontales et verticales...), inventaire des commutateurs, équipements télécoms... le service à déployer : data ou data et téléphonie sur IP (nombre de postes, type d'équipement, capacité...)
- définir avec précision les éléments nécessaires à la mise en place du projet ;
- valider la faisabilité des installations souhaitées par la direction.

Un guide est mis à disposition des équipes SIL sous Polaris :

[Documentation par structure](#) > [Directions à Compétences Nationale ou Spécialisée](#) > [DISI](#) > [ESI - Assistance de proximité](#) > [\(DD5\) Audit et vérification des locaux informatiques des sites territoriaux](#) > [Accès GP](#)



Recommandations aux directions

- intégrer dès le début du projet, les équipes SIL,

- mettre à disposition des équipes SIL tous les documents en leur possession (recette de câblage, plan détaillé du bâtiment...).

Evolution du document papier Audit LAN

ARES (Gestion des Audits Réseau) est le nouvel outil mis à disposition des équipes SIL pour faciliter leur travail de collecte détaillée et de contrôle. Il a vocation à remplacer les documents bureautiques saisis par les équipes SIL lors des audits réseau réalisés sur les sites de la DGFIP.

L'application permet la saisie et la consultation des audits réalisés par les équipes SIL (Support des infrastructures locales) de la DGFIP.

Au niveau local, l'application permet l'enregistrement des audits réseaux des infrastructures et leur matérialisation (production du rapport) pour restitution aux directions concernées, ce qui leur permet d'engager les travaux qu'elles jugent nécessaires.

Ces échanges permettent également aux DISI et ESI de sensibiliser les directions aux enjeux réseau du Système d'Information (SI) de la Direction Générale et des risques lorsque les réseaux ne sont plus efficaces.

Au niveau national, les bureaux SI2B et SPIB disposent de la visualisation de l'ensemble des audits et peuvent utiliser les outils statistiques. Cela permet d'envisager, à court et moyen terme, les investissements nécessaires pour :

- mettre à niveau les réseaux des sites jugés sensibles ou à forts enjeux,
- accompagner la mise en œuvre de nouveaux services techniques validés par le SSI.

Au niveau assistance, la connaissance des audits par les différents acteurs peut permettre de localiser plus précisément les sources de dysfonctionnement des réseaux et de faciliter les opérations de dépannage.

III.1.6.2 Prototype / pilote : qualification du projet

Lorsque le projet présente une transformation majeure (nouvelle plate-forme, nouvelle architecture, intégration de nouveaux services...), il est recommandé de procéder au nouveau déploiement, en deux phases : la phase prototypage et la phase de pilotage. Elles permettent de réaliser des tests en mode hors production (prototype) ou en mode production (pilote) afin de mettre en exergue les avantages et inconvénients des architectures et solutions à déployer. Elles permettent aussi de corriger les problèmes techniques et les procédures à appliquer.

Le succès de ces deux phases conditionnera directement la réalisation de la suite du projet, à savoir le déploiement généralisé.

III.1.6.2.1 La phase Prototypage

Elle valide une (ou plusieurs solutions) solution (s) technique(s) hors production ainsi que la (ou les) procédure(s) de déploiement. Cette phase suivra le cycle de développement, de test hors production et de modifications si besoin de l'ensemble de la chaîne de liaison des services souscrits.

III.1.6.2.2 La phase Pilotage

Elle valide une solution technique en situation quasi réel sur un périmètre réduit. Elle permet d'affiner la procédure de déploiement. La solution technique et la procédure finale seront mis à disposition des prestataires concernés. La durée du pilote sera définie conjointement entre les parties prenantes du projet, à savoir le ministère et le (ou les) prestataire(s).

A l'issue de la phase de pilotage, le pilote pourra :

- mettre à disposition l'architecture LAN cible sur le site concerné avec la configuration cible décrite dans le dossier de spécifications détaillées ;
- valider le bon fonctionnement de l'architecture et des services déployés conformément aux besoins exprimés par le ministère.

Recommandation 25

Phase Prototype / Pilote :

Il est recommandé de définir le périmètre et la durée de la phase prototype et pilote :

- Réaliser le prototype sur la base des architectures définies et validées ;
- Choisir les sites représentatifs des modèles d'architectures définies lors de la phase de spécifications (1 site par type d'architecture/typologie pour qualifier le bon fonctionnement) ;
- Mettre en place un questionnaire et recueillir l'avis des utilisateurs durant la phase pilote avant de passer à l'étape de déploiement généralisé ;
- Ajuster les processus, procédures de déploiement et d'exploitation, puis les configurations associées à chaque architecture durant cette étape.

III.1.6.3 Déploiement généralisé

Le déploiement généralisé se déroulera en 2 phases :

- la mise en place de la solution selon les procédures validées lors de la phase de qualification,
- la phase de recette.

Recommandation 26**Phase d'installation sur site**

L'équipe SIL se chargera de configurer les équipements au préalable et de les déployer sur site.

Il existe plusieurs méthodes de déploiement de commutateurs en local ou sur un site distant.

- Ajouter une configuration minimale sur le commutateur (adresse IP LAN pour la joignabilité par l'équipe d'administration et supervision, pour permettre la prise en main, le téléchargement de la configuration cible à distance et l'activation de la supervision de l'équipement) ;
- Injecter la configuration cible pour le site concerné avant l'installation physique sur site et dans la baie dédiée

Dans les deux cas, il faut valider la prise en main de l'équipement à distance et la supervision de ce dernier dès la fin de l'installation.

Recommandation 27**Phase recette**

Il est recommandé de faire valider le bon fonctionnement des équipements avant le départ de l'équipe SIL du site (vérification visuelle de l'activation des ports, test de joignabilité des serveurs du site ou du site principal et quelques postes de travail critiques (cf. procédure de recette).

Enfin, il est recommandé :

- de faire une lecture du fichier de log de l'équipement pour savoir si ce dernier ne rencontre pas de dysfonctionnement.
- de se connecter à distance sur les nouveaux équipements (test de la connexion SSH et test de l'authentification Radius).

III.1.6.4 Les livrables

Les livrables constituent le dossier de spécifications et d'intégration sur site.

La liste ci-dessous est un exemple non exhaustif de livrables à fournir à chaque étape du projet LAN :

- Organisation du projet :
 - o les documents de suivi du projet (modèle de compte rendus de réunion, planning).
- Étude et Conception du service :
 - o un dossier d'architecture globale et détaillée ;
 - o un dossier de configurations détaillées par typologie de plate-forme ;
 - o la liste de prérequis pour le bon déploiement du service.
- Déploiement de la solution
 - o un planning détaillé pour chaque phase du déploiement (prototype, pilote et généralisé) ;
 - o la liste de prérequis ;
 - o le dossier d'audit de site ;

- o le dossier de site intégrant l'ensemble des composants/équipements installés par site ;
- o le PV de recette d'installation du nouvel équipement ou nouveau service validant le service unitairement sur chaque site ;
- o le cahier de test validant les équipements, l'architecture et les fonctionnalités testés ;
- o le dossier de transfert en phase exploitation du service.

III.2 Les changements en mode correctif

III.2.1 Les fondamentaux

- avoir la connaissance de son réseau ==> référentiels-documentation de site, cartographie et audit LAN
- respecter les normes de la Charte LAN
- une supervision efficace ==> OpManager
- Ces points, une fois respectés, permettront de résoudre rapidement les incidents et de répondre facilement à une demande d'évolution.

