Caisse **N**ationale d'**A**ssurance **M**aladie

409NA002
Version 10.4

Département **R**éseau

REFERENTIEL LAN des Organismes & Guides de configuration des switches

SIEGES, AGENCES et ETABLISSEMENTS

(CPAM, UGECAM, IRSA, UC-CMP, CGSS, CTI et CN)

Note d'Application

Service : Déploiement
Auteur(s) : David Faucheux
Pascal Achard
Stéphane Duval
Jonathan Galeine
Benjamin HUGUET

Niveau de diffusion		Niveau de confidentialité	
DR	☒	Public	☐
Cnam	☒	Restreint	☒
Assurance Maladie	☒	Confidentiel	☐
Extérieur	☐		

Résumé : Référentiel pour les LAN des Organismes (CPAM , MEDICAL, UGECAM, IRSA, UC-CMP, CGSS, CTI et CN) de l'Assurance Maladie. Il concerne les SIEGES, les AGENCES et les ETABLISSEMENTS. Les guides de configuration des switches HP et Aruba y ont été intégrés.

Les nouveautés de cette version 10.x sont rédigées en marron.

Révisions

VERSIONS 9.6 **Janvier 2023 – Equipe Déploiement DR**	- Ajout vlan 900 : ADMIN-UCOPIA
VERSIONS 10.0 **Juin 2023 – Equipe Déploiement DR**	**- FUSION DES REFERENTIELS ET DES GUIDES DE CONFIGURATIONS DANS UN DOCUMENT UNIQUE DE REFERENCE** - Normalisation des noms de VLAN et de la description des interfaces VLAN pour les outils d'exploitation. De nombreux VLAN sont à renommer. - Nommage des switches - Description des agrégats et des liens trunks - VLAN pour les CTI - Ajout du VLAN 254 « VLAN-WIFI-PATIENTS » pour les UGECAM - Ajout des switches HP 5500 et HP 5120 dans les gammes obsolètes - OSE : Audits : ajouts des audits OSE - Suppression des architectures Ramage v5 - Ajout des switches dans le SI via le VLAN ADMIN-RESEAU - Changement de serveurs SYSLOG - OSE : suppression de l'accès en HTTPS sur les switches HP - OSE : bannière : précisions et normalisation - Abandon du retour au DR des 3600-v2 (hors panne) - Interconnexion des 55XX avec les 51XX
VERSIONS 10.1 **Juin 2023 – Equipe Déploiement DR**	**Syslog :** ajout d'une commande pour présiser la source **NCM** : récupération de la configuration des switches
VERSION 10.2 **Nov 2025 – Equipe Déploiement DR**	**Pour les swiths en comware V7** **Dns :** ajout d'une commande pour présiser la source **ntp :** ajout d'une commande pour présiser la source **dhcp relay** : ajout d'une commande pour présiser la source **vlan 903** :ajout vlan 903 suite à migration VLAN Routeur WIFI INVITE **Ping** : modification du ping
VERSION 10.3 **Nov 2025 – Equipe Déploiement DR**	**VLAN-SERVEURS-MEDICAL :** Création du vlan dédié au serveur des MEDICAL.
VERSION 10.4 **fev 2026 – Equipe Déploiement DR**	**Suppression DRSM et ELSM et remplacement par MEDICAL** **Configuration SDWAN (Port , interface)** **1.5.1 SDWAN - OSPF**

Liste de diffusion

CPAM, UGECAM, IRSA, UC-CMP, CGSS, CTI et CN	Tous les Services Informatiques / Equipes Réseau
DR	Tous les agents

Sommaire

1 REFERENTIEL LAN DES ORGANISMES DE L'ASSURANCE-MALADIE 9

1.1 REGLES « OSE » 9
1.1.1 Introduction OSE 9
1.1.2 Recommandations d'ordre général 9
1.1.3 Durcissement de l'accès aux switches 10
1.1.4 Evolution de la politique VLAN 10
1.2 GAMMES DE SWITCHES HP 12
1.3 AJOUT D'UN NOUVEL EQUIPEMENT AU SI 13
1.4 CONSIGNES GENERALES 15
1.4.1 Nommages normalisés et obligatoires 15
1.4.2 Nommage des switches (hors CGSS) 15
1.4.3 Cas spécifique des CGSS 16
1.4.4 Nommage des équipements wifi 16
1.4.5 Description des interfaces d'agrégation et des liens trunks 19
1.4.6 DHCP / DHCP-Relais / DHCP-Snooping 19
1.4.7 SSH 20
1.4.8 Spanning-Tree 20
1.4.9 Stackage et interconnexion des switches HP 21
1.4.10 Interfaces modulaires d'interconnexion des switches 21
1.4.11 Interfaces : speed / duplex 21
1.4.12 Description des interfaces 22
1.4.13 Shutdown des interfaces non utilisées 23
1.4.14 Câblage 23
1.4.15 Version logicielle des switches 23
1.4.16 LLDP 23
1.4.17 Interfaces / usages 23
1.5 RACCORDEMENT DES SITES A RAMAGE 26
1.5.1 SDWAN – OSPF 26
1.5.2 RV6 - BGP 28
1.6 ARCHITECTURES TYPES 34
1.6.1 Architecture type EN SIEGE d'Organisme 34
1.6.2 Architecture EN SIEGE d'Organisme : interconnexion 55XX /51XX 35
1.6.3 Architecture pour les serveurs EN SIEGE d'Organisme 36
1.6.4 Architectures en AGENCE et ETABLISSEMENT 36
1.7 CAS DU VLAN-ACCESS-PART (PARTENAIRES) 41
1.8 GTC/GTB/ANTI-INTRUSION, VIDEO-SURVEILLANCE … HORS PROJET NATIONAUX 41
1.9 VLAN ET ADRESSAGE IP NORMALISES EN SIEGE DE CPAM ET CGSS 42
1.9.1 Nommage normalisé des VLAN et interfaces VLAN en CPAM 42
1.9.2 Tableau des VLAN normalisés en Siège de CPAM : 43
1.10 VLAN ET ADRESSAGE IP NORMALISES EN SIEGE D'UGECAM 46
1.10.1 Nommage normalisé des VLAN et des interfaces VLAN en siège d'UGECAM 46
1.10.2 Tableau des VLAN normalisés en siège d'UGECAM 47
1.11 ADRESSAGE IP NORMALISE / ADRESSES RESERVEES (CPAM, CGSS, MEDICAL, UGECAM) 49
1.12 VLAN ET ADRESSAGE IP NORMALISES EN AGENCES ET ETABLISSEMENTS 50
1.12.1 Nommage normalisé des VLAN et interfaces VLAN 50
1.12.2 Listes et fonctions des VLAN en AGENCES et ETABLISSEMENTS 51
1.12.3 VLAN 2 – VLAN-Nom-Org : organismes hébergés (IRSA, UC-CMP,CDS…) 53
1.12.4 VLAN 3 – VLAN-MEDICAL 54
1.12.5 VLAN 4 – VLAN-DATA 54
1.12.6 VLAN 5 – VLAN-INTERCOWAN 55
1.12.7 VLAN 30 – VLAN-VOIX 57
1.12.8 VLAN 50 – VLAN-WIFI-AGENTS 57
1.12.9 VLAN 53 – VLAN-WIFI-AGENTS-MEDICAL 58

1.12.10 VLAN 172 – VLAN-SD-WAN 59
1.12.11 VLAN 216 – VLAN-CONSOLES-SERVEURS (ILO – IDRAC) 59
1.12.12 VLAN 224 – VLAN-ACCES-PART 60
1.12.13 VLAN 225 - VLAN-ACCES-PART-MEDICAL 63
1.12.14 VLAN 226 –VLAN-IMPRIMANTES 63
1.12.15 VLAN 227 –VLAN-IMPRIMANTES-MEDICAL 64
1.12.16 VLAN 229 - VLAN- IMPRIMANTES-CDS 64
1.12.17 VLAN 901 – VLAN-ADMIN-RESEAU 65
1.12.18 VLAN 902 – VLAN-ADMIN-WIFI 66
1.12.19 VLAN 903 – VLAN-ROUTEUR-WIFI-INVITE 66
1.13 VLAN ET ADRESSAGE IP NORMALISES POUR LES CTI 67
1.14 ADRESSAGE IP NORMALISE POUR IRSA, UC-CMP 67
1.15 AUTRES SUJETS TECHNIQUES 70
1.15.1 SNMP / SYSLOG 70
1.15.2 Wifi 70
1.15.3 Wake On LAN 70
1.15.4 NTP 70
1.15.5 QoS 70
1.15.6 Déploiement de téléphones IP 71
1.16 GESTION DES SWITCHES 72
1.16.1 Demandes de switches 72
1.16.2 Attribution de switches de secours (« SPARE ») 72
1.16.3 Maintenance : que faire en cas de panne ? 73
1.16.4 Que faire des switches obsolètes ? 73
1.17 AUDITS DE CONFORMITE 74

2 GUIDE DE CONFIGURATION DES HP 5510, 5520, 5130 ET 5140 75

2.1 IMPORTANT : ORDRE DE CONFIGURATION SUGGERE 75
2.2 DIFFERENCE ENTRE SWITCH NIVEAU 2 ET SWITCH NIVEAU 3 76
2.3 LES GAMMES HP 55XX ET HP 51XX 76
2.3.1 HP 5130 / HP 5140 76
2.3.2 La gamme HP 5510 / 5520 77
2.3.3 Présentation des équipements 77
2.3.4 Accessoires 82
2.3.5 Mise en baie 82
2.3.6 Prise en main 83
2.3.7 Commandes de base 83
2.3.8 Alias 84
2.4 STACKAGE (IRF) 85
2.4.1 Présentation 85
2.4.2 Configuration 87
2.4.3 Elément 1 du stack 88
2.4.4 Elément 2 du stack 88
2.4.5 Cas d'un switch seul (non stacké) 91
2.4.6 Vérification 91
2.5 NOMMER LE SWITCH 92
2.6 CONFIGURATION DES ACCES 92
2.6.1 Règle de construction du mot de passe 92
2.6.2 Accès console, SSH et HTTPS 93
2.7 BANNIERE 94
2.7.1 Résolution DNS 94
2.8 CONFIGURATIONS DU SPANNING-TREE 95
2.8.1 Cas des HP 5510 ou 5520 niveau 3 95
2.8.2 Cas des HP 5130 ou 5140 niveau 2 97
2.8.3 Au niveau des interfaces 97
2.8.4 Protéger le root-bridge, limiter les boucles, broadcasts et multicasts 98
2.9 SNMP / SYSLOG 100

2.9.1 SNMP 100
2.9.2 SYSLOG 100
2.10 SECURITE 102
2.10.1 ACL 2099 pour SNMP 102
2.10.2 ACL 2922 pour RV6 et SDWAN 102
2.10.3 ACL 3002 WOL 102
2.10.4 ACL 3224 pour le VLAN 224 102
2.10.5 ACLs 3900 et 3901 - Vlan 900 (Admin Ucopia) 102
2.10.6 Fonction packet-filter 104
2.11 CONFIGURATION DES VLAN 105
2.11.1 Nommage des Vlan et des interfaces VLAN 105
2.11.2 Déclarer les VLAN (niveau 2) 105
2.11.3 Création des interfaces VLAN (niveau 3) 106
2.11.4 VLAN 901 (ADMIN-RESEAU) en AGENCES 108
2.11.5 VLAN 902 (ADMIN-RESEAU-WIFI) en AGENCES 111
2.11.6 VLAN 900 (ADMIN-UCOPIA) en SIEGE 111
2.11.7 VLAN 22X 111
2.11.8 Suppression du VLAN 249 VISIO 116
2.12 CONFIGURATION DES INTERFACES 117
2.12.1 Interfaces non utilisées 117
2.12.2 Description des interfaces 117
2.12.3 Speed / Duplex 117
2.12.4 Routeurs opérateurs RV6 (RAMAGE) 118
2.12.5 Routeurs opérateurs SDWAN (RAMAGE) 120
2.12.6 Box Evasion Internet 122
2.12.7 Serveur physique (non VMWARE) 122
2.12.8 PMF + TEL 122
2.12.9 PMF + TEL pour SERVICE MEDICAUX 123
2.12.10 Equipement e-GFA 123
2.12.11 Imprimante 124
2.12.12 Imprimante SERVICE MEDICAL 124
2.12.13 Serveur Virtuel (VMWARE) mono ou multi-Vlan 124
2.12.14 Borne wifi 125
2.12.15 Contrôleur wifi 125
2.12.16 Boitier pour portail captif wifi 126
2.12.17 IPBX (hors Cetiam) 126
2.12.18 Passerelle « Audiocodes » (hors Cetiam) 126
2.12.19 Passerelle « CETIAM » 127
2.12.20 Interconnexion des switches 128
2.12.21 Règles de nommage 128
2.12.22 Utilisation des ports « combo » 129
2.12.23 Interconnexion de switches AVEC AGREGATION 130
2.12.24 Interconnexion de switches SANS AGREGATION 135
2.13 CONFIGURATION DU DHCP 136
2.13.1 DHCP RELAIS 136
2.13.2 DHCP SNOOPING 137
2.13.3 Routage dans les HP 5130 et 5140 niveau 2 d'extrémité 139
2.14 AUTRES CONFIGURATIONS 139
2.14.1 LLDP : découverte 139
2.14.2 NTP: Tous à la même heure 140
2.14.3 Wake On LAN : réveil des PMF à distance 140
2.14.4 QoS pour la voix et la videoconference 142
2.15 L'EXPLOITATION 143
2.15.1 Ping 143
2.15.2 Mirroring d'interface 143
2.15.3 Sauvegardes 145
2.15.4 Restaurations 146

2.15.5 Remplacement d'un switch non maitre en panne dans un stack 149
2.15.6 Remplacement d'un switch maitre en panne dans un stack 149
2.15.7 Remplacement d'un stack complet 151
2.15.8 Ajout d'un switch dans un stack (en production) 151
2.15.9 Mise à jour de la version des HP 5510, 5520, 5130, 5140 151
2.15.10 Récupération d'un switch sans version 159
2.15.11 Remettre un switch en configuration usine 162
2.15.12 Accéder à la console du switch sans authentification 163
2.15.13 Annexe : exemple complet de configuration 164

3 GUIDE DE CONFIGURATION DES HP 3600-V2 178

3.1 IMPORTANT : ORDRE DE CONFIGURATION SUGGERE 178
3.2 DIFFERENCE ENTRE SWITCH NIVEAU 2 ET SWITCH NIVEAU 3 179
3.3 LA GAMME HP A3600 V2 179
3.3.1 Prise en main 181
3.3.2 Commandes de base 181
3.3.3 Alias 182
3.4 STACKAGE (IRF) 183
3.4.1 Présentation 183
3.4.2 Configuration 185
3.4.3 Cas d'un switch seul (non stacké) 187
3.4.4 Vérification 187
3.5 NOMMER LE SWITCH 188
3.6 CONFIGURATION DES ACCES 188
3.6.1 Règle de construction du mot de passe 188
3.6.2 Accès console, SSH et HTTP 188
3.6.3 Bannière 189
3.6.4 Résolution DNS 190
3.7 CONFIGURATION DU SPANNING-TREE 191
3.7.1 Spanning-tree : mode et root-bridge 191
3.7.2 Spanning-tree au niveau des interfaces 192
3.7.3 Protéger le root-bridge, limter les boucles, broadcasts et multicasts 193
3.8 SNMP / SYSLOG 195
3.8.1 SNMP 195
3.8.2 SYSLOG 195
3.9 SECURITE 196
3.9.1 ACL 3224 pour le VLAN 224 196
3.9.2 ACL 2099 pour SNMP 196
3.9.3 ACL 3002 WOL 196
3.9.4 Fonction packet-filter 196
3.10 CONFIGURATION DES VLAN 197
3.10.1 Nommage des Vlan et des interfaces VLAN 197
3.10.2 Déclarer les VLAN (niveau 2) 197
3.10.3 Création des interfaces VLAN (niveau 3) 197
3.10.4 VLAN 901 (ADMIN-RESEAU) en AGENCES 199
3.10.5 VLAN 902 (ADMIN-RESEAU-WIFI) en AGENCES 200
3.10.6 VLAN 22X 201
3.10.7 Suppression du VLAN 249 « VISIO » 206
3.11 CONFIGURATION DES INTERFACES DES 3600 206
3.11.1 Interfaces non utilisées 206
3.11.2 Description des interfaces 206
3.11.3 Speed / Duplex 206
3.11.4 Routeurs opérateurs (RAMAGE) 207
3.11.5 Téléphone + PMF : standard CETIAM 210
3.11.6 PMF seul 214
3.11.7 Serveurs 215
3.11.8 Equipement e-GFA 215

3.11.9 Imprimante ... 216
3.11.10 BOX « Evasion internet » ... 216
3.11.11 Borne wifi ... 216
3.11.12 Contrôleur wifi ... 217
3.11.13 Boitier pour portail captif wifi ... 217
3.11.14 Passerelle CETIAM ... 218
3.11.15 IPBX (hors Cetiam) ... 218
3.11.16 Passerelle « Audiocodes » (hors Cetiam) ... 219
3.12 INTERCONNEXION DES SWITCHES ... 219
3.12.1 Règles de nommage ... 219
3.12.2 Utilisation des ports « combo » ... 220
3.12.3 Interconnexion de switches AVEC AGREGATION ... 221
3.13 INTERCONNEXION DE SWITCHES SANS AGREGATION ... 226
3.14 CONFIGURATION DU DHCP ... 226
1.1 DHCP-RELAY ... 226
3.14.1 DHCP-Snooping ... 230
3.15 ROUTAGE ... 231
3.15.1 Routage dans les fédérateurs niveau 3 TOUS SITES ... 231
3.15.2 Routage « Evasion Internet » dans les stacks niveau 3 ... 232
3.15.3 Routage dans les HP 3600 niveau 2 d'extrémité ... 233
3.15.4 Autres configurations ... 234
3.15.5 NTP : tous à la même heure ... 234
3.15.6 Wake On LAN : réveil des PMF à distance ... 235
3.16 QOS POUR LA VOIX ET LA VIDEOCONFERENCE ... 235
3.17 L'EXPLOITATION ... 237
3.17.1 Mirroring d'interface ... 237
3.17.2 Sauvegardes ... 238
3.17.3 Restaurations ... 238
3.17.4 Remplacement d'un switch non maitre en panne dans un stack ... 241
3.17.5 Remplacement du switch maitre en panne dans un stack ... 241
3.17.6 Remplacement d'un stack complet ... 243
3.17.7 Ajout d'un switch dans un stack (en production) ... 243
3.17.8 Mise à jour de la version ... 243
3.17.9 Récupération d'un switch sans version ... 245
3.17.10 Remettre un switch en configuration usine ... 248
3.17.11 Annexes : exemples complets de configuration ... 248

4 GUIDE DE CONFIGURATION DES ARUBA 2930F ... 266

4.1 LE MODELE ARUBA 2930F ... 266
4.2 PRISE EN MAIN ... 266
4.3 COMMANDES DE BASE ... 267
4.4 CONFIGURATION POUR UNE INSTALLATION AU N2 A L'EXTREMITE ... 268
4.4.1 Accès console, SSH et HTTPS ... 268
4.4.2 Sauvegarde de la configuration (running) ... 269
4.4.3 Résolution DNS ... 269
4.4.4 Configuration du Spanning-Tree et protection des boucles ... 269
4.4.5 SNMP / SYSLOG ... 269
4.4.6 Nommer le switch ... 270
4.4.7 Configuration du VLAN d'Amin-réseau ... 270
4.4.8 Configuration des interfaces du 2930F ... 271
4.4.9 Interconnexion des switches ... 276
4.4.10 Interconnexion de switches SANS AGREGATION ... 276
4.4.11 Interconnexion de switches AVEC AGREGATION ... 276
4.5 CONFIGURATION DU DHCP ... 278
4.5.1 DHCP relais ... 278
4.5.2 DHCP Snooping ... 278
4.6 ROUTAGE ... 279

4.7 AUTRES CONFIGURATIONS 279
4.7.1 LLDP : découverte 279
4.7.2 NTP : tous à la même heure 279
4.8 EXEMPLES COMPLETS DE CONFIGURATION 281
4.8.1 Avec Agrégat en INT 7 et 8 en SIEGE d'organisme 281
4.8.2 Sans agrégat mais interconnexion INT 8 en Agence 283
4.9 L'EXPLOITATION 285
4.9.1 Mirroring d'interface 285
4.9.2 Sauvegardes 285
4.9.3 Restaurations 286
4.9.4 Mise à jour de la version 289
4.9.5 Remettre un switch en configuration usine 291

1 REFERENTIEL LAN DES ORGANISMES DE L'ASSURANCE-MALADIE

Il est grandement recommandé de lire l'ensemble de ce REFERENTIEL avant toute demande de support.

Ce référentiel s'applique à tous les organismes de l'Assurance Maladie : CPAM, MEDICAL, UGECAM, IRSA, UC-CMP, CGSS (hors interconnexion avec les FW), CTI et sites nationaux, sièges, agences et établissements.

Il ne concerne pas les CSH.

Ce référentiel liste les normes et bonnes pratiques à appliquer au niveau de chaque LAN de l'Assurance Maladie avec des switches HP. Pour faciliter encore leur configuration, nous avons préparé des Guides de configuration HP. Pour toutes les configurations évoquées dans ce référentiel, veuillez-vous reporter systématiquement à ces guides qui sont mis à jour régulièrement et disponibles plus bas dans ce document.

Bien que le contexte y soit parfois différent, tous les organismes ci-dessus listés doivent se conformer à ces préconisations :

- Architecture
- VLAN
- Plan d'adressage
- Normes et nommages
- Configurations
- …etc.

1.1 REGLES « OSE »

1.1.1 Introduction OSE

OSE est un label d'état et signifie Opérateur de Service Essentiels.

Un OSE est un opérateur utilisant des réseaux ou des systèmes d'information, qui fournit un service essentiel dont l'interruption aurait un impact significatif sur le fonctionnement de l'économie ou de la société Française.

- La Cnam et les organismes de Sécurité Sociale sont définis comme un OSE
- Dans ce cadre, le DR (Département Réseau) reçoit les objectifs du DS (Département Sécurité) et les décline dans ce document pour que vous les mettiez en place dans vos organismes.

1.1.2 Recommandations d'ordre général

Vous pouvez connecter sur le réseau de l'assurance maladie, uniquement les équipements qui ont fait l'objet de projets validés par la Cnam. (PMF, IMP, SERVEURS, ESX, BOX, BORNES WIFI ,..).

Pour les autres équipements, le directeur de l'organisme de l'Assurance Maladie (CPAM, MEDICAL, UGECAM, IRSA, UC-CMP, CGSS, CTI….) est garant de l'application des recommandations réseaux et des règles de sécurité imposées par la PSSI MCAS et OSE.

1.1.3 Durcissement de l'accès aux switches

Le projet OSE impose donc de durcir les configurations de nos équipements réseaux avec :

- Passage de la clé RSA de 1024 à 2048,
- Suppression du SSH V1,
- Verrouillage des connexions VTY,
- Durcissement de la politique de mots de passe
- Certains switches HP ne supportant que le TLS v1.1, nous supprimons tout accès aux switches en HTTPS (le DR préconise la connexion en SSH et la configuration en CLI). La surveillance est à faire via les outils Centéon et ceux du projet Netlix.

1.1.4 Evolution de la politique VLAN

Le projet OSE impose également d'isoler les flux de nature différente dans un VLAN particulier et par la suite de les contrôler avec des ACL .

⇨ **Le VLAN 3 est dédié aux agents du Service Médical**

- Le VLAN SERVICE MEDICAL (Vlan3) doit être mis en place dès que l'organisme (CPAM, CP) héberge un service medical.

⇨ **Le VLAN 224 est utilisé pour le projet EGFA (Flux Egfa) et doit être utilisé pour des projets locaux nécessitant un accès à des machines par des partenaires extérieurs**

- Lorsque vous installez des équipements dans le cadre du projet EGFA ou dans le vlan224 vous devez activer l'ACL 3224 associée

⇨ **Un VLAN 22X sera déclaré pour tous les projets nationaux avec éventuelle interconnexion partenaire suite validation par la DS et le DR :**

- Imprimantes (VLAN 226 : VLAN-IMPRIMANTES) (Flux imprimante)
  - Pas d'interconnexion partenaire à ce jour
- Autres à venir

⇨ **Un VLAN 90X sera déclaré pour chaque flux d'admin après validation du DR**

- VLAN 901 (Flux admin réseau)
- VLAN 902 (Flux admin WIFI)
- VLAN 900 (Flux admin Ucopia)
- Autres à venir

⇨ **Une bannière OFFICIELLE et UNIQUE doit être OBLIGATOIREMENT configurée dans les swiches. La voici :**

```
****************************************
*             ! Attention !            *
*                                      *
*    Acces reserve aux personnels du   *
*         service informatique         *
*                                      *
*  Toutes les activites sur ce systeme *
*           sont enregistrees          *
*                                      *
*    Toutes preuves d activites non    *
*   autorisees seront traitees par les *
*    autorites competentes             *
*                                      *
*     Toute intrusion sur un systeme   *
*   informatique est interdite par les *
*     articles 323-2 du code penal     *
*                                      *
****************************************
```

Veuillez consulter les documents spécifiques sur l'intranet du DR

➔ https://www.cngr.cnamts.fr/contenu/symfony/253

et appliquer les recommandations dès que possible.

1.2 GAMMES DE SWITCHES HP

Le modèle HP A3600 v2 :

C'est un switch 10/100 avec 4 ports giga. Un guide de configuration est toutefois dédié : 409NT007 (voir **[1]**).

Il peut être utilisé :

- au niveau 2 et à l'extrémité dans tout site
- au niveau 3 et en tête de réseau dans toutes les agences (de type CP, Agence,… par exemple).

Les modèles HP 5510/5520 (55X0*) et 5130/5140 (51X0*) :

- Embarquent l'OS COMWARE 7 (COMWARE 5 amélioré…).
  COMWARE est le nom du système d'exploitation qui tourne sur les switches HP, et est basé sur Linux.

- Les 51X0-24G non POE seront utilisés pour la connexion des serveurs à 1 Gb/s, car ceux-ci ont généralement leur propre prise d'alimentation électrique.

- Les 51X0 ne peuvent pas être utilisés en fédérateurs car ils ne supportent pas le protocole e-BGP.

- Les 51X0-24G-POE et 51X0-48G-POE seront utilisés sur certains gros sites pour fournir une connexion d'extrémité POE en Gigabit.
  Ils seront alors capables par exemple de fournir de l'électricité aux téléphones branchés sur ces ports.
  Dans ce cas, il est recommandé de prévoir des 55X0 en fédérateurs.

- Les 55X0G-24 (cuivre ou fibre optique) seront utilisés en tant que fédérateurs dans les sièges et si besoin dans certains gros sites d'extrémités (CP, Agence, Etablissements).

- Les 5520 se configurent de la même manière que les 5510.

- Les 5140 se configurent de la même manière que les 5130.

* : dans la suite du document :

- 55X0 = 5510 ou 5520
- 51X0 = 5130 ou 5140

1.3 AJOUT D'UN NOUVEL EQUIPEMENT AU SI

Pensez à consulter les tutoriels disponibles sur l'intranet du DR :

url : https://www.cngr.cnamts.fr/faq/



Lorsque vous installez un nouvel équipement réseau, vous devez le déclarer obligatoirement sur le portail du DR via l'URL ci-dessous.
Cela mettra à jour automatiquement le SI (Système d'information) de la CNAM/DR et les outils d'administration du réseau (aujourd'hui CENTREON, Netlix et l'inventaire réseau).

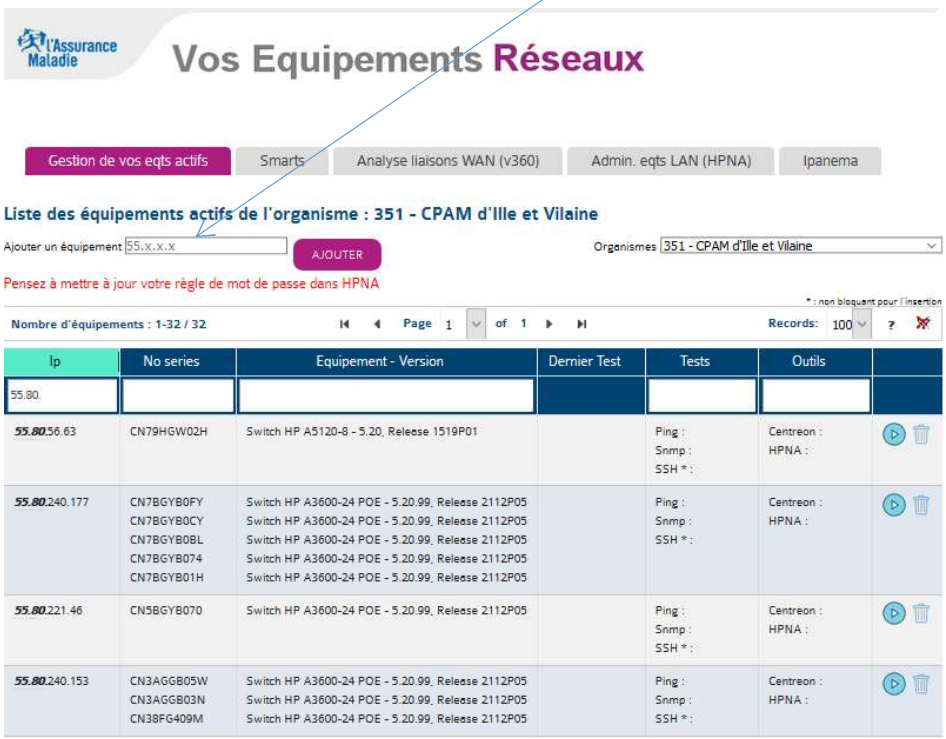
ATTENTION : La création d'un nouveau sous réseau implique la prise en compte de cette information dans le SI, aussi, si vous constatez le message suivant « L'adresse IP: 55.xx.xx.xx n'est pas reconnue par le DR. Un gestionnaire LAN est prévenu.", vous pouvez :

- *** Effectuer une demande PNS « RESEAU » à destination de l'équipe support LAN du département réseau.**
- *** Attendre la découverte automatique des subnets qui est lancé sur l'ensemble du parc le dimanche.**

Pour cela, utilisez le portail suivant :

https://www.cngr.cnamts.fr/supervision/equipementActif/

1/ Sélectionner votre organisme dans la liste déroulante (ici 351- CPAM d'Ille et vilaine)
2/ Ajouter l'adresse IP (*) de votre équipement dans le champ (respecter votre plan d'adressage)
3/ Cliquez sur le bouton AJOUTER Tout est automatique – Vous avez terminé.



- Les switches doivent être insérés dans le SI via leur adresse IP d'administration déclarée sur le VLAN-ADMIN-RESEAU (90X, loopback1).

L'ajout et la suppression des équipements réseaux s'effectuent uniquement par cette interface Web :
https://www.cngr.cnamts.fr/supervision/equipementActif/

1.4 CONSIGNES GENERALES

1.4.1 Nommages normalisés et obligatoires

En plus de la normalisation du nommage des VLAN et de la description des interfaces VLAN qui est expliqué plus bas dans ce document, il est également obligatoire de respecter la norme de nommage et/ou de description des éléments suivants :

- **Nommage des switches**
- **Description des interfaces d'agrégation (int bridge-agregation)**
- **Description des interfaces (trunks) placées dans un agrégat**

1.4.2 Nommage des switches (hors CGSS)

Il est demandé de nommer les équipements de manière homogène afin de les repérer plus facilement et d'intégrer automatiquement les équipements à la supervision nationale sur CENTREON et NETLIX.

Grâce au portail web, vos équipements sont classés automatiquement dans la partition de votre organisme.

Sous CENTREON et NCM, le portail web classe automatiquement tous vos switches dans votre partition :

CENTREON :

☐	OK	memory	75f-sw-cn-cnam-rennes-130-n3	2d 23h	1/1 (H)	39s	OK: Memory '212' Total: 1.94 GB Used: 676.16 MB (34.00%) Free: 1.28 GB (66.00%)
☐	OK	hardware	75f-sw-cn-cnam-rennes-130-n3	2d 23h	1/2 (H)	42s	OK: All 6 components are ok [1/1 chassis, 2/2 fans, 2/2 module, 1/1 stack].
☐	OK	cpu	75f-sw-cn-cnam-rennes-130-n3	2d 23h	1/2 (H)	42s	OK: CPU '212' Usage : 21.00 %
☐	OK	interface-routeur	75f-sw-cn-cnam-rennes-130-n3	2d 23h	1/1 (H)	1m 10s	OK: All interfaces are ok

NCM :

☐	75f-sw-cn-rennes-066-n2-5130...	H3C Switch	5130-48G-PoE+-4SFP+ (370W)...	5130-48G-PoE+-4SFP+ (370W)...	Backup	En synchronisation
☐	75f-sw-cn-rennes-067-n2-5130...	H3C Switch	5130-24G-PoE+-4SFP+ (370W)...	5130-24G-PoE+-4SFP+ (370W)...	Backup	En synchronisation
☐	75f-sw-cn-rennes-068-n2-5120...	H3C Switch	5120-8G-PoE+ (65W) SI JG310B	5120-8G-PoE+ (65W) SI JG310B	Backup	En synchronisation

Voici la norme :

[code-orga]-[sw]-[type-site-Nom-Site]-[num]-[niv]-[mod]-*[description]*

[code-orga] = code Organisme sur 3 digits (031 ; 221; 101 ; ….)
[sw] = type de l'équipement (sw : switch)
[type-site-nom-site] =

- Type du site base Ramage sur 2 digits :
  - Siège CPAM : cp
  - CTI (CSM) : cs
  - Siège UGECAM : ug
  - Siège MEDICAL : dr
  - Sites nationaux : cn
  - Agences / établissements :
    - agence : ag
    - établissement : et
- Nom du site : celui de la base Ramage (https://www.cngr.cnamts.fr/rt/organisme/)

[num] = dernier octet de l'@IP de l'interface VLAN ADMIN-RESEAU (Num = 1 si @ip = 55.X.221.1)
[niv] = niveau du switch (N2, N3)
[mod] = modèle de switch (3600, 5510, 5520, 5130, 2930F….)
[description] = optionnel ➔ répartiteur ou local ou baie

Exemples :

SIEGE CPAM :
351-sw-cp-rennes-001-n3-5510-*description*

SIEGES UGECAM :
33G-sw-ug-alsace-010-n2-3600- *description*

SIEGE MEDICAL :
351-dr-normandie-003-n2-3600- *description*

CTI :
94C-sw-cs-cestif-065-n2-3600- *description*

Agence :
351-sw-ag-redon-001-n3-3600

Etablissement :
351-sw-et-redon-001-n3-3600

1.4.3 Cas spécifique des CGSS

Les agences des CGSS ne sont pas dans la base Ramage. Nous proposons le nommage suivant :

XXX-sw-cg-*CGSS*-XXX-nx-3600-site… où CGSS = Réunion, Guadeloupe, Martinique, Guyane, Mayotte

Exemples :

- 974-sw-cg-reunion-001-n3-3600-StLouis pour le site « St Louis »
- 974-sw-cg-reunion-016-n2-3600-StDenis pour le siège
- 973-sw-cg-guyane-106-n2-3600-Cayenne pour le siège
- 973-sw-cg-guyane-106-n2-3600-StLaurent pour le site « St Laurent »

…etc.

1.4.4 Nommage des équipements wifi

Les équipements wifi pourront être ajoutés via le portail R&T. Ils seront provisionnés automatiquement sur Netlix et CENTREON.

Cependant, pour des raisons de licences, seuls les contrôleurs wifi et les contrôleurs virtuels (VIP du cluster IAP) seront intégrés sur CENTREON.

N.B : Toutes les bornes wifi seront enregistrées sur ces outils.

Néanmoins, avec la VIP du cluster IAP, CENTREON pourra afficher l'état des bornes gérées dans le cluster :



Concernant la supervision des bornes rattachées à un contrôleur physique, la supervision pourra se faire directement depuis le contrôleur.

Voici la norme :

- **Contrôleur Wifi**

[code-orga]-cw-[marque]-[type-site-nom-site]-[num]

[code] = code Organisme sur 3 digits (031; 221; 101 …)
[cw] = contrôleur wifi (physique)
[marque] : aruba, cisco …
[type-site-nom-site] =

- Type du site base Ramage sur 2 digits :
  - Siège CPAM : cp
  - CTI (CSM) : cs
  - Siège UGECAM : ug
  - Siège MEDICAL : dr
  - Sites nationaux : cn
  - Agences / établissements :
    - agence : ag
    - établissement : et
- Nom du site : celui de la base Ramage (https://www.cngr.cnamts.fr/rt/organisme/)

[num] = dernier octet de l'@IP de l'interface vlan 902 (Num = 001 si @IP = 55.X.220.1)

Exemple pour la Cnam Rennes:

75f-cw-aruba-cn-rennes-010 (IP : 55.18.220.10)

- **Bornes (y compris le contrôleur Wifi virtuel) :**

[code-orga]-bw-[marque]-[type-site-nom-site]-[num]

[code-orga] = code Organisme sur 3 digits (031; 221; 101 …)
[bw] = @IP borne ou VIP cluster IAP
[marque] = aruba, cisco …
[type-site-nom-site] =

- Type du site base Ramage sur 2 digits :
  - Siège CPAM : cp
  - CTI (CSM) : cs
  - Siège UGECAM : ug
  - Siège MEDICAL : dr
  - Sites nationaux : cn
  - Agences / établissements : voir référentiel « agences » plus bas
- Nom du site : celui de la base Ramage (https://www.cngr.cnamts.fr/rt/organisme/)

[num] = Dernier octet de l'@IP de l'interface vlan 902 (Num = 011 si @IP = 55.X.220.11)

Exemple pour la Cnam Rennes :

Ex : 75f-bw-aruba-cn-rennes-011 (IP : 55.18.220.11)

1.4.5 Description des interfaces d'agrégation et des liens trunks

Description des agrégats ou d'un lien trunk simple :

[type]-[num]-[niv]-[mod]-*[description]*

[type] = type de lien sur 3 digits (AGG; LIEN; ...)
[num] = numéro de l'agrégat (Num = 10, 20, 30,… (Suggestion 10 : 1er étage, 20 : 2ème étage...)
[niv] = vers un Niveau du switch (N2, N3)
[mod] = modèle de switch (3600, 5510, 5520, 5130, 5140, 2930F….)
[description] = optionnel ➔ répartiteur ou baie ou étage ou @IP du switch distant

Exemples :

AGG-010-N2-5130-ETAGE1➔Agrégat numéro 10 vers niveau2 de type HPE5130 du 1er ETAGE
AGG-010-N3-5510-RG ➔ Agrégat numéro 10 vers niveau3 de type HPE5510 du Répartiteur Général

Autres possibilités :

AGG-010-N2-5130-SW-020 ➔ Agrégat numéro 10 vers niveau2 de type HPE5130 @ip 55.xx.221.20
LIEN-010-N2-3600-ETAGE1➔Lien simple numéro 10 vers niveau2 de type HP 3600 du 1er ETAGE

Lien(s) dans un agrégat :

[type]-[num]-[niv]-[mod]-[description]-[N°]

[type] = type de lien sur 3 digits (AGG ;LIEN ;…..)
[num] = numéro de l'agrégat (Num = 10, 20, 30,… (Suggestion 10 : 1er étage, 20 : 2ème étage...)
[niv] = vers un Niveau du switch (N2, N3)
[mod] = modèle de switch (3600, 5510, 5520, 5130, 5140, 2930F….)
[description] = optionnel ➔ répartiteur ou local ou baie ou étage
[lien n°] = lien (lien1, lien2, …. lienN)
Remarque : le nombre de liens dans un agrégat doit toujours être pair et au maximum de 8.

Exemples :

AGG-010-N2-5130-ETAGE1-LIEN1 | description du 1er lien de l'agrégat 10

AGG-010-N2-5130-ETAGE1-LIEN2 | description du 2ème lien de l'agrégat 10

1.4.6 DHCP / DHCP-Relais / DHCP-Snooping

Merci de vous conformer aux procédures de configuration du DHCP **[2]** :

[2]	NA-072-001	*Préconisations DHCP* Service Architecture DR, 1er janvier 2009 http ://www.cngr.cnamts.fr/prodserv/prodserv.php?theme=dhcp

Ce service DHCP installé sur le serveur de proximité Windows doit permettre :
- l'attribution des adresses IP des PMF (pas des serveurs) dans les VLAN de type « PMF » : 4, 18…
- l'attribution des adresses IP des IP Phones dans les VLAN VOIX : 30 …

Veuillez consulter les tableaux des VLAN pour le plan d'adressage et les adresses réservées afin de bien définir les pools DHCP. Vous trouverez ces tableaux plus loin dans ce document.

Pour la ToIP, veuillez aussi consulter les documentations DHCP des constructeurs afin de bien configurer les options nécessaires. Vous trouverez ces documentations sur le portail du DR **rubrique téléphonie**.

Le DHCP-Snooping doit être mis en œuvre. Reportez-vous aux guides de configuration des switches.

1.4.7 SSH

OSE nous impose de sécuriser l'accès aux switches :
- login et mot de passe pour l'accès console
- accès à distance en SSH exclusivement avec login et mot de passe

1.4.8 Spanning-Tree

1.4.8.1 Spanning-tree en central :

Le mode à appliquer sur la gamme des switches HP est le ***RSTP (Rapid Spanning-Tree)***.

Le root du Spanning-Tree doit être configuré et figé. Dans les sièges d'Organismes, il existe obligatoirement deux switches fédérateurs en redondance. Deux cas :

- **Fédérateurs stackés** : il est nécessaire que le stack soit « root –bridge » **(priorité à 0),**

- Fédérateurs non stackés **(cas rare)** : il est nécessaire que le fédérateur maître soit « root-bridge » primaire **(priorité à 0)** et le fédérateur backup soit secondaire **(priorité à 4096).**

Attention : le spanning-tree n'est pas actif par défaut **dans les HP** : il faut l'activer.

1.4.8.2 Spanning-tree au niveau des interfaces des switches

Les mécanismes de limitation du spanning-tree (*edge-port)* et de détection de boucles (*loopback-detection…*) ne seront appliqués que sur les interfaces de connexion des PMF, IP Phones, serveurs, pas au niveau des interfaces d'interconnexion de switches.

Routeurs RAMAGE : le spanning-tree doit être désactivé sur les interfaces des switches face aux routeurs. Reportez-vous aux guides de configuration.

1.4.9 Stackage et interconnexion des switches HP

STACKAGE = EMSTACKMENT PROPRIETAIRE. Chez HP on parle d'IRF.

Les switches HP peuvent se stacker. La procédure est décrite dans les guides de configuration pour chaque gamme.

NB 1 : on ne peut stacker entre eux que des switches HP d'une même gamme
NB 2 : on peut stacker des switches d'une même gamme ayant un nombre de ports différents (des 24 ports avec des 48 ports par exemple).

1.4.10 Interfaces modulaires d'interconnexion des switches

Les interconnexions de switches se font via les ports 1 ou 10 Gb/s en cuivre ou en fibre optique à travers des « trunks ». Lors d'une demande de switches, il ne faut pas oublier de demander aussi des modules SFP côté stack d'extrémité et côté fédérateur.

Une connexion Ethernet en cuivre ou en fibre sur un SFP fonctionne à 1 Gb/s ou ne fonctionne pas : on ne peut pas baisser la vitesse. Idem pour les SFP+ à 10 Gb/s.

SFP (Small Form-factor Pluggable) :

SFP-SX (Fibre optique) : 1 Gb/s	SFP+ (Fibre optique) : 10 Gb/s	SFP-T (cuivre) : 1 Gb/s
		
Connexion d'une jarretière fibre avec Connecteur « LC » de ce côté	Connexion d'une jarretière fibre avec Connecteur « LC » de ce côté	Pour connexion d'une jarretière cuivre avec connecteur RJ45.

1.4.11 Interfaces : speed / duplex

Cas des PMF et des serveurs :

Par défaut chaque interface est configurée de manière à gérer une auto-négociation de débit avec le client connecté. La plupart du temps ce débit est correctement négocié mais il est recommandé de vérifier. Pour cela, il existe sur les HP la commande « display brief interface » qui permet de visualiser rapidement et globalement le débit en cours sur chaque interface.

PRECONISATION DR :

Entre des PMF, des téléphones IP ou des serveurs et des switches, il faut laisser le mode AUTO sur les interfaces du switch. Ensuite, lorsque :

- **le débit négocié est inférieur à celui escompté (vérifier l'état des interfaces)**
- **des erreurs sont constatées sur les interfaces**
- **un quelconque problème apparaît (lenteurs, accès à des ressources…)**

➔ il faut alors le forcer côté switch et côté client.

Exemple sur un stack de 3600-v2 :

```
<3600>dis int brief
The brief information of interface(s) under route mode:
Link: ADM - administratively down; Stby - standby
Protocol: (s) - spoofing
Interface            Link Protocol Main IP         Description
NULL0                UP   UP(s)    --
Vlan901              UP   UP       55.18.221.86

The brief information of interface(s) under bridge mode:
Link: ADM - administratively down; Stby - standby
Speed or Duplex: (a)/A - auto; H - half; F - full
Type: A - access; T - trunk; H - hybrid

Interface    Link Speed   Duplex Type PVID Description
Eth1/0/1     UP   100M    F      A    4    imprimante
Eth1/0/2     UP   100M(a) F      A    4    PMF
Eth1/0/3     UP   100M(a) F(a)   A    4    PMF
```

Lorsque « (a) » est indiqué dans la colonne « SPEED », cela signifie que le port est configuré par défaut en auto-négociation. Si ce « (a) » est absent, cela signifie que la vitesse (speed) et le mode (duplex full ou half) ont été forcés. Dans l'exemple ci-dessus :

- le port 1/0/1 a été forcé à 100 Mb/s – full duplex ;
- le port 1/0/2 a été auto-négocié à 100 Mb/s mais le duplex a été forcé à « full » ;
- le port 1/0/3 a été auto-négocié à 100 Mb/s et full duplex ;

Côté switch cela se configure grâce aux commandes « speed » et « duplex ». Exemple :

```
System-view
Interface 1/0/1
 speed 100
 duplex full
```

Il est conseillé ne pas forcer speed et duplex sur les interfaces de connexion des téléphones IP et sur les téléphones.

1.4.12 Description des interfaces

Il est demandé de préciser une description la plus précise possible sur toutes les interfaces :

- **Routeurs RAMAGE : « ROUTEUR-BTE » ou « ROUTEUR-NXO » (obligatoire)**
- **Interfaces utilisées pour le stackage des HP (ex : 1/0/27, 28…) :**
  - **Description = STACKAGE (obligatoire)**
- Interconnexion de switches : « *Switch-nom* » ou « *3600-IP* » etc…
- Serveur : « Serveur-*nom* »
- Téléphone + PMF : « TEL+PMF-*nom* »
- PMF : « PMF-*nom* »

- Etc … Badgeuse, Borne, Caméra…
- Agrégats et lien trunks

Les règles de nommage sont décrites dans la suite du document.

Exemples :

interface GigabitEthernet1/0/1 des ROUTEUR-BTE	interface Ethernet1/0/2 des TEL+PMF – F. Pignon	interface GigabitEthernet1/0/25 des LIEN-01-N2-3600-86-RG-LIEN1

1.4.13 Shutdown des interfaces non utilisées

Pour des raisons de sécurité, au moins dans les lieux sensibles comme les accueils… (possibilité pour un inconnu de se connecter au réseau sur une prise dans les lieux ouverts au public, possibilité de connecter un PC « non PLC » ou un hub ou un switch ou un sniffer sur une prise libre dans son bureau….) :

⇨ **il est préconisé de mettre à « shutdown » toutes les interfaces Ethernet et GigaEthernet non utilisées.**

1.4.14 Câblage

Avant toute rénovation d'un LAN, il est essentiel de s'assurer de la conformité du pré câblage aux préconisations du DR. Vous les trouverez sur le portail du DR : http ://www.cngr.cnamts.fr rubrique « CÂBLAGE ».

1.4.15 Version logicielle des switches

Les versions **minimum** normalisées sont disponibles sur le site du DR : le portail du DR : http ://www.cngr.cnamts.fr rubrique Infrastructure ➔ LAN ➔ Versions. Une version est disponible pour chaque gamme de switches.
De nouvelles versions logicielles de switches seront mises à disposition au moins une fois par an. Elles devront être alors déployées dès que possible.

1.4.16 LLDP

LLDP = Link Layer Discovery Protocol : protocole standard (802.1ab). Permet la découverte des topologies réseau de proche en proche.

► Commande intéressante HP : display lldp neighbor-information [brief] [interface] [list]

Il est demandé de valider LLDP dans tous les switches HP avec la commande : lldp enable

1.4.17 Interfaces / usages

Interconnexion de switches :

Les interfaces d'interconnexion de switches doivent être configurées en mode « TRUNK 802.1q » à 1 Gb/s minimum en cuivre ou en fibre optique. Chaque trunk doit être limité aux vlan à distribuer sur le ou les switches distants :

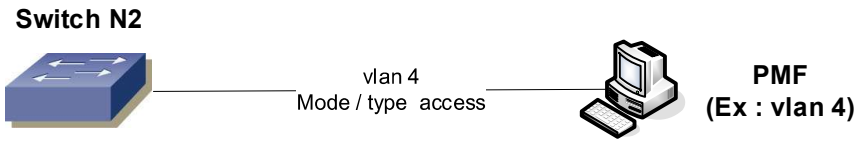
➔ notion de « trunk permit VLAN X Y Z » en HP.

Dès que c'est possible, les switches seront interconnectés entre eux via des agrégations de liens à n x 2 Gb/s, (n = 1, 2 ou 4 (maximum)) – pour les HP 55X0 et HP 3600 et à 2 x 10 Gb/s pour les HP 55X0 et HP 51X0.

PMF seul :

Nous ne fournissons que des switches POE pour les connexions d'extrémité. Les PMF sont à connecter sur des switches HP POE 24 ou 48 ports à 10/100 voire 10/100/1000 Mb/s :

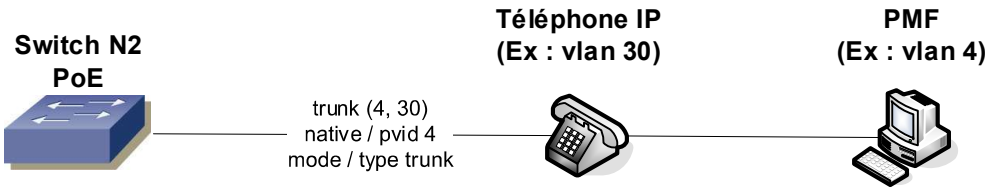
Exemple avec VLAN 4 :



Téléphone IP + PMF :

Dans le cas de la ToIP, les téléphones IP sont à connecter sur des switches HP 24 ou 48 ports **PoE** à 10/100 voire 10/100/1000 Mb/s. Les PMF sont alors connectés aux téléphones. Veuillez-vous reporter aux procédures de configuration des téléphones. Le trunk doit être limité à 2 VLAN (celui du téléphone et celui du PMF) :

Cas général – exemple avec les VLAN 4 et 30 :



Serveurs :

Dans la plupart des cas, les serveurs, physiques ou virtuels, sont dans le même VLAN (le VLAN 4). Les ports de switches doivent être configurés en « link-type access ».

Certaines applications (téléphonie Asterisk par exemple…) utilisent des serveurs virtuels et plusieurs VLAN parmi les VLAN normalisés (4, 30 par exemple). Dans ce cas, les serveurs seront connectés sur des ports en mode « trunk ». Pour la connexion des serveurs VMWare, veuillez suivre les recommandations de la procédure de connexion des ESX dans les guides :

https ://www.cngr.cnamts.fr rubrique Infrastructure / LAN / HP ➔ AGREGAT ESX/HP.

Une extraction via GEDIFF montre que le nombre de serveurs est très variable mais souvent faible. En fonction de leur nombre et de leur « capacité gigabit », les serveurs pourront être connectés sur :

- un switch HP 51X0

ou

- un cluster de 2 (maximum) switches HP 51X0 stackés lorsque le nombre de serveurs est important

ou

- directement sur les fédérateurs :
  - si les serveurs sont dans le local hébergeant les fédérateurs (Répartiteur Général)
  - et que suffisamment d'interfaces sont libres sur les fédérateurs

En effet, des switches Gigabits ne seront donc pas systématiquement attribués dans ce cas.

Au maximum, 2 HP 51X0 24 ports seront attribués dans les sièges d'organismes.

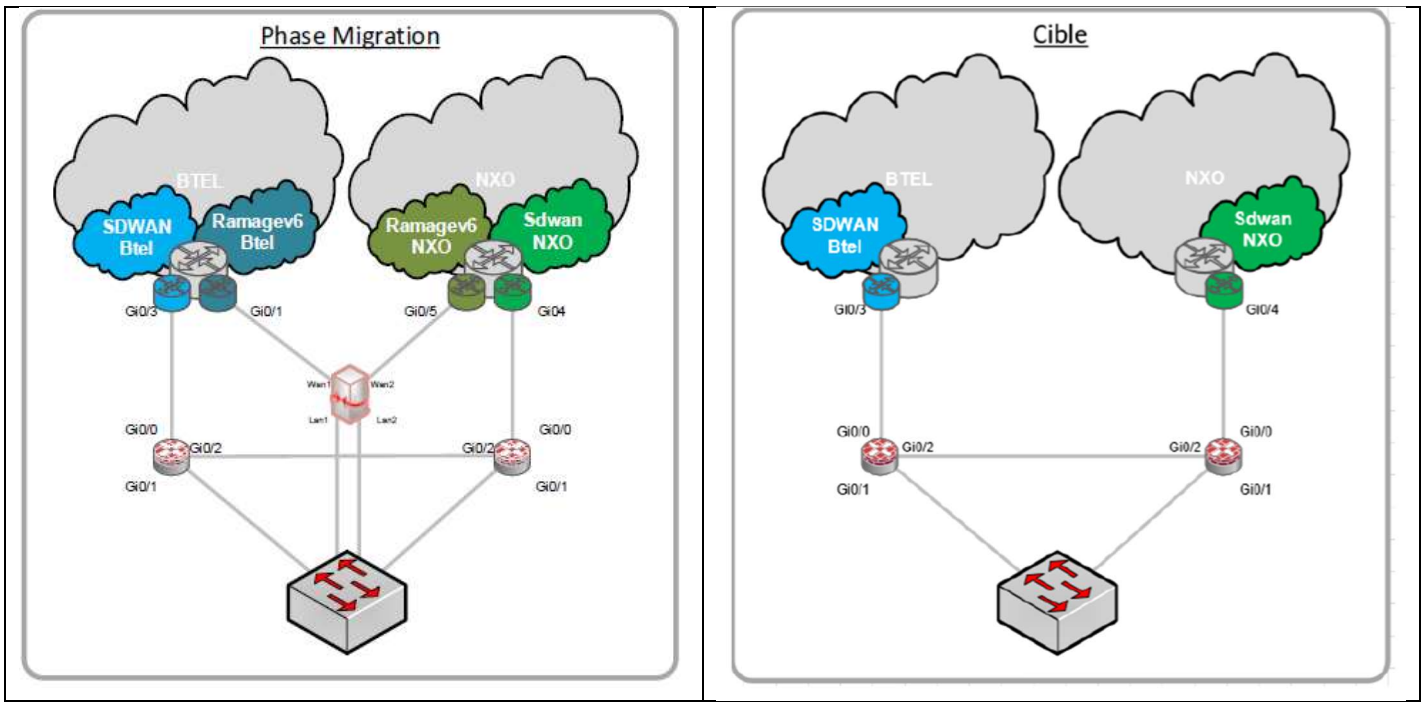
Les serveurs sont des « Bundle 1 » ou des « Bundle 2 » possédant 1 carte avec 4 ou 8 interfaces gigabit. Il n'est pas nécessaire de connecter les 4 ou 8 interfaces : 2 interfaces connectées en redondance sur deux switches doivent suffire.
Il ne sera pas attribué de switches gigabit pour la connexion des interfaces ILO. **Si besoin**, l'interface ILO devra être connectée sur un port de switch 10/100 Mb/s (HP 3600) ou un port gigabit cuivre du 51X0 non utilisé.

Les CPAM ayant fusionné et qui ont conservé une annexe administrative importante (sur le site de l'autre siège) pourront être dotées d'un switch pour les serveurs si nécessaire et durable.

1.5 RACCORDEMENT DES SITES A RAMAGE

1.5.1 SDWAN – OSPF

1.5.1.1 L'architecture SDWAN



1.5.1.2 Les ports mis en jeu avec SDWAN

- •Le port **Gi0/0** du boitier SDWAN 1 sera raccordé sur le port Gi0/3 du routeur BTEL
- •Le port **Gi0/0** du boitier SDWAN 2 sera raccordé sur le port Gi0/4 du routeur NXO
- •Les deux boitiers SDWAN devront être raccordés entre eux sur leur port **Gi0/2**
- •Le port **Gi0/1** de chaque boitier sera raccordé sur les nouveaux ports du switch niveau 3 (si vous avez un STACK de switch N3 nous recommandons de raccorder un boitier sur chaque switch).

Remarques :

Dans **la phase de migration** les routeurs opérateurs sont biconnectés (aux switches N3, sonde Ipanema) et la sonde ipanema est toujours en place.

Dans **la phase cible** les routeurs opérateurs sont monoconnectés (aux switches N3) et il n'y a plus de sonde ipanema

1.5.1.3 Routages / SDWAN

► Les fédérateurs (niveau 3) :

- ont une interface VLAN pour chaque VLAN à router
- ont une adresse IP sur chaque interface VLAN à router

➔ cela permet la commutation de niveau 3 entre les VLAN

- **Avec le projet SDWAN, le routage est configuré dans les switches par le Département Réseau.**
- **Le protocole utilisé est OSPF**
- **Vous ne devez pas modifier la configuration OSPF**

Pour information voici un exemple de configuration OSPF :

```
#Définition du process OSPF
ospf 100 router-id 55.248.X.X
 import-route direct type 1 route-policy DIRECT-TO-OSPF
 import-route static type 1 route-policy STATIC-TO-OSPF
 area 0.0.0.100
  network 172.X.X.X 0.0.0.0


#Route Policy pour l'export des routes locales
route-policy DIRECT-TO-OSPF permit node 10
 if-match acl 2922
 apply tag 100
route-policy STATIC-TO-OSPF permit node 10
 if-match acl 2922
 apply tag 100
```

1.5.2 RV6 - BGP

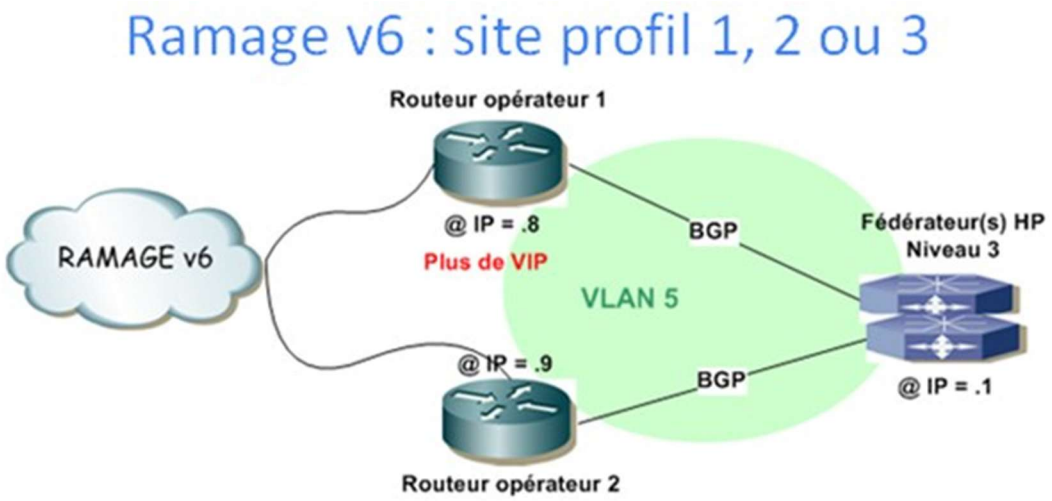
1.5.2.1 Switches fédérateurs compatibles ramage v6

Dans les Organismes, selon la taille du site, on trouvera obligatoirement les switches fédérateurs HP suivants :

- Switch 3600-24 seul
- Switch 3600-48 seul
- Stack de 3600-24
- Stack de 3600-48
- Stack de 5510-24G
- Stack de 5510-24G-SFP
- Stack de 5520-24G
- Stack de 5520-24G-SFP
- Stack de 58XX
- Stack de 57XX

Attention : les HP 51X0 (5130 et 5140) en fédérateurs ne sont pas compatibles Ramage v6 car ils ne supportent pas le protocole BGP !! Vous devez demander dès que possible leur remplacement au DR via le PSN.

1.5.2.2 Sites sans sonde



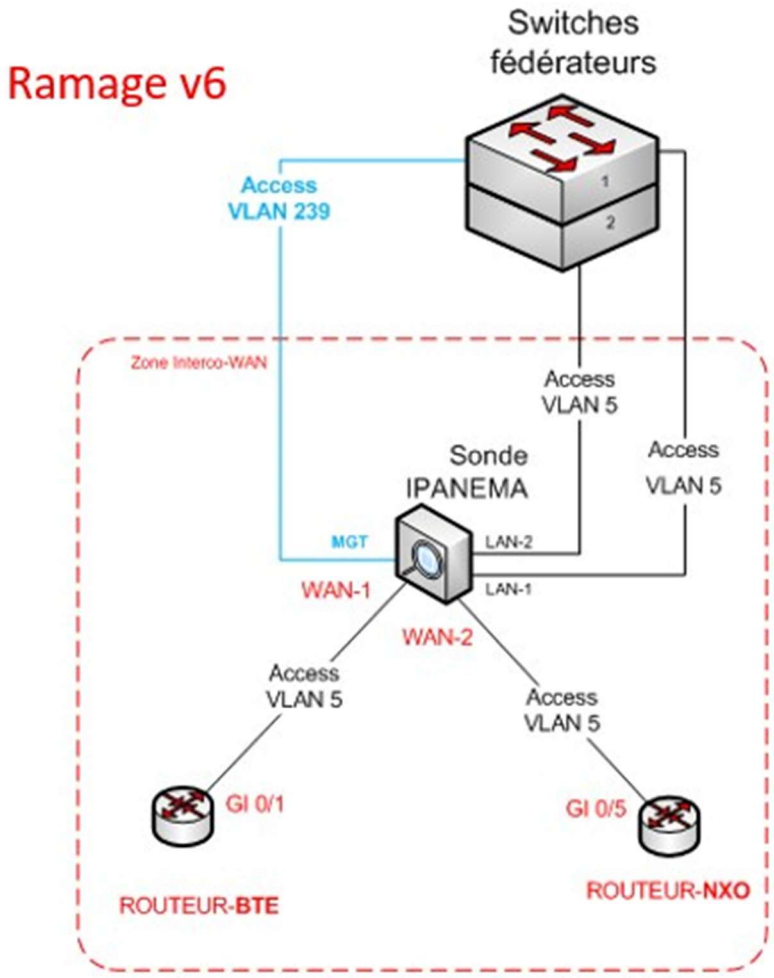
*** NB : cas particulier, si le débit proposé sur l'un des accès opérateur est en FTTH (possiblement supérieur à 100Mb/s) alors le DR vous contactera pour confirmer le port GIGABIT à utiliser sur le switch N3.**

1.5.2.3 Sites avec sonde

Dans le cas où une SONDE est mise en place, elle s'intercale entre le(s) routeur(s) et les switch(es) fédérateurs via les ports WAN1, WAN2, LAN1 et LAN2. Une interface de management est à connecter dans le vlan 239.

Connectez TOUJOURS :

- **Le routeur BTE sur le port WAN-1 de la sonde**
- **Le routeur NXO sur le port WAN-2 de la sonde**



➔ Consulter les guides de configuration pour la mise en œuvre.

⚠ **La présence d'une sonde ne change aucunement la configuration des interfaces de switches face aux routeurs. La sonde est « transparente ».**

1.5.2.4 La connexion et le nommage des routeurs sur les switches sont normalisés !

La normalisation reste la même pour Ramage v5 et Ramage v6. Dans le cas où des adaptations sur certains sites seraient judicieuses, le DR vous contactera.

Sur tous les sites (sauf exception gérée par le DR) :

- Les ports des switches face aux routeurs RAMAGE doivent être forcés à 100 FULL (sauf FTTH à 1000 Full)
- Le spanning-tree doit être désactivé
- Profils 1, 2, et 3 : les descriptions doivent être « ROUTEUR-BTE » et « ROUTEUR-NXO »
- Profils 4 : la description doit être « ROUTEUR-BTE » (4a) **ou** « ROUTEUR-NXO » (4b)

Les routeurs des opérateurs devront être connectés sur des ports normalisés. De même, pour qu'un routeur 4G puisse être mis rapidement en service, il faut laisser libre et préparer une interface, elle aussi normalisée :

Sont listés ci-dessous les différents cas d'architecture que l'on trouve dans les Organismes. Pour chaque site, appliquez obligatoirement la norme.

1.5.2.5 Accès Ramage v6 SANS FTTH :

Le but est de connecter les routeurs Ramage v6 à la place des routeurs Ramage v5 pour faciliter la migration.

CAS STANDARD – LES FEDERATEURS SONT EN STACK :

FEDERATEURS EN STACK

Cas d'un switch N3 seul

			Interfaces normalisées sur le switch pour la connexion des routeurs						
			Switches HP à ports RJ45				Switches HP à ports Fibre		Description
PROFILS	Gammes de switches ==>		3600	5500	5800	5510	5500	5510	-
Profils 1, 2 et 3	port 1 Routeur BTE		ET 1/0/1	GI 1/0/1	GI 1/0/1	GI 1/0/1	GI 1/0/25	GI 1/0/24	ROUTEUR-BTE
(2 opérateurs)	Port 5 routeur NXO		ET 1/0/2	GI 1/0/2	GI 1/0/2	GI 1/0/2	GI 1/0/26	GI 1/0/23	ROUTEUR-NXO
Profil 4	Profil 4a (BTE)	port 1 Routeur BTE	ET 1/0/1	GI 1/0/1	GI 1/0/1	GI 1/0/1	GI 1/0/25	GI 1/0/24	ROUTEUR-BTE
(1 opérateur)	Profil 4b (NXO)	Port 5 routeur NXO	ET 1/0/2	GI 1/0/2	GI 1/0/2	GI 1/0/2	GI 1/0/26	GI 1/0/23	ROUTEUR-NXO

Cas d'un stack N3

			Interfaces normalisées sur le STACK de N switches pour la connexion des routeurs						
			Switches HP à ports RJ45				Switches HP à ports Fibre		Description
PROFILS	Gammes de switches ==>		3600	5500	5800	5510	5500	5510	-
Profils 1, 2 et 3	port 1 Routeur BTE		ET 1/0/1	GI 1/0/1	GI 1/0/1	GI 1/0/1	GI 1/0/25	GI 1/0/24	ROUTEUR-BTE
(2 opérateurs)	Port 5 routeur NXO		ET N/0/1	GI N/0/1	GI N/0/1	GI N/0/1	GI N/0/25	GI N/0/24	ROUTEUR-NXO
Profil 4	Profil 4a (BTE)	port 1 Routeur BTE	ET 1/0/1	GI 1/0/1	GI 1/0/1	GI 1/0/1	GI 1/0/25	GI 1/0/24	ROUTEUR-BTE
(1 opérateur)	Profil 4b (NXO)	Port 5 routeur NXO	ET N/0/1	GI N/0/1	GI N/0/1	GI N/0/1	GI N/0/25	GI N/0/24	ROUTEUR-NXO

N = numéro du dernier switch du stack

⇨ **ET configuration à 100 FULL.**

1.5.2.6 Accès Ramage v6 AVEC FTTH :

CAS STANDARD – LES FEDERATEURS SONT DES HP 55X0 ou 58X0 :

Cas d'un switch N3 seul

			Interfaces normalisées sur le switch pour la connexion des routeurs					
			Switches HP à ports RJ45			Switches HP à ports Fibre		Description
PROFILS	Gammes de switches ==>		5500	5800	5510-24 ou 48	5500	5510-24	-
Profils 2 et 3 (2 opérateurs)	Un des 2 opérateurs est en FTTH	port 1 Routeur BTE	GI 1/0/1	GI 1/0/1	GI 1/0/1	GI 1/0/25	GI 1/0/24	ROUTEUR-BTE
		Port 5 routeur NXO	GI 1/0/2	GI 1/0/2	GI 1/0/2	GI 1/0/26	GI 1/0/23	ROUTEUR-NXO
Profil 4 (1 opérateur)	Profil 4a (BTE)	port 1 Routeur BTE FTTH	GI 1/0/1	GI 1/0/1	GI 1/0/1	GI 1/0/25	GI 1/0/24	ROUTEUR-BTE
	Profil 4b (NXO)	Port 5 routeur NXO FTTH	GI 1/0/2	GI 1/0/2	GI 1/0/2	GI 1/0/26	GI 1/0/23	ROUTEUR-NXO

Cas d'un stack N3

			Interfaces normalisées sur le STACK de N switches pour la connexion des routeurs					
			Switches HP à ports RJ45			Switches HP à ports Fibre		Description
PROFILS	Gammes de switches ==>		5500	5800	5510-24 ou 48	5500	5510-24	-
Profils 2 et 3 (2 opérateurs)	Un des 2 opérateurs est en FTTH	port 1 Routeur BTE	GI 1/0/1	GI 1/0/1	GI 1/0/1	GI 1/0/25	GI 1/0/24	ROUTEUR-BTE
		Port 5 routeur NXO	GI N/0/1	GI N/0/1	GI N/0/1	GI N/0/25	GI N/0/24	ROUTEUR-NXO
Profil 4 (1 opérateur)	Profil 4a (BTE)	port 1 Routeur BTE FTTH	GI 1/0/1	GI 1/0/1	GI 1/0/1	GI 1/0/25	GI 1/0/24	ROUTEUR-BTE
	Profil 4b (NXO)	Port 5 routeur NXO FTTH	GI N/0/1	GI N/0/1	GI N/0/1	GI N/0/25	GI N/0/24	ROUTEUR-NXO

N = numéro du dernier switch du stack

⇨ **ET configuration à 1000 FULL.**

1.5.2.7 CAS DE FEDERATEURS HP 3600 :

Lors de la MISE EN PRODUCTION (MEP), il faut changer de port et utiliser un port à 1 GB/S (à préconfigurer).