III.2.2 Anticiper les pannes

- Prendre en compte le facteur fiabilité dès la conception du réseau
 - le câblage est un investissement à long terme... il doit être sûr
 - maîtriser le choix des équipements en anticipant une évolution possible
 - la topologie a une importance majeure
- Ne pas essayer de dépasser les règles, éviter les solutions hors-normes
 - câbles dépassant la longueur limite
 - nombre de niveau de commutation
 - commutateurs non administrables
 - doubleurs RJ45
 - ...
- Permettre l'évolutivité
 - éviter les solutions propriétaires
- Éviter les solutions 'temporaires'
 - elles deviennent une source d'ennuis permanente
 - elles sont généralement peu évolutives
- Avoir une attitude pro-active
 - détecter les anomalies avant qu'elles ne gênent les utilisateurs (Supervision)
 - identifier les points d'engorgement et le niveau de trafic

III.2.3 Outil de cartographie

Un outil de cartographie est indispensable pour répondre à trois usages :

- l'aide à la résolution d'incident,
- l'aide à la préparation d'une évolution de site (gestion des changements),
- la connaissance et la maîtrise du réseau de la DGFIP.

L'enjeu de cet outil est d'augmenter la qualité de service des acteurs en apportant :

- la réduction du délai de résolution d'un incident,
- une meilleure conformité des travaux demandés avec l'existant dans les sites,
- une meilleure productivité des acteurs.

Les objectifs :

- favoriser la connaissance des architectures réseau de l'ensemble des sites de la DGFIP,
- faciliter la réalisation de la documentation de site telle qu'elle est définie dans la Charte LAN,
- assurer l'unicité des données en réutilisant les données collectées par d'autres outils,
- permettre de préparer les interventions des équipes SIL lors des audits de sites,
- proposer diverses restitutions pour les équipes de directions (SSI, DISI, ESI et directions locales) et ainsi faciliter les prises de décision par les directions.
- L'Outil de Cartographie (ODC) est une application web qui permet la cartographie réseau de l'ensemble des sites de la DGFIP.
- Afin d'éviter une redondance des informations, cette application s'appuie sur les données stockées dans les applications GPAR (Gestion du Plan d'Adressage Réseau) et les découvertes réseau de la documentation de site.
- Plusieurs groupes d'utilisateurs ont été créés dans l'application, la visualisation offerte est donc différente selon les équipes concernées.

Pour les équipes SIL :

- L'authentification se fait via l'identifiant fonctionnel et le mot de passe de messagerie associé,
- Les droits accordés dépendent de la compétence géographique.

Pour les autres utilisateurs :

- L'authentification se fait via l'identifiant personnel et le mot de passe de messagerie associé,
- Les droits accordés dépendent de la compétence fonctionnelle.

IV. Dépannage des réseaux LAN de la DGFIP

Pour résoudre les dysfonctionnements, il est nécessaire de rassembler les informations préliminaires, et parfois de reproduire l'anomalie signalée.

IV.1 Les informations préliminaires à collecter :

- Descriptif de l'anomalie par l'utilisateur à l'origine de la demande de dépannage,
- Chaîne de remontée d'incident complexe. Pour gagner un maximum de temps:
 - Quelles entités ont traité l'anomalie jusqu'à présent ?
 - Qu'ont-elles constaté ? Quelles actions ont-elles réalisées ? (éventuellement les recontacter)
- Recherche d'antécédents...
 - Pour le même utilisateur ? (profil utilisateur et personne physique)
 - Pour le même poste de travail ou serveur ?
 - Pour le même LAN ?
 - Pour la même application ?
 - Présentant des symptômes similaires ?
- Y a-t-il eu des modifications récentes sur le réseau ?
 - Changement d'équipements réseau ou mise en place de nouveaux équipements
 - Opération de maintenance
 - Déploiement d'une nouvelle application
 - Arrivée de nouveaux utilisateurs
- Quand l'anomalie est-elle apparue pour la première fois? Pour la dernière fois? (à rapprocher du point précédent)

IV.2 Méthode pour mise en condition et reproduction de l'anomalie :

- L'anomalie est-elle permanente ou intermittente ?
 - Se produit-elle à des moments précis de la journée ou de la semaine ? Avec quelle fréquence ?
 - Une séquence d'actions particulière de l'utilisateur est-elle nécessaire pour déclencher l'anomalie ?
- La charge réseau est souvent un facteur clef dans le déclenchement des anomalies
 - Tenter de reproduire l'anomalie pendant les pointes de trafic
 - Générer du trafic artificiel pour tenter de la déclencher (à faire dans les périodes de faible utilisation du réseau)
- La mise en place d'outils de surveillance long terme peut être nécessaire pour repérer les conditions de déclenchement de l'anomalie

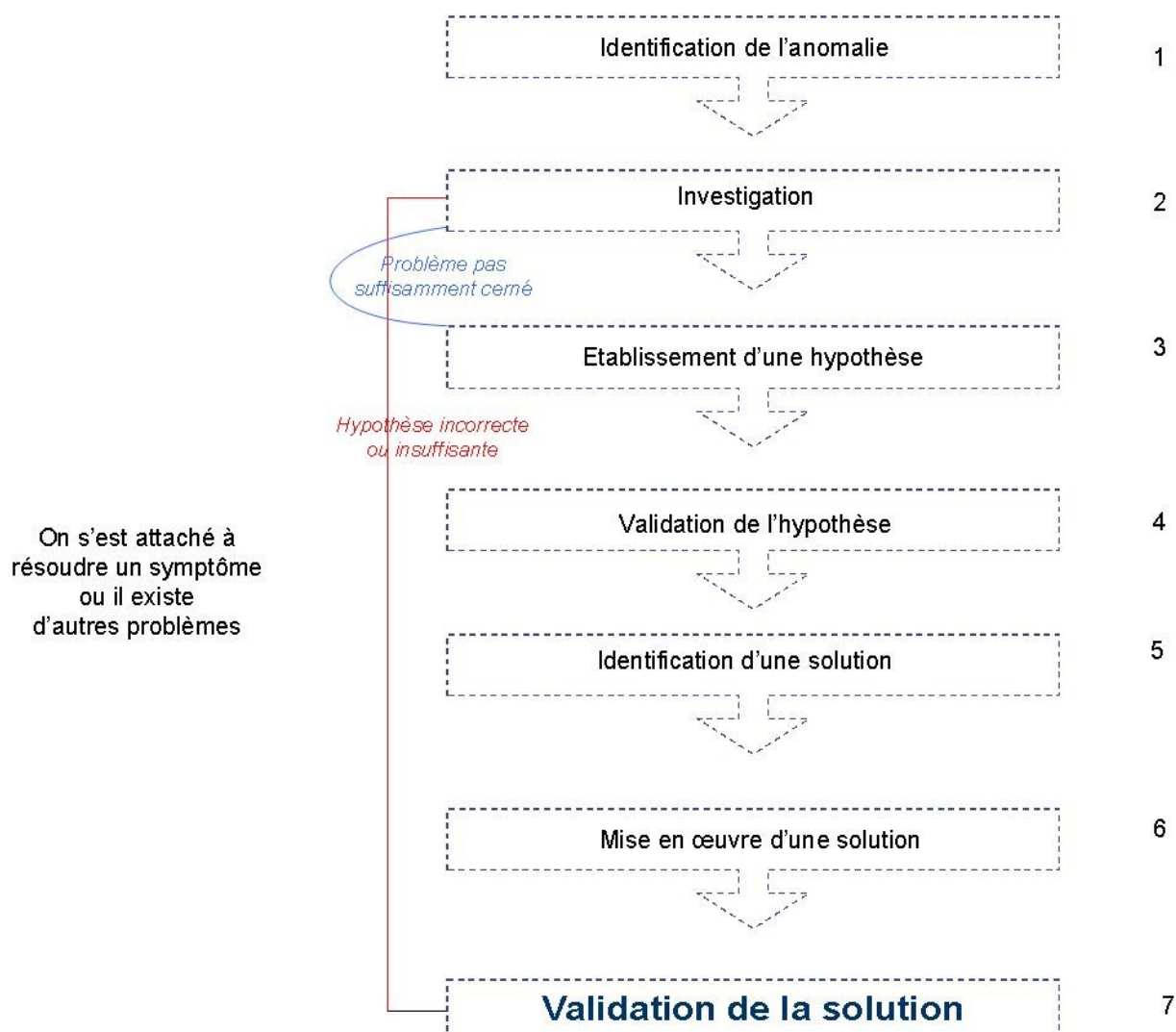
IV.3 Éléments à analyser :

- Conformité du câblage,
- Indicateurs de santé Ethernet,
- Configuration des équipements,
- Échanges applicatifs,
- Volume de trafic par application.