⇨ **Configuration à 1000 FULL.**

1.5.2.7.1 FTTH avec BTE :

Cas d'un switch N3 seul

			Interfaces normalisées sur le switch pour la connexion des routeurs		
			Switches HP à ports RJ45		Description
PROFILS	Gammes de switches ==>		3600-24	3600-48	-
Profils 2 et 3 (2 opérateurs)	port 1 routeur BTE FTTH		GI 1/0/25	GI 1/0/49	ROUTEUR-BTE
	Port 5 routeur NXO		ETH 1/0/2	ETH 1/0/2	ROUTEUR-NXO
Profil 4	Profil 4a (BTE)	port 1 Routeur BTE FTTH	GI 1/0/25	GI 1/0/49	ROUTEUR-BTE

Cas d'un stack N3

			Interfaces normalisées sur le STACK de N switches pour la connexion des routeurs		
			Switches HP à ports RJ45		Description
PROFILS	Gammes de switches ==>		3600-24	3600-48	-
Profils 2 et 3 (2 opérateurs)	port 1 routeur BTE FTTH		GI 1/0/25	GI 1/0/49	ROUTEUR-BTE
	Port 5 routeur NXO		ETH N/0/1	ETH N/0/1	ROUTEUR-NXO
Profil 4	Profil 4a (BTE)	port 1 Routeur BTE FTTH	GI 1/0/25	GI 1/0/49	ROUTEUR-BTE

N = numéro du dernier switch du stack

1.5.2.7.2 FTTH avec NXO :

Cas d'un switch N3 seul

PROFILS	Gammes de switches ==>		Interfaces normalisées sur le switch pour la connexion des routeurs		
			Switches HP à ports RJ45		Description
			3600-24	3600-48	-
Profils 2 et 3 (2 opérateurs)	port 1 routeur BTE		ETH 1/0/1	ETH 1/0/1	ROUTEUR-BTE
	Port 5 routeur FTTH NXO		GI 1/0/26	GI 1/0/50	ROUTEUR-NXO
Profil 4	Profil 4b (NXO)	Port 5 routeur FTTH NXO	GI 1/0/26	GI 1/0/50	ROUTEUR-NXO

Cas d'un stack N3

PROFILS	Gammes de switches ==>		Interfaces normalisées sur le STACK de N switches pour la connexion des routeurs		
			Switches HP à ports RJ45		Description
			3600-24	3600-48	-
Profils 2 et 3 (2 opérateurs)	port 1 routeur BTE		ETH 1/0/1	ETH 1/0/1	ROUTEUR-BTE
	Port 5 routeur FTTH NXO		GI N/0/26	GI N/0/50	ROUTEUR-NXO
Profil 4	Profil 4b (NXO)	Port 5 routeur FTTH NXO	GI N/0/26	GI N/0/50	ROUTEUR-NXO

N = numéro du dernier switch du stack

⇨ **ET configuration à 1000 FULL.**

1.5.2.8 Routeurs XG (4G / 5G):

- **Switch ou Stack HP 3600 ou HP 55X0 ou HP 58X0 ou HP 55X0 CUIVRE (24 ou 48 ports RJ45) :**

► Le ROUTEUR-XG est à connecter :
- SI STACK : sur le port 1/0/2 du fédérateur maitre
- SI SWICH SEUL et pas de routeur secours : sur le port 1/0/2 du switch
- SI SWICH SEUL et routeur secours : sur le port 1/0/3 du switch

- Stack de HP 55X0-SFP FIBRE OPTIQUE ayant 24 ports SFP ou 16 ports SFP +8 ports RJ45 :

► Le ROUTEUR-XG est à connecter sur :
- SI STACK : sur le port 1/0/26 du fédérateur maitre
- SI SWITCH SEUL et pas de routeur secours : sur le port 1/0/26 du switch
- SI SWITCH SEUL et routeur secours : sur le port 1/0/27 du switch

- Stack de HP 55X0G-24-SFP-EI FIBRE OPTIQUE (24 ports SFP ou 16 ports SFP +8 ports RJ45) :

► Le ROUTEUR-XG est à connecter :
- SI STACK : sur le port 1/0/23 (RJ45) du fédérateur maitre
- SI SWITCH SEUL et pas de routeur secours : sur le port 1/0/23 du switch
- SI SWITCH SEUL et routeur secours : sur le port 1/0/22 du switch

Stack de HP 55X0G-24-SFP-EI FIBRE OPTIQUE (24 ports SFP ou 16 ports SFP +8 ports RJ45) :

► Le ROUTEUR-XG est à connecter :
- SI STACK : sur le port 1/0/23 (RJ45) du fédérateur maitre
- SI SWITCH SEUL et pas de routeur secours : sur le port 1/0/23 du switch
- SI SWITCH SEUL et routeur secours : sur le port 1/0/22 du switch

En fonction du contexte, les configurations à mettre en œuvre dans le cas de l'utilisation d'un routeur 4G sont décrites sur le portail du DR (Rubrique Infrastructure / WAN / Offre 4G).

1.5.2.9 Routages / RV6

► Les fédérateurs (niveau 3) :

- ont une interface VLAN pour chaque VLAN à router
- ont une adresse IP sur chaque interface VLAN à router

➔ cela permet la commutation de niveau 3 entre les VLAN

Avec Ramage v6, le routage est configuré dans les switches par le Département Réseau.
Le protocole RIP utilisé pour Ramage v5 a été remplacé par le protocole e-BGP.

Vous ne devez pas modifier cette configuration e-BGP.

Le RIP et les routes statiques seront aussi supprimées par le DR le moment venu.

► Les switches d'extrémité (HP 3600, HP 5130, HP 5140, Aruba 2930F) :

- n'ont qu'une seule interface VLAN : celle du VLAN 901
- n'ont qu'une seule adresse IP : sur l'interface VLAN 901
- n'ont qu'une seule route (0.0.0.0 0.0.0.0) vers l'interface VLAN 901 du fédérateur

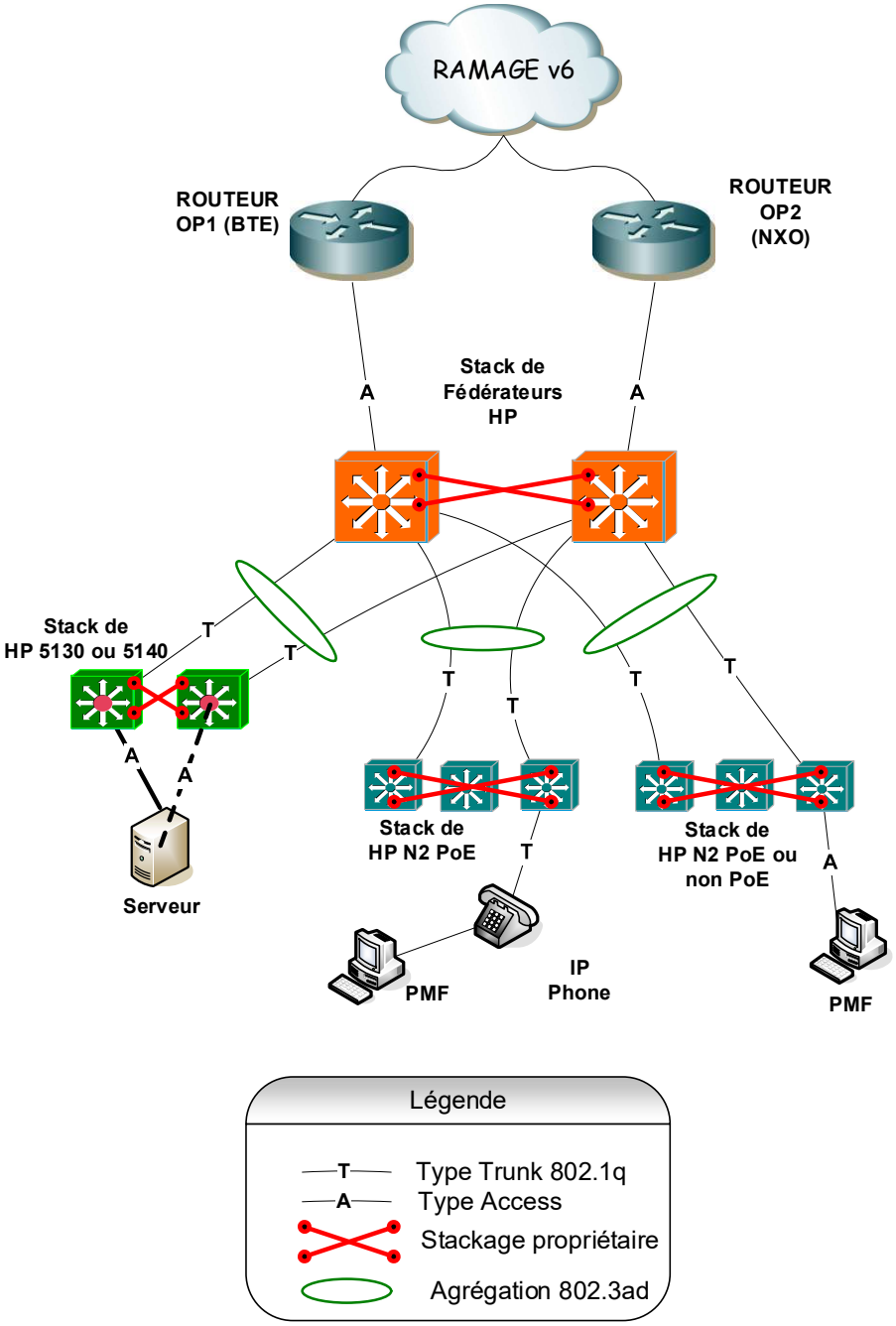
► Cas particuliers

Dans les sites où il n'y a qu'un switch ou un seul stack (donc niveau 3), le vlan 901 ne peut pas être utilisé car il ne monterait pas (aucune interface ou trunk dans le VLAN 901), il faut alors utiliser une interface virtuelle : loopback 1.

1.6 ARCHITECTURES TYPES

1.6.1 Architecture type EN SIEGE d'Organisme

- ► Fédérateurs stackés (HP 5510, 5520)
- ► 2 switches gigabit maximum (HP 5130 ou 5140) pour les serveurs
- ► Switches HP PoE stackés à l'extrémité (HP 3600, 5130 ou 5140)



1.6.2 Architecture EN SIEGE d'Organisme : interconnexion 55XX /51XX

Dans certains sièges, les HP 3600 ont été remplacés par des HP 5130 ou HP 5140. De même que les fédérateurs HP 55XX, ces switches possèdent 4 ports 10 Gb/s dont :

- 2 sont utilisés pour le stackage
- 2 sont disponibles pour les interconnexions de switches

Les deux méthodes suivantes peuvent être utilisées :

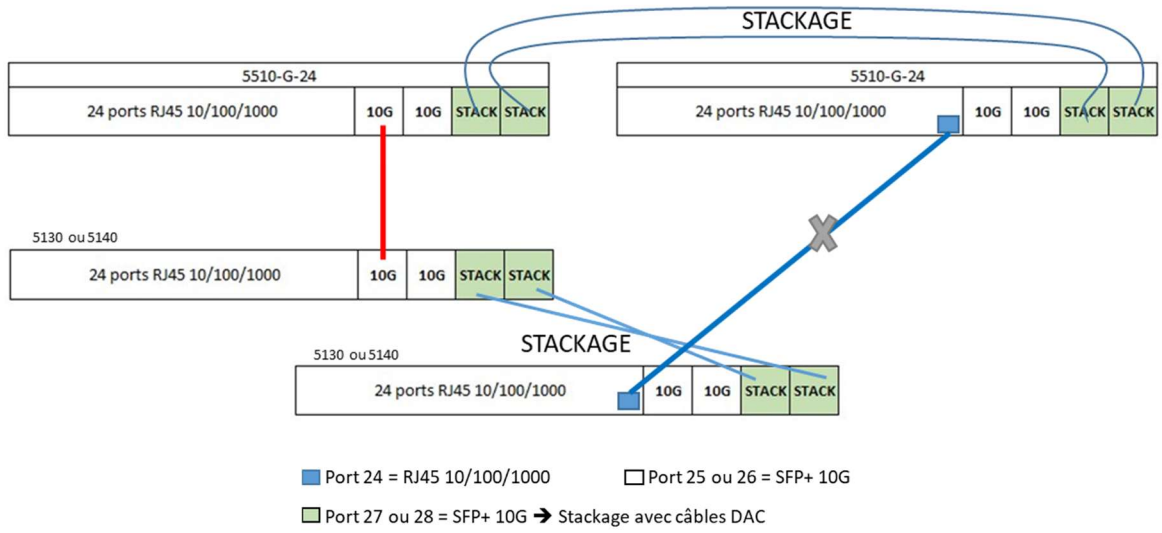
Interconnexion de 2 stacks de 55XX / 51XX via agrégat 2 X 10 Gb/s :

Il n'est possible de connecter que 2 stacks de 51XX via un agrégat à 2 x 10 Gb/s sur le N3 55XX.
S'il n'y a que 2 stacks de 51XX, on utilisera obligatoirement cette méthode.

S'il y a plus que 2 stacks de 51XX, la méthode ci-dessous est préférable mais il est possible néanmoins de choisir cette méthode : on identifiera les 2 stacks de 51XX les plus importants (stack vers 51XX « Serveurs » notamment), les autres stacks de 51XX seront alors connectés via un AGG à N x 1 Gb/s.

Interconnexion de 4 stacks de 55XX / 51XX via des liens simples à 10 Gb/s secourus en 1 Gb/s :

S'il y a plus que 2 stacks de 51XX, il est possible d'en connecter 4 via un lien à 10 Gb/s secouru par un lien à 1 Gb/s, les autres stacks de 51XX seront alors connectés via un AGG à N x 1 Gb/s. La méthode est shématisée ci-dessous :

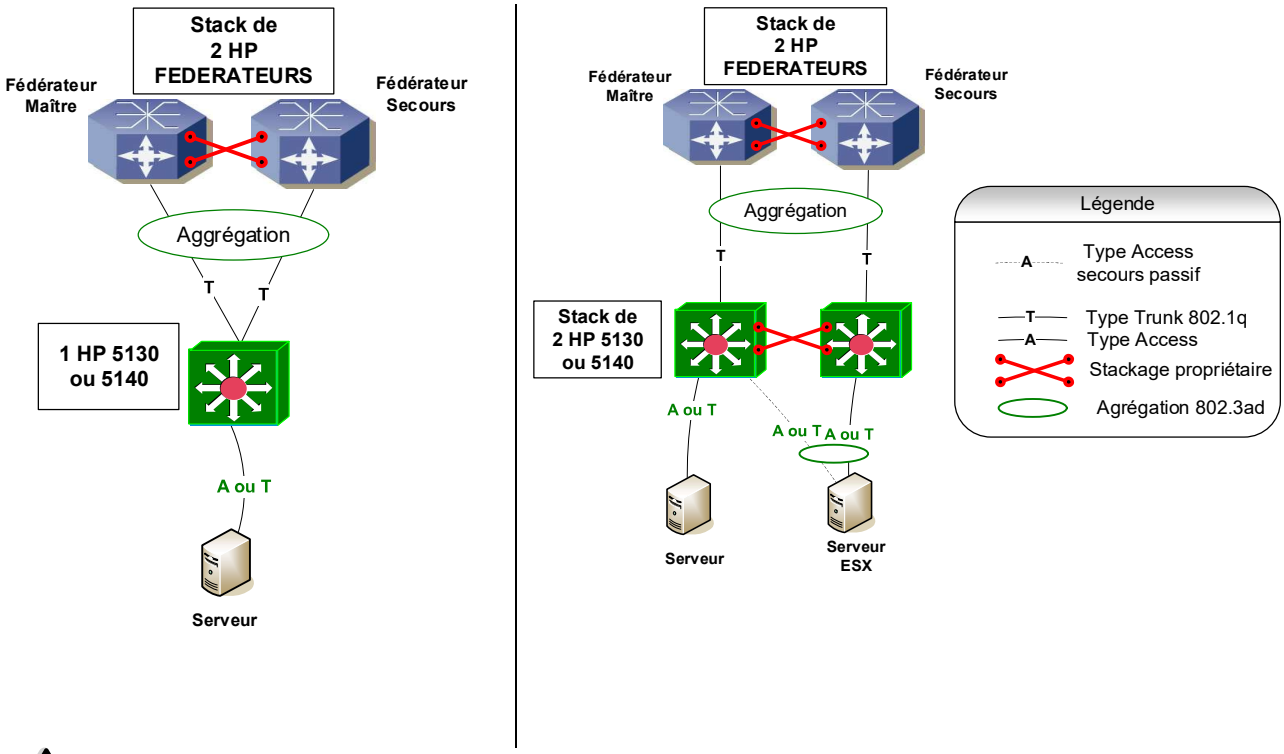


Tant que le lien à 10 Gb/s est actif, **le spanning-tree va bloquer le lien à 1 Gb/s**.

Si le lien à 10 Gb/s tombe, le lien à 1 Gb/s montera immédiatement et la coupure sera négligeable.

1.6.3 Architecture pour les serveurs EN SIEGE d'Organisme

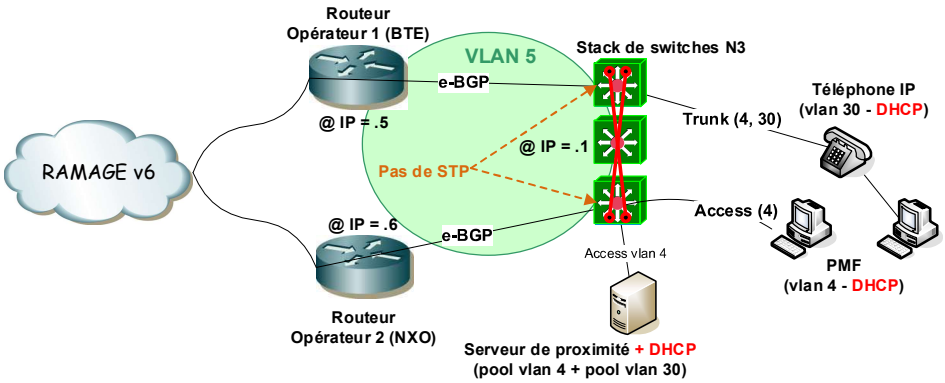
Ci-dessous, des architectures normalisées pour les serveurs



⚠ **SPECIAL ESX : Si le serveur est un ESX, il faut construire un agrégat ESX/HP. Une procédure spécifique est à disposition sur le portail du DR https://www.cngr.cnamts.fr rubrique Infrastructure / LAN / HP ➔ AGREGAT ESX/HP :**

1.6.4 Architectures en AGENCE et ETABLISSEMENT

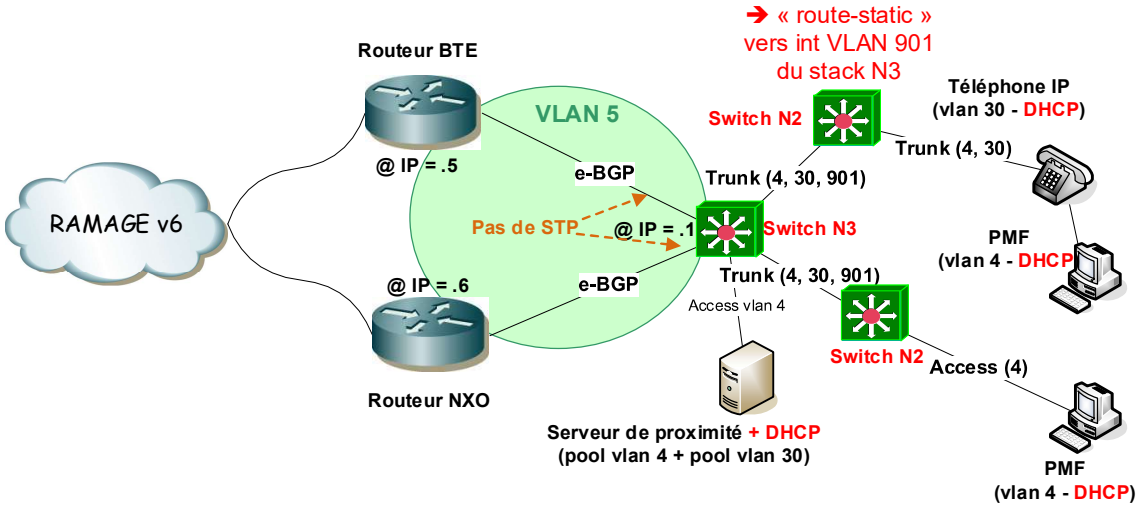
Cas 1 : répartiteur unique :



Dans ce cas, le VLAN d'ADMIN-RESEAU sera remplacé par une interface loopback1.

Cas 2 : plusieurs répartiteurs non maillés :

Il n'est pas toujours possible de monter un stack redondé même en utilisant le pré câblage et les ports 25 des 3600 (il manque un lien entre deux répartiteurs pour redonder).



Un seul HP A3600 assurera des fonctionnalités de niveau 3. Les autres switches n'auront qu'une seule interface VLAN, l'interface VLAN 901..

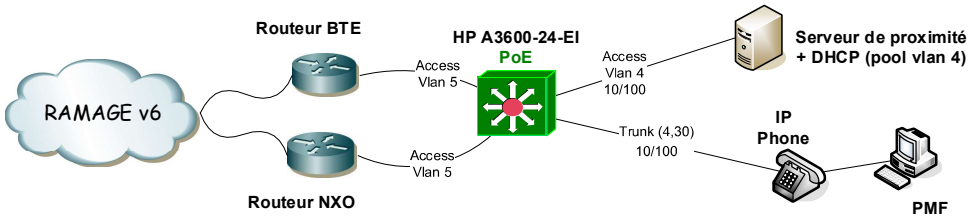
NB : pour les profils 4a et 4b de Ramage v6, il n'y aura qu'un seul routeur.

Autres cas :

Les schémas suivants représentent les différents types de montages que l'on doit retrouver dans les CP. A chaque fois 2 routeurs opérateurs sont représentés ; lorsqu'il n'y en a qu'un, le lien avec le deuxième routeur n'existe pas.

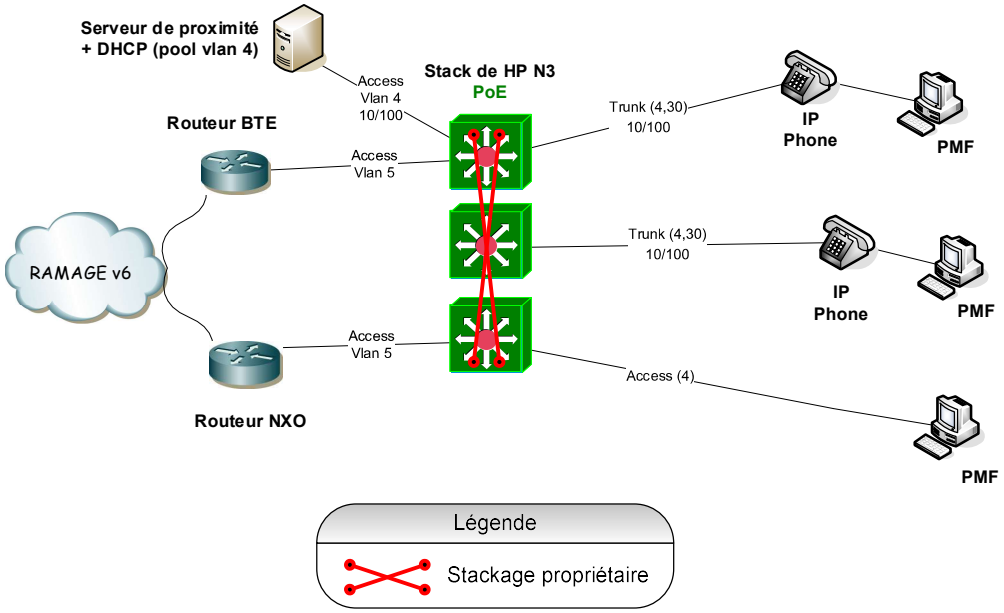
En cas de spécificités locales différentes de ces stanadards, contactez le DR.

CAS 1 : Moins de 24 clients au total (téléphones + serveur(s) + routeurs + PMF) :



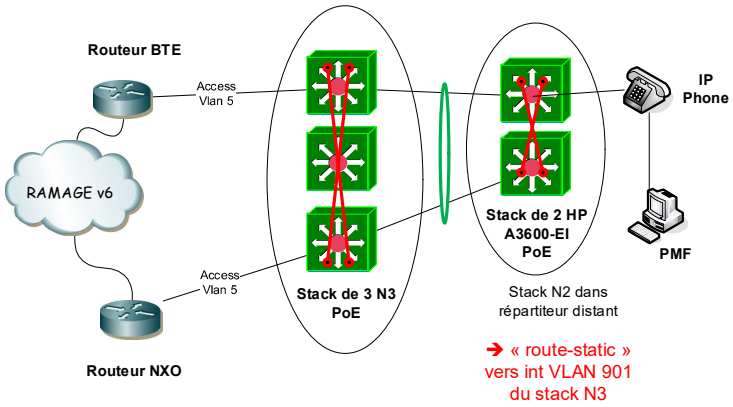
Dans ce cas, le VLAN d'ADMIN-RESEAU sera remplacé par une interface loopback1.

CAS 2 : Jusqu'à 6 switches 24 ports ou 6 switches 48 ports (limite conseillée du nombre de switchs par pile) :



CAS 3 : si, pour des raisons techniques ou de taille, un petit site est équipé de plusieurs stacks :

- 1 stack ou 1 switch fédérateur N3
- N stacks ou N switches d'extrémité N2

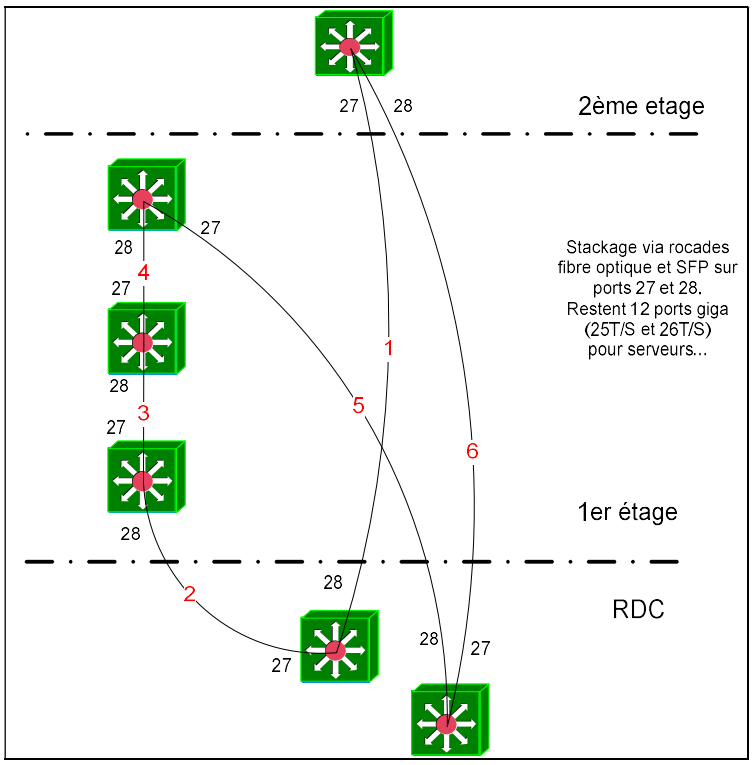


Il est nécessaire dans ce cas de configurer une route statique pour assurer la communication entre les switches ou stacks d'extrémité et les HP 3600 de niveau 3 fédérateurs. Cela va être fait grâce à une route statique par défaut via l'adressage du VLAN 901.

CAS 4 : un seul stack N3 via rocades (si pas trop de répartiteurs) :

Dans le cas ci-dessus, on peut tout aussi bien ne faire qu'un seul stack de niveau 3 utilisant les rocades cuivre (ports 25T (ou 49T)) ou fibre optique (port 27/28 (ou 51/52) avec des SFP SX).

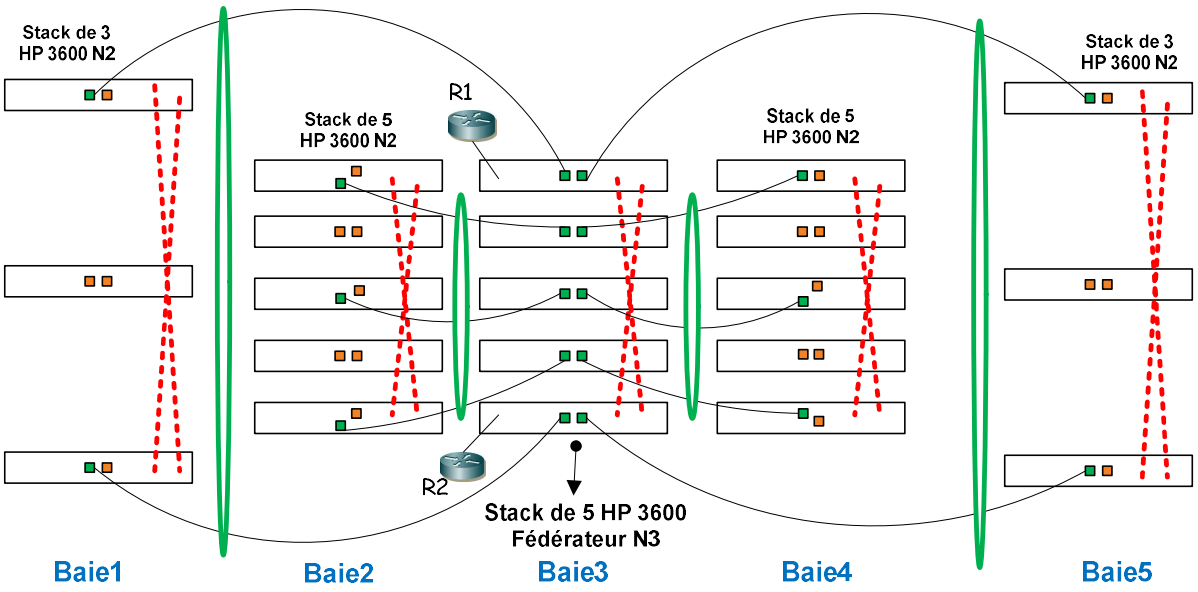
Exemple avec un bâtiment de 3 étages disposant chacun d'un répartiteur. Les répartiteurs du 2ème et du 1er sont reliés à celui du RDC via fibre optique. On peut monter un seul stack de cette manière.



Dans ce cas, le VLAN d'ADMIN-RESEAU sera remplacé par une interface loopback1.

CAS 5 : un stack N3 dans un répartiteur unique (ou pas …) avec plusieurs baies :

Dans ce cas, on construira un stack de 3600 N3 en central interconnecté via des agrégats doubles ou triples à des stacks de 3600 N2. Il restera de nombreux ports 10/100/1000 Mb/s pour des serveurs (en orange) :



Il est nécessaire dans ce cas de configurer une route statique pour assurer la communication entre les switches ou stacks d'extrémité et les 3600 niveau 3 fédérateurs. Cela va être fait grâce à une route par défaut via l'adressage du VLAN 901.

1.7 CAS DU VLAN-ACCESS-PART (PARTENAIRES)

Le VLAN 224 est le premier VLAN créé pour l'accès d'un partenaire extérieur (projet Egfa). **Il est dédié à tous les partenaires se connectant via l'accès partenaire de Ramage**. Dans le cadre de projets nationaux, d'autres VLAN seront utilisés.

Tous les VLAN accédés à distance par un partenaire extérieur doivent être validés par la DS.

Voir : https://www.cngr.cnamts.fr/contenu/symfony/162

Des ACL consistant à filtrer les communications à l'initiative des actifs présents dans ce VLAN sont à mettre en œuvre pour les limiter **aux seules destinations que constitue « la zone partenaires de RAMAGE » et quelques hosts ciblés sur le LAN local.**

Les ACL à appliquer sont dans les guides de configuration ci-dessous.

1.8 GTC/GTB/ANTI-INTRUSION, VIDEO-SURVEILLANCE … HORS PROJET NATIONAUX

CAS 1 : le besoin ne nécessite pas l'accès d'un partenaire extérieur (pour maintenance, support …) :

- ⇨ Prendre contact avec le DR pour valider la connexion et donner des consignes

CAS 2 : le besoin nécessite l'accès d'un partenaire extérieur (pour maintenance, support …) :

- ⇨ Utiliser le VLAN 224 en adaptant l'ACL comme décrit plus bas.

1.9 VLAN ET ADRESSAGE IP NORMALISES EN SIEGE DE CPAM ET CGSS

1.9.1 Nommage normalisé des VLAN et interfaces VLAN en CPAM

Nous avons défini le nommage des VLAN et des interfaces vlan dans le but d'automatiser le contrôle des configurations par le DR et de préparer la génération automatique des configurations (voir tableau ci-dessous les principaux VLAN). Nous avons choisi de renseigner le champ « name » pour la déclaration du VLAN et le champ « description » pour l'interface VLAN.

VLAN	NOM DU VLAN	DESCRIPTION DE L'INTERFACE VLAN
2	name VLAN-*nom-org*	description INT-VLAN- *nom-org*
3	name VLAN-MEDICAL	description INT-VLAN-MEDICAL
4	name VLAN-DATA	description INT-VLAN-DATA
5	name VLAN-INTERCOWAN	description INT-VLAN-INTERCOWAN
17	name VLAN-EVASION-INTERNET	description INT-VLAN-EVASION-INTERNET
30	name VLAN-VOIX	description INT-VLAN-VOIX
50	name VLAN-WIFI-AGENTS	description INT-VLAN-WIFI-AGENTS
53	name VLAN-WIFI-AGENTS- MEDICAL	description INT-VLAN-WIFI-AGENTS- MEDICAL
54	name VLAN-WIFI-INVITES	description INT-VLAN-WIFI-INVITES
55	name VLAN-ROUTEUR-4G	description INT-VLAN-ROUTEUR-4G
172	name VLAN-SDWAN	description INT-VLAN-SDWAN
211	name VLAN-SERVEURS- MEDICAL	description INT-VLAN-SERVEURS- MEDICAL
216	name VLAN-CONSOLES-SERVEURS	description INT VLAN-CONSOLES-SERVEURS
219	name VLAN-PCA-DATA	description INT-VLAN-PCA-DATA
220	name VLAN-PCA-VOIX	description INT VLAN-PCA-VOIX
224	name VLAN-ACCES-PART	description INT-VLAN-ACCES-PART
225	name VLAN-ACCES-PART- MEDICAL	description INT-VLAN-ACCES-PART- MEDICAL
226	name VLAN-IMPRIMANTES	description INT-VLAN-IMPRIMANTES
227	name VLAN-IMPRIMANTES-MEDICAL	description INT-VLAN-IMPRIMANTES-MEDICAL
230	name VLAN-GW-CETIAM	description INT-VLAN-GW-CETIAM
239	name VLAN-MGT-IPANEMA	description INT-VLAN-MGT-IPANEMA
900	name VLAN-ADMIN-UCOPIA	description INT-VLAN-ADMIN-UCOPIA
901	name VLAN-ADMIN-RESEAU	description INT-VLAN-ADMIN-RESEAU
902	name VLAN-ADMIN-WIFI	Description INT-VLAN-ADMIN-WIFI

1.9.2 Tableau des VLAN normalisés en Siège de CPAM :

En bleu : les vlan de type « voix » avec un adressage IP en 58.

N°	Nom	@ Réseau	@ Int VLAN	Rôle – Commentaires - Consignes
1	-	-	-	L'interface VLAN 1 doit être supprimée (undo).
2	**VLAN-*NOM-ORG***	55.X.222.0 / 24	55.X.222.1	VLAN pour sites hébergés ➔ Ex : IRSA, UC-CMP, CDS (Centre de Santé)…
3	**VLAN-MEDICAL**	55.X.223.0 / 24	55.X.223.1	Dans le cas d'un SERVICE MEDICAL au siège de la CPAM
4	**VLAN-DATA**	55.X.4.0 / 22	55.X.4.1	Contient les serveurs et les PMF de la CPAM Les serveurs de « production » du site peuvent être dissociés de ce VLAN historique. Dans ce cas, utiliser pour ces serveurs un des VLAN optionnels.
5	**VLAN-INTERCOWAN**	55.X.225.0 / 28	55.X.225.1	VLAN d'interconnexion avec RAMAGE. Contient les routeurs Opérateur. Les Organismes ayant fusionné conservent le VLAN 5 existant d'avant la fusion.
6	**Voir DR**	55.X.226.0 / 24	55.X.226.1	Contient jusqu'à 254 équipements – optionnel.
7	**Voir DR**	55.X.227.0 / 24	55.X.227.1	Contient jusqu'à 254 équipements – optionnel.
8	**Voir DR**	55.X.228.0 / 24	55.X.228.1	Contient jusqu'à 254 équipements – optionnel.
9	**Voir DR**	55.X.229.0 / 24	55.X.229.1	Contient jusqu'à 254 équipements – optionnel.
10	**Voir DR**	55.X.230.0 / 24	55.X.230.1	Contient jusqu'à 254 équipements – optionnel.
11	**Voir DR**	55.X.231.0 / 24	55.X.231.1	Contient jusqu'à 254 équipements – optionnel.
12	**Voir DR**	55.X.232.0 / 24	55.X.232.1	Contient jusqu'à 254 équipements – optionnel.
13	**Voir DR**	55.X.233.0 / 24	55.X.233.1	Contient jusqu'à 254 équipements – optionnel.
14	**Voir DR**	55.X.234.0 / 24	55.X.234.1	Contient jusqu'à 254 équipements – optionnel.
15	**Voir DR**	55.X.235.0 / 24	55.X.235.1	Contient jusqu'à 254 équipements – optionnel.
16	**Voir DR**	55.X.236.0 / 24	55.X.236.1	Contient jusqu'à 254 équipements – optionnel.
17	**VLAN-EVASION-INTERNET**	**192.168.1.0 / 24**	**192.168.1.4**	**Contient la BOX EVASION-INTERNET (192.168.1.1)**
18	**VLAN-PFS**	55.X.238.0 / 23	55.X.238.1	Contient tous les PMF et équipements PFS. Cela vaut lorsque la PFS est localisée au sein du Siège de la CPAM. Le masque utilisé est /23 (255.255.254.0) de manière à permettre une éventuelle augmentation du nombre de PMF dans la PFS (jusqu'à 510). La plage va donc de 55.X.238.1 à 55.X.239.254.
19 à 29	*Non utilisés pour l'instant.*			
30	**VLAN-VOIX**	58.X.4.0 /22	58.X.4.1	Contient tous les IPBX (si présents) et les téléphones du siège. C'est en 58.X.X.X le sous-réseau « symétrique » du sous-réseau 55.X.X.X associé au vlan PMF utilisé localement.
31	**Voir DR**	58.X.226.0 / 24	58.X.226.1	Optionnels.
32	**Voir DR**	58.X.227.0 / 24	58.X.227.1	

33	**Voir DR**	58.X.228.0 / 24	58.X.228.1	Si des VLAN optionnels de PMF ont été créés (de 6 à 16), il est possible de créer des vlan VOIX « en phase ». Le VLAN 37 pour Asterisk Régional sera libéré suite au déploiement CETIAM.
34	**Voir DR**	58.X.229.0 / 24	58.X.229.1	
35	**Voir DR**	58.X.230.0 /24	58.X.230.1	
36	**Voir DR**	58.X.231.0 /24	58.X.231.1	
37	**Voir DR**	58.X.232.0 /24	58.X.232.1	
38	**Voir DR**	58.X.233.0 /24	58.X.233.1	
39	**Voir DR**	58.X.234.0 /24	58.X.234.1	
40	**Voir DR**	58.X.235.0 /24	58.X.235.1	
41	**Voir DR**	58.X.236.0 /24	58.X.236.1	
42 à 49	*Non utilisés pour l'instant.*			
50	**VLAN-WIFI-AGENTS**	55.X.250.0 /24	55.X.250.1	VLAN dédié aux clients WIFI des agents (agents AM).
51 à 52	*Non utilisés pour l'instant.*			
53	**VLAN-WIFI-AGENTS-MEDICAL**	**55.X.253.0/24**	**55.X.253.1**	**VLAN dédié aux agents du service medical**
54	**VLAN-WIFI-INVITES**	Voir documentations WIFI du DR		VLAN dédié aux clients WIFI des invités (externes AM ou professionnels).
55	**VLAN-ROUTEUR-4G**	55.224.X.Y – fourni par DR		VLAN utilisé pour le secours Ramage en 4G.
56 à 171	*Non utilisés pour l'instant.*			
172	**VLAN-SDWAN**	172.19.X.X	1ère du subnet	Interconnection entre le switch n3 et les routeurs SD-WAN. Ce réseau est donné par le DR.
173 à 210	*Non utilisés pour l'instant.*			
211	**VLAN- SERVEURS-MEDICAL**	**55.X.211.0/24**	**55.X.211.1**	**VLAN dédié aux serveurs des services médicaux.**
212-215	*Non utilisés pour l'instant.*			
216	**VLAN-CONSOLES-SERVEURS**	**55.X.21[6-8].0 /24**	**55.X.21[6-8].1**	**Vlan dédié aux ports console des serveurs et Esx (Ilo ou Idrac).**
219	**VLAN-PCA-DATA**	55.X.219.0 /24	55.X.219.1	VLAN pour PCA de type données.
220	**VLAN-PCA-VOIX**	58.X.219.0 /24	58.X.219.1	VLAN pour PCA de type voix.
221 à 223	*Non utilisés pour l'instant.*			
224	**VLAN-ACCES-PART**	55.X.224.0 /25 (de .1 à .126)	55.X.224.1	**Contient tous les équipements accédés par un tiers en VPN officiel Cnam** **UN ACL OBLIGATOIRE DOIT ETRE CONFIGURE SUR L'INTERFACE VLAN 224 (voir les guides de configuration).** **Dans le cas d'un besoin d'interconnexion d'autres partenaires (projets nationaux)**
226	**VLAN-IMPRIMANTES**	**55.x.248.0/25**	**55.X.248.1**	**Contient les imprimantes**
227	**VLAN-IMPRIMANTES-MEDICAL**	**55.x.248.128/25**	**55.X.248.129**	**Contient les imprimantes des services médicaux**
228	*Non utilisés pour l'instant.*			
229	**VLAN-IMPRIMANTES-CDS**	55.x.x.x/27	30 adresses	Consulter la CNAM/DR pour adressage
230	**VLAN-GW-CETIAM**	58.230.X.Y /29	1ère du subnet Fournie par DR	Contient la ou les passerelle(s) analogique(s) / IP (Gateway) CETIAM si besoin. Sera fournie par le DR le moment venu.
231 à 238	***Non utilisés pour l'instant.***			
239	**VLAN-MGT-IPANEMA**	55.239.X.Y /29	1ère du subnet Fournie par DR	VLAN dédié à l'interface de management IPANEMA sur les sites équipés. Les valeurs de X et Y sont attribuées par le DR au cas par cas et fournies lors de l'installation.

240 à 899	*Non utilisés pour l'instant.*			
900	**VLAN-ADMIN-UCOPIA**	**55.x.237.0/30**	**55.x.237.1**	**Vlan servant uniquement à l'administration de l'Ucopia. L'Ucopia doit être en 55.x.237.2/30** **Ce vlan doit être isolé via les ACL 3900 et 3901**
901	**VLAN-ADMIN-RESEAU**	55.X.221.0 / 24	55.X.221.1	**ATTENTION : NE CONTIENT PLUS LES EQUIPEMENTS WIFI.** Le VLAN 901 : VLAN de management des switches. Les fédérateurs ont l'adresse .1 (interface VLAN 901). Les switches d'extrémité n'ont qu'une seule adresse IP : interface VLAN 901 ➔à partir de .11. NE PAS Y METTRE LES CARTES ILO DE SERVEURS.
902	**VLAN-ADMIN- WIFI**	**55.X.220.0 / 24**	**55.X.220.1**	**ATTENTION : NOUVEAU VLAN POUR LES EQUIPEMENTS WIFI.** **Le VLAN 902 : VLAN de management des équipements WIFI.** **Les switches fédérateurs ont l'adresse .1 dans ce VLAN (interface VLAN 902). Les équipements WIFI ont une adresse VLAN 902 ➔ à partir de .11.**
903	**VLAN-ROUTEUR-WIFI-INVITE**	**55.xx.237.4 / 30**	**55.xx.237.5**	**Le VLAN 903 est utilisé pour migrer le routeur WIFI INVITE du vlan 5 au vlan 903 suite au passage des organismes sur la solution SDWAN**
904 et +	.			

1.10 VLAN ET ADRESSAGE IP NORMALISES EN SIEGE D'UGECAM

1.10.1 Nommage normalisé des VLAN et des interfaces VLAN en siège d'UGECAM

Nous avons défini le nommage des VLAN et des interfaces vlan dans le but d'automatiser le contrôle des configurations par le DR et de préparer la génération automatique des configurations (voir tableau ci-dessous les principaux VLAN). Nous avons choisi de renseigner le champ « name » pour la déclaration du VLAN et le champ « description » pour l'interface VLAN.

VLAN	NOM DU VLAN	DESCRIPTION DE L'INTERFACE VLAN
3	name VLAN-MEDICAL	description INT-VLAN-MEDICAL
4	name VLAN-DATA	description INT-VLAN-DATA
5	name VLAN-INTERCOWAN	description INT-VLAN-INTERCO
17	name VLAN-EVASION-INTERNET	description INT-VLAN-EVASION-INTERNET
30	name VLAN-VOIX	description INT-VLAN-VOIX
50	name VLAN-WIFI-AGENTS	description INT-VLAN-WIFI-AGENTS
54	name VLAN-WIFI-INVITES	description INT-VLAN-WIFI-INVITES
55	name VLAN-ROUTEUR-4G	description INT-VLAN-ROUTEUR-4G
172	name VLAN-SDWAN	description INT-VLAN-SDWAN
216	name VLAN-CONSOLES-SERVEURS	Description INT VLAN-CONSOLES-SERVEURS
219	name VLAN-PCA-DATA	description INT-VLAN-PCA-DATA
220	name VLAN-PCA-VOIX	description INT VLAN-PCA-VOIX
224	name VLAN-ACCES-PART	description INT-VLAN-ACCES-PART
226	name VLAN-IMPRIMANTES	description INT-VLAN-IMPRIMANTES
239	name VLAN-MGT-IPANEMA	description INT-VLAN-MGT-IPANEMA
254	name VLAN-WIFI-PATIENTS	description INT-VLAN-WIFI-PATIENTS
900	name VLAN-ADMIN-UCOPIA	N/A (niveau 2)
901	name VLAN-ADMIN-RESEAU	description INT-VLAN-ADMIN-RESEAU
902	name VLAN-ADMIN-WIFI	description INT-VLAN-ADMIN-WIFI

1.10.2 Tableau des VLAN normalisés en siège d'UGECAM

En bleu : les vlan de type « voix » avec un adressage IP en 58.

N°	Nom	@ Réseau	@ Int VLAN	Rôle – Commentaires – Consignes
1	-	-	-	L'interface VLAN 1 doit être supprimée (undo).
2 à 3	*Non utilisés pour l'instant.*			
4	**VLAN-DATA**	55.X.4.0 / 22	55.X.4.1	Contient les serveurs et les PMF de l'UGECAM. Les serveurs de « production » du site peuvent être dissociés de ce VLAN historique. Dans ce cas, utiliser pour ces serveurs un des VLAN optionnels.
5	**VLAN-INTERCO**	55.X.225.0 / 28	55.X.225.1	VLAN d'interconnexion avec RAMAGE. Contient les routeurs Opérateur. Les Organismes ayant fusionné conservent le VLAN 5 existant d'avant la fusion.
6	**Voir DR**	55.X.226.0 / 24	55.X.226.1	Contient jusqu'à 254 équipements – optionnel.
7	**Voir DR**	55.X.227.0 / 24	55.X.227.1	Contient jusqu'à 254 équipements – optionnel.
8	**Voir DR**	55.X.228.0 / 24	55.X.228.1	Contient jusqu'à 254 équipements – optionnel.
9	**Voir DR**	55.X.229.0 / 24	55.X.229.1	Contient jusqu'à 254 équipements – optionnel.
10	**Voir DR**	55.X.230.0 / 24	55.X.230.1	Contient jusqu'à 254 équipements – optionnel.
11	**Voir DR**	55.X.231.0 / 24	55.X.231.1	Contient jusqu'à 254 équipements – optionnel.
12	**Voir DR**	55.X.232.0 / 24	55.X.232.1	Contient jusqu'à 254 équipements – optionnel.
13	**Voir DR**	55.X.233.0 / 24	55.X.233.1	Contient jusqu'à 254 équipements – optionnel.
14	**Voir DR**	55.X.234.0 / 24	55.X.234.1	Contient jusqu'à 254 équipements – optionnel.
15	**Voir DR**	55.X.235.0 / 24	55.X.235.1	Contient jusqu'à 254 équipements – optionnel.
16	**Voir DR**	55.X.236.0 / 24	55.X.236.1	Contient jusqu'à 254 équipements – optionnel.
17	**VLAN-EVASION-INTERNET**	**192.168.1.0 / 24**	**192.168.1.4**	**Contient la BOX EVASION-INTERNET (192.168.1.1)**
18 à 29	*Non utilisés pour l'instant.*			
30	**VLAN-VOIX**	58.X.4.0 /22	58.X.4.1	Contient tous les IBX (si présents) et les téléphones du siège. C'est en 58.X.X.X le sous-réseau « symétrique » du sous-réseau 55.X.X.X associé au vlan PMF utilisé localement.
31	**Voir DR**	58.X.226.0 / 24	58.X.226.1	Optionnels. Si des VLAN optionnels de PMF ont été créés (de 6 à 16), il est possible de créer des vlan VOIX « en phase ».
32	**Voir DR**	58.X.227.0 / 24	58.X.227.1	
33	**Voir DR**	58.X.228.0 / 24	58.X.228.1	
34	**Voir DR**	58.X.229.0 / 24	58.X.229.1	
35	**Voir DR**	58.X.230.0 /24	58.X.230.1	
36	**Voir DR**	58.X.231.0 /24	58.X.231.1	
37	**Voir DR**	58.X.232.0 /24	58.X.232.1	
38	**Voir DR**	58.X.233.0 /24	58.X.233.1	
39	**Voir DR**	58.X.234.0 /24	58.X.234.1	
40	**Voir DR**	58.X.235.0 /24	58.X.235.1	
41 à 49	*Non utilisés pour l'instant.*			
50	**VLAN-WIFI-AGENTS**	55.X.250.0 /24	55.X.250.1	VLAN dédié aux clients WIFI des agents (agent AM).
51 à 53	*Non utilisés pour l'instant.*			
54	**VLAN-WIFI-INVITES**	Voir documentations WIFI du DR		VLAN dédié aux clients WIFI des invités (externes AM ou professionnels).
55	**VLAN-ROUTEUR-4G**	55.224.X.Y – fourni par DR		VLAN utilisé pour le secours Ramage en 4G.
56 à 171	*Non utilisés pour l'instant.*			
172	**VLAN-SDWAN**	172.19.X.X	1ère du subnet	Interconnection entre le switch n3 et les routeurs SD-WAN. Ce réseau est donné par le DR.
173 à 215	*Non utilisés pour l'instant.*			
216	**VLAN-CONSOLES-SERVEURS**	**55.X.21[6-8].0 /24**	**55.X.21[6-8].1**	**Vlan dédié aux ports consoles des serveurs et Esx (Ilo ou Idrac).**
219	**VLAN-PCA-DATA**	55.X.219.0 /24	55.X.219.1	VLAN pour PCA de type données.

220	**VLAN-PCA-VOIX**	58.X.219.0 /24	58.X.219.1	VLAN pour PCA de type voix.
221 à 223	*Non utilisés pour l'instant.*			
224	**VLAN-ACCES-PART**	55.X.224.0 /25 (de .1 à .126)	55.X.224.1	Contient tous les équipements **accédés par un tiers en VPN officiel Cnam d'accès partenaire** (ex : serveurs télé-maintenus…). UN ACL OBLIGATOIRE DOIT ETRE CONFIGURE SUR L'INTERFACE VLAN 224.
226	**VLAN-IMPRIMANTES**	55.x.248.0/25	55.x.248.1	Contient les imprimantes
225 à 238	*Non utilisés pour l'instant.*			
239	**VLAN-MGT-IPANEMA**	55.239.X.Y /29	1ère du subnet Fournie par DR	VLAN dédié à l'interface de management IPANEMA sur les sites équipés. Les valeurs de X et Y sont attribuées par le DR au cas par cas et fournies lors de l'installation.
240 à 253	*Non utilisés pour l'instant.*			
254	**VLAN-WIFI-PATIENTS**	**Niveau 2**	**Niveau 2**	**VLAN dédié aux clients WIFI des PATIENTS.**
255 à 899				
900	**VLAN-ADMIN-UCOPIA**	-	-	**Vlan en N2**
901	**VLAN-ADMIN-RESEAU**	55.X.221.0 / 24	55.X.221.1	**ATTENTION : NE CONTIENT PLUS LES EQUIPEMENTS WIFI.** Le VLAN 901 : VLAN de management des switches. Les fédérateurs ont l'adresse .1 (interface VLAN 901). Les switches d'extrémité n'ont qu'une seule adresse IP : interface VLAN 901 ➔à partir de .11. NE PAS Y METTRE LES CARTES ILO DE SERVEURS.
902	**VLAN-ADMIN-WIFI**	**55.X.220.0 / 24**	**55.X.220.1**	**ATTENTION : NOUVEAU VLAN POUR LES EQUIPEMENTS WIFI.** **Le VLAN 902 : VLAN de management des équipements WIFI.** **Les switches fédérateurs ont l'adresse .1 dans ce VLAN (interface VLAN 902). Les équipements WIFI ont une adresse VLAN 902 ➔ à partir de .11.**
903	**VLAN-ROUTEUR-WIFI-IVITE**	**55.xx.237.4/30**	**55xx.237.5**	**Le VLAN 903 est utilisé pour migrer le routeur WIFI INVITE du vlan 5 au vlan 903 suite au passage des organismes sur la solution SDWAN**
904 et +	*Non utilisés pour l'instant.*			

1.11 ADRESSAGE IP NORMALISE / ADRESSES RESERVEES (CPAM, CGSS, MEDICAL, UGECAM)

Dans chaque VLAN, la passerelle par défaut est la première adresse du sous-réseau associé. C'est l'adresse IP de l'interface VLAN dans les switches fédérateurs. VOIR LE TABLEAU CI-DESSUS, colonne « @ IP int VLAN ».
En fonction des VLAN, il est demandé de réserver des adresses. Voir le tableau ci-dessous.

En bleu : les VLAN de type « voix » avec un adressage IP en 58.

Synthèse (fédérateurs stackés) :				
VLAN	**Réseau**	**Masque**	**Fédérateur (@IP int VLAN)**	**Adresses Réservées**
1	-	-	-	-
2	55.X.222.0	/24 : 255.255.255.0	.1	de .1 à .10
3	55.X.223.0	/24 : 255.255.255.0	.1	de .1 à .31
4	55.X.4.0	/22 : 255.255.252.0	.1	de .1 à .31
5	55.X.225.0	/28 : 255.255.255.240	.1	de .1 à .10
6	55.X.226.0	/24 : 255.255.255.0	.1	de .1 à .31
7	55.X.227.0			
8	55.X.228.0			
9	55.X.229.0			
10	55.X.230.0			
11	55.X.231.0			
12	55.X.232.0			
13	55.X.233.0			
14	55.X.234.0			
15	55.X.235.0			
16	55.X.236.0			
18	55.X.238.0	/24 : 255.255.255.0	.1	de .1 à .31
30	58.X.4.0	/22 : 255.255.252.0	.1	de .1 à .31
31	58.X.226.0	/24 : 255.255.255.0	.1	de .1 à .31
32	58.X.227.0			
33	58.X.228.0			
34	58.X.229.0			
35	58.X.230.0			
36	58.X.231.0			
37	58.X.232.0			
38	58.X.233.0			
39	58.X.234.0			
40	58.X.235.0			
41	58.X.236.0			
50	55.X.250.0	/24 : 255.255.255.0	.1	de .1 à .31
53	**55.X.253.0**	**/24 : 255.255.255.0**	**.1**	**de .1 à .10**
172	172.19.X.X		**.1**	
54	Voir documentations « WIFI » sur le portail du DR.16			
172	**172.19.xxx.xxx**	**/29 : 255.255.255.248**		
219	55.X.219.0	/24 : 255.255.255.0	.1	de .1 à .31
220	58.X.219.0	/24 : 255.255.255.0	.1	de .1 à .31
224	55.X.224.0	/25 : 255.255.255.128	.1	de .1 à .10
226	**55.X.248.0**	**/25 : 255.255.255.128**	**.1**	**de .1 à .10**
230	58.230.X.Y	/29 255.255.255.248 - Fournies par le DR avant le déploiement		
239	55.239.X.Y	/28 255.255.255.240 - Fournies par le DR avant le déploiement		
254	**Niveau 2**			
900	**55.X.237.0 (Niveau 2 pour les Ugecam)**	**/30 : 255.255.255.252**	**.1**	**-**
901	55.X.221.0	/24 : 255.255.255.0	.1	de .1 à .10
902	**55.X.220.0**	**/24 : 255.255.255.0**	**.1**	**de .1 à .10**

1.12 VLAN ET ADRESSAGE IP NORMALISES EN AGENCES ET ETABLISSEMENTS

1.12.1 Nommage normalisé des VLAN et interfaces VLAN

Nous avons défini le nommage des VLAN et des interfaces vlan dans le but d'automatiser le contrôle des configurations par le DR et de préparer la génération automatique des configurations (voir tableau ci-dessous les principaux VLAN). Nous avons choisi de renseigner le champ « name » pour la déclaration du VLAN et le champ « description » pour l'interface VLAN.

VLAN	NOM DU VLAN	DESCRIPTION DE L'INTERFACE VLAN
2	name VLAN-*nom-org*	description INT-VLAN- *nom-org*
3	name VLAN-MEDICAL	description INT-VLAN-MEDICAL
4	name VLAN-DATA	description INT-VLAN-DATA
5	name VLAN-INTERCOWAN	description INT-VLAN-INTERCOWAN
17	name VLAN-EVASION-INTERNET	description INT-VLAN-EVASION-INTERNET
30	name VLAN-VOIX	description INT-VLAN-VOIX
50	name VLAN-WIFI-AGENTS	description INT-VLAN-WIFI-AGENTS
53	name VLAN-WIFI-AGENTS-MEDICAL	description INT-VLAN-WIFI-AGENTS- MEDICAL
54	name VLAN-WIFI-INVITES	description INT-VLAN-WIFI-INVITES
55	name VLAN-ROUTEUR-4G	description INT-VLAN-ROUTEUR-4G
172	name VLAN-SDWAN	description INT-VLAN-SDWAN
216	name VLAN-CONSOLES-SERVEURS	description INT VLAN-CONSOLES-SERVEURS
224	name VLAN-ACCES-PART	description INT-VLAN-ACCES-PART
225	name VLAN-ACCES-PART-MEDICAL	description INT-VLAN-ACCES-PART-MEDICAL
226	name VLAN-IMPRIMANTES	description INT-VLAN-IMPRIMANTES
227	name VLAN-IMPRIMANTES-MEDICAL	description INT-VLAN-IMPRIMANTES-MEDICAL
230	name VLAN-GW-CETIAM	description INT-VLAN-GW-CETIAM
239	name VLAN-MGT-IPANEMA	description INT-VLAN-MGT-IPANEMA
*254**	*name VLAN-WIFI-PATIENTS (UGECAM)*	*Description INT- VLAN-WIFI-PATIENTS*
*900**	*name VLAN-ADMIN-UCOPIA*	*N/A (niveau 2)*
901	name VLAN-ADMIN-RESEAU	description INT-VLAN-ADMIN-RESEAU
902	name VLAN-ADMIN-WIFI	Description INT-VLAN-ADMIN-WIFI

* 254 : VLAN-WIFI-PATIENTS : ne concerne que les UGECAM.
* 900 : VLAN-ADMIN-UCOPIA : ne concerne que les UGECAM dans certains de leurs établissements

Rq : Pas de norme IEEE rigide → limite pratique = 32 caractères pour être tranquille sur la majorité des équipements

1.12.2 Listes et fonctions des VLAN en AGENCES et ETABLISSEMENTS

Il s'agit des VLAN qu'il est obligatoire de déployer au minimum dans le cas standard. En cas d'exception, contactez le DR pour validation.

L'interface VLAN 1 doit être supprimée.
Les VLAN 901 et 902 doivent être mis en œuvre et doivent être réservés respectivement aux switches et aux équipements wifi.

Voici le tableau des VLAN normalisés- En bleu : les vlan de type « voix » avec un adressage ip en 58.

N°	Nom	@ Réseau	@ Int VLAN	Rôle – Commentaires – Consignes
1	*Par défaut*	-	-	L'interface VLAN 1 doit être supprimée (undo)
2	**VLAN-*Nom-Org»***	55.X.243.Y /Z	1ère du subnet	VLAN Données pour les organismes hébergés en CP : IRSA, UC-CMP… Remplacer « ORG » par le nom de l'organisme. Ex : DONNEES-IRSA
3	**VLAN-MEDICAL**	55.X.24**(4-5)**.Y /Z	1ère du subnet	Si un Service Médical est hébergé, ce VLAN contient les équipements bureautiques (Serveurs et PMF) du SM
4	**VLAN-DATA**	55.X.Y.Z / 22	1ère du subnet	Contient tous les PMFet les serveurs. La première agence a le 55.X.4.0 /22 , la deuxième 55.X.8.0 /22…
5	**VLAN-INTERCOWAN**	55.X.24**(0-1)**.Z / 29	1ère du subnet	Interconnexion WAN RAMAGE – voir tableau plus loin
30	**VLAN-VOIX**	58.X.Y.Z /22	1ère du subnet	Contient les téléphones IP du site. C'est en 58.X.X.X le sous-réseau « symétrique » du sous-réseau 55.X.X.X associé au vlan 4 PMF utilisé localement. La première agence a le 58.X.4.0 /22 , la deuxième 58.X.8.0 /22…
50	**VLAN-WIFI-AGENTS**	55.X.25**(1-2)**.Z / ??	1ère du subnet	VLAN dédié aux clients WIFI des agents (agents AM).
53	**VLAN-WIFI-AGENTS-MEDICAL**	**55.X.25(4-5).Y /Z**	1ère du subnet	**VLAN dédié aux WIFI du SERVICE MEDICAL**
54	**VLAN-WIFI-INVITES**	Voir documentations WIFI du DR		VLAN dédié aux clients WIFI invités (externes AM ou professionnels)
55	**VLAN-ROUTEUR-4G**	55.224.XXXXXXXXX		Procédure fournie lors de l'envoi d'un routeur
172	**VLAN-SDWAN**	172.19.X.X	1ère du subnet	Interconnection entre le switch n3 et les routeurs SD-WAN. Ce réseau est donné par le DR.
216	**VLAN-CONSOLES-SERVEURS**	**55.X.21(2-5).Z /28**	**1ère du subnet**	**Vlan dédié aux consoles des serveurs (Ilo, Idrac, etc…).**
224	**VLAN-ACCESS-PART**	55.X.24**(6-7)**.Z / 29	1ère du subnet	Contient tous les équipements accédés par un tiers en VPN officiel Cnam d'accès de partenaires
225	**VLAN-ACCES-PART- MEDICAL**	55.X.24**(6-7)**.Z / 29	1ère du subnet	Contient tous les équipements **accédés par un tiers en VPN officiel Cnam** (**POUR LE MEDICAL** UN ACL OBLIGATOIRE DOIT ETRE CONFIGURE SUR L'INTERFACE VLAN 225.
226	**VLAN-IMPRIMANTES**	**55.x.249.x /29** **55.x.248.128 /29**		**Imprimantes (Gateway + Imprimante)** **Si non utilisé par la CPAM**
227	**VLAN-IMPRIMANTES-MEDICAL**	**55.2XX.249.0 /29**		**Découpage à établir en collaboration avec la MEDICAL hébergée**
230	**VLAN-GW-CETIAM**	58.230.X.Y /29	1ère du subnet Fournie par DR	Contient passerelle analogique / IP (Gateway) si besoin (CETIAM). Sera fournie par le DR le moment venu.
239	**VLAN-MGT-IPANEMA**	55.239.X.Y /29	1ère du subnet (Fournie par DR)	VLAN dédié à l'interface de management IPANEMA sur les sites équipés. Les valeurs de X, Y et Z sont attribuées par le DR au cas par cas et fournies lors de l'installation.

254	**VLAN-WIFI-PATIENTS**	**Niveau 2**	**Niveau 2**	**VLAN dédié aux clients WIFI des PATIENTS Pour les UGECAM.**
901	**VLAN-ADMIN-RESEAU**	**55.X.[0-1].Z /28**	**1ère du subnet**	**Sous-réseau réservé à l'administration des switches**
902	**VLAN-ADMIN-WIFI**	**55.X.[2-3].Z /28**	**1ère du subnet**	**Sous-réseau réservé à l'administration des équipements WIFI**

➔ La passerelle par défaut dans un VLAN X est l'adresse IP de l'interface VLAN X du switch N3. Celle-ci est toujours la première adresse IP du sous-réseau.

➔ Le serveur de proximité (DHCP) devra être connecté directement sur le switch niveau 3 si possible.

➔ Le(s) port(s) Giga du switch niveau 3 seront utilisé(s) pour la connexion d'autres switches d'abord, de serveurs ensuite.

*** VLAN « Accès-Partenaire » pour le SERVICE MEDICAL hébergé : utilisation d'un sous réseau 55.X.24[6-7].X disponible dans la liste (cf tableau plus bas).**

1.12.3 VLAN 2 – VLAN-*Nom-Org :* organismes hébergés (IRSA, UC-CMP,CDS…)

Le VLAN2 est utilisé lorsqu'un organisme exterieur est hébergé au sein de l'assurance maladie. Il sera utilisé très prochainement pour les anciens CES hébergés en CPAM et transformés en CDS (Centre De Santé). La gestion de ces organismes sera déléguée aux UGECAM.