IV.4 La méthode d'analyse :

- S'assurer de l'absence d'une panne électrique locale (disjoncteur non réarmé)
- Procéder par ordre pour isoler le problème, chaque test devant être le résultat d'une démarche logique
- Une fois le problème suffisamment isolé
 - Remplacer le système défectueux dans son ensemble (par exemple, un commutateur et toutes ses cartes d'extension)
 - Terminer de circonscrire l'anomalie en laboratoire (S'agit-il du boîtier ? D'une des cartes d'extension ?)
- Le hasard n'entre en jeu que si des investigations plus poussées prendraient trop de temps; il est le dernier recours

Plan d'un audit de maintenance corrective (dépannage)



IV.5 Les fiches de résolution d'incidents

La gestion des incidents décrit :

- les différentes catégories d'incidents en fonction de leur impact sur les agents et sur le métier,
- l'organisation des équipes d'exploitants,
- les processus d'alertes et d'initialisation,
- les processus et outils de résolution,
- les processus et outils de traçabilité et d'historisation,
- les processus d'éradication,
- la communication vers les utilisateurs.

CF annexe 3

Recommandation 29***Maintenance corrective :***

Il est recommandé pour les sites de DGFIP de tenir à jour une liste des équipements, des applications et des contrats de services associés.

Il est également recommandé de disposer d'une base d'inventaire centralisée et d'équipements de « Spare » à l'ESI pour les matériels réseau.

La procédure de maintenance doit comporter a minima :

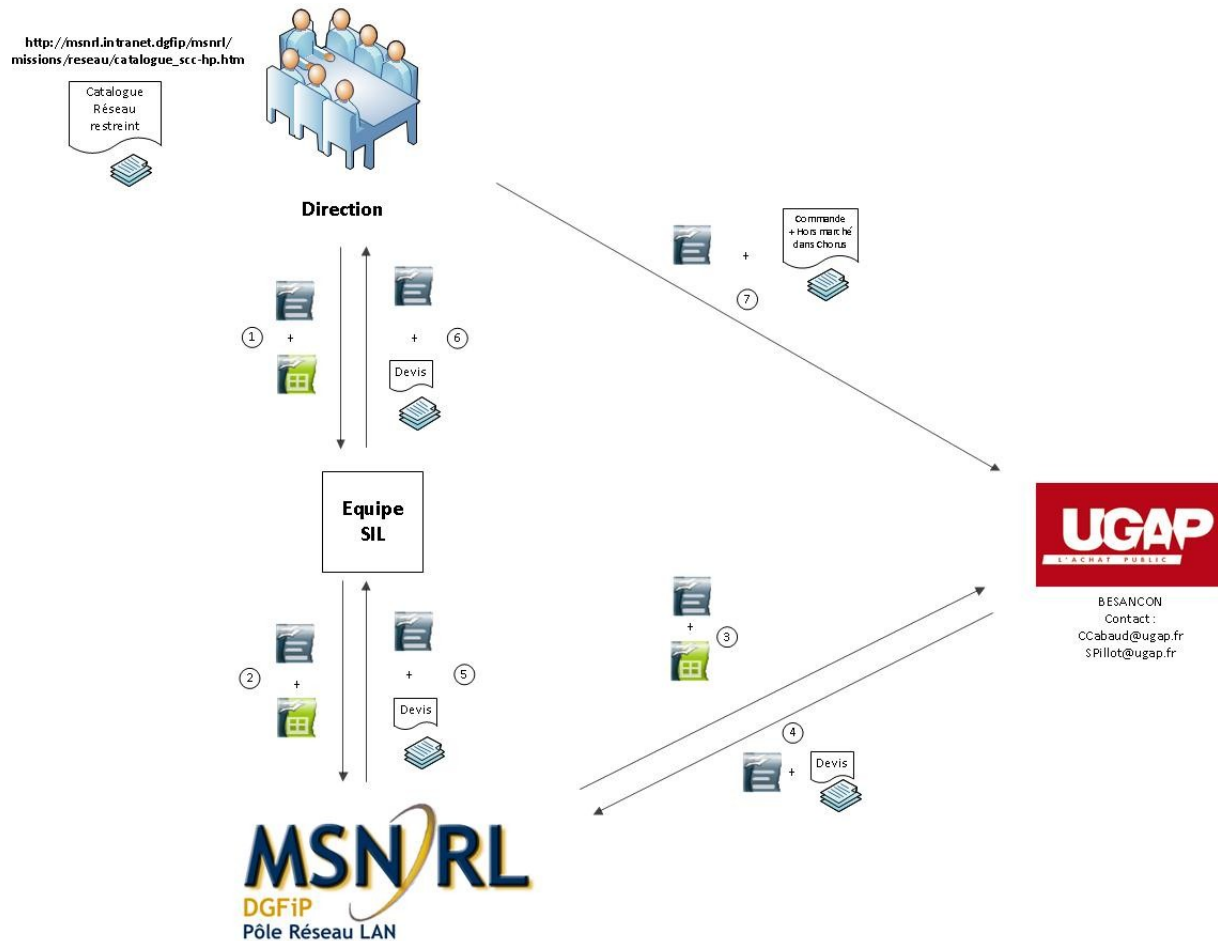
- Le processus de gestion de la maintenance corrective (synoptique de traitement des incidents, escalades et gestion de crises...
- Les modalités de remplacement d'un équipement et la gestion du Spare ;
- La définition des niveaux de sévérité .

Suivant l'importance des changements et leur impact sur les utilisateurs, les étapes peuvent être fortement allégées.

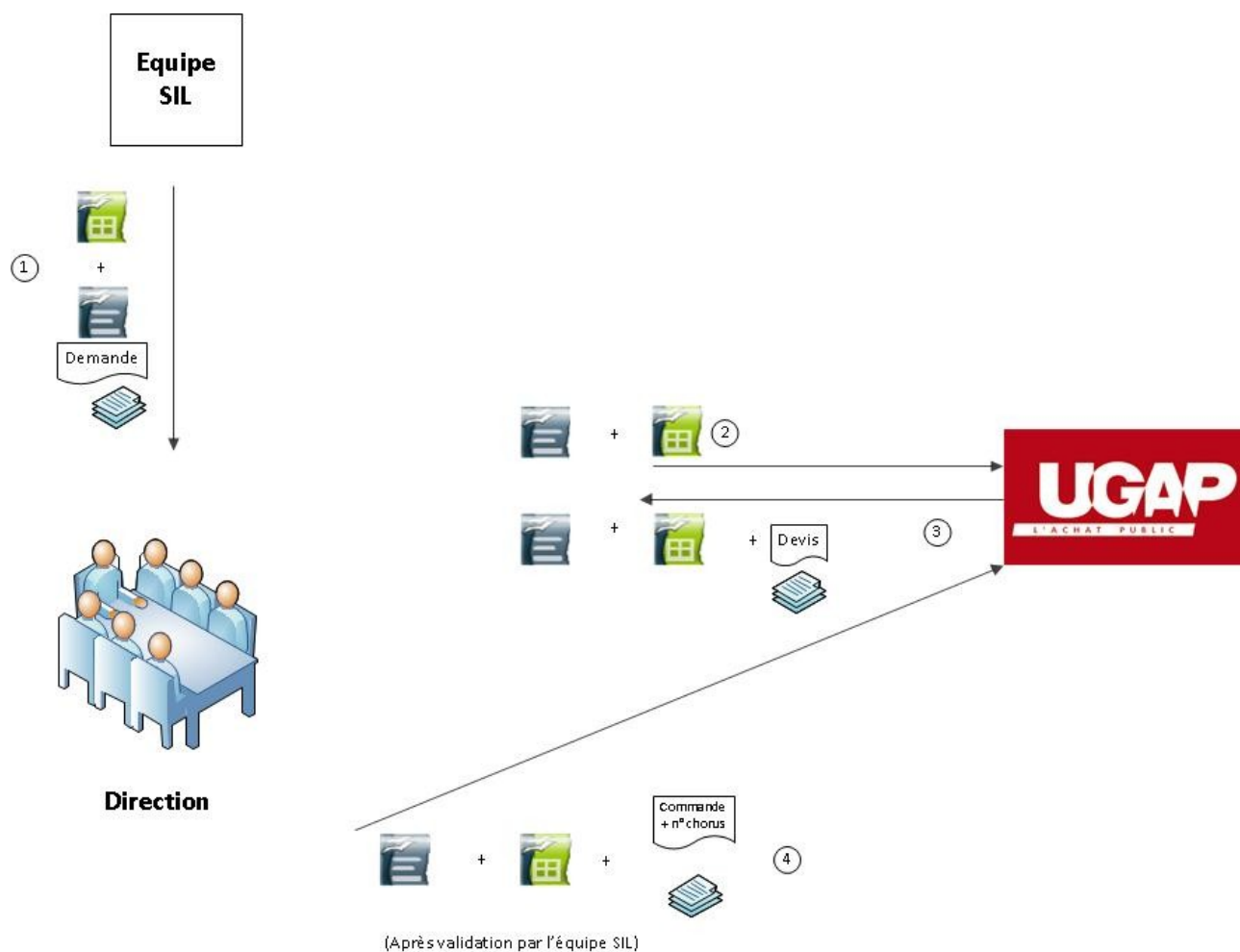
Ce qui importe vraiment aux décideurs, c'est de disposer de réseaux aptes à assurer en permanence le support des applications métier avec une qualité irréprochable dans le respect des contraintes budgétaires.

La maîtrise des réseaux nécessite que les équipements soient administrables à distance et supervisés par les administrateurs réseaux pour prévenir les dysfonctionnements et que des systèmes d'alertes préviennent en cas de défaillance réelle ou potentielle. Une documentation à jour et des outils associés réduiront sensiblement les délais de remise en service en cas d'incident, ainsi que les délais d'information sur les capacités d'extensions (déménagements,...).

V. Annexe 1- Circuit des commandes des directions sur le marché UGAP-LAN



VI. Annexe 2 - Circuit des commandes des directions sur le marché UGAP – Connectique



①② : expression et formalisation du besoin – fichiers odt et ods

③ : après validation, la MSNRL adresse la demande à l'UGAP

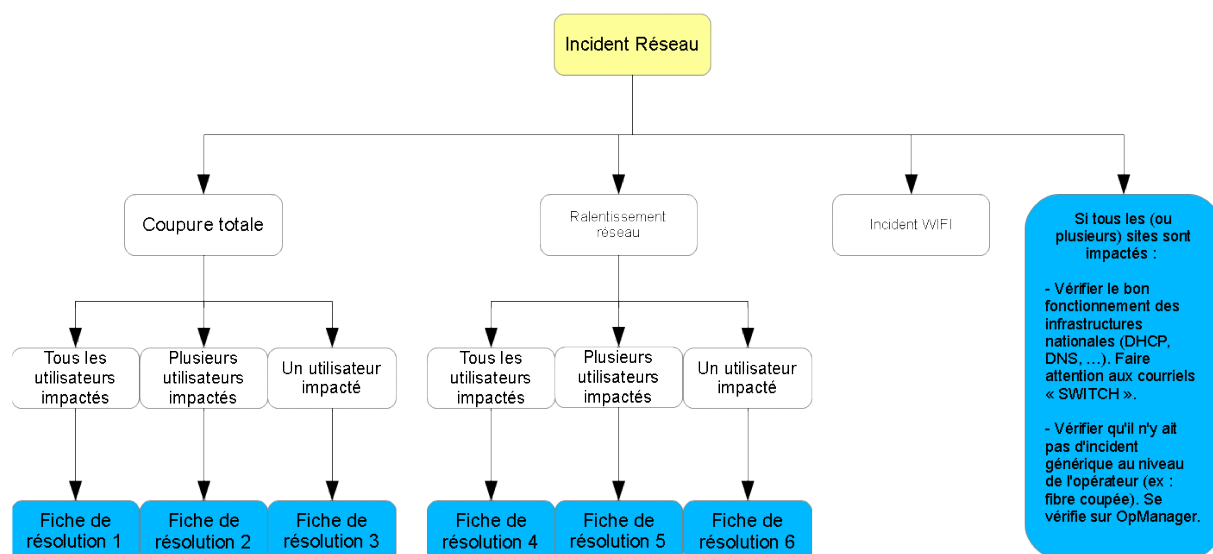
④ : l'UGAP retourne à la MSNRL un devis correspondant à la demande

⑤⑥ : La MSNRL envoie le fichier odt validé et le devis à l'équipe SIL. Celle-ci transfère les documents au service logistique concerné

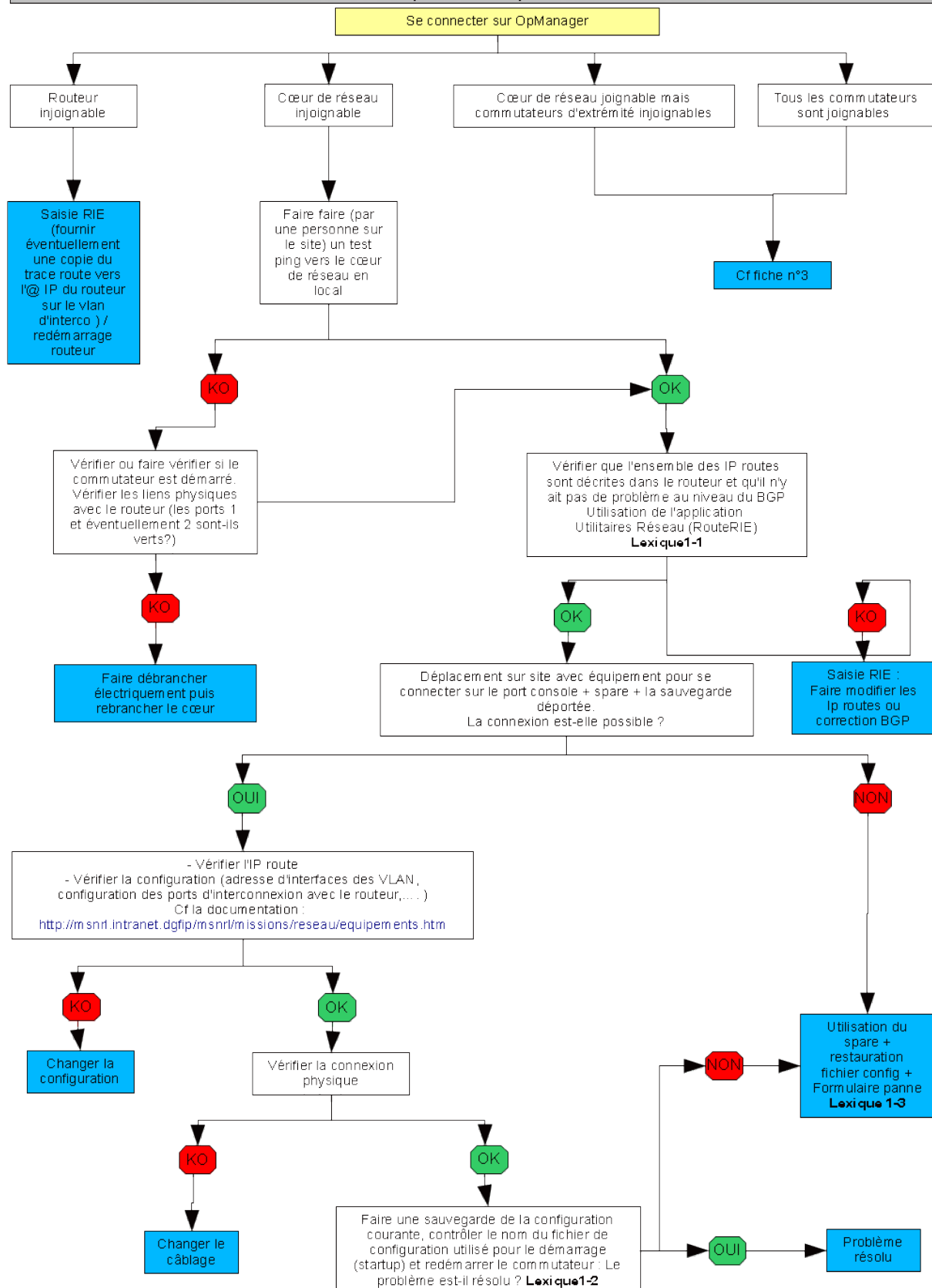
⑦ : après enregistrement de la commande dans Chorus (MAPA¹), la direction notifie le bon de commande à l'UGAP de Besançon