VLAN 2 – VLAN-nom-*org*

Plages d'adresses proposées :

Le nombre de clients (PMF, Serveurs…) propres à ces organismes est variable. La plage d'adresses définie va de 55.X.243.1 à 55.X.243.254 : à utiliser dans N sous-réseaux avec masque libre à adapter en fonction du nombre de clients dans le CP :

Le VLAN est toujours le VLAN 2 mais le plan d'adressage peut être différent sur chaque site en fonction du nombre de clients : on pourra trouver de minimum 1 sous-réseau de 254 adresses à maximum 64 sous-réseaux de 6 adresses …ou un mixte de sous-réseaux de tailles différentes…

Voici le tableau des masques à utiliser sur les plages 55.X.243.0 :

Masque		Nb d'adresses dans le sous-réseau	Nombre de sous-réseaux possibles
/24	255.255.255.0	254	1
/25	255.255.255.128	126	2
/26	255.255.255.192	62	4
/27	255.255.255.224	30	8
/28	255.255.255.240	14	16
/29	255.255.255.248	6	32

L'adresse de l'interface VLAN 2 dans le switch fédérateur du site est toujours la première adresse de la plage.



MERCI DE CONTACTER LE DR POUR VALIDATION !!

1.12.4 VLAN 3 – VLAN-MEDICAL

(Anciennement vlan ELSM et ou DRSM)
Suite au projet TAM, les DRSM et les ELSM ont été fusionnés dans les CPAM. Toutefois Les flux medicaux resteronnt séparés des flux assurance maladie. Il a été convenu de conserver le VLAN 3 pour les flux des Services Médicaux dans les CP et les CPAM.

Plages d'adresses proposées :
Le nombre de clients (PMF, Serveurs…) propres aux SM dans ces sites sont variables. La plage d'adresses définie va de 55.X.244.0 à 55.X.245.254 : à utiliser dans N sous-réseaux avec masque libre à adapter en fonction du nombre de PMF du service médical dans le CP.

Le VLAN est toujours le VLAN 3 mais le plan d'adressage peut être différent sur chaque site en fonction du nombre de clients : on pourra trouver de minimum 1 sous-réseau de 254 adresses à maximum 64 sous-réseaux de 6 adresses …ou un mixte de sous-réseaux de tailles différentes…

Voici le tableau des masques à utiliser sur les plages 55.X.244.0 à 55.X.245.254 :

Masque		Nb d'adresses dans le sous-réseau	Nombre de sous-réseaux possibles
/24	255.255.255.0	254	2
/25	255.255.255.128	126	4
/26	255.255.255.192	62	8
/27	255.255.255.224	30	16
/28	255.255.255.240	14	32
/29	255.255.255.248	6	64

L'adresse de l'interface VLAN 3 dans le switch fédérateur du site est toujours la première adresse de la plage.



MERCI DE CONTACTER LE DR POUR VALIDATION !!

Rq : Le nommage choisi est : VLAN-MEDICAL (pour VLAN-SERVICE MEDICAL)

1.12.5 VLAN 4 – VLAN-DATA

C'est le VLAN pour les PMF et les serveurs du site. Il correspond au plan d'adressage IP historique de tout site découpage en /22 à partir de 8 – Le siège ayant 4) :

- Siège : 55.X.4.0 /22

- Agences et établissements
    - 1 : 55.X.8.0 /22
    - 2 : 55.X.12.0 /22
    - 3: 55.X.16.0 /22
    - …etc.

1.12.6 VLAN 5 – VLAN-INTERCOWAN

Les CP utiliseront un des sous-réseaux suivants pour le VLAN 5. Il s'agit de choisir un sous-réseau par CP. Si la plage proposée est déjà utilisée dans votre région ou le nombre de sous-réseaux proposé insuffisant, veuillez contacter le DR.

C'est ce plan d'adressage qui est à appliquer au moment d'un passage au niveau pour déploiement ToIP via un « MOD-CONF » : modification de configuration des routeurs RAMAGE.

Site	subnet	Masque	Première @	Dernière @	Int vlan 5 Switch N3	ROUTEUR OP1	ROUTEUR OP2	RESERVEES	
1	55.X.240.0	255.255.255.248 (/29)	1	6	1	5	6	2	3
2	55.X.240.8	255.255.255.248 (/29)	9	14	9	13	14	10	11
3	55.X.240.16	255.255.255.248 (/29)	17	22	17	21	22	18	19
4	55.X.240.24	255.255.255.248 (/29)	25	30	25	29	30	26	27
5	55.X.240.32	255.255.255.248 (/29)	33	38	33	37	38	34	35
6	55.X.240.40	255.255.255.248 (/29)	41	46	41	45	46	42	43
7	55.X.240.48	255.255.255.248 (/29)	49	54	49	53	54	50	51
8	55.X.240.56	255.255.255.248 (/29)	57	62	57	61	62	58	59
9	55.X.240.64	255.255.255.248 (/29)	65	70	65	69	70	66	67
10	55.X.240.72	255.255.255.248 (/29)	73	78	73	77	78	74	75
11	55.X.240.80	255.255.255.248 (/29)	81	86	81	85	86	82	83
12	55.X.240.88	255.255.255.248 (/29)	89	94	89	93	94	90	91
13	55.X.240.96	255.255.255.248 (/29)	97	102	97	101	102	98	99
14	55.X.240.104	255.255.255.248 (/29)	105	110	105	109	110	106	107
15	55.X.240.112	255.255.255.248 (/29)	113	118	113	117	118	114	115
16	55.X.240.120	255.255.255.248 (/29)	121	126	121	125	126	122	123
17	55.X.240.128	255.255.255.248 (/29)	129	134	129	133	134	130	131
18	55.X.240.136	255.255.255.248 (/29)	137	142	137	141	142	138	139
19	55.X.240.144	255.255.255.248 (/29)	145	150	145	149	150	146	147
20	55.X.240.152	255.255.255.248 (/29)	153	158	153	157	158	154	155
21	55.X.240.160	255.255.255.248 (/29)	161	166	161	165	166	162	163
22	55.X.240.168	255.255.255.248 (/29)	169	174	169	173	174	170	171
23	55.X.240.176	255.255.255.248 (/29)	177	182	177	181	182	178	179
24	55.X.240.184	255.255.255.248 (/29)	185	190	185	189	190	186	187
25	55.X.240.192	255.255.255.248 (/29)	193	198	193	197	198	194	195
26	55.X.240.200	255.255.255.248 (/29)	201	206	201	205	206	202	203
27	55.X.240.208	255.255.255.248 (/29)	209	214	209	213	214	210	211
28	55.X.240.216	255.255.255.248 (/29)	217	222	217	221	222	218	219
29	55.X.240.224	255.255.255.248 (/29)	225	230	225	229	230	226	227
30	55.X.240.232	255.255.255.248 (/29)	233	238	233	237	238	234	235
31	55.X.240.240	255.255.255.248 (/29)	241	246	241	245	246	242	243
32	55.X.240.248	255.255.255.248 (/29)	249	254	249	253	254	250	251
33	55.X.241.0	255.255.255.248 (/29)	1	6	1	5	6	2	3
34	55.X.241.8	255.255.255.248 (/29)	9	14	9	13	14	10	11
35	55.X.241.16	255.255.255.248 (/29)	17	22	17	21	22	18	19
36	55.X.241.24	255.255.255.248 (/29)	25	30	25	29	30	26	27
37	55.X.241.32	255.255.255.248 (/29)	33	38	33	37	38	34	35
38	55.X.241.40	255.255.255.248 (/29)	41	46	41	45	46	42	43
39	55.X.241.48	255.255.255.248 (/29)	49	54	49	53	54	50	51
40	55.X.241.56	255.255.255.248 (/29)	57	62	57	61	62	58	59
41	55.X.241.64	255.255.255.248 (/29)	65	70	65	69	70	66	67

42	55.X.241.72	255.255.255.248 (/29)	73	78	73	77	78	74	75
43	55.X.241.80	255.255.255.248 (/29)	81	86	81	85	86	82	83
44	55.X.241.88	255.255.255.248 (/29)	89	94	89	93	94	90	91
45	55.X.241.96	255.255.255.248 (/29)	97	102	97	101	102	98	99
46	55.X.241.104	255.255.255.248 (/29)	105	110	105	109	110	106	107
47	55.X.241.112	255.255.255.248 (/29)	113	118	113	117	118	114	115
48	55.X.241.120	255.255.255.248 (/29)	121	126	121	125	126	122	123
49	55.X.241.128	255.255.255.248 (/29)	129	134	129	133	134	130	131
50	55.X.241.136	255.255.255.248 (/29)	137	142	137	141	142	138	139
51	55.X.241.144	255.255.255.248 (/29)	145	150	145	149	150	146	147
52	55.X.241.152	255.255.255.248 (/29)	153	158	153	157	158	154	155
53	55.X.241.160	255.255.255.248 (/29)	161	166	161	165	166	162	163
54	55.X.241.168	255.255.255.248 (/29)	169	174	169	173	174	170	171
55	55.X.241.176	255.255.255.248 (/29)	177	182	177	181	182	178	179
56	55.X.241.184	255.255.255.248 (/29)	185	190	185	189	190	186	187
57	55.X.241.192	255.255.255.248 (/29)	193	198	193	197	198	194	195
58	55.X.241.200	255.255.255.248 (/29)	201	206	201	205	206	202	203
59	55.X.241.208	255.255.255.248 (/29)	209	214	209	213	214	210	211
60	55.X.241.216	255.255.255.248 (/29)	217	222	217	221	222	218	219
61	55.X.241.224	255.255.255.248 (/29)	225	230	225	229	230	226	227
62	55.X.241.232	255.255.255.248 (/29)	233	238	233	237	238	234	235
63	55.X.241.240	255.255.255.248 (/29)	241	246	241	245	246	242	243
64	55.X.241.248	255.255.255.248 (/29)	249	254	249	253	254	250	251

1.12.7 VLAN 30 – VLAN-VOIX

C'est le VLAN pour les téléphones IP du site. Il correspond au plan d'adressage IP historique de tout site pour les PMF mais sur le plan d'adressage en 58.X.X.X. Il faut utiliser le même 3ème octet :

- Siège : 58.X.4.0 /22

- Agences et établissements
  - 1 : 58.X.8.0 /22
  - 2 : 58.X.12.0 /22
  - 3 : 58.X.16.0 /22
  - …etc.

Ce VLAN VOIX local doit intégrer tous les téléphones IP du site, y compris ceux des organismes hébergés.

1.12.8 VLAN 50 – VLAN-WIFI-AGENTS

Le VLAN est toujours le VLAN 50 mais, le plan d'adressage peut être différent à chaque site en fonction du nombre de clients : on pourra trouver de minimum 1 sous-réseau de 254 adresses à maximum 64 sous-réseaux de 6 adresses …ou un mixte de sous-réseaux de tailles différentes…

Voici le tableau des masques à utiliser sur les plages 55.X.251.0 à 55.X.252.254 :

Masque		Nb d'adresses dans le sous-réseau	Nombre de sous-réseaux possibles
/24	255.255.255.0	254	2
/25	255.255.255.128	126	4
/26	255.255.255.192	62	8
/27	255.255.255.224	30	16
/28	255.255.255.240	14	32
/29	255.255.255.248	6	64

L'adresse de l'interface VLAN 50 dans le switch fédérateur du site est toujours la première adresse de la plage.

Exception pour les UGECAM :

Vu la superficie des bâtiments et l'étendue du besoin de couverture, la plage réseau ci-dessus est peut-être insuffisante pour le déploiement wifi dans les Ugecam.

Les VLAN SERVICE MEDICAL et ACCES-PART n'étant pas utilisés dans les Ugecam, nous vous proposons les plages IP ci-dessous :

Voici le tableau des masques à utiliser sur les plages 55.X.244.0 à 55.X.255.254 :

Les plages IP 55.x.246.0 et 55.x.247.0 étant normalement réservées aux accès partenaires (vlan 224), elles ne sont à utiliser qu'en dernier recours.

Masque		Nb d'adresses dans le sous-réseau	Nombre de sous-réseaux possibles
/24	255.255.255.0	254	12
/25	255.255.255.128	126	24
/26	255.255.255.192	62	48
/27	255.255.255.224	30	96
/28	255.255.255.240	14	192
/29	255.255.255.248	6	384

L'adresse de l'interface VLAN 50 dans le switch fédérateur du site est toujours la première adresse de la plage.



MERCI DE CONTACTER LE DR POUR VALIDATION !!

1.12.9 VLAN 53 – VLAN-WIFI-AGENTS-MEDICAL

Comme pour le vlan 3, il a été convenu de dédier un VLAN aux équipements du Service Médical dans les CP des CPAM, cela pour faciliter la gestion bureautique propre au Service Médical. Merci aux Responsables Informatique des CPAM de bien vouloir coopérer avec les MEDICAL qui souhaiteraient bénéficier de ce VLAN

Plages d'adresses proposées :

Le nombre de clients (PMF, Serveurs…) propres aux SM dans ces sites sont variables. La plage d'adresses définie va de **55.X.254.0 à 55.X.255.254** : à utiliser dans N sous-réseaux avec masque libre à adapter en fonction du nombre de PMF du service medical dans le CP.

Le VLAN est toujours le **VLAN 53** mais le plan d'adressage peut être différent sur chaque site en fonction du nombre de clients : on pourra trouver de minimum 1 sous-réseau de 254 adresses à maximum 64 sous-réseaux de 6 adresses …ou un mixte de sous-réseaux de tailles différentes…

Voici le tableau des masques à utiliser sur les plages 55.X.254.0 à 55.X.255.254 :

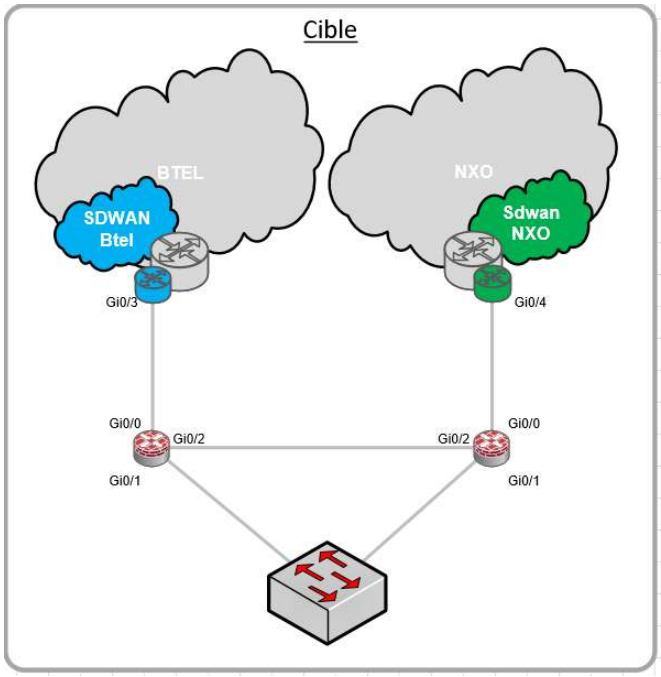
Masque		Nb d'adresses dans le sous-réseau	Nombre de sous-réseaux possibles
/24	255.255.255.0	254	2
/25	255.255.255.128	126	4
/26	255.255.255.192	62	8
/27	255.255.255.224	30	16
/28	255.255.255.240	14	32
/29	255.255.255.248	6	64

L'adresse de l'interface VLAN 53 dans le switch fédérateur du site est toujours la première adresse de la plage.

MERCI DE CONTACTER LE DR POUR VALIDATION !!

1.12.10 VLAN 172 – VLAN-SD-WAN

Ce VLAN sert à l'interconnexion entre le switch n3 et les routeurs SD-WAN.



1.12.11 VLAN 216 – VLAN-CONSOLES-SERVEURS (ILO – IDRAC)

C'est le VLAN pour les consoles des serveurs du type Ilo ou Idrac. Ce vlan sera découpé en /28 pour permettre l'attribution de 13 hosts plus la passerelle par défaut.

Site	Sous-Réseau	Masque	1ère adresse Pour le FEDERATEUR	Equipement console 1	Equipement console 2	…Etc.	Dernière adresse disponible

1	55.X.212.0	28	1	2	3	4	14
2	55.X.212.16	28	17	18	19	20	30
3	55.X.212.32	28	33	34	35	36	46
4	55.X.212.48	28	49	50	51	52	62
5	55.X.212.64	28	65	66	67	68	78
6	55.X.212.80	28	81	82	83	84	94
7	55.X.212.96	28	97	98	99	100	110
8	55.X.212.112	28	113	114	115	116	126
9	55.X.212.128	28	129	130	131	132	142
10	55.X.212.144	28	145	146	147	148	158
11	55.X.212.160	28	161	162	163	164	174
12	55.X.212.176	28	177	178	179	180	190
13	55.X.212.192	28	193	194	195	196	206
14	55.X.212.208	28	209	210	211	212	222
15	55.X.212.224	28	225	226	227	228	238
16	55.X.212.240	28	241	242	243	244	254
17	55.X.213.0	28	1	2	3	4	14
18	55.X.213.16	28	17	18	19	20	30
19	55.X.213.32	28	33	34	35	36	46
20	55.X.213.48	28	49	50	51	52	62
21	55.X.213.64	28	65	66	67	68	78
22	55.X.213.80	28	81	82	83	84	94
23	55.X.213.96	28	97	98	99	100	110
24	55.X.213.112	28	113	114	115	116	126
25	55.X.213.128	28	129	130	131	132	142
26	55.X.213.144	28	145	146	147	148	158
27	55.X.213.160	28	161	162	163	164	174
28	55.X.213.176	28	177	178	179	180	190
29	55.X.213.192	28	193	194	195	196	206
30	55.X.213.208	28	209	210	211	212	222
31	55.X.213.224	28	225	226	227	228	238
32	55.X.213.240	28	241	242	243	244	254
…	55.X.21[4-5].Y	28	…	…	…	…	…

1.12.12 VLAN 224 – VLAN-ACCES-PART

Tous les VLAN accédés à distance par un partenaire extérieur doivent être validés par la DS.

Voir : https://www.cngr.cnamts.fr/contenu/symfony/162

Des ACL consistant à filtrer les communications à l'initiative des actifs présents dans ce VLAN sont à mettre en œuvre pour les limiter **aux seules destinations que constitue « la zone partenaires de RAMAGE » et quelques hosts ciblés sur le LAN local.**

Les ACL à appliquer sont dans les guides de configuration ci-dessous.

Pour des besoins locaux (hors projets nationaux), les équipements doivent être intégrés dans le VLAN 224.

Les CP utiliseront un des sous-réseaux suivants pour le VLAN 224. Il s'agit de choisir un sous-réseau par CP. Si le nombre d'adresses est insuffisant pour un site, veuillez adapter le masque de sous-réseau.

CP	subnet	Masque	Première @	Dernière @	Int vlan 224 Switch N3	Disponibles pour clients				
1	55.X.246.0	255.255.255.248 (/29)	1	6	1	4	5	6	2	3
2	55.X.246.8	255.255.255.248 (/29)	9	14	9	12	13	14	10	11
3	55.X.246.16	255.255.255.248 (/29)	17	22	17	20	21	22	18	19
4	55.X.246.24	255.255.255.248 (/29)	25	30	25	28	29	30	26	27
5	55.X.246.32	255.255.255.248 (/29)	33	38	33	36	37	38	34	35
6	55.X.246.40	255.255.255.248 (/29)	41	46	41	44	45	46	42	43
7	55.X.246.48	255.255.255.248 (/29)	49	54	49	52	53	54	50	51
8	55.X.246.56	255.255.255.248 (/29)	57	62	57	60	61	62	58	59
9	55.X.246.64	255.255.255.248 (/29)	65	70	65	68	69	70	66	67
10	55.X.246.72	255.255.255.248 (/29)	73	78	73	76	77	78	74	75
11	55.X.246.80	255.255.255.248 (/29)	81	86	81	84	85	86	82	83
12	55.X.246.88	255.255.255.248 (/29)	89	94	89	92	93	94	90	91
13	55.X.246.96	255.255.255.248 (/29)	97	102	97	100	101	102	98	99
14	55.X.246.104	255.255.255.248 (/29)	105	110	105	108	109	110	106	107
15	55.X.246.112	255.255.255.248 (/29)	113	118	113	116	117	118	114	115
16	55.X.246.120	255.255.255.248 (/29)	121	126	121	124	125	126	122	123
17	55.X.246.128	255.255.255.248 (/29)	129	134	129	132	133	134	130	131
18	55.X.246.136	255.255.255.248 (/29)	137	142	137	140	141	142	138	139
19	55.X.246.144	255.255.255.248 (/29)	145	150	145	148	149	150	146	147
20	55.X.246.152	255.255.255.248 (/29)	153	158	153	156	157	158	154	155
21	55.X.246.160	255.255.255.248 (/29)	161	166	161	164	165	166	162	163
22	55.X.246.168	255.255.255.248 (/29)	169	174	169	172	173	174	170	171
23	55.X.246.176	255.255.255.248 (/29)	177	182	177	180	181	182	178	179
24	55.X.246.184	255.255.255.248 (/29)	185	190	185	188	189	190	186	187
25	55.X.246.192	255.255.255.248 (/29)	193	198	193	196	197	198	194	195
26	55.X.246.200	255.255.255.248 (/29)	201	206	201	204	205	206	202	203
27	55.X.246.208	255.255.255.248 (/29)	209	214	209	212	213	214	210	211
28	55.X.246.216	255.255.255.248 (/29)	217	222	217	220	221	222	218	219
29	55.X.246.224	255.255.255.248 (/29)	225	230	225	228	229	230	226	227
30	55.X.246.232	255.255.255.248 (/29)	233	238	233	236	237	238	234	235
31	55.X.246.240	255.255.255.248 (/29)	241	246	241	244	245	246	242	243
32	55.X.246.248	255.255.255.248 (/29)	249	254	249	252	253	254	250	251
33	55.X.247.0	255.255.255.248 (/29)	1	6	1	4	5	6	2	3
34	55.X.247.8	255.255.255.248 (/29)	9	14	9	12	13	14	10	11
35	55.X.247.16	255.255.255.248 (/29)	17	22	17	20	21	22	18	19
36	55.X.247.24	255.255.255.248 (/29)	25	30	25	28	29	30	26	27
37	55.X.247.32	255.255.255.248 (/29)	33	38	33	36	37	38	34	35
38	55.X.247.40	255.255.255.248 (/29)	41	46	41	44	45	46	42	43
39	55.X.247.48	255.255.255.248 (/29)	49	54	49	52	53	54	50	51
40	55.X.247.56	255.255.255.248 (/29)	57	62	57	60	61	62	58	59
41	55.X.247.64	255.255.255.248 (/29)	65	70	65	68	69	70	66	67
42	55.X.247.72	255.255.255.248 (/29)	73	78	73	76	77	78	74	75
43	55.X.247.80	255.255.255.248 (/29)	81	86	81	84	85	86	82	83
44	55.X.247.88	255.255.255.248 (/29)	89	94	89	92	93	94	90	91
45	55.X.247.96	255.255.255.248 (/29)	97	102	97	100	101	102	98	99
46	55.X.247.104	255.255.255.248 (/29)	105	110	105	108	109	110	106	107
47	55.X.247.112	255.255.255.248 (/29)	113	118	113	116	117	118	114	115
48	55.X.247.120	255.255.255.248 (/29)	121	126	121	124	125	126	122	123
49	55.X.247.128	255.255.255.248 (/29)	129	134	129	132	133	134	130	131
50	55.X.247.136	255.255.255.248 (/29)	137	142	137	140	141	142	138	139
51	55.X.247.144	255.255.255.248 (/29)	145	150	145	148	149	150	146	147

52	55.X.247.152	255.255.255.248 (/29)	153	158	153	156	157	158	154	155
53	55.X.247.160	255.255.255.248 (/29)	161	166	161	164	165	166	162	163
54	55.X.247.168	255.255.255.248 (/29)	169	174	169	172	173	174	170	171
55	55.X.247.176	255.255.255.248 (/29)	177	182	177	180	181	182	178	179
56	55.X.247.184	255.255.255.248 (/29)	185	190	185	188	189	190	186	187
57	55.X.247.192	255.255.255.248 (/29)	193	198	193	196	197	198	194	195
58	55.X.247.200	255.255.255.248 (/29)	201	206	201	204	205	206	202	203
59	55.X.247.208	255.255.255.248 (/29)	209	214	209	212	213	214	210	211
60	55.X.247.216	255.255.255.248 (/29)	217	222	217	220	221	222	218	219
61	55.X.247.224	255.255.255.248 (/29)	225	230	225	228	229	230	226	227
62	55.X.247.232	255.255.255.248 (/29)	233	238	233	236	237	238	234	235
63	55.X.247.240	255.255.255.248 (/29)	241	246	241	244	245	246	242	243
64	55.X.247.248	255.255.255.248 (/29)	249	254	249	252	253	254	250	251

1.12.13 VLAN 225 - VLAN-ACCES-PART-MEDICAL

Dans le cas d'un site 100% MEDICAL, le VLAN est le 224 auquel il faut associer une plage d'adresses disponible dans le tableau ci-dessus.

Lorsque le service médical est hébergé dans une agence de CPAM, le VLAN 224 étant utilisé par la CPAM, le VLAN « Acces-Part » pour le service medical est le 225 auquel il faut associer une plage d'adresses disponible dans le tableau ci-dessus.

1.12.14 VLAN 226 –VLAN-IMPRIMANTES

Les CP utiliseront les plans d'adressage suivant pour le VLAN226 : 55.xx.249.x/29

Site	CPAM xxx	Masque	Masque	Nombre d'imp	INT-VLAN225-IMP	IMP-CANON1	IMP-CANON2	IMP-CANON3	IMP-CANON4	IMP-CANON5
CP1	55.xx.249.0	255.255.255.248	/29	5	55.xx.249.1	55.xx.249.2	55.xx.249.3	55.xx.249.4	55.xx.249.5	55.xx.249.6
CP2	55.xx.249.8	255.255.255.248	/29	5	55.xx.249.9	55.xx.249.10	55.xx.249.11	55.xx.249.12	55.xx.249.13	55.xx.249.14
CP3	55.xx.249.16	255.255.255.248	/29	5	55.xx.249.17	55.xx.249.18	55.xx.249.19	55.xx.249.20	55.xx.249.21	55.xx.249.22
CP4	55.xx.249.24	255.255.255.248	/29	5	55.xx.249.25	55.xx.249.26	55.xx.249.27	55.xx.249.28	55.xx.249.29	55.xx.249.30
CP5	55.xx.249.32	255.255.255.248	/29	5	55.xx.249.33	55.xx.249.34	55.xx.249.35	55.xx.249.36	55.xx.249.37	55.xx.249.38
CP6	55.xx.249.40	255.255.255.248	/29	5	55.xx.249.41	55.xx.249.42	55.xx.249.43	55.xx.249.44	55.xx.249.45	55.xx.249.46
CP7	55.xx.249.48	255.255.255.248	/29	5	55.xx.249.49	55.xx.249.50	55.xx.249.51	55.xx.249.52	55.xx.249.53	55.xx.249.54
CP8	55.xx.249.56	255.255.255.248	/29	5	55.xx.249.57	55.xx.249.58	55.xx.249.59	55.xx.249.60	55.xx.249.61	55.xx.249.62
CP9	55.xx.249.64	255.255.255.248	/29	5	55.xx.249.65	55.xx.249.66	55.xx.249.67	55.xx.249.68	55.xx.249.69	55.xx.249.70
CP10	55.xx.249.72	255.255.255.248	/29	5	55.xx.249.73	55.xx.249.74	55.xx.249.75	55.xx.249.76	55.xx.249.77	55.xx.249.78
CP11	55.xx.249.80	255.255.255.248	/29	5	55.xx.249.81	55.xx.249.82	55.xx.249.83	55.xx.249.84	55.xx.249.85	55.xx.249.86
CP12	55.xx.249.88	255.255.255.248	/29	5	55.xx.249.89	55.xx.249.90	55.xx.249.91	55.xx.249.92	55.xx.249.93	55.xx.249.94
CP13	55.xx.249.96	255.255.255.248	/29	5	55.xx.249.97	55.xx.249.98	55.xx.249.99	55.xx.249.100	55.xx.249.101	55.xx.249.102
CP14	55.xx.249.104	255.255.255.248	/29	5	55.xx.249.105	55.xx.249.106	55.xx.249.107	55.xx.249.108	55.xx.249.109	55.xx.249.110
CP15	55.xx.249.112	255.255.255.248	/29	5	55.xx.249.113	55.xx.249.114	55.xx.249.115	55.xx.249.116	55.xx.249.117	55.xx.249.118

Le VLAN peut être différent sur chaque site en fonction du nombre de clients : on pourra trouver de minimum 1 sous-réseau 32 sous-réseaux de 6 adresses …ou un mixte de sous-réseaux de tailles différentes…

Masque		Nb d'adresses dans le sous-réseau	Nombre de sous-réseaux possibles
/27	255.255.255.224	30	8
/28	255.255.255.240	14	16
/29	255.255.255.248	6	32

1.12.15 VLAN 227 –VLAN-IMPRIMANTES-MEDICAL

Les agences utiliseront les plans d'adressage suivants pour le VLAN227 : 55.2XX.249.Y/29 en collaboration avec la MEDICAL qu'ils hébergent.

Machines IP dans les ERSM

ORGANISMES	Numero reseau IP	Masque	Adresses disponibles
BORDEAUX	55.208.0.0	255.255.0.0	55.208.0.1 à 55.208.255.254
CLERMONT-FERRAND	55.209.0.0	255.255.0.0	55.209.0.1 à 55.209.255.254
DIJON	55.210.0.0	255.255.0.0	55.210.0.1 à 55.197.255.254
LILLE	55.211.0.0	255.255.0.0	55.211.0.1 à 55.198.255.254
LIMOGES	55.212.0.0	255.255.0.0	55.212.0.1 à 55.212.255.254
LYON	55.213.0.0	255.255.0.0	55.213.0.1 à 55.213.255.254
MARSEILLE	55.214.0.0	255.255.0.0	55.214.0.1 à 55.214.255.254
MONTPELLIER	55.215.0.0	255.255.0.0	55.215.0.1 à 55.215.255.254
NANCY	55.216.0.0	255.255.0.0	55.216.0.1 à 55.202.255.254
NANTES	55.217.0.0	255.255.0.0	55.217.0.1 à 55.203.255.254
ORLEANS	55.218.0.0	255.255.0.0	55.218.0.1 à 55.204.255.254
RENNES	55.219.0.0	255.255.0.0	55.219.0.1 à 55.205.255.254
TOULOUSE	55.220.0.0	255.255.0.0	55.220.0.1 à 55.206.255.254
ROUEN	55.221.0.0	255.255.0.0	55.221.0.1 à 55.221.255.254
ILLE DE FRANCE(SMAMIF)	55.169.0.0	255.255.0.0	55.169.0.1 à 55.169.225.254

Adressage pour les SERVICE MEDICAUX :

Site	DRSM XX	Masque	Masque	Nombre d'imp	INT-VLAN227-CANON-	IMP-CANON1	IMP-CANON2	IMP-CANON3	IMP-CANON4	IMP-CANON5
ELSM 1	55.2xx.249.0	255.255.255.248	/29	5	55.2xx.249.1	55.2xx.249.2	55.2xx.249.3	55.2xx.249.4	55.2xx.249.5	55.2xx.249.6
ELSM 2	55.2xx.249.8	255.255.255.248	/29	5	55.2xx.249.9	55.2xx.249.10	55.2xx.249.11	55.2xx.249.12	55.2xx.249.13	55.2xx.249.14
ELSM 3	55.2xx.249.16	255.255.255.248	/29	5	55.2xx.249.17	55.2xx.249.18	55.2xx.249.19	55.2xx.249.20	55.2xx.249.21	55.2xx.249.22
ELSM 4	55.2xx.249.24	255.255.255.248	/29	5	55.2xx.249.25	55.2xx.249.26	55.2xx.249.27	55.2xx.249.28	55.2xx.249.29	55.2xx.249.30
ELSM 5	55.2xx.249.32	255.255.255.248	/29	5	55.2xx.249.33	55.2xx.249.34	55.2xx.249.35	55.2xx.249.36	55.2xx.249.37	55.2xx.249.38
ELSM 6	55.2xx.249.40	255.255.255.248	/29	5	55.2xx.249.41	55.2xx.249.42	55.2xx.249.43	55.2xx.249.44	55.2xx.249.45	55.2xx.249.46
ELSM 7	55.2xx.249.48	255.255.255.248	/29	5	55.2xx.249.49	55.2xx.249.50	55.2xx.249.51	55.2xx.249.52	55.2xx.249.53	55.2xx.249.54
ELSM 8	55.2xx.249.56	255.255.255.248	/29	5	55.2xx.249.57	55.2xx.249.58	55.2xx.249.59	55.2xx.249.60	55.2xx.249.61	55.2xx.249.62
ELSM 9	55.2xx.249.64	255.255.255.248	/29	5	55.2xx.249.65	55.2xx.249.66	55.2xx.249.67	55.2xx.249.68	55.2xx.249.69	55.2xx.249.70
ELSM 10	55.2xx.249.72	255.255.255.248	/29	5	55.2xx.249.73	55.2xx.249.74	55.2xx.249.75	55.2xx.249.76	55.2xx.249.77	55.2xx.249.78
ELSM 11	55.2xx.249.80	255.255.255.248	/29	5	55.2xx.249.81	55.2xx.249.82	55.2xx.249.83	55.2xx.249.84	55.2xx.249.85	55.2xx.249.86
ELSM 12	55.2xx.249.88	255.255.255.248	/29	5	55.2xx.249.89	55.2xx.249.90	55.2xx.249.91	55.2xx.249.92	55.2xx.249.93	55.2xx.249.94
ELSM 13	55.2xx.249.96	255.255.255.248	/29	5	55.2xx.249.97	55.2xx.249.98	55.2xx.249.99	55.2xx.249.100	55.2xx.249.101	55.2xx.249.102
ELSM 14	55.2xx.249.104	255.255.255.248	/29	5	55.2xx.249.105	55.2xx.249.106	55.2xx.249.107	55.2xx.249.108	55.2xx.249.109	55.2xx.249.110
ELSM 15	55.2xx.249.112	255.255.255.248	/29	5	55.2xx.249.113	55.2xx.249.114	55.2xx.249.115	55.2xx.249.116	55.2xx.249.117	55.2xx.249.118
ELSM 16	55.2xx.249.120	255.255.255.248	/29	5	55.2xx.249.121	55.2xx.249.122	55.2xx.249.123	55.2xx.249.124	55.2xx.249.125	55.2xx.249.126
ELSM 17	55.2xx.249.128	255.255.255.248	/29	5	55.2xx.249.129	55.2xx.249.130	55.2xx.249.131	55.2xx.249.132	55.2xx.249.133	55.2xx.249.134
ELSM 18	55.2xx.249.136	255.255.255.248	/29	5	55.2xx.249.137	55.2xx.249.138	55.2xx.249.139	55.2xx.249.140	55.2xx.249.141	55.2xx.249.142
ELSM 19	55.2xx.249.144	255.255.255.248	/29	5	55.2xx.249.145	55.2xx.249.146	55.2xx.249.147	55.2xx.249.148	55.2xx.249.149	55.2xx.249.150
ELSM 20	55.2xx.249.152	255.255.255.248	/29	5	55.2xx.249.153	55.2xx.249.154	55.2xx.249.155	55.2xx.249.156	55.2xx.249.157	55.2xx.249.158
ELSM 21	55.2xx.249.160	255.255.255.248	/29	5	55.2xx.249.161	55.2xx.249.162	55.2xx.249.163	55.2xx.249.164	55.2xx.249.165	55.2xx.249.166
ELSM 22	55.2xx.249.168	255.255.255.248	/29	5	55.2xx.249.169	55.2xx.249.170	55.2xx.249.171	55.2xx.249.172	55.2xx.249.173	55.2xx.249.174
ELSM 23	55.2xx.249.176	255.255.255.248	/29	5	55.2xx.249.177	55.2xx.249.178	55.2xx.249.179	55.2xx.249.180	55.2xx.249.181	55.2xx.249.182
ELSM 24	55.2xx.249.184	255.255.255.248	/29	5	55.2xx.249.185	55.2xx.249.186	55.2xx.249.187	55.2xx.249.188	55.2xx.249.189	55.2xx.249.190
ELSM 25	55.2xx.249.192	255.255.255.248	/29	5	55.2xx.249.193	55.2xx.249.194	55.2xx.249.195	55.2xx.249.196	55.2xx.249.197	55.2xx.249.198
ELSM 26	55.2xx.249.200	255.255.255.248	/29	5	55.2xx.249.201	55.2xx.249.202	55.2xx.249.203	55.2xx.249.204	55.2xx.249.205	55.2xx.249.206
ELSM 27	55.2xx.249.208	255.255.255.248	/29	5	55.2xx.249.209	55.2xx.249.210	55.2xx.249.211	55.2xx.249.212	55.2xx.249.213	55.2xx.249.214
ELSM 28	55.2xx.249.216	255.255.255.248	/29	5	55.2xx.249.217	55.2xx.249.218	55.2xx.249.219	55.2xx.249.220	55.2xx.249.221	55.2xx.249.222
ELSM 29	55.2xx.249.224	255.255.255.248	/29	5	55.2xx.249.225	55.2xx.249.226	55.2xx.249.227	55.2xx.249.228	55.2xx.249.229	55.2xx.249.230
ELSM 30	55.2xx.249.232	255.255.255.248	/29	5	55.2xx.249.233	55.2xx.249.234	55.2xx.249.235	55.2xx.249.236	55.2xx.249.237	55.2xx.249.238
ELSM 31	55.2xx.249.240	255.255.255.248	/29	5	55.2xx.249.241	55.2xx.249.242	55.2xx.249.243	55.2xx.249.244	55.2xx.249.245	55.2xx.249.246
ELSM 32	55.2xx.249.248	255.255.255.248	/29	5	55.2xx.249.249	55.2xx.249.250	55.2xx.249.251	55.2xx.249.252	55.2xx.249.253	55.2xx.249.254

Le VLAN peut être différent sur chaque site en fonction du nombre de clients : on pourra trouver de minimum 1 sous-réseau 32 sous-réseaux de 6 adresses …ou un mixte de sous-réseaux de tailles différentes…

Masque		Nb d'adresses dans le sous-réseau	Nombre de sous-réseaux possibles
/27	255.255.255.224	30	8
/28	255.255.255.240	14	16
/29	255.255.255.248	6	32

1.12.16 VLAN 229 - VLAN- IMPRIMANTES-CDS

Suite à la reprise des CDS (Centre De Santé) par les UGECAM, les imprimantes des CDS seront sur le VLAN 229. Le plan d'adressage sera fourni par le DR à la demande.