¹Marché UGAP SCC/HP mais dans l'application Chorus utiliser l'option MAPA (Marché selon Procédure Adaptée)

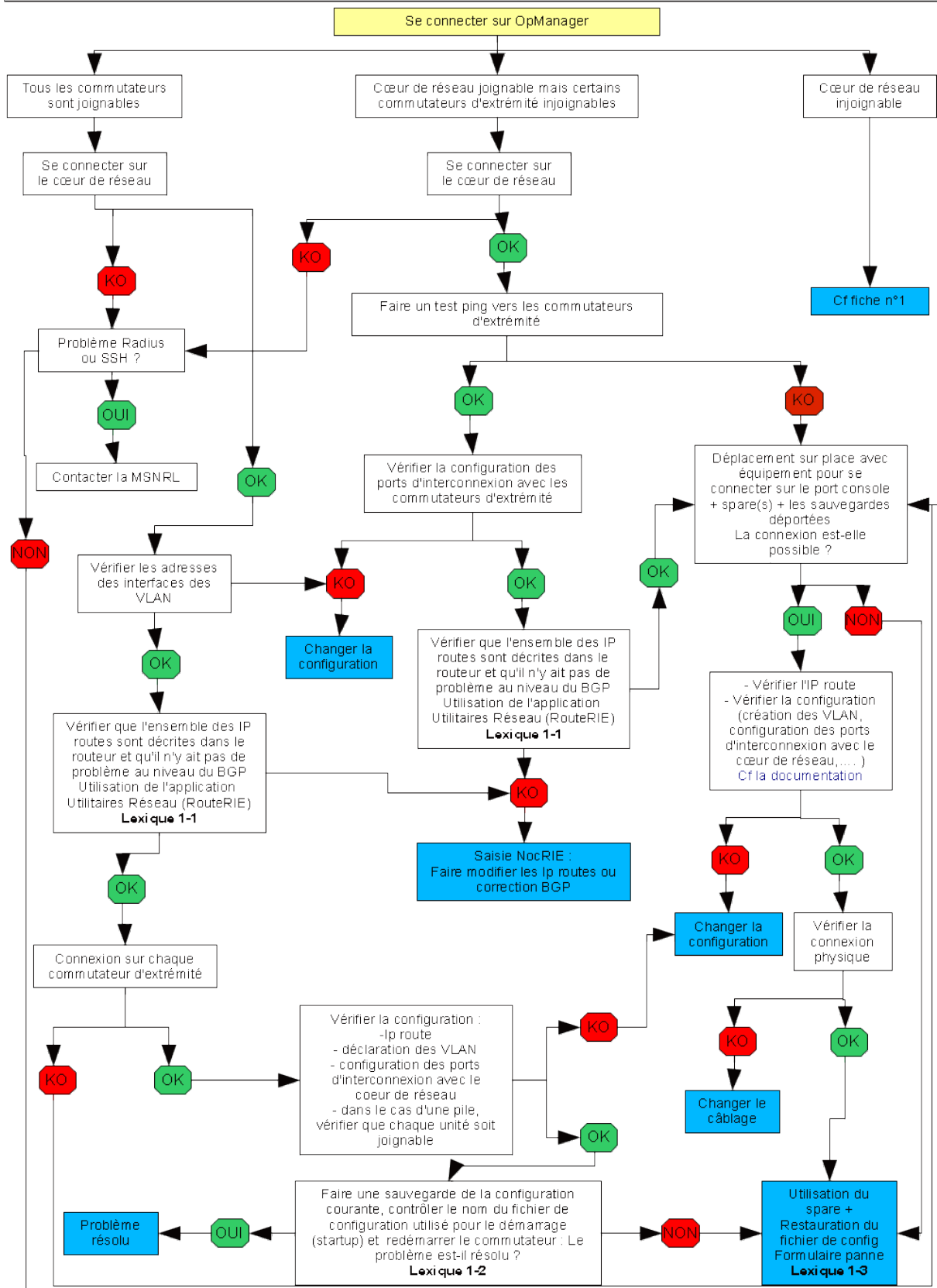
VII. Annexe 3 - Les fiches de résolution d'incidents



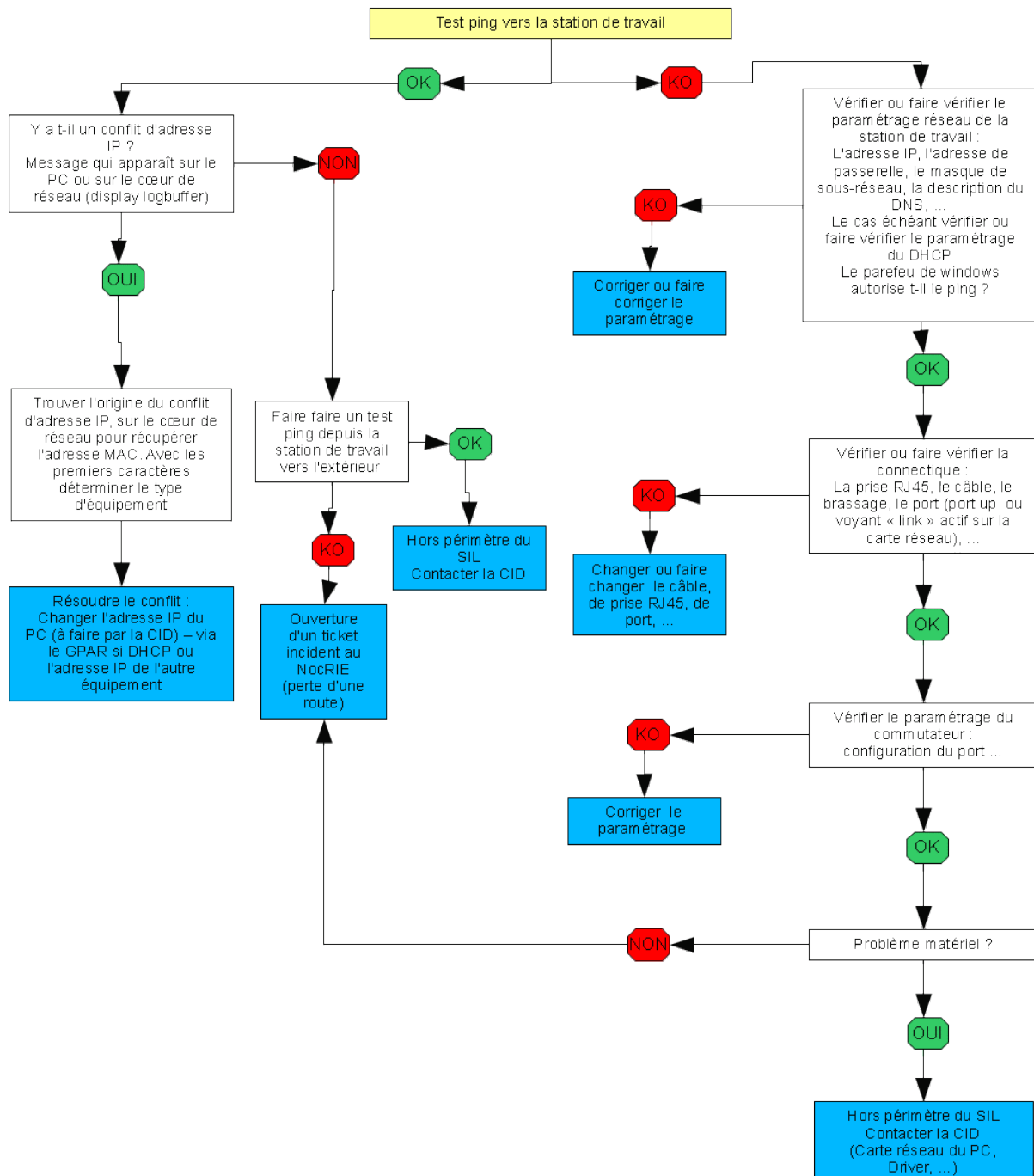
Fiche de résolution n°1 : Coupure totale pour l'ensemble des utilisateurs



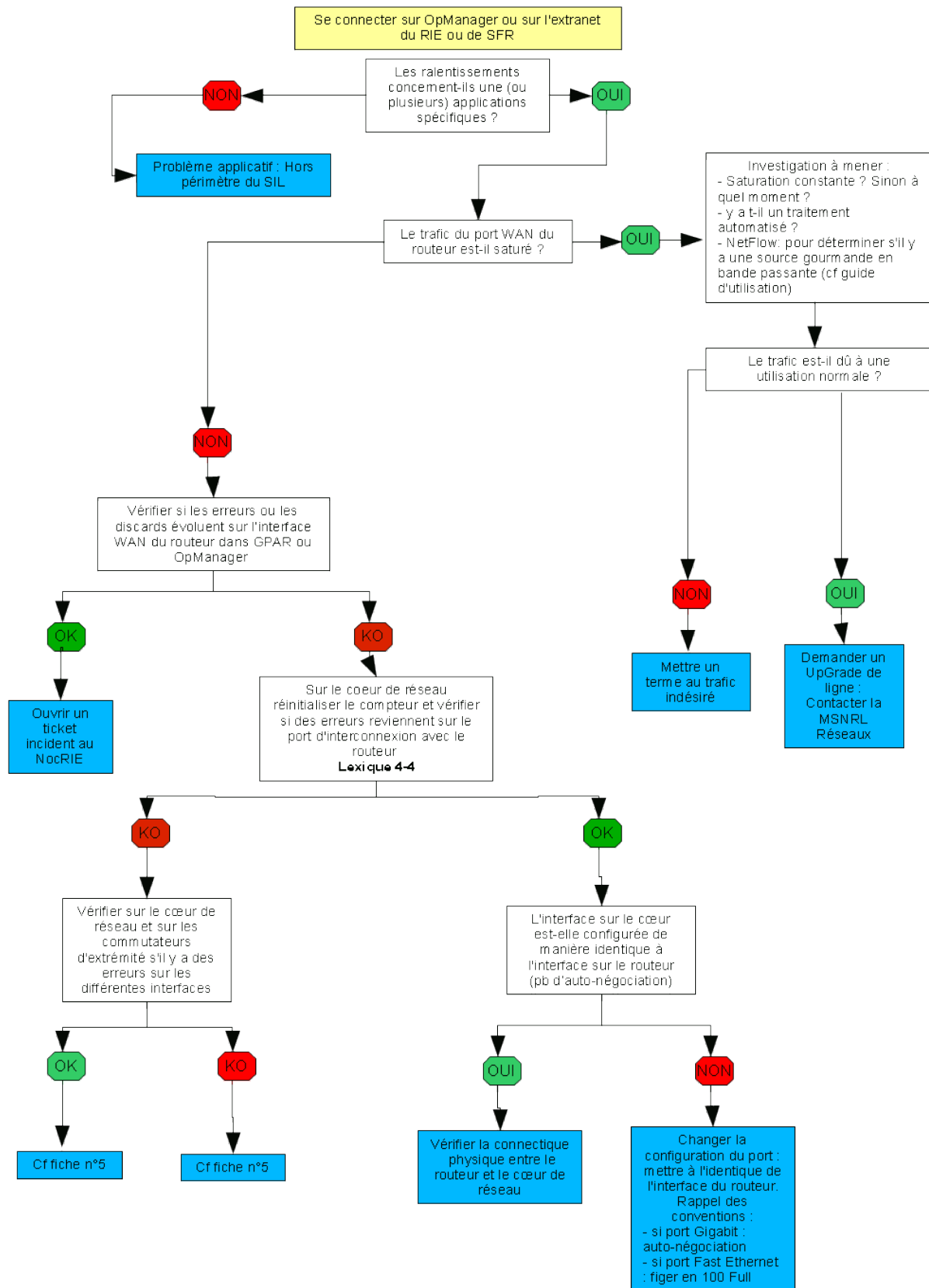
Fiche de résolution n°2 : Coupure totale pour une partie des utilisateurs



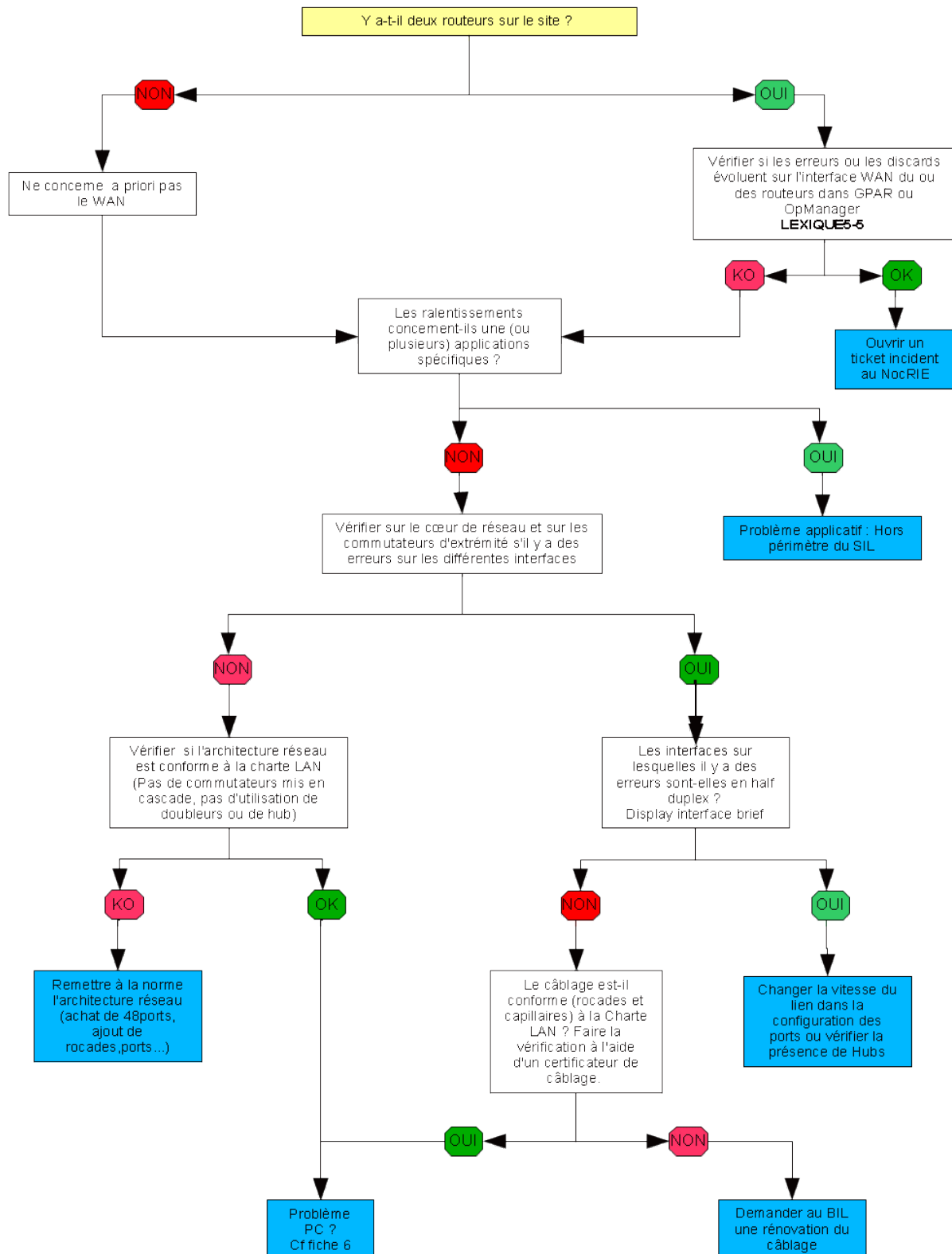
Fiche de résolution n°3 : Coupure totale pour un utilisateur