1.12.17 VLAN 901 – VLAN-ADMIN-RESEAU

➔ **Dans le VLAN 901, la première adresse du sous-réseau est à attribuer au fédérateur.**

Ce tableau permet d'attribuer des adresses à un maximum de 14 switches ou stacks dans un maximum de 32 sites.

ATTENTION :
Dans le cas où le site ne contient qu'un seul switch ou qu'un seul stack, l'interface vlan 901 n'est pas à créer car elle resterait « DOWN ». Dans ce cas, à défaut de VLAN d'Admin, il faut créer une interface loopback1 en /32 (255.255.255.255) à laquelle on attribue la dernière adresse IP du VLAN :

- ⇨ **Voir le tableau plus bas**
- ⇨ **Voir les guides de configuration**

N.B : L'adresse de loopback sera diffusée sur le réseau RAMAGE via votre interface VLAN 5.

Site	Sous-réseau	Masque	1ère adresse Pour le FEDERATEUR	Switch ou stack d'extrémité 1	Switch ou stack d'extrémité 2	…Etc.	Dernière adresse POUR LA LOOPBACK1
1	55.X.0.0	255.255.255.240 (/28)	1	2	3	…	14
2	55.X.0.16	255.255.255.240 (/28)	17	18	19	…	30
3	55.X.0.32	255.255.255.240 (/28)	33	34	35	…	46
4	55.X.0.48	255.255.255.240 (/28)	49	50	51	…	62
5	55.X.0.64	255.255.255.240 (/28)	65	66	67	…	78
6	55.X.0.80	255.255.255.240 (/28)	81	82	83	…	94
7	55.X.0.96	255.255.255.240 (/28)	97	98	99	…	110
8	55.X.0.112	255.255.255.240 (/28)	113	114	115	…	126
9	55.X.0.128	255.255.255.240 (/28)	129	130	131	…	142
10	55.X.0.144	255.255.255.240 (/28)	145	146	147	…	158
11	55.X.0.160	255.255.255.240 (/28)	161	162	163	…	174
12	55.X.0.176	255.255.255.240 (/28)	177	178	179	…	190
13	55.X.0.192	255.255.255.240 (/28)	193	194	195	…	206
14	55.X.0.208	255.255.255.240 (/28)	209	210	211	…	222
15	55.X.0.224	255.255.255.240 (/28)	225	226	227	…	238
16	55.X.0.240	255.255.255.240 (/28)	241	242	243	…	254
Si vous avez plus de 16 sites continuez avec le plan d'adressage ci-dessous							
Site	Sous-réseau	Masque	1ère adresse Pour le FEDERATEUR	Switch ou stack d'extrémité 1	Switch ou stack d'extrémité 2	…Etc.	Dernière adresse POUR LA LOOPBACK1
17	55.X.1.0	255.255.255.240 (/28)	1	2	3	…	14
18	55.X.1.16	255.255.255.240 (/28)	17	18	19	…	30
19	55.X.1.32	255.255.255.240 (/28)	33	34	35	…	46
20	55.X.1.48	255.255.255.240 (/28)	49	50	51	…	62
21	55.X.1.64	255.255.255.240 (/28)	65	66	67	…	78
22	55.X.1.80	255.255.255.240 (/28)	81	82	83	…	94
23	55.X.1.96	255.255.255.240 (/28)	97	98	99	…	110
24	55.X.1.112	255.255.255.240 (/28)	113	114	115	…	126
25	55.X.1.128	255.255.255.240 (/28)	129	130	131	…	142
26	55.X.1.144	255.255.255.240 (/28)	145	146	147	…	158
27	55.X.1.160	255.255.255.240 (/28)	161	162	163	…	174
28	55.X.1.176	255.255.255.240 (/28)	177	178	179	…	190
29	55.X.1.192	255.255.255.240 (/28)	193	194	195	…	206
30	55.X.1.208	255.255.255.240 (/28)	209	210	211	…	222
31	55.X.1.224	255.255.255.240 (/28)	225	226	227	…	238
32	55.X.1.240	255.255.255.240 (/28)	241	242	243	…	254

En cas de difficulté, contacter le DR via le PSN.

Normalisation du nommage de l'interface loopback1 :

interface LoopBack1
description INT-LOOPBACK-ADMIN-RESEAU
ip address 55.xx.xx.xx 255.255.255.255

1.12.18 VLAN 902 – VLAN-ADMIN-WIFI

Ce tableau permet d'attribuer des adresses à un maximum de 14 équipements WIFI (AP, contrôleurs…) dans un maximum de 32 sites.

Site	Sous-réseau	Masque	Pour le FEDERATEUR	Equipement wifi 1	Equipement wifi 2	…Etc.	Dernière adresse POUR LA LOOPBACK2
1	55.X.2.0	255.255.255.240 (/28)	1	2	3	…	14
2	55.X.2.16	255.255.255.240 (/28)	17	18	19	…	30
3	55.X.2.32	255.255.255.240 (/28)	33	34	35	…	46
4	55.X.2.48	255.255.255.240 (/28)	49	50	51	…	62
5	55.X.2.64	255.255.255.240 (/28)	65	66	67	…	78
6	55.X.2.80	255.255.255.240 (/28)	81	82	83	…	94
7	55.X.2.96	255.255.255.240 (/28)	97	98	99	…	110
8	55.X.2.112	255.255.255.240 (/28)	113	114	115	…	126
9	55.X.2.128	255.255.255.240 (/28)	129	130	131	…	142
10	55.X.2.144	255.255.255.240 (/28)	145	146	147	…	158
11	55.X.2.160	255.255.255.240 (/28)	161	162	163	…	174
12	55.X.2.176	255.255.255.240 (/28)	177	178	179	…	190
13	55.X.2.192	255.255.255.240 (/28)	193	194	195	…	206
14	55.X.2.208	255.255.255.240 (/28)	209	210	211	…	222
15	55.X.2.224	255.255.255.240 (/28)	225	226	227	…	238
16	55.X.2.240	255.255.255.240 (/28)	241	242	243	…	254
Si vous avez plus de 16 sites continuez avec le plan d'adressage ci-dessous							
Site	Sous-réseau	Masque	Pour le FEDERATEUR	Equipement wifi 1	Equipement wifi 2	…Etc.	Dernière adresse POUR LA LOOPBACK2
17	55.X.3.0	255.255.255.240 (/28)	1	2	3	…	14
18	55.X.3.16	255.255.255.240 (/28)	17	18	19	…	30
19	55.X.3.32	255.255.255.240 (/28)	33	34	35	…	46
20	55.X.3.48	255.255.255.240 (/28)	49	50	51	…	62
21	55.X.3.64	255.255.255.240 (/28)	65	66	67	…	78
22	55.X.3.80	255.255.255.240 (/28)	81	82	83	…	94
23	55.X.3.96	255.255.255.240 (/28)	97	98	99	…	110
24	55.X.3.112	255.255.255.240 (/28)	113	114	115	…	126
25	55.X.3.128	255.255.255.240 (/28)	129	130	131	…	142
26	55.X.3.144	255.255.255.240 (/28)	145	146	147	…	158
27	55.X.3.160	255.255.255.240 (/28)	161	162	163	…	174
28	55.X.3.176	255.255.255.240 (/28)	177	178	179	…	190
29	55.X.3.192	255.255.255.240 (/28)	193	194	195	…	206
30	55.X.3.208	255.255.255.240 (/28)	209	210	211	…	222
31	55.X.3.224	255.255.255.240 (/28)	225	226	227	…	238
32	55.X.3.240	255.255.255.240 (/28)	241	242	243	…	254

En cas de difficulté, contacter le DR via le PSN.

1.12.19 VLAN 903 – VLAN-ROUTEUR-WIFI-INVITE

Suite au projet SDWAN, nous migrons le routeur WIFI INVITE du vlan 5 au vlan903 sur le switch N3:

Pour une CPAM :

interface Vlan-interface 903

Description INT-VLAN-ROUTEUR-WIFI-INVITE

55.xx.237.5 / 255.255.255.252 (/30) **|suite à migration SDWAN – VLAN ROUTEUR WIFI INVITE**

1.13 VLAN ET ADRESSAGE IP NORMALISES POUR LES CTI

Voici la liste des VLAN, leur nom, la description des interfaces et le plan d'adressage IP normalisé.

SITE	PLAGE IP	VLAN	NOM VLAN	DESCRIPTION INT VLAN	RESEAU	GATEWAY	COMMENTAIRES
NORME	55.250.X.0/20 (55.250.X.1-55.250.[X+15].254)	5	VLAN-INTERCOWAN	INT-VLAN-INTERCOWAN	55.250.[X+14].0 /27	.1	
		55	VLAN-ROUTEUR-4G	INT VLAN-ROUTEUR-4G	fourni par DR		
		16	VLAN-DATA	INT-VLAN-DATA	55.250.[X+0].0 /24	.1	
		33	VLAN-VOIX	INT-VLAN-VOIX	58.250.[X+0].0 /24	.1	
		216	VLAN-CONSOLE-SERVEURS	INT-VLAN-CONSOLE-SERVEURS	55.250.[X+15].32 /27	.33	
		226	VLAN-IMPRIMANTES	INT-VLAN-IMPRIMANTES	55.250.[X+1].0 /28	.1	
		66	VLAN-CTRL-ACCES	INT-VLAN-CTRL-ACCES	55.250.[X+2].0 /24	.1	Si besoin
		230	VLAN-GW-CETIAM	INT-VLAN-GW-CETIAM	55.249.X.X /29		Automatique DR
		239	VLAN-MGT-IPANEMA	INT-VLAN-MGT-IPANEMA	55.239.x.x /29		Automatique DR
		902	VLAN-ADMIN-RESEAU	INT-VLAN-ADMIN-RESEAU	55.250.[X+15].64 /27	.65	
		904	VLAN-ADMIN-WIFI	INT-VLAN-ADMIN-WIFI	55.250.[X+15].0 /28	.1	Si wifi sur site
		50	VLAN-WIFI-AGENTS	INT-VLAN-WIFI-AGENTS	55.250.[X+3].0 /24	.1	Si wifi sur site

Valeur de X pour chaque CTI :

CTI-SAINT-ETIENNE : 0
CTI-ROUEN : 80
CTI-ANGERS : 96
CTI-MELUN : 32
CRIP : 48
CTI-SOPHIA-ANTIPOLIS : 64
CICOA : 112

Certains CTI ont déployés des VLAN supplémentaires pour des besoins spécifiques. Ils peuvent les conserver. Dans le cas d'un nouveau besoin, veuillez prendre contact avec le DR.

1.14 ADRESSAGE IP NORMALISE POUR IRSA, UC-CMP

Il s'agit de nouveaux Organismes (exemple : IRSA) qui intègrent le réseau RAMAGE. Ce ne sont ni des CPAM, , ni des UGECAM.

Le plan d'adressage est tiré un découpage du réseau 55.24/16 en 8 subnets /19 : 55.24.0.0/19, 55.24.32.0/19, ... 55.24.224.0/19.

Pour ces sites, seul le plan d'adressage est spécifique. Toutes les autres recommandations sont à suivre selon le même modèle.

Le plan d'adressage IP est détaillé page suivante. Pour une vision globale, il explique le plan d'adressage IP des sièges et des agences / établissements.



MERCI DE CONTACTER LE DR POUR VALIDATION !!

CAS GENERAL :

Plages IP par Organisme			
1	55.24.0.0	/19	255.255.224.0
2	55.24.32.0	/19	255.255.224.0
3	55.24.64.0	/19	255.255.224.0
4	55.24.96.0	/19	255.255.224.0
5	55.24.128.0	/19	255.255.224.0
6	55.24.160.0	/19	255.255.224.0
7	55.24.192.0	/19	255.255.224.0
8	55.24.224.0	/19	255.255.224.0

Détail par site		
55.24.Y.0	/22	SIEGE (PC / Serveurs)
55.24.Y+4.0	/24	Etablissement-1
55.24.Y+5.0	/24	Etablissement-2
55.24.Y+6.0	/24	Etablissement-3
55.24.Y+7.0	/24	Etablissement-4
55.24.Y+8.0	/24	Etablissement-5
55.24.Y+9.0	/24	Etablissement-6
55.24.Y+10.0	/24	Etablissement-7
55.24.Y+11.0	/24	Etablissement-8
55.24.Y+12.0	/24	Etablissement-9
55.24.Y+13.0	/24	Etablissement-10
55.24.Y+14.0	/24	Etablissement-11
55.24.Y+15.0	/24	Etablissement-12
55.24.Y+16.0	/24	Etablissement-13
55.24.Y+17.0	/24	Etablissement-14
55.24.Y+18.0	/24	Etablissement-15
55.24.Y+19.0	/24	Etablissement-16
55.24.Y+20.0	/24	Etablissement-17
55.24.Y+21.0	/24	Etablissement-18
55.24.Y+22.0	/24	Etablissement-19
55.24.Y+23.0	/24	Etablissement-20
55.24.Y+24.0	/24	Etablissement-21
55.24.Y+25.0	/24	Etablissement-22
55.24.Y+26.0	/24	Etablissement-23
55.24.Y+27.0	/24	Etablissement-24
55.24.Y+28.0	/24	Etablissement-25
55.24.Y+29.0	/24	Etablissement-26
55.24.Y+30.0	/24	SIEGE (autres VLAN)
55.24.Z.0 (Z = Y + 31	/24	SIEGE (autres VLAN)

SIEGE

VLAN POUR LES DONNEES

VLAN		Adressage					
N°	Nom	Réseau	1ère adresse	Dernière adresse	Masque	Adresses	Commentaire
5	VLAN-INTERCOWAN	55.24.Z.0	55.24.Z.1	55.24.Z.6	/29	6 adresses	3 @ routeurs, 1 @ switch, 1 @ Ipanema
900	VLAN-ADMIN-UCOPIA	55.24.Z.0	55.24.31.1	55.24.31.2	/30	2 adresses	Réservé pour admin UCOPIA - wifi invités
-	Non utilisé	55.24.Z.4	55.24.31.5	55.24.31.6	/30	2 adresses	*réservé pour plus tard*
224	VLAN-ACCES-PART	55.24.Z.16	55.24.Z.17	55.24.Z.31	/28	14 adresses	Equipements accédés par des tiers (+ACL !)
901	VLAN-ADMIN-RESEAU	55.24.Z.32	55.24.Z.33	55.24.Z.63	/27	30 adresses	Switches
219	VLAN-PCA-DATA	55.24.Z.64	55.24.Z.65	55.24.Z.94	/27	30 adresses	Clients PCA
50	VLAN-WIFI-AGENTS	55.24.Z.96	55.24.Z.97	55.24.Z.126	/27	30 adresses	Clients wifi
902	VLAN-ADMIN-WIFI	55.24.Z.128	55.24.Z.129	55.24.Z.254	/25	126 adresses	AP et contrôleur wifi
6	VLAN-DATA	55.24.Y.0	55.24.Y.1	55.24.Y+3.254	/22	1022 adresses	PC et serveurs
226	VLAN-IMPRIMANTES	55.24.Y+30.0	55.24.Y+30.1	55.24.Y+30.62	/26	62 adresses	Imprimantes
-	*Non utilisé*	55.24.Y+30.64	55.24.Y+30.65	55.24.Y+30.126	/26	62 adresses	*réservé pour plus tard*

SIEGE

VLAN POUR LA VOIX

VLAN		Adressage					
N°	Nom	Réseau	1ère adresse	Dernière adresse	Masque	Adresses	Commentaire
220	VLAN-PCA-VOIX	58.24.Y.64	58.24.Y.65	58.24.Y.126	/26	62 adresses	Clients PCA
30	VLAN-VOIX	58.24.Y.0	58.24.Y.1	58.24.Y+3.254	/22	1022 adresses	Téléphones IP

ETABLISSEMENTS : Etablissement-1 : X = Y+4 - ...etc... Etablissement 27 : X = Y+30

VLAN POUR LES DONNEES

VLAN		Adressage					
N°	Nom	Réseau	1ère adresse	Dernière adresse	Masque	Adresses	Commentaire
5	VLAN-INTERCOWAN	55.24.X.0	55.24.X.1	55.24.X.6	/29	6 adresses	3 @ routeurs, 1 @ switch, 1 @ ipanema
-	*Non utilisé*	*55.24.X.8*	*55.24.X.9*	*55.24.X.15*	/29	*6 adresses*	*réservé pour plus tard*
901	VLAN-ADMIN-RESEAU	*55.24.X.16*	*55.24.X.17*	*55.24.X.31*	/28	*14 adresses*	Switches
902	VLAN-ADMIN-WIFI	*55.24.X.32*	*55.24.X.33*	*55.24.X.46*	/28	*14 adresses*	AP et contrôleur wifi
224	VLAN-ACCES-PART	55.24.X.48	55.24.X.49	55.24.X.63	/28	14 adresses	Equipements accédés par des tiers (+ACL !)
226	VLAN-IMPRIMANTES	*55.24.X.64*	*55.24.X.65*	*55.24.X.94*	/27	*30 adresses*	Imprimantes
50	VLAN-WIFI-AGENTS	55.24.X.96	55.24.X.97	55.24.X.126	/27	30 adresses	Clients wifi
4	VLAN-DATA	55.24.X.128	55.24.X.129	55.24.X.254	/25	126 adresses	PC et serveurs

VLAN POUR LA VOIX

VLAN		Adressage					
N°	Nom	Réseau	1ère adresse	Dernière adresse	Masque	Adresses	Commentaire
30	VLAN VOIX	58.24.X.128	58.24.X.129	58.24.X.254	/25	126 adresses	Téléphones IP

Dans les agences / établissements, s'il n'y a qu'un seul switch ou stack, le vlan 901 ne montera pas : ne pas le créer mais utiliser un interface de loopback1 ayant la dernière adresse IP de sous réseau (55.24.X.16, donc 55.24.X.31 avec le masque à /32).

EXEMPLE (cas du premier organisme en 55.24.0.0 /19) :

PLAGES IP PAR ORGANISME			
1	55.24.0.0	/19	255.255.224.0
2	55.24.32.0	/19	255.255.224.0
3	55.24.64.0	/19	255.255.224.0
4	55.24.96.0	/19	255.255.224.0
5	55.24.128.0	/19	255.255.224.0
6	55.24.160.0	/19	255.255.224.0
7	55.24.192.0	/19	255.255.224.0
8	55.24.224.0	/19	255.255.224.0

Exemple pour le site en 55.24.0.0 /19		
55.24.0.0	/22	SIEGE (PC / Serveurs)
55.24.4.0	/24	Etablissement-1
55.24.5.0	/24	Etablissement-2
55.24.6.0	/24	Etablissement-3
55.24.7.0	/24	Etablissement-4
55.24.8.0	/24	Etablissement-5
55.24.9.0	/24	Etablissement-6
55.24.10.0	/24	Etablissement-7
55.24.11.0	/24	Etablissement-8
55.24.12.0	/24	Etablissement-9
55.24.13.0	/24	Etablissement-10
55.24.14.0	/24	Etablissement-11
55.24.15.0	/24	Etablissement-12
55.24.16.0	/24	Etablissement-13
55.24.17.0	/24	Etablissement-14
55.24.18.0	/24	Etablissement-15
55.24.19.0	/24	Etablissement-16
55.24.20.0	/24	Etablissement-17
55.24.21.0	/24	Etablissement-18
55.24.22.0	/24	Etablissement-19
55.24.23.0	/24	Etablissement-20
55.24.24.0	/24	Etablissement-21
55.24.25.0	/24	Etablissement-22
55.24.26.0	/24	Etablissement-23
55.24.27.0	/24	Etablissement-24
55.24.28.0	/24	Etablissement-25
55.24.29.0	/24	Etablissement-26
55.24.30.0	/24	SIEGE (autres VLAN)
55.24.31.0	/24	SIEGE (autres VLAN)

SIEGE : y = 0 - Z = 31

VLAN POUR LES DONNEES

VLAN		Adressage					
N°	Nom	Réseau	1ère adresse	Dernière adresse	Masque	Nb adresses	Commentaire
5	VLAN-INTERCOWAN	55.24.31.0	55.24.31.1	55.24.31.6	/29	6 adresses	3 @ routeurs, 1 @ switch, 1 @ Ipanema
900	VLAN-ADMIN-UCOPIA	55.24.31.0	55.24.31.1	55.24.31.2	/30	2 adresses	Réservé pour admin UCOPIA - wifi invités
-	Non utilisé	55.24.31.4	55.24.31.5	55.24.31.6	/30	2 adresses	*réservé pour plus tard*
224	VLAN-ACCES-PART	55.24.31.16	55.24.31.17	55.24.31.31	/28	14 adresses	Equipements accédés par des tiers (+ACL !)
901	VLAN-ADMIN-RESEAU	55.24.31.32	55.24.31.33	55.24.31.63	/27	30 adresses	Switches
219	VLAN-PCA-DATA	55.24.31.64	55.24.31.65	55.24.31.94	/27	30 adresses	Clients PCA
50	VLAN-WIFI-AGENTS	55.24.31.96	55.24.31.97	55.24.31.126	/27	30 adresses	Clients wifi
902	VLAN-ADMIN-WIFI	55.24.31.128	55.24.31.129	55.24.31.254	/25	126 adresses	AP et contrôleur wifi
6	VLAN-DATA	55.24.0.0	55.24.0.1	55.24.3.254	/22	1022 adresses	PC et serveurs
226	VLAN-IMPRIMANTES	55.24.30.0	55.24.30.1	55.24.30.62	/26	62 adresses	Imprimantes
-	*Non utilisé*	**55.24.30.64**	**55.24.30.65**	**55.24.30.126**	/26	**62 adresses**	*réservé pour plus tard*

SIEGE : y = 0 - Z = 31

VLAN POUR LA VOIX

VLAN		Adressage					
N°	Nom	Réseau	1ère adresse	Dernière adresse	Masque	Adresses	Commentaire
220	VLAN-PCA-VOIX	58.24.0.64	58.24.0.65	58.24.0.126	/26	62 adresses	Clients PCA
30	VLAN-VOIX	58.24.0.0	58.24.0.1	58.24.3.254	/22	1022 adresses	Téléphones IP

ETABLISSEMENTS : Etablissement-1 : X = Y+4 - ...etc... Etablissement 27 : X = Y+30

Exemple : Etablissement-1

VLAN POUR LES DONNEES

VLAN		Adressage					
N°	Nom	Réseau	1ère adresse	Dernière adresse	Masque	Adresses	Commentaire
5	VLAN-INTERCOWAN	55.24.4.0	55.24.4.1	55.24.4.6	/29	6 adresses	3 @ routeurs, 1 @ switch, 1 @ ipanema
-	*Non utilisé*	55.24.4.8	55.24.4.9	55.24.4.15	/29	*6 adresses*	*réservé pour plus tard*
901	VLAN-ADMIN-RESEAU	55.24.4.16	55.24.4.17	55.24.4.31	/28	*14 adresses*	Switches
902	VLAN-ADMIN-WIFI	55.24.4.32	55.24.4.33	55.24.4.46	/28	*14 adresses*	AP et contrôleur wifi
224	VLAN-ACCES-PART	55.24.4.48	55.24.4.49	55.24.4.63	/28	14 adresses	Equipements accédés par des tiers (+ACL !)
226	VLAN-IMPRIMANTES	55.24.4.64	55.24.4.65	55.24.4.94	/27	*30 adresses*	Imprimantes
50	VLAN-WIFI-AGENTS	55.24.4.96	55.24.4.97	55.24.4.126	/27	30 adresses	Clients wifi
4	VLAN-DATA	55.24.4.128	55.24.4.129	55.24.4.254	/25	126 adresses	PC et serveurs

VLAN POUR LA VOIX

VLAN		Adressage					
N°	Nom	Réseau	1ère adresse	Dernière adresse	Masque	Adresses	Commentaire
30	VLAN-VOIX	58.24.4.128	58.24.4.129	58.24.4.254	/25	126 adresses	Téléphones IP

Dans les agences / établissements, s'il n'y a qu'un seul switch ou stack, le vlan 901 ne montera pas : ne pas le créer mais utiliser un interface de loopback1 ayant la dernière adresse IP de sous réseau (55.24.X.16, donc 55.24.X.31 avec le masque à /32).

1.15 AUTRES SUJETS TECHNIQUES

1.15.1 SNMP / SYSLOG

Deux sujets nécessitent la configuration de SYSLOG et SNMP dans les switches : les outils de supervision et de gestion des configurations et le contrôle de l'inventaire physique et comptable.

Des commandes sont à entrer sur chaque switch N2 ou N3 : voir les guides de configuration des switches ci-dessous.

La configuration SNMP et SYSLOG est obligatoire pour tous les switches fournis par le DR.

1.15.2 Wifi

Tout ce qui concerne le wifi est décrit dans des documentations spécifiques sur l'intranet du DR rubrique Infrastructure / WIFI.

1.15.3 Wake On LAN

Dans le cadre de l'application GEDIFF et de la GPO, il est demandé de permettre le fonctionnement du Wake On LAN (WoL). **Veuillez consulter les guides de configuration ci-dessous**.

1.15.4 NTP

L'horloge de chaque équipement réseau doit être synchronisée via NTP.

Il existe une adresse IP unique de référence pour NTP. **Veuillez consulter les guides de configuration ci-dessous.**

1.15.5 QoS

Afin de prioriser les flux sensibles que sont la voix et la vidéo, il est préconisé de mettre en œuvre la QoS telle que définie **dans les guides de configuration.**

1.15.6 Déploiement de téléphones IP

Reportez-vous aux documentations concernant la téléphonie sur l'intranet du DR. Des conseils quant aux méthodes de déploiement sont aussi donnés dans les guides de configuration des switches.

La ToIP nécessite l'utilisation d'un serveur DHCP. Ce serveur DHCP doit être le serveur Windows de proximité. Il peut être centralisé au siège.

Les « pools » DHCP doivent intégrer les options spécifiques de la solution déployée. S'il s'agit d'IPBX propriétaire (Alcatel, Mitel, …), les intégrateurs vous aideront pour réaliser cette configuration DHCP. Là encore, voyez les guides sur le portail du DR.

Pour Cetiam, si besoin, une ou plusieurs passerelles seront fournies pour la connexion d'équipements de téléphonie analogique. Elles devront être positionnées dans le VLAN 230 (58.230.X.Y) **SUR LE FEDERATEUR AUTANT QUE POSSIBLE**. Les adresses seront fournies par le DR. Les configurations sont détaillées dans les guides.

L'utilisation de la configuration avec « VOICE VLAN » facilitera le déploiement. Voir les guides de configuration.

Voici cependant comment cela fonctionne :

- L'intégrateur a préparé l'IPBX pour la connexion des téléphones
- le téléphone neuf en configuration usine est connecté au switch
- le téléphone s'allume car alimenté par le PoE
- Via LLDP le switch reconnait le téléphone avec son adresse MAC grâce aux commandes globales « VOICE VLAN » entrées dans les switches ➔ le téléphone est mis dans le VLAN 30 grâce à la commande (« voice vlan 30 enable »)
- le téléphone envoie un broadcast dans le vlan 30 pour trouver un serveur DHCP
- le serveur DHCP lui attribue adresse IP, passerelle… dans l'étendue en phase avec le sous-réseau de l'interface VLAN VOIX (30)
- grâce à la configuration des options liées au téléphone et à son constructeur, le serveur DHCP reconnaît le modèle de téléphone et lui indique l'adresse IP de son serveur = IPBX
- l'IPBX lui envoie sa configuration (soit car son adresse MAC permet de l'identifier dans l'IBPX, soit car il est demandé d'entrer le numéro de poste)
- le téléphone charge une mise à jour logicielle si nécessaire puis redémarre
- le téléphone affiche le nom de l'utilisateur et son numéro. Il est prêt à fonctionner.

Dans le cadre de Cetiam, pour les organismes concernés, cela sera géré par le DR avec vous et le prestataire.

1.16 GESTION DES SWITCHES

1.16.1 Demandes de switches

Les switches HP sont acquis par la Cnam pour le compte des Organismes. Merci d'adresser vos demandes via le SDN.

Afin d'optimiser les dotations / livraisons, il faut bâtir l'architecture cible en fonction de l'existant et des projets à intégrer. Il ne faut rien oublier et être le plus précis possible. En fonction des préconisations il faut penser au nombre de ports à prévoir dans chaque répartiteur afin de compter :

- le nombre de switches nécessaires (24 ou 48 ports)
- le nombre de stacks ou stacks avec le nombre de switches dans chaque stack
- les kits de stackage
- les technologies de précâblage utilisées (cuivre, FO…sur le site et donc les modules SFP si nécessaires.

De plus, la fourniture d'un schéma du LAN existant et d'un schéma du LAN envisagé nous paraît indispensable afin de statuer ensemble sur une architecture cible.

Plus la demande sera claire et documentée, plus vite elle pourra être traitée.

POUR CELA : il faut ouvrir une demande auprès du CSN, le DR donnera suite.

1.16.2 Attribution de switches de secours (« SPARE »)

Une gestion rigoureuse est effectuée en terme d'attribution de switches de secours. En effet, au fil des années un trop grand nombre de switches se sont entassés sur les étagères…

Les règles sont les suivantes :

*** Switches fédérateurs ou serveurs stackés ➔** sont de base redondés : aucun secours sur place.

➔ Procédure en cas de panne : après ouverture d'un ticket d'incident, le DR livre un nouveau switch dans les plus brefs délais. Le switch en panne devra être retourné rapidement au DR pour échange standard et mise en stock. Voir les détails dans le § suivant.

*** Autres Switches ➔** chaque organisme se verra attribué en secours 2% de son volume de switches pour tous les LAN sous sa responsabilité (sièges et agences).

➔ Exemple : une CPAM équipée de 100 HP 3600-24 ou 48 ports pour son siège et ses agences bénéficiera de 2 HP 3600 de secours (par exemple 1 24 port et 1 48 ports).

➔ Procédure en cas de panne : remplacer le switch en panne par celui de secours puis ouvrir un incident. Le DR enverra un switch pour remplacer celui en secours. Le switch en panne devra être retourné rapidement au DR pour échange standard et mise en stock. Voir les détails dans le § suivant.