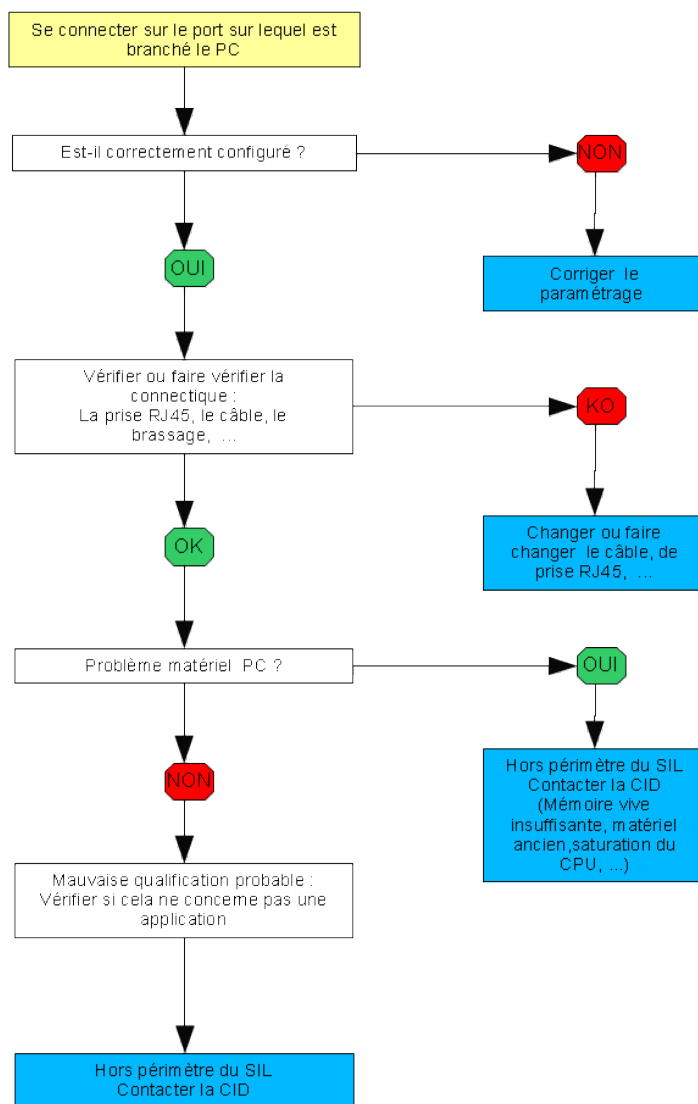
Fiche de résolution n°4 : Ralentissement réseau pour tous les utilisateurs



Fiche de résolution n°5 : Ralentissement réseau pour une partie des utilisateurs




Fiche de résolution n°6 : Ralentissement réseau pour un utilisateur



Fiche de résolution : LEXIQUE

Lexique 1-1	<p>RouteRIE 100.126.74.42 (R2) (C) ip route 10.17.5.16 255.255.255.248 directement connecté ip route 10.17.5.20 255.255.255.255 directement connecté ip route 100.126.74.42 255.255.255.255 directement connecté .../... (R2) (C) ip route 10.17.109.0 255.255.255.0 via 10.17.5.17 statique(3) (R2) (C) ip route 10.17.110.0 255.255.255.0 via 10.17.5.18 statique(3) (R2) (C) ip route 10.17.212.64 255.255.255.192 via 10.17.5.17 statique(3) (R2) ip route 10.17.253.0 255.255.255.0 via 10.17.5.17 statique(3) (R2) (C) ip route 10.17.254.0 255.255.255.0 via 10.17.5.17 statique(3) (R2) (C) ip route 10.152.17.48 255.255.255.240 via 10.17.5.17 statique(3) .../... ip route 0.0.0.0 0.0.0.0 via 86.79.3.161 bgp(14) ip route 0.0.0.0 0.0.0.0 via 86.79.3.165 bgp(14) ip route 100.126.74.44 255.255.255.255 via 86.79.3.158 bgp(14) .../... routes présentes ne participant pas au routage DGFIP ### ip route 77.155.169.5 255.255.255.255 directement connecté .../... (R) signifie que la route est correctement redistribuée dans le Backbone le nombre de routeurs acheminant la route est mentionné exemple R2 dans le cas des sites redondés (C) existe sur le cœur routeRIE est un outil DGFIP permettant de voir les routes sur le réseau RIE</p>
spare	<p>Les équipements en spare permettent de : - réaliser des économies sur les contrats de maintenance - réduire le temps de remplacement d'un commutateur Le stock de SPARE est situé dans les ESI et géré par les SIL.</p>
Lexique 1-2	<p><i>Sauvegarde configuration</i> save « puis nom du fichier de sauvegarde » display startup (pour le contrôle du paramètre de redémarrage) Cf la documentation : http://msnrl.intranet.dgfip/msnrl/missions/reseau/equipements.htm</p>
Lexique 1-3	<p><i>Restauration fichier de config (.cfg)</i> ftp 10.xx.yyy.zzz get sf001_5510_02500000_20170414.cfg sf001_5510_02500000.cfg Cf la documentation : http://msnrl.intranet.dgfip/msnrl/missions/reseau/equipements.htm</p>
Lexique 4-4	<p>Réinitialisation des compteurs d'erreurs pour un port reset counters interface GigabitEthernet x/y/z Cf la documentation : http://msnrl.intranet.dgfip/msnrl/missions/reseau/equipements.htm</p>
Lexique 5-5	<p>Contrôle de l'état des interfaces WAN dans GPAR Routeur DGFIP => interface Cf la documentation : ftp://ftp.oc.dgfip/Besancon/Commutateurs/GPAR/Guide-Utilisation_GPAR_vxx.pdf</p>

VIII. Annexe 4 - Présentation synthétique des actions à réaliser par chaque entité

Direction	DISI	ESI		MSNRL
		CID	SIL	
Demande un devis à sa DISI à l'aide de l'onglet « Description du projet » du fichier « devis_installation_WIFI »	Prend en compte l'expression de besoin et la transmet à l'ESI 		<ul style="list-style-type: none"> Réalise un plan avec les PC Initialise l'onglet « devis établi par le SIL et MSNRL » du fichier « devis_installation_WIFI » Initialise une demande d'étude à la MSNRL de l'ESI de Besançon via EDWAR 	<ul style="list-style-type: none"> Prend en compte la demande Réalise l'étude
Étudie le devis avec le fichier « devis_installation_WIFI » complété et le plan complété des bornes	Prend en compte le fichier « devis_installation_WIFI » complété et le plan complété des bornes et les transmet à la Direction		<ul style="list-style-type: none"> Prend en compte l'étude et transmet le fichier « devis_installation_WIFI » complété à la DISI ainsi que le plan complété des bornes 	<ul style="list-style-type: none"> Transmet le résultat de l'étude via EDWAR avec : <ul style="list-style-type: none"> le plan complété des bornes , le fichier « devis_installation_WIFI » complété, le fichier « WIFI_IP_bornes »
Refuse le devis d'installation WIFI et le notifie à la DISI			<ul style="list-style-type: none"> Notifie via EDWAR le refus de la Direction 	<ul style="list-style-type: none"> Clôture la demande dans EDWAR