1.16.3 Maintenance : que faire en cas de panne ?

Les switches ont été acquis :

- soit par l'organisme via OC de 2002 à 2005 ➔ l'organisme est propriétaire ; la destruction du switch est donc à sa charge
- soit par le DR (cas général depuis 2006) : il possède une étiquette code barre.

Dans les deux cas, le DR prend en charge le remplacement par un switch équivalent (stock magasin DR) qui sera expédié dans les plus brefs délais (J+1).

POUR CELA : il faut ouvrir un ticket d'incident auprès du SDN :

et fournir :

- Le modèle du switch
- le n° de série du switch (étiquette en face arrière)
- le n° de code barre DR ou Cnam

Le DR vous indiquera la marche à suivre.

1.16.4 Que faire des switches obsolètes ?

Tous les switches HP 3600-v1, les HP 5500 et les HP 5120 **DOIVENT être détruits localement** par les Organismes. **Il ne faut plus les retourner au DR**.

En cas de panne, les 3600-v2 doivent être retournés au DR suite à ouverture d'une demande PSN.

Les 3600-v2 encore opérationnels mais non utilisés ne doivent plus être retournés au DR mais être détruits ou conservés dans votre organisme. Dans les deux cas, il doivent être sortis de l'inventaire.

Etape 1 : Il faut mettre à jour le SI en supprimant les switches via le portail :
https://www.cngr.cnamts.fr/supervision/equipementActif/

Etape 2 : remplir le bon (https://www.cngr.cnamts.fr ➔ Infrastructure ➔ LAN ➔ Inventaire ➔ documentation) et nous le retourner **signé du Directeur ou la Directrice de l'Organisme**.

1.17 AUDITS DE CONFORMITE

Dans la cadre de sa mission, le DR réalise des audits de conformité à ce référentiel LAN. Ils seront effectués grâce aux outils de type NCM ou sondes d'analyse distantes (Fluke par exemple) ou en connexion SSH sur les switches.

Le but sera de vérifier un certain nombre des recommandations listées dans ce référentiels. Exemples :

- Architecture
- Connexion des routeurs RAMAGE sur ports normalisés et en redondance
- Configuration des interfaces switch de connexion des routeurs
- Version des switches
- Configuration SNMP / SYSLOG
- Intégration complète des switches dans le SI
- Respect des plans d'adressage
- Respect des VLAN
- DHCP et DHCP-Snooping configurés
- Topologie Spanning-tree
- …etc.

Ces audits pourront être faits à la demande des organismes ou réalisés à l'initiative du DR.

Une conformité d'un siège ou d'une agence à ce référentiel entrainera un « LABEL » pour ce site.

De même, les sites rattachés (Agences et Etablissements…) seront aussi audités / labellisés dès 2018 / 2019.

Les IRSA, UC-CMP, CGSS et CN seront aussi audités.

La cible est la conformité 100% des LAN du siège et de toutes les agences d'un Organisme.

A partir de 2022, vous serez aussi audités sur les sujets liés à la sécurité OSE (Organismes de Services Essentiels).

Retrouvez le résultat des audits ici : https://www.cngr.cnamts.fr/audit/listeAudit.

2 GUIDE DE CONFIGURATION DES HP 5510, 5520, 5130 ET 5140

2.1 IMPORTANT : ORDRE DE CONFIGURATION SUGGERE

Nous conseillons de configurer les HP 5XXX dans l'ordre suivant.

1/ Commencer par vérifier la version du switch et appliquer la mise à jour si nécessaire

⇨ Les versions sont sur l'intranet du CNGR

2/ Si un stackage est envisagé, configurer la partie stackage (domaine IRF, member priority)

3/ Configurer le sysname, les accès (SSH…), bannière, le DNS

4/ Configurer le Spanning-tree

5/ Configurer les VLAN et les interfaces VLAN

6/ Configurer les agrégats

7/ Configurer les interfaces (trunk associées aux agrégats)

8/ Configurer les interfaces (trunk, access)

9/ Configurer la partie DHCP (relais)

10/ Configurer les routages (sur les switches niveau 2)

11/ Configurer SNMP / SYSLOG

12/ Configurer NTP, LLDP, WAKE ON LAN

12/ Mettre en place la sécurité (ACL, Packet-Filter, Dhcp snooping)

Dans la suite du document, la plupart des lignes ou blocs de lignes de commandes peuvent être copiés-collés. Dans ces blocs de commandes :

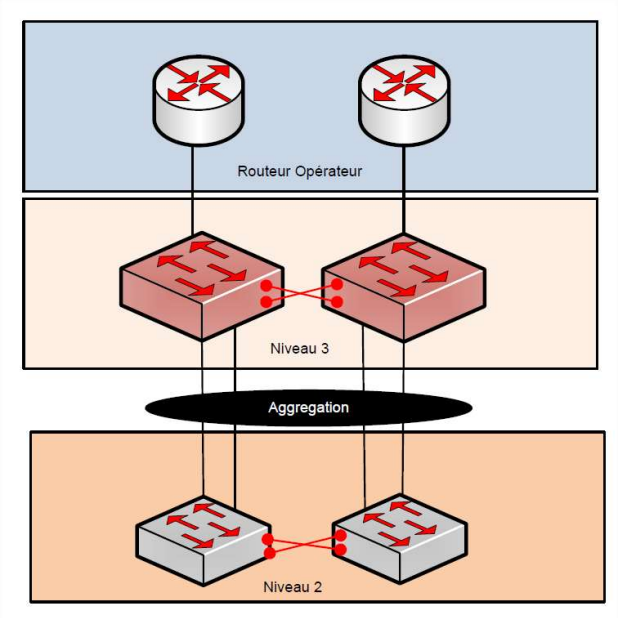
- les paramètres à personnaliser sont en rouge
- les explications sur certaines commandes sont en vert
- les « commentaires » du switch en réponse aux commandes sont en bleu et en italique
- les paramètres optionnels sont mis entre crochet (ex : [speed 100])

Toute la suite du document (après l'introduction de présentation) est rédigée dans le même ordre pour faciliter la compréhension et la configuration.

2.2 DIFFERENCE ENTRE SWITCH NIVEAU 2 ET SWITCH NIVEAU 3

Un **switch niveau 2** établit et met à jour dynamiquement une table d'adresses MAC, qui lui indique sur quels ports diriger les trames destinées à une adresse MAC donnée. Un switch niveau 2 ne fait que de la commutation au niveau des adresses MAC (niveau 2). Si vous créez plusieurs VLAN, chaque VLAN sera isolé.

Un **switch niveau 3** permet en plus d'assigner une adresse IP par Vlan et de pouvoir faire communiquer des machines connectées à différents vlans. Il réalise ainsi le routage Inter Vlan. Il permet aussi de mettre en œuvre les politiques de sécurité entre les vlan via des ACL (access list). Enfin, Il est connecté aux routeurs opérateurs pour accéder aux réseaux externes à l'organisme (réseau public (internet), réseau csh (applications nationales)…).



2.3 LES GAMMES HP 55XX ET HP 51XX

2.3.1 HP 5130 / HP 5140

Cette gamme de switch permet:

- De gérer la commutation de niveaux 2
- La connexion:
    - des ordinateurs,
    - des téléphones,
    - des serveurs physiques et VMware
    - d'audiocodes

À 100Mb ou 1Gb cuivre RJ45 ou Fo.

Ce modèle sera donc utilisé au niveau des LAN des sièges d'Organismes (CPAM, UGECAM, CGSS, CSM…) pour connecter des serveurs et des PMF, il est appelée à remplacer dans certains cas en fonction du stock les HP 3600 et les HP 5120.

Au minimum sauf cas particulier, il sera délivré au minimum 2 switches afin de permettre la constitution d'un stack et permettre la connexion des serveurs ou de switches de manière redondée si besoin.

2.3.2 La gamme HP 5510 / 5520

Cette gamme de switch permet:

- De gérer la commutation de niveaux 2 et 3
- La connexion:
    - des ordinateurs,
    - des téléphones,
    - des serveurs physiques et VMware
    - d'audiocodes
    - des routeurs opérateurs

  À 100Mb ou 1Gb cuivre RJ45.

Ce modèle sera donc utilisé en niveau3 sur les LAN des Organismes (CPAM, UGECAM, CGSS, CSM, CP…) pour fédérer des switches, il est appelée à remplacer les HP 5500.

Au maximum sauf cas particulier, il ne sera délivré que 2 switches afin de permettre la constitution d'un stack et permettre la connexion des serveurs ou de switches de manière redondée si besoin.

Si:

- les 5510 ou 5520 fédérateurs disposent de suffisamment d'interfaces libres pour connecter les serveurs

et

- si les serveurs sont situés dans le même local que les fédérateurs

Alors les serveurs seront connectés directement sur les 5510 ou 5520.

2.3.3 Présentation des équipements

2.3.3.1 HP 51X0-24G-4SFP+ EI



Dimension: 44x16x4.36 (1U)

Il contient :

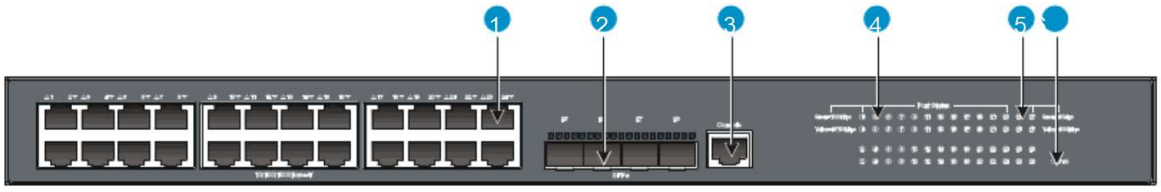
- **24 ports 10/100/1000 cuivre RJ45 (GigabitEthernet1/0/1 – GigabitEthernet 1/0/24)**
- **4 ports SFP+ 1000/10000 (Ten-GigabitEthernet1/0/25 - Ten-GigabitEthernet 1/0/28**).

Les ports Ten-GigabitEthernet1/0/27 et 28 **sont réservés au stackage.**

Les ports SFP(+) 25 et 26 ne seront utilisés que pour la connexion aux fédérateurs si le pré-câblage est en fibre optique : ils seront alors garnis de SFP 1000 SX (auto-adaptation). L'interconnexion avec le stack fédérateur se fera donc à 1 Gb/s (des SFP 1000 SX seront insérés dans les 5500).
Si le pré-câblage est de type cuivre, on utilisera les ports 10/100/1000 RJ45.

HP 5130-24G-4SFP+

Figure 34 Front panel



(1) 10/100/1000Base-T autosensing Ethernet port	(2) SFP+ port
(3) Console port	(4) 10/100/1000Base-T autosensing Ethernet port LED
(5) SFP+ port LED	(6) System status LED (SYS)

ManualsLib.com

2.3.3.2 HP-51X0-24G-SFP-4SFP+ EI



8 ports combo 17S-24S avec les ports 17T-24T



Il contient:

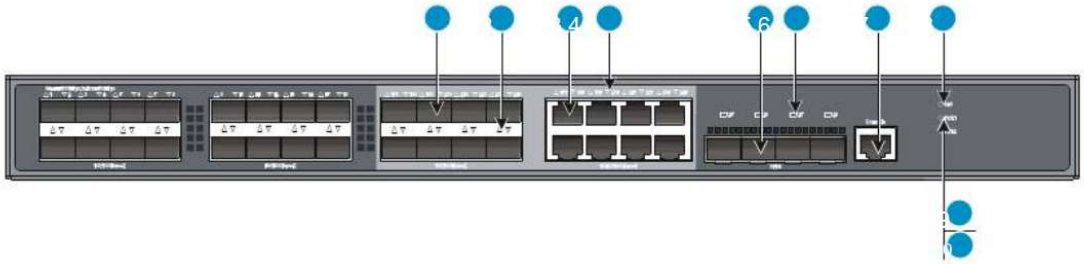
- **16 ports 10/100/1000 SFP ou RJ45 (GigabitEthernet1/0/1 – 1/0/16)**
- **8 ports combo Gb (GigabitEthernet1/0/17 – 1/0/24)**
- **4 ports SFP+ 1000/10000 (Ten-GigabitEthernet1/0/25 à 28).**

Les ports Ten-GigabitEthernet1/0/27 et 28 **sont réservés au stackage.**

Dimension: 44x36x4.36 (1U)

HP 5130-24G-SFP-4SFP+ EI

Figure 50 Front panel



(1) 100/1000Base-X SFP port	(2) 100/1000Base-X SFP port LED
(3) 10/100/1000Base-T autosensing Ethernet port	(4) 10/100/1000Base-T autosensing Ethernet port LED
(5) SFP+ port	(6) SFP+ port LED
(7) Console port	(8) System status LED (SYS)
(9) Power supply 1 status LED (PWR1)	(10) Power supply 2 status LED (PWR2)

2.3.3.3 HP-51X0-48G-POE+4SFP+ EI



- **48 ports autosensing 10/100/1000 SFP ou RJ45 (GigabitEthernet1/0/1 – 1/0/48)**
- **4 ports SFP+ 1000/10000 (Ten-GigabitEthernet1/0/49 à 52).**
- **1 port console**

Dimension: 44x36x4.36 (1U)

2.3.3.4 HPE 5510-24G-4SFP+ HI



Il contient :

- **24 ports 10/100/1000 cuivre RJ45 (GigabitEthernet1/0/1 – GigabitEthernet 1/0/24)**
- **4 ports SFP+ 1000/10000 (Ten-GigabitEthernet1/0/25 - Ten-GigabitEthernet 1/0/28**).
- **3 Port de management (console, out of band, 1 USB 2.0)**

Les ports Ten-GigabitEthernet1/0/27 et 28 **sont réservés au stackage.**

Les ports SFP(+) 25 et 26 ne seront utilisés que pour la connexion aux fédérateurs si le pré-câblage est en fibre optique : ils seront alors garnis de SFP 1000 SX (auto-adaptation). L'interconnexion avec le stack fédérateur se fera donc à 1 Gb/s (des SFP 1000 SX seront insérés dans les 5500).
Si le pré-câblage est de type cuivre, on utilisera les ports 10/100/1000 RJ45.



Description de gauche à droite

- **1 port extension**
- **2 ventilateurs**
- **2 ports alimentations (optionnels)**

2.3.3.5 HPE 5520-24G-4SFP+ HI



Il contient :

- **16 ports 10/100/1000 cuivre RJ45 (GigabitEthernet1/0/1 – GigabitEthernet 1/0/16)**
- **8 ports 100/1000 combo cuivre RJ45/FO (GigabitEthernet1/0/17 – GigabitEthernet 1/0/24)**
- **4 ports SFP+ 1/10G (Ten-GigabitEthernet1/0/25 - Ten-GigabitEthernet 1/0/28**).
- **3 Port de management (console, out of band, 1 USB 2.0)**

Les ports Ten-GigabitEthernet1/0/27 et 28 **sont réservés au stackage.**



Description de gauche à droite

- **1 port extension**
- **2 ventilateurs**
- **2 ports alimentations (optionnels)**

2.3.3.6 HPE-55X0-24G-SFP-4SFP+ HI



8 ports combo 17S-24S avec les ports 17T-24T



Il contient:

- **16 ports 10/100/1000 SFP (GigabitEthernet1/0/1 – 1/0/16)**
- **8 ports combo Gb SFP ou RJ45 (GigabitEthernet1/0/17 – 1/0/24)**
- **4 ports SFP+ 1000/10000 (Ten-GigabitEthernet1/0/25 à 28).**
- **3 Port de management (console, out of band, 1 USB 2.0)**

Les ports Ten-GigabitEthernet1/0/27 et 28 **sont réservés au stackage.**



Description de gauche à droite

- 1 port extension
- 2 ventilateurs
- 2 ports alimentations (optionnel)

2.3.4 Accessoires

Cables de stackage : Cordon 10Gb constructeur SFP+

Figure 52 SFP+ DAC cable

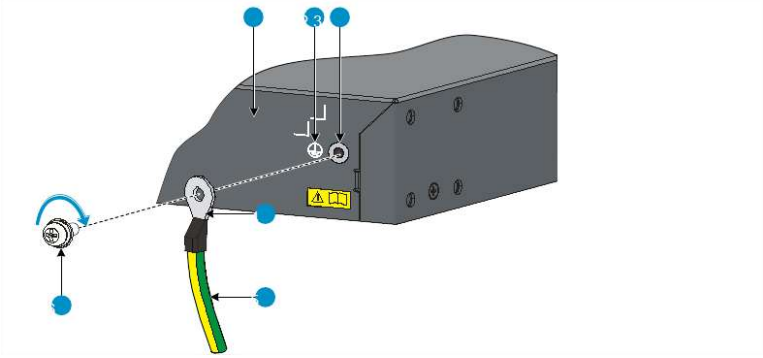


(1) Connector	(2) Pull latch

La partie « **Pull latch**» ❷ permet de débrancher le cordon une fois qu'il est en service

2.3.5 Mise en baie





Prérequis:

Veuillez-vous assurer auprès des services généraux que vos baies informatiques sont bien reliées à la masse avant de mettre à la masse vos switches.

2.3.6 Prise en main

La connexion aux switches se fait via le câble bleu fourni dans le carton d'emballage du switch que l'on connecte sur le port série d'un PC. Ensuite, la prise en main se fait via « Putty » ou « Hyperterminal » par exemple.

Pour passer les commandes, il faut être en mode « configuration ». Pour cela, il faut taper « system-view » au prompt de base (>). Le prompt change pour un # . C'est l'équivalent du « conf t » de Cisco, et comme pour Cisco :

```
Starting……

Press Ctrl+D to access BASIC BOOT MENU

(Tapez Ctrl+D)

<sw-buro-86>system-view
System View: return to User View with Ctrl+Z.
```

Le Ctrl+Z permet de revenir au prompt initial hors mode configuration
Le « ? » permet de visualiser les commandes disponibles à l'endroit où on se trouve
La touche tabulation permet de compléter automatiquement une commande commencée
La commande « save » permet de sauvegarder la configuration (« write memory » de Cisco – voir § « Sauvegarde »).

Dans la suite du document, par défaut les commandes à passer sont en mode de configuration « system-view » (prompt [ ]). Sinon, le symbole < > placé devant la commande signifiera qu'il faut revenir au prompt initial (hors configuration). Pour revenir à ce prompt initial, tapez CTRL+z.

2.3.7 Commandes de base

< > = Mode sans privilège (Prompt de base)
[ ] = Mode System-View

< >undo screen-length disable (active la visualisation page par page)

< >display cur (voir la configuration courante)

< >display interface brief (voir le status des interfaces)

< >display interface ethernet…: informations importantes sur les interfaces (erreurs, CRC…)

[ ]display lldp neighbor-information […] (voir les voisins lldp)

[ ]display ntp-service status (voir le serveur ntp)

[ ]display cpu unit 1 (voir le pourcentage cpu utilise)

< >dir [/all ou slotN#flash:] (voir les fichiers de la flash)

< >schedule reboot at 00:00 (rebooter le switch à une heure donnée)

< > display vlan static ou dynamic

[ ]interface range int gi1/0/1 to gi1/0/10 gi2/0/1 to gi2/0/10 etc…. : configuration de groupes d'interfaces.

Limites : il faut entrer les commandes une à une (le copier-coller de plusieurs lignes ne fonctionne pas)

< >dis counters inbound interface : statistiques sur les interfaces en entrée

< >dis counters outbound interface : statistiques sur les interfaces en sortie

< >reset counters interface

< >dis packet-filter statistics sum inbound 3224 : Statistique ACL/Packet-filter 224
< >dis acl 2099 : Statistique ACL 2099

< >dis logbuffer : affiche les logs

Les commandes « reset counters interface » et « reset logbuffer » remettent les compteurs ci-dessus à zéro.

<>dis device manuinfo : affichage d'information **dont le n° de série**

Retour d'un port en configuration usine :

[CP-XXX-N3-HP 5500-GigabitEthernet1/0/1]default
This command will restore the default settings. Continue? [Y/N]:y

[sur l'interface] shutdown : éteindre une interface

[sur l'interface] undo shutdown : allumer une interface

<> ou [] save : sauvegarde de la configuration (switch / stack) avec demande de confirmation

<> ou [] save force : Forcer une sauvegarde, sans avoir à répondre « yes », aux questions intermédiaires

2.3.8 Alias

Permet de renommer des commandes HP "à la mode Cisco". Exemple : display ←→ show :

System-view
#
command-alias mapping display show

Suppression:

System-view
#
undo command-alias show

Il semble qu'un alias ne soit pas complété automatiquement lorsqu'on « tabule » (touche « TAB »)…

2.4 STACKAGE (IRF)

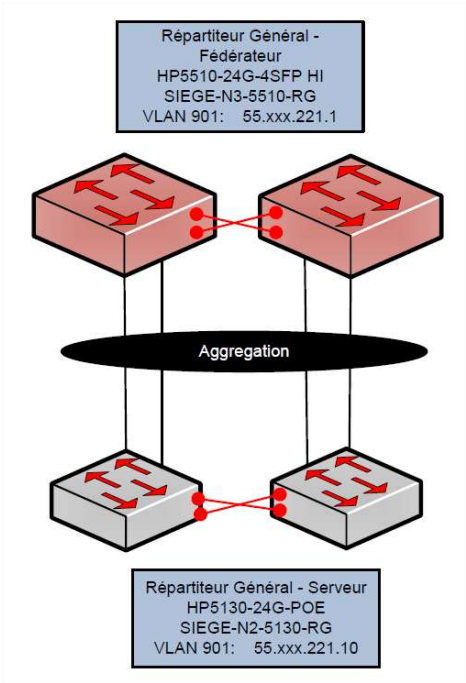
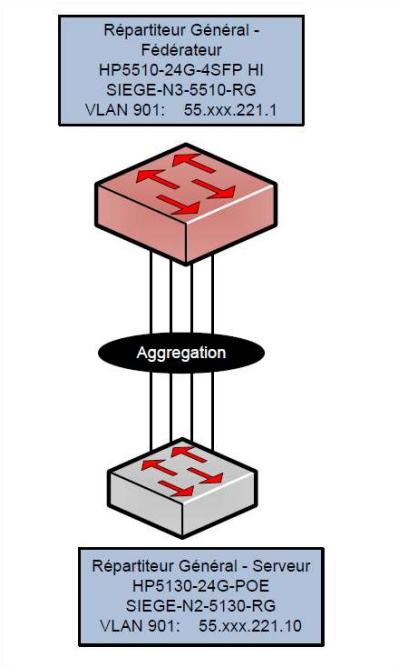
2.4.1 Présentation



A quoi ça sert ?

Le stackage (IRF) est une technique propriétaire permettant de transformer plusieurs switches physiques en un seul switch logique en utilisant des éléments de connectique particuliers (fournis par le CNGR avec les switches lorsqu'un stackage est prévu). Le numéro de domaine IRF est unique pour chaque stack. La configuration globale est alors commune et les interfaces s'additionnent.

Il est possible de réaliser des agrégats entre des groupes de switches stackés. Exemple :

Ainsi :	Equivaut à :
	

Les switches HP 55X0_HI & HP 51X0 peuvent être stackés. C'est un vrai stack : les switches stackés entre eux sont vus comme **un seul switch logique** : toute la configuration est commune, le stack n'ayant qu'une seule adresse IP. Le stackage fonctionne à 10 Gb/s.

- Le principe de stackage est le même pour les deux modèles.
- La mise à jour de version est automatique du maître vers les secondaires.

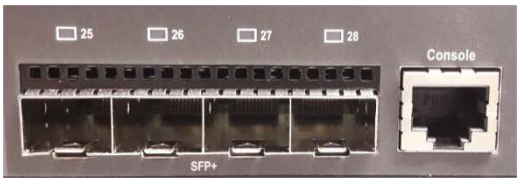
Les limites du nombre de switches dans un stack :

- HP 5510 et 5520 : 9 maximun
- HP 5130 et 5140 : 9 maximum

Cependant, compte tenu de l'utilisation que nous allons faire de ces modèles (fédération (HP 5510-24G), connexion des serveurs (HP 5130-24G)), sauf exception, on ne constituera que des stacks de 2 switches.

La version doit être identique sur les switches d'une même stack.

- **Les ports de connexion IRF : Ten-Gigabitethernet x/0/27 et x/0/28**



4 ports SFP+ intégrés dont le 27 et 28 (réservés pour le stackage)

- **IRF local (distance entre 2 switches 0,65m ou 1,2 m):**

Des câbles spécifiques Direct-Attach-Cables (propriétaires) sont à utiliser 10Gb:



Stackage IRF : il faut croiser les DA-câbles
(unité 1 port 27 sur unité 2 port 28)

- **IRF Etendu (distance entre 2 switches 0m à 300m):**
  (par exemple entre deux baies, deux salles, deux bâtiments)

Vous pouvez stacker vos éléments d'un stack entre 2 locaux distants pour cela vous devez disposer de:

- 4 Gbic 10G SFP+ LC SR (voir schéma ci-dessous)
- 4 Fibres LC ou 2 paires LC (1 Fo émission + 1 Fo réception par paire (voir schéma ci-dessous))



4 Gbic 10G SFP+SR Transceiver
(JD092B)



1 Paire de Fibre LC

L'insertion du Gbic dans le slot génère le message log suivant:
Jan1 02:20:49:635 2013 HP 5130-N3-ILLKIRCH-URG OPTMOD/4/MODULE_IN:-Slot=3;Ten-GigabitEthernet3/0/28: The transceiver is 10G_BASE_SR_SFP.



Stackage IRF: il faut croiser les fibres optiques dans la paire
*(**Rouge**-noir et Noir-**rouge**)*

2.4.2 Configuration

Avec certaines versions, un login est demandé via la console lors du premier démarrage : utilisez le login admin avec un mot de passe vide et choisissez un mot de passe :

Login: admin
Password : (***vide)***
First login or password reset. For security reason, you need to change your password.
Old password: (***vide)***
New password:XXXXXXXXX

Etapes de configuration du stackage :

1 - Démarrer les switches et **si besoin les remettre en configuration usine – voir plus bas**

2 - Entrer en mode « system-view »

3 - Configurer les numéros unités du stack

4 - Paramétrer les ports IRF de chaque unité

5 - Connecter les liens physiques

6 – Le switch « slave » reboot automatiquement puis le stack est opérationnel

Ne pas connecter les câbles. Il faut d'abord configurer les switches que l'on veut stacker UN à UN.

En détail :

Commandes en ligne à appliquer sur le commutateur « Master » :
Remarque : on paramétrera par défaut l'unité 1 en tant que master (priorité maximum)

Par défaut, le switch est member 1 et priorité 1 mais il faut vérifier :

<>display irf

```
Switch  Role   Priority  CPU-Mac        Description
 *+1   Master  1         3822-d609-1c99  -----
-------------------------------------------------

 * indicates the device is the master.
 + indicates the device through which the user logs in.

 The Bridge MAC of the IRF is: 3822-d609-1c86
 Auto upgrade            : yes
 Mac persistent          : 6 min
 Domain ID               : 0
```

2.4.3 Elément 1 du stack

```
<HPE>system-view
#                                  | NE GENERE PAS DE COUPURE si fait après un stackage déjà opérationnel
[HPE] irf domain YY                | remplacer YY par la fin de l'@IP du stack – ex : 1 pour 55.X.221.1
irf member 1 priority 32           | TOUJOURS 32 pour le premier
#
[HPE]interface Ten-GigabitEthernet1/0/27
 shutdown
#
[HPE]interface Ten-GigabitEthernet1/0/28
 shutdown
#
quit
#
[HPE]irf-port 1/1
 port group interface Ten-GigabitEthernet 1/0/27
Info: You are recommended to save the configuration after completing your IRF configuration;
      otherwise, it may be lost after system reboot.
#
quit
#
[HPE]irf-port 1/2
 port group interface Ten-GigabitEthernet 1/0/28
#
quit
#
[HPE]irf-port-configuration active
#
[HPE]interface Ten-GigabitEthernet1/0/27
 undo shutdown
 description STACKAGE
#
[HPE]interface Ten-GigabitEthernet1/0/28
 undo shutdown
 description STACKAGE
#
quit
save force
```

Commandes en ligne à appliquer sur le commutateur « secours » :

2.4.4 Elément 2 du stack

```
<HPE> system-view
#                                  | NE GENERE PAS DE COUPURE si fait après un stackage déjà opérationnel
[HPE]irf domain YY                 | remplacer YY par le même nombre que pour le 1er switch (dans notre ex : 1)
[HPE]irf member 1 renumber 2
Warning: Renumbering the switch number may result in configuration change or loss. Continue?[Y/N]y   Répondre « Y »
#
Save force
#
quit
<HPE> reboot                       Répondre « Y »
#
```

Pour les HP 5510 et 5520 (disposant de plusieurs slots)

```
[HPE]fan prefer-direction slot 2 port-to-power
```

Contrôle
[HPE]dis fan
Slot 2:
Fan 1:
State : **Normal**
Airflow Direction: Port-to-power
Prefer Airflow Direction: Port-to-power
Fan 2:
State : **Normal**
Airflow Direction: Port-to-power
Prefer Airflow Direction: Port-to-power

Suite au redémarrage :

<HPE> system-view
↙ | NE GENERE PAS DE COUPURE si fait après un stackage déjà opérationnel
[HPE]irf member 2 priority 30 | priorité du précédent -2 (ici 32 – 2 = 30)
[HPE]interface Ten-GigabitEthernet2/0/27
shutdown
#
[HPE]interface Ten-GigabitEthernet2/0/28
shutdown
#
quit
#
[HPE]irf-port 2/1
port group interface Ten-GigabitEthernet 2/0/27 *Info: You are recommended to save the configuration after completing your IRF configuration;*
otherwise, it may be lost after system reboot.
#
quit
#
[HPE]irf-port 2/2
port group interface Ten-GigabitEthernet 2/0/28
quit
#
[HPE]irf-port-configuration active
#
[HPE]interface Ten-GigabitEthernet2/0/27
undo shutdown
description STACKAGE
#
[HPE]interface Ten-GigabitEthernet2/0/28
undo shutdown
description STACKAGE
#
Save force
#
quit

2.4.4.1 Elément N du stack (ici N = 3) :

<>system-view

#
[HPE]irf domain YY | NE GENERE PAS DE COUPURE si fait après un stackage déjà opérationnel
| remplacer YY par le même nombre que pour le 1er switch (dans notre ex : 1)
[HPE]irf member 1 renumber N
*Warning: Renumbering the switch number may result in configuration change or loss. Continue?[Y/N]*y *Répondre* « Y »
#
[HPE]Save force
#
quit
<HPE> reboot *Répondre* « Y »

Pour les HP 5510 et 5520 (disposant de plusieurs ventilateurs)

[HPE]fan prefer-direction slot 3 port-to-power

[HPE]dis fan (Contrôle)
Slot 3:
Fan 1:
State : **Normal**
Airflow Direction: Port-to-power
Prefer Airflow Direction: Port-to-power
Fan 2:
State : **Normal**
Airflow Direction: Port-to-power
Prefer Airflow Direction: Port-to-power

Suite au redémarrage :

<>system-view
#
[HPE]irf member 3 priority 28 | NE GENERE PAS DE COUPURE si fait après un stackage déjà opérationnel
| priorité du précédent -2 (ici 30 – 2 = 28)
[HPE]interface Ten-GigabitEthernet3/0/27
[HPE] shutdown
#
[HPE]interface Ten-GigabitEthernet3/0/28
shutdown

#
quit
#
[HPE]irf-port 3/1
port group interface Ten-GigabitEthernet 3/0/27 *Info: You are recommended to save the configuration after completing your IRF configuration;*
otherwise, it may be lost after system reboot.
#
quit
#
[HPE]irf-port 3/2
port group interface Ten-GigabitEthernet 3/0/28
quit
#
irf-port-configuration active
#
[HPE]interface Ten-GigabitEthernet3/0/27
undo shutdown
description STACKAGE
#
[HPE]interface Ten-GigabitEthernet3/0/28

```
 undo shutdown
 description STACKAGE
#
Save force
#
quit
```

Lorsque le stack doit contenir plus de switches (cas rare pour des HP A5510_HI), répéter la partie "switch « n » " en adaptant les numéros dans les configurations (IRF domain identique, member+1, priority – 2).

Vous pouvez connecter les câbles en les croisant :

⇨ Les switches n° 2 à n du stack redémarrent automatiquement dès qu'un des câbles est branché.



HP 51X0 & HP 55X0 en DA SFP+ to SFP+

Lorsque le switch n° 2 a fini son redémarrage, le stack doit être opérationnel.

2.4.5 Cas d'un switch seul (non stacké)

Dans le cas où un switch est seul à l'extrémité (5130 ou 5140), il est recommandé de configurer aussi un numéro de domaine.

```
<>system-view
#
irf domain YY                    | remplacer YY par la fin de l'@IP du stack – ex : 11 pour 55.X.221.11
```

2.4.6 Vérification

Commandes d'affichage pour vérification :

<>display irf

```
Switch  Role   Priority  CPU-Mac        Description
 *+1   Master   32        3822-d609-40d9 -----
  2    Standby  30        3822-d609-1c99 -----
-------------------------------------------------

* indicates the device is the master.
+ indicates the device through which the user logs in.

The Bridge MAC of the IRF is: 3822-d609-40c6
Auto upgrade           : yes
Mac persistent         : 6 min
```

```
Domain ID              : 0
```

<>display irf topology

```
                  Topology Info
------------------------------------------------------------------------
          IRF-Port1            IRF-Port2
Switch    Link     neighbor    Link     neighbor    Belong To
1         UP       2           UP       2           3822-d609-40d9
2         UP       1           UP       1           3822-d609-40d9
```

<>display irf configuration

```
MemberID NewID   IRF-Port1                IRF-Port2
 1       1       Ten-GigabitEthernet1/1/1 Ten-GigabitEthernet1/1/2
 2       2       Ten-GigabitEthernet2/1/1 Ten-GigabitEthernet2/1/2
```

2.5 NOMMER LE SWITCH

Le nommage des switches est normalisé : voir le § « Nommage des switches » plus haut dans ce document.

La commande à utiliser est « sysname ».