Direction	DISI	ESI		MSNRL
		CID	SIL	
<ul style="list-style-type: none"> Accepte le devis d'installation WIFI et le notifie à la DISI Prépare l'information du projet en CHSCT 	<ul style="list-style-type: none"> Prend en compte la décision de la Direction et la notifie à l'ESI 	<ul style="list-style-type: none"> le chef d'ESI peut être sollicité pour participer au CHSCT en tant qu'expert technique. Pour l'aider, une documentation mise au point par la MSNRL et SI2B est mise à sa disposition. Il peut être également sollicité pour aider le chef du ou des services concernés à porter l'information aux agents. Une foire aux questions les plus fréquemment posées est mise à jour par la MSNRL et SI2B 		
Après consultation et information du CHSCT, commande les matériels et les interventions nécessaires (prises RJ45, bornes, PC, adaptateurs, commutateurs) selon le circuit déjà utilisé pour les commutateurs	<ul style="list-style-type: none"> Prend en compte la décision de la Direction et la notifie à l'ESI 	<ul style="list-style-type: none"> Demande via ODACE les certificats pour les postes fixes WIFI 	<ul style="list-style-type: none"> Notifie via EDWAR l'accord de la Direction et joint le fichier « WIFI_IP_bornes » qu'il aura validé Configure les commutateurs selon la « fiche_WIFI_réseau » 	<ul style="list-style-type: none"> Demande l'ouverture des flux entre les bornes et les contrôleurs
<ul style="list-style-type: none"> Prise en compte du planning des services techniques 	<ul style="list-style-type: none"> Information de la Direction 	<ul style="list-style-type: none"> Planifie avec le SIL l'intervention sur les postes de travail fixes 	<ul style="list-style-type: none"> Planifie avec la MSNRL l'installation des bornes (faite par le SIL) et leur connexion sur le réseau pour être validées sur les contrôleurs. 	<ul style="list-style-type: none"> Notifie via EDWAR l'ouverture effective des flux entre les bornes et les contrôleurs et demande à planifier le provisionnement des bornes (NB : la MSNRL ne peut provisionner les bornes que lorsqu'elle a reçu les certificats ID pour générer les clés sur les contrôleurs).
		<ul style="list-style-type: none"> Migration des postes de travail fixes en WIFI 	<ul style="list-style-type: none"> Informe la CID : les postes de travail peuvent migrer en WIFI 	<ul style="list-style-type: none"> Notifie via EDWAR le provisionnement effectif des bornes et la fin du traitement de la demande.

IX. Lexique

Ci-dessous les différentes terminologies qui sont utilisées dans ce document :

Acronyme / Terme	Définition
LAN	Local Area Network
WAN	Wide area network (réseau étendu)
MSNRL	Mission de Support National des Réseaux Locaux
SIL	Support aux Infrastructures Locales
CID	Cellule Informatique Départementale
RBL	Responsable Bureautique Local
UGAP	Union de Groupements d'Achats Publics
ToIP	Téléphonie sur IP (Telephony over Internet Protocol)
Qos	Qualité de service (quality of service)
Visio-conférence	Technique permettant de voir et de dialoguer avec plusieurs interlocuteurs en implémentant au minimum deux terminaux.
WiFi	Le <i>Wifi</i> est une technologie de transmission du Haut Débit sans fil qui permet de relier par ondes radio plusieurs appareils informatiques. Il correspond à un ensemble de protocoles de communication sans fil régis par les normes du groupe IEEE 802.11.
SSID	Service Set Identifier : Nom du réseau WIFI permettant de connecter un terminal à un point d'accès
PoE	Power over Ethernet. La technologie PoE, norme IEEE 802.3af, permet d'alimenter les équipements IP et de transmettre les données via un seul et même câble, pour une puissance maximale de 15,4 W pour le PoE et de 25,5 W pour le PoE+.
Cœur de réseau	premier commutateur directement raccordé au routeur d'accès du réseau WAN
Équipement d'accès	Équipement d'accès ou équipement d'extrémité : il sert à connecter les équipements terminaux (PC, imprimantes...).
Routage	Le routage est le mécanisme par lequel des chemins sont sélectionnés dans un réseau pour acheminer les données d'un expéditeur jusqu'à un ou plusieurs destinataires.
VID	numéro de VLAN (VLAN ID, ou VID)
VLAN	Réseau Local Virtuel (Virtual LAN)
SPARE	Stock de commutateurs de différents types géré au niveau de l'équipe SIL
Spanning Tree	Protocole réseau de niveau 2 permettant de déterminer une topologie réseau sans boucle ; (appelé aussi STP et RSTP pour Rapide STP).
NTP	Network Time Protocol (ou protocole d'heure réseau). Protocole qui permet de synchroniser, via un réseau informatique, l'horloge locale d'ordinateurs sur une référence d'heure.
MDI/MDI-X	Implanté dans un switch, la fonction <i>MDI/MDIX</i> permet de détecter automatiquement les câbles croisés et droits.
Mode Trunk	Le mode <i>trunk</i> est utilisé dans le cas où plusieurs vlans doivent circuler sur un même lien.
Mode Access	Le mode <i>access</i> est utilisé pour la connexion terminale d'un équipement (PC, imprimante, serveur...) appartenant à un seul vlan

Acronyme / Terme	Définition
SNMP	Simple Network Management Protocol. Protocole de communication qui permet aux administrateurs réseau de gérer les équipements du réseau, de superviser et de diagnostiquer des problèmes réseaux et matériels à distance.
Upgrade	Upgrader signifie mettre à jour, passer à la version la plus récente d'un logiciel ou d'un firmware.
Downgrade	Downgrader c'est revenir à la version précédente d'un logiciel ou d'un firmware.
Agrégat de lien	Technique utilisée dans les réseaux informatiques, permettant le regroupement de plusieurs ports réseau et de les utiliser comme s'il s'agissait d'un seul. LACP est un protocole standardisé par l'IEEE, implémenté par différents constructeurs. Il fournit un mécanisme permettant de contrôler le groupement de plusieurs ports physiques en un canal logique de communication.
IRF	I ntelligent R esilient F ramework de HPE Dispositif virtuel qui permet de faire apparaître plusieurs commutateurs interconnectés en mode IRF comme un seul. Avantages : simplification de la topologie et de la gestion ; haute résilience ; grande fiabilité.
VRRP	V irtual R outer R edundancy P rotocol Protocole de redondance de routeur virtuel : Le principe est de définir la passerelle par défaut pour les hôtes du réseau comme étant une adresse IP virtuelle (VIP) référençant un groupe de routeurs. VRRP utilise la notion de routeur virtuel, auquel est associée une adresse IP virtuelle ainsi qu'une adresse MAC virtuelle. Les rôles de routeur <i>master</i> et routeur <i>backup</i> sont également utilisés et associés aux routeurs d'un groupe VRRP. Le routeur <i>master</i> (ou maître en français) est associé à l'adresse IP virtuelle du groupe. C'est lui qui va répondre aux requêtes ARP des clients sur cette adresse IP. Le routeur <i>backup</i> (ou routeur de secours en français) pourra reprendre le rôle de <i>master</i> en cas de défaillance de celui-ci. Nota : Ce dispositif tend à disparaître dans les architectures de la DGFIP au profit de la mise en place d'IRF plus facile à gérer et plus fiable.
HSRP	H ot S tandby R outer P rotocol est un protocole propriétaire de chez Cisco Ce dispositif permet une continuité de service. HSRP est principalement utilisé pour assurer la disponibilité de la passerelle par défaut dans un sous-réseau en dépit d'une panne d'un routeur.