Exemples : Etablissement Redon

[] sysname 351-sw-et-redon-001-n3-3600-RG

2.6 CONFIGURATION DES ACCES

2.6.1 Règle de construction du mot de passe

- **Taille :** le mot de passe doit avoir au moins 12 caractères
- **Complexité :** le mot de passe doit contenir au moins 4 types de caractères différents, et au moins 2 caractères pour chaque type

Exemple de mot de passe :

. Exemple : « 12ABcd$!12AB »

2 x Caractères spéciaux : $!
2x Majuscules : AB
2x Minuscules : cd
2x Nombres : 12

2.6.2 Accès console, SSH et HTTPS

A appliquer sur un switch seul (non stacké) ou sur le stack. Cela est valable pour tous les switches HP.
Ces commandes permettront de paramétrer un accès au switch ou au stack en console, ssh et http via le login « admin » et un mot de passe (à personnaliser). Le mot clé « cipher » signifie que le mot de passe sera crypté lors des visualisations de configuration :

```
<>system-view
#
local-user admin
        password simple motdepasse                          | Remplacer «motdepasse» par le vôtre
        service-type ssh terminal https                     | si présent enlever « telnet » : undo service-type telnet
        authorization-attribute user-role network-admin     | Rôle associé à la connexion
#
        undo ip http enable                 | Suppression de l'accès http
        undo ip https enable                | Suppression de l'accès HTTPS
#
line aux 0 X                                | où x = NB de switches dans le stack – 1 (ex : stack de 3, x=2)
 authentication-mode scheme
#
line vty 0 63
        authentication-mode scheme
        user-role network-admin
        protocol inbound ssh

public-key local create rsa
        The range of public key size is (512 ~ 2048).
        NOTES: If the key modulus is greater than 512,
        It will take a few minutes.
        Press CTRL+C to abort.
        Input the bits of the modulus[default = 1024]:2048      |validez avec la touche "Entrée")
        Generating Keys...
                +++++
                ++++++++++++++++++++++
                ++++++++++
                ++++
ssh server enable
ssh user admin service-type stelnet authentication-type password

undo ssh server compatible-ssh1x enable     | désactive sshv1 (n'apparait pas en lecture de conf (dis cu))

ip ttl-expires enable                       | validation de la réponse au « traceroute »
ip unreachables enable                      | validation de l'envoi de paquet ICMP destination injoignable
```

Sauvegarder le switch (ou stack) :

```
<>Save force
```

Remarque:

✶Controle de la désactivation ssh1x

```
[35N-SW-CNGR-N2-012-5510]dis ssh server status
 Stelnet server: Enable
 SSH version : 2.0                          | la version 1 est bien désactivée
 SSH authentication-timeout : 60 second(s)
 SSH server key generating interval : 0 hour(s)
 SSH authentication retries : 3 time(s)
 SFTP server: Disable
 SFTP Server Idle-Timeout: 10 minute(s)
 NETCONF server: Disable
 SCP server: Disable
```

2.7 BANNIERE

OBLIGATION OSE :

Une bannière de mise en garde doit être configurée sur tous les switches. Voici la configuration. Commencez et finissez avec le même caractère (ici %)

Ne pas donner d'information de localisation de l'équipement (@ip, adresse physique, type de matériel, nom organisme…) **et utiliser obligatoirement et uniquement la bannière suivante** :

```
System-view
#
header shell %
****************************************
*             ! Attention !            *
*                                      *
*    Acces reserve aux personnels du   *
*         service informatique         *
*                                      *
*  Toutes les activites sur ce systeme *
*          sont enregistrees           *
*                                      *
*    Toutes preuves d activites non    *
*   autorisees seront traitees par les *
*    autorites competentes             *
*                                      *
*     Toute intrusion sur un systeme   *
*   informatique est interdite par les *
*     articles 323-2 du code penal     *
*                                      *
****************************************
%
```

2.7.1 Résolution DNS

Nouveauté v2.3 : pour permettre l'utilisation de nom DNS au lieu d'adresses IP (ex : serveur syslog), il est nécessaire d'entrer ces commandes :

➔ **Préciser la source dns pour les swiths Comware V7**

dns server 55.223.10.1
dns domain cnamts.fr
dns source-interface Vlan-interface 901 | **si site avec une vlan interface 901**
ou
dns source-interface loopback1 | **si site avec une interface loopback1**

2.8 CONFIGURATIONS DU SPANNING-TREE



A quoi ça sert ?

Le spanning-tree est un protocole utilisant un algorithme de détection des boucles de niveau 2 sur un LAN. Une adresse MAC (celle d'un PMF par exemple) ne doit être apprise que par un seul chemin. Sur la base d'une structure d'arbre, les branches redondantes sont bloquées. Le sommet de l'arbre est le « root-bridge ».

- Soit les HP 5510 et 5520 sont utilisés comme **niveau 3** ou Cœur de réseau (comme switch fédérateur)
  cf. configuration §5.1
- Soit les HP 5130 et 5140 sont utilisés comme **niveau 2** (ils permettent la connexion des baies de serveurs physiques ou virtuels, des PMF, des téléphones …)
  cf. configuration §5.2

2.8.1 Cas des HP 5510 ou 5520 niveau 3

(Utilisés comme switch fédérateur)

Les 5510 seront configurés en stack de 2 switches en tant que fédérateurs «niveau 3» en siège d'organismes ou centre de paiement. Dans ce cas, il faudra positionner les paramètres suivants:

- **stp instance 0 priority 0 (root-bridge** du spanning-tree)
- **bridge diameter 2**
- **stp pathcost-standard dot1t**
- **stp bpdu-protection**

Comme ils sont stackés, ils forment un seul switch. Il n'y a donc pas de notion de switch de secours et il est inutile de configurer un root secondaire.

Configuration :

```
<>system-view
#
stp global enable
stp mode rstp
stp instance 0 priority 0                    | ce switch ou stack sera toujours root-bridge
loopback-detection global enable vlan all    | détection des boucles
loopback-detection global action shutdown    | détection des boucles
stp pathcost-standard dot1t                  | optimisation standard du STP
stp bridge-diameter 2                        | optimisation des temps de convergence STP
```

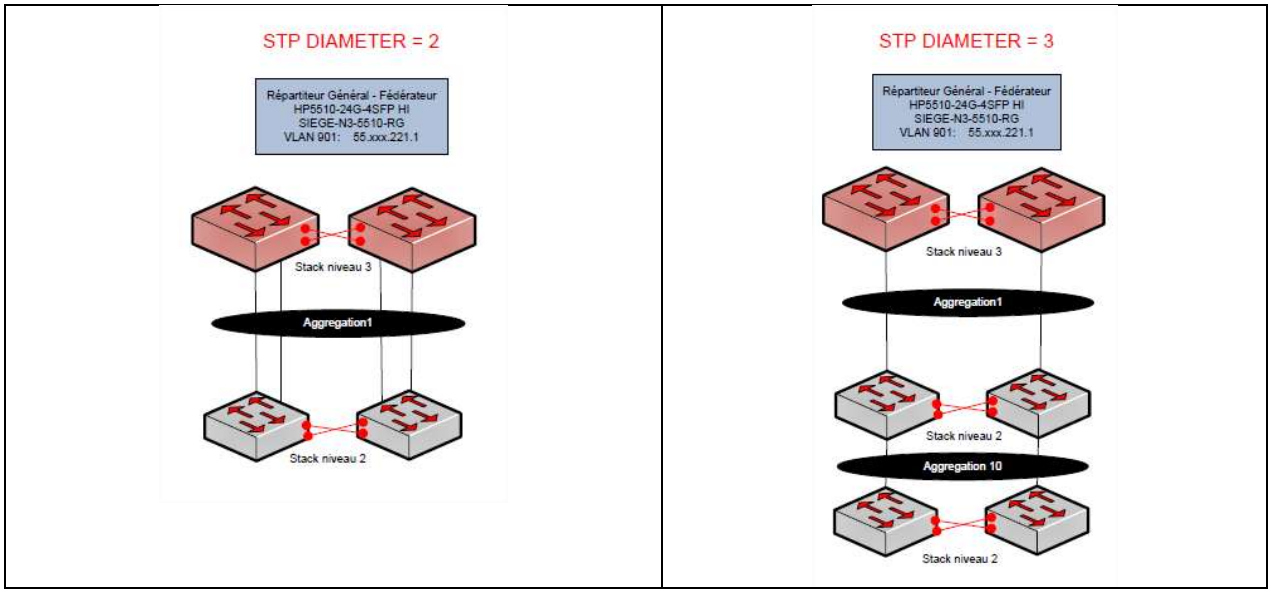
Remarque : une fois tapée, cette commande engendre automatiquement les suivantes :
stp timer forward-delay 700
stp timer max-age 1000

```
stp bpdu-protection                          | Blocage des interfaces recevant des BPDU* à tort
```

Attention : les HP 5130 et 5140 en fédérateurs ne sont pas compatibles Ramage v6

Stp diameter, explications avec des schémas :

CAS STANDARD	CAS PARTICULIER (RARE)



⇨ Stp diameter **2** sera adéquat dans la très grande majorité des cas

ATTENTION

La commande « stp bpdu-protection » doit être renseignée sur tous les switches

2.8.2 Cas des HP 5130 ou 5140 niveau 2

Dans ce cas, il faudra positionner les paramètres suivants:

- **stp mode rstp**
- **stp pathcost-standard dot1t**

Les 5130 et 5140 seront configurés en stack de 2 switches en tant que fédérateurs de VM ou de serveurs physiques en siège d'organisme

<>system-view
#
stp global enable
stp mode rstp
loopback-detection global enable vlan all | détection des boucles
loopback-detection global action shutdown | détection des boucles
stp pathcost-standard dot1t | optimisation standard du STP
stp bpdu-protection | Blocage des interfaces recevant des BPDU* à tort

Les BPDU sont des messages de type spanning-tree. Une interface connectée à un hôte final (PMF, imprimante, téléphone…) ne doit recevoir aucun BPDU. Si c'est le cas, cela signifie qu'un switch est connecté (à tort) ou qu'il y a une boucle niveau 2 sur le LAN. Cette commande bloquera toute interface configurée avec « stp edge- port enable » pour éviter les boucles.

ATTENTION

- **Ne pas renseigner la commande stp instance 0 priority 0 sur un switch niveau 2**

2.8.3 Au niveau des interfaces

Se reporter au § « Configuration des interfaces ».

Une fois configuré en global, le spanning-tree est validé de base sur toutes les interfaces. La commande « stp enable » est implicitement active au niveau des interfaces même si elle n'apparaît pas lors d'un « display current-configuration ».

Il faudra ajouter la commande « stp edged-port» sur les interfaces suivantes :

- Interfaces connectées à des téléphones IP, téléphones IP+PMF, PMF, imprimantes…
- Interfaces connectées à des serveurs

ATTENTION

PAS SUR LES INTERFACES SUIVANTES :

- **Trunks d'interconnexion de switches**
- **Routeurs RAMAGE**

Cette commande allège l'algorithme du Spanning-tree et, associée à la commande globale « stp bpdu-protection », permet le blocage de l'interface recevant du trafic Spannig-tree (BPDU*) à tort.

Exemple pour une interface Gi1/0/6 d'un 5130 utilisée pour un serveur :

```
interface GigabitEthernet1/0/6
 description Serveur
 stp enable                          | n'apparaît pas en « display current-configuration »
 stp edged-port
 port access vlan 4
```

Le spanning-tree doit être désactivé sur les interfaces de connexion des routeurs RAMAGE avec la commande :

[007-SW-xxx-N3-5510-RG-GigabitEthernet1/0/1] undo stp enable.

2.8.4 Protéger le root-bridge, limiter les boucles, broadcasts et multicasts

Commandes à appliquer en mode global:

- loopback-detection global enable vlan 1 to 4094
- loopback-detection global action shutdown

Afin d'éviter des pannes provoquées par des problèmes de spanning-tree (boucles de niveau 2, changement de root-bridge…), nous demandons la mise en œuvre de mécanismes de protection en utilisant des commandes **sur certaines interfaces, dans certains cas** :

- loopback-detection enable vlan 1 to 4094
- loopback-detection action shutdown
- stp loop-protection
- stp root protection
- multicast-suppression 20
- broadcast-suppression 20

A appliquer sur les **switches niveau 2** ➔ dans le cadre de ce guide de configuration, seuls les HP 5120 sont concernés. Cette commande doit être appliquée :

- sur les toutes les interfaces « bridge-agregation » des 5130 vers les 5500
- sur les interfaces trunks des 5130 non agrégées apparaissant « root » ou « alternate » avec la commande « display stp brief » :

stp loop-protection (protection anti-boucles) :

A appliquer sur les **switches niveau 2** ➔ dans le cadre de ce guide de configuration, seuls les HP 5120 sont concernés. Cette commande doit être appliquée :

- sur les toutes les interfaces « bridge-agregation » des 5130 vers les 5500
- sur les interfaces trunks des 5130 non agrégées apparaissant « root » ou « alternate » avec la commande « display stp brief » :

```
<3600>display stp brief
 MSTID      Port                        Role  STP State     Protection
   0        Bridge-Aggregation5         ROOT  FORWARDING    LOOP
   0        Bridge-Aggregation51        DESI  FORWARDING    LOOP
   0        Ethernet1/0/3               DESI  FORWARDING    BPDU
   0        Ethernet1/0/4               DESI  FORWARDING    BPDU
   0        Ethernet1/0/5               DESI  FORWARDING    BPDU
```

loop-protection appliquée

stp root-protection (protection du root-bridge) :

A appliquer sur les **switches niveau 3** ➔ dans le cadre de ce guide de configuration, seuls les HP 5500 et les 58XX sont concernés. Cette commande doit être appliquée :

- sur les toutes les interfaces « bridge-agregation » :
  - des fédérateurs 5510 et 5130 vers les 5130
  - des fédérateurs 5510 et 5130 vers les 3600

- sur les interfaces trunks des 5130 non agrégées apparaissant « designated » avec la commande « display stp brief » :

```
<5500>display stp brief
 MSTID      Port                        Role  STP State     Protection
   0        Bridge-Aggregation1         DESI  FORWARDING    ROOT
   0        Bridge-Aggregation2         DESI  FORWARDING    ROOT
   0        Bridge-Aggregation3         DESI  FORWARDING    ROOT
   0        Bridge-Aggregation4         DESI  FORWARDING    ROOT
   0        Bridge-Aggregation5         DESI  FORWARDING    ROOT
   0        Bridge-Aggregation6         DESI  FORWARDING    ROOT
   0        Bridge-Aggregation7         DESI  FORWARDING    ROOT
   0        Bridge-Aggregation8         DESI  FORWARDING    ROOT
   0        Bridge-Aggregation9         DESI  FORWARDING    ROOT
   0        Bridge-Aggregation10        DESI  FORWARDING    ROOT
   0        Bridge-Aggregation11        DESI  FORWARDING    ROOT
   0        Bridge-Aggregation12        DESI  FORWARDING    ROOT
   0        Bridge-Aggregation13        DESI  FORWARDING    ROOT
   0        Bridge-Aggregation14        DESI  FORWARDING    ROOT
   0        GigabitEthernet1/0/26       DESI  FORWARDING    NONE
   0        GigabitEthernet1/0/28       DESI  FORWARDING    NONE
   0        GigabitEthernet2/0/26       DESI  FORWARDING    NONE
   0        GigabitEthernet2/0/27       DESI  FORWARDING    NONE
<5500>
```

root-protection appliquée

root-protection non appliquée car l'interface n'est pas utilisée (shut)

loopback-detection enable et loopback-detection action shutdown :

Sont deux commandes à appliquer sur toutes les interfaces :

- port-link-type access ➔ serveurs non vmware, PMF seuls…
- port link-type trunk de connexion « TELEPHONE + PMF » **UNIQUEMENT**

multicast-suppression 20 et broadcast-suppression 20

Sont deux commandes à appliquer sur toutes les interfaces :

- port-link-type access ➔ serveurs non vmware, PMF seuls…
- port link-type trunk de connexion « TELEPHONE + PMF » **UNIQUEMENT**
- port trunk d'agrégation

⇨ **Reportez-vous au § « Configuration des Interfaces »**

2.9 SNMP / SYSLOG

2.9.1 SNMP

Il est indispensable de configurer cette partie SNMP sur tous les switches pour deux raisons :

1. Les switchs doivent avoir la communauté TOKTAB22! pour être pris en compte dans la SI
2. Les switches fournis par le DR (Cnam) font l'objet d'un contrôle d'inventaire
3. Les outils d'exploitation : Centréon, Netlix.

⇨ **Inventaire :** Veuillez prendre connaissance de la procédure : « Commandes à passer pour mettre à jour l'inventaire.pdf » : voir sur le site du CNGR.

Une access-list va permettre de définir quels sites sont autorisés à lancer des requêtes SNMP en lecture (polling) vers le switch (ou stack) ; ce sont notamment les serveurs du DR en CSH ou au DR.

"**COM_SNMP**" est la communauté en écriture, que vous aurez paramétré dans chacun de vos switches.

```
acl number 2099                                  | n° d'ACL normalisé
 description SNMP RW ACCESS POUR DR              | Description
 rule 0 permit source 55.X.0.0 0.0.255.255       | Si besoin en local, adaptez à votre plan d'adressage
 rule 1 permit source 55.18.0.0 0.0.255.255      | DR
 rule 2 permit source 55.245.0.0 0.0.255.255     | CSH GE
 rule 3 permit source 55.244.0.0 0.0.255.255     | CSH SUD

snmp-agent
snmp-agent community read TOKTBAT22! acl 2099    | ➔ UNIQUE pour serveurs de polling
snmp-agent community write COM_SNMP acl 2099     | ➔ remplacez « COM_SNMP » par votre nom de communauté
snmp-agent sys-info contact François Pignon      | nom d'un contact)
snmp-agent sys-info location RG                  | nom du répartiteur et/ou de la baie
snmp-agent sys-info version v2c                  | version SNMP
snmp-agent trap enable                           | Envoi des traps
```

2.9.2 SYSLOG

SYSLOG : Il s'agit d'un serveur national qui recueille les logs des switches dans le cadre du projet Netlix. Cette commande est à renseigner dans tous les switches car elle permet d'alimenter le puit de log (SONAR/ElasticSearch) :

➔ **Préciser la source pour les swiths Comware V7**

```
<>system-view

info-center loghost source Vlan-interface 901   | cas vlan 901 (cohérence avec l'entrée DNS sur Efficient ip (Netlix) )
info-center loghost source loopback1            | cas loopback 1 (cohérence avec l'entrée DNS sur Efficient ip (Netlix) )
info-center loghost slog-reseau-org.ramage.     | adresse unique valable pour tous – résolution DNS à paramétrer avant !!

dhcp
```

Ces modifications n'entrainent pas de coupure. Le CNGR pourra les déclencher en automatique à partir de NCM (avec votre accord).

Pour retirer le ou les anciens serveur syslog qui existaient, utiliser la commande :
« undo info-center loghost ….. »

Vérification de la configuration :

« display current-configuration | include info » (ou « di cu | i info ».

2.10 SECURITE

2.10.1 ACL 2099 pour SNMP

```
acl number 2099                                  | n° d'ACL normalisé
 description SNMP RW ACCESS POUR CNGR            | Description
 rule 0 permit source 55.X.0.0 0.0.255.255       | Si besoin : plan d'adressage de votre organisme
 rule 1 permit source 55.18.0.0 0.0.255.255      | CNGR
 rule 2 permit source 55.245.0.0 0.0.255.255     | CSH GE
 rule 3 permit source 55.244.0.0 0.0.255.255     | CSH SUD
```

2.10.2 ACL 2922 pour RV6 et SDWAN

```
#Acl pour ne filtrer que des IP CNAM
acl number 2922 name FILTER-DIRECT-NETWORK-RV6
 rule 0 permit source 55.0.0.0 0.255.255.255
 rule 5 permit source 58.0.0.0 0.255.255.255
```

2.10.3 ACL 3002 WOL

```
acl number 3002                                  | n° d'ACL normalisé
 description WOL                                 | Description
 rule 1 permit udp source 55.245.0.0 0.0.255.255 | CSH GE
 rule 2 permit udp source 55.xxx.24.0 0.0.3.255  | SITE Exterieur 1
 rule 3 permit udp source 55.xxx.xxx.0           | SERVEUR LOCAL
```

2.10.4 ACL 3224 pour le VLAN 224

Voir ci-dessous dans le chapitre suivant « VLAN 224 – VLAN-ACCES-PART.

2.10.5 ACLs 3900 et 3901 - Vlan 900 (Admin Ucopia)

L'objectif de cette ACL est de limiter les rebonds sur le LAN organisme depuis l'Ucopia, notamment depuis son tunnel de maintenance (lorsqu'il est activé).

Ainsi, seuls les PMF susceptibles d'administrer le boitier, et/ou de gérer la création des comptes utilisateurs, doivent être autorisés à joindre l'Ucopia.

De même, l'Ucopia ne doit pas avoir accès aux autres ressources du LAN.

```
acl number 3900
description RESTRICTION ACCES UCOPIA VERS LE LAN
rule 1 permit tcp source 55.X.237.2 0 destination 55.X.Y.Z 0 source-port eq www destination-port gt 1024 logging
rule 1 comment UCOPIA VERS PMF1 SUR PORT 80
rule 2 permit tcp source 55.X.237.2 0 destination 55.X.Y.Z 0 source-port eq 443 destination-port gt 1024 logging
rule 2 comment UCOPIA VERS PMF1 SUR PORT 443
rule 3 permit tcp source 55.X.237.2 0 destination 55.X.Y.Z 0 source-port eq 222 destination-port gt 1024 logging
rule 3 comment UCOPIA VERS PMF1 SUR PORT 222 WEB-CLI
rule 10 permit icmp source 55.X.237.2 0 destination 55.X.Y.Z 0 logging
rule 10 comment AUTORISER PING UCOPIA
rule 100 deny ip logging
rule 100 comment INTERDICTION TOUT AUTRE FLUX
#
```

acl number 3901
description RESTRICTION ACCES LAN VERS UCOPIA
rule 1 permit tcp source 55.X.Y.Z 0 destination 55.X.237.2 0 source-port gt 1024 destination-port eq www logging
rule 1 comment PMF1 VERS UCOPIA SUR PORT 80
rule 2 permit tcp source 55.X.Y.Z 0 destination 55.X.237.2 0 source-port gt 1024 destination-port eq 443 logging
rule 2 comment PMF1 VERS UCOPIA SUR PORT 443
rule 3 permit tcp source 55.X.Y.Z 0 destination 55.X.237.2 0 source-port gt 1024 destination-port eq 222 logging
rule 3 comment PMF1 VERS UCOPIA SUR PORT 222 WEB-CLI
rule 10 permit icmp source 55.X.Y.Z 0 destination 55.X.237.2 0 logging
rule 10 comment AUTORISER PING UCOPIA
rule 100 deny ip logging
rule 100 comment INTERDICTION TOUT AUTRE FLUX
#
interface Vlan-interface900
description INT-VLAN-ADMIN-UCOPIA
ip address 55.X.237.1 255.255.255.252
packet-filter 3900 inbound
packet-filter 3901 outbound

N.B :
55.X.237.2 = ip-admin-Ucopia
55.X.Y.Z = Adresse IP du PMF autorisé, merci d'ajouter le nombre de rule nécessaire en fonction du nombre de PMF à autoriser.
→ Ces adresses sont à adapter en fonction du plan d'adressage de votre organisme.

2.10.6 Fonction packet-filter

Cette fonction permet d'appliquer une ACL sur un VLAN.

[SYSNAME-Vlan-interface224]packet-filter 3224 inbound | Application pour le vlan 224

[SYSNAME-Vlan-interface900]packet-filter 3900 inbound | Application pour le vlan 900
[SYSNAME-Vlan-interface900]packet-filter 3901 outbound | Application pour le vlan 900

Visualisation des statistiques :

[SYSNAME] dis packet-filter statistics sum inbound **XXXX** | Contrôle de la fonction XXXX = n°acl

2.11 CONFIGURATION DES VLAN



A quoi ça sert ?

Les Vlans permettent de gérer des domaines de broadcast distincts. Ils présentent les intérêts suivants:

- **Améliorer la gestion du réseau.**
- **Optimiser la bande passante.**
- **Séparer les flux.**
- **Fragmentation: réduire la taille d'un domaine de broadcast,**
- **Sécurité: permet de créer un ensemble logique isolé pour améliorer la sécurité.**

Vous pouvez gérer vos vlans de 2 façons :

- Soit statiquement : Déclaration manuelle des vlans sur les équipements niveau 3 et niveau 2
- Soit dynamiquement en utilisant le protocole GVRP (pas recommandé par la Cnam)

Nous conseillons donc de créer les VLAN manuellement sur tous les switches et de ne pas utiliser GVRP.

2.11.1 Nommage des Vlan et des interfaces VLAN

Le nommage des VLAN et des interfaces vlan est **normalisé et obligatoire**. Consulter les référentiels plus haut dans le document.

2.11.2 Déclarer les VLAN (niveau 2)

Exemple avec le VLAN 30 :

CREATION	SUPPRESSION
<>system-view # vlan 30 **name VLAN-VOIX**	<>system-view # undo vlan 30

⇨ **Appliquez le nommage normalisé.**

2.11.3 Création des interfaces VLAN (niveau 3)

Seuls les fédérateurs niveau 3 (5510 et 5510) possèdent plusieurs interfaces VLAN. Les switches d'extrémité (5130 et 5140) n'ont qu'une seule interface VLAN : VLAN 901 (VLAN-ADMIN-RESEAU).

Ne configurez que celle dont vous avez besoin (en phase avec vos VLAN).

La VLAN-interface 1 doit être supprimée. Les autres VLAN-interfaces ont une adresse.

➔ **Préciser la source dhcp relay pour les swiths Comware V7**

Ne pas oublier d'appliquer les descriptions normalisées OBLIGATOIRES.

Nous donnons icies interfaces VLAN et leur adressage en **SIEGE** : pour connaître les plans d'adressage IP à utiliser, **reportez-vous aux référentiels LAN ci-dessus.**

```
<>system-view
#
undo interface Vlan-interface 1
#
interface Vlan-interface 4
 description INT-VLAN-DATA
 ip address 55.X.4.1 255.255.252.0                | ou ip address 55.X.4.1 22
dhcp relay source-address 55.X.4.1                | pour renseigner le champ source des requêtes dhcp si server DHCP
                                                  | externe
#
interface Vlan-interface 30
 description INT-VLAN-VOIX
 ip address 58.X.4.1 255.255.252.0                | ou ip address 58.X.4.1 22
 dhcp select relay
 dhcp relay server-address 55.x.4.y               | ou ip address du serveur dns
dhcp relay source-address 58.X.4.1                | pour renseigner le champ source des requêtes dhcp
#
interface Vlan-interface 5
 description INT-INTERCOWAN
 ip address 55.X.225.1 255.255.255.240            | ou ip address 55.X.225.1 28
#
interface Vlan-interface 17
 description INT-VLAN-EVASION-INTERNET
 ip address 192.168.1.4 255.255.255.0             | ou ip address 192.168.1.4 24
#
interface Vlan-interface172
 description INT-VLAN-SDWAN
 ip address 172.X.X.X 255.255.255.248
#
interface Vlan-interface224
 description INT-VLAN-ACCESS-PART
 ip address 55.X.224.1 255.255.255.128            | ou ip address 55.X.224.1 25
 packet-filter 3224 inbound   (*)
#
interface Vlan-interface226
 description INT-VLAN-IMPRIMANTES
 ip address 55.X.248.1 255.255.255.128            | ou ip address 55.X.248.1 25
 packet-filter 3226 inbound   (*)
#
interface Vlan-interface 901
 description INT-VLAN-ADMIN-RESEAU
 ip address 55.X.221.1 255.255.255.0              | ou ip address 55.X.221.1 24
#
interface Vlan-interface 902
```

description INT-VLAN-ADMIN-WIFI
ip address 55.X.220.1 255.255.255.0 **| ou** ip address 55.X.220.1 **24**

interface Vlan-interface903
description INT-VLAN-ROUTEUR-WIFI-INVITE
ip address 55.40.237.5 255.255.255.252 **| Suite connexion evasion au boitier SDWAN**

…etc.

(*) : Voir paragraphe « Sécurité »

2.11.4 VLAN 901 (ADMIN-RESEAU) en AGENCES



Attention à la coupure réseau

Principe : L'interface VLAN 1 ou VLAN4 doit être supprimée et remplacée par l'interface VLAN 901.

A partir de 2021 et Ramage V6, le VLAN 901 sera à déclarer sur tous les sites de l'assurance maladie, car tous les sites seront niveau 3.

Pour connaître les plans d'adressage IP à utiliser, reportez-vous aux référentiels.

	Agence avec 1 stack	Agence avec 1 switch	Agence avec plusieurs switches ou stacks
Déclaration vlan 901 Niveau 2	Non	Non	Oui
Déclaration Vlan interface 901	Non	Non	Oui
Déclaration loopback 1	Oui	Oui	Non

2.11.4.1 Cas d'un site multi stack (avec plusieurs stacks)

Le paramètrage est identique à celui d'une CPAM.

Dans l'exemple l'agence a pour réseau d'ADMIN-RESEAU (901) le 55.xxx.0.16/28.

Adresse Stack N3:55.xxx.0.17 | Première adresse du réseau
Adresse Stack N2(Stack2): 55.xxx.0.18 | Deuxième adresse du réseau
Adresse Stack N2(Stack3): 55.xxx.0.19 |Troisième adresse du réseau
…
Adresse Stack N2(Stack12): 55.xxx.0.29
Adresse Stack N2(Stack13): 55.xxx.0.30 |Treizième adresse du réseau

Switch N2 & Switch N3

```
<351-SW-N3-SITE-HP 5510-RG>system-view
#
[351-SW-N3-SITE-HP 5510-RG]Vlan 901
[351-SW-N3-SITE-HP 5510-RG]name VLAN-ADMIN-RESEAU          | A renseigner obligatoirement)
```

Switch N3:

```
<351-SW-N3-SITE-HP 5510-RG>system-view
#
undo interface Vlan-interface 1
#
[351-SW-N3-SITE-HP 5510-RG]interface Vlan-interface 901
 description INT-VLAN-ADMIN-RES
 ip address 55.xxx.0.17 255.255.255.240          | Voir le référentiel LAN-Agences plus haut
```

Switch N2(Stack2):

```
<351-SW-N2-SITE-HP 5130-STACK2>system-view
#
undo interface Vlan-interface 1
#
[351-SW-N2-SITE-HP 5130-STACK2]interface Vlan-interface 901
 description INT-VLAN-ADMIN-RESEAU
```

ip address 55.xxx.0.18 255.255.255.240 **| Voir le référentiel LAN-Agences plus haut**

Remarque : dans les switches d'extrémité, ne pas oublier de modifier la route vers le fédérateur (Coupure à prévoir / opération en HNO) : 0.0.0.0 .0.0.0.0 @IP interface-VLAN-901-du-fédérateur.

Connectez-vous en port console sur chaque switch.

Ajoutez la nouvelle route :
[] **ip route-static 0.0.0.0 0.0.0.0** 55.xxx.0.17 | Vers adresse ip de la vlan interface 901 du switch N3

Supprimez l'ancienne route:
[] undo **ip route-static 0.0.0.0 0.0.0.0** 55.xxx.4.1 | Vers adresse ip de la vlan interface 4 du switch N3

2.11.4.2 Cas d'un site avec une seule stack de switch : Loopback1

Vous ne pouvez pas configurer un VLAN d'ADMIN-RESEAU puisque vous ne disposez que d'un seul switch ou d'une seule stack (stack) : comme aucun équipement n'est connecté dans ce VLAN, il resterait « DOWN ».

Vous allez donc déclarer une adresse de loopback qui sera diffusée sur le réseau RAMAGE via votre interface VLAN 5. Cette loopback doit être la loopback1 et doit avoir comme adresse IP la dernière du sous-réseau : consultez les tableaux dans le référentiel LAN des agences.

Pour connaître les plans d'adressage IP à utiliser, reportez-vous aux référentiels plus haut.

Dans l'exemple, le SITE a pour reseau d'ADMIN-RESEAU (901) le 55.xxx.0.240/28.

Adresse Loopback N3:55.xxx.0.241 | Voir le référentiel LAN-Agences plus haut

```
<>system-view
#
undo interface Vlan-interface 1
#
interface LoopBack1                          | Respecter le n° d'interface de loopback 1
 description INT-LOOPBACK-ADMIN-RESEAU       | DESCRIPTION NORMALISEE OBLIGATOIRE
 ip address 55.xxx.0.241 255.255.255.255     | Voir le référentiel LAN-Agences plus haut @loopback /32)
#
```

Exemples :

Interface loopback1
 Ip address *55.X.0.14*

Interface loopback1
 Ip address *55.X.0.30*

Interface loopback1
 Ip address *55.X.1.126*

2.11.5 VLAN 902 (ADMIN-RESEAU-WIFI) en AGENCES

Le VLAN 902 sera déclaré sur tous les sites de l'assurance maladie, il correspond au vlan VLAN-ADMIN-WIFI qui aujourd'hui était confondu avec le vlan 901 VLAN-ADMIN-RES.

1/ Déclaration Vlan niveau II

```
#
vlan 902
name VLAN-ADMIN-WIFI (à renseigner obligatoirement si wifi sur site)
```

2/Déclaration Vlan interface niveau III

```
#
interface Vlan-interface 902
 description INT-VLAN-ADMIN-WIFI                | A renseigner obligatoirement si wifi sur site
 ip address 55.X.2.1 255.255.255.240            | Voir le référentiel LAN-Agences plus haut
```

2.11.6 VLAN 900 (ADMIN-UCOPIA) en SIEGE

Le vlan 900 sera déclaré sur le site où se trouve le portail captif Ucopia (c'est-à-dire au siège).

Le vlan 900 vise à isoler, au maximum, l'ucopia sur le réseau de l'Assurance-Maladie. Pour ce faire, l'ACL 3900 doit être positionnée sur ce vlan 900.

1/ Déclaration Vlan niveau 2

```
#
vlan900
name VLAN-ADMIN-UCOPIA
```

2/Déclaration Vlan interface niveau 3

```
#
interface vlan 900
description INT-VLAN-ADMIN-UCOPIA
ip address 55.x.237.1 255.255.255.252
packet-filter 3900 inbound
packet-filter 3901 outbound                    | cf § « SECURITE » ACL 3900 et 3901 VLAN 900 (ADMIN-UCOPIA)
```

2.11.7 VLAN 22X

Tous les VLAN 22X permettront d'isoler des équipements pouvant être accédés à distance par un partenaire extérieur.

Ils doivent répondre à un projet national validé par la DS (la demande sera postée travers le psn).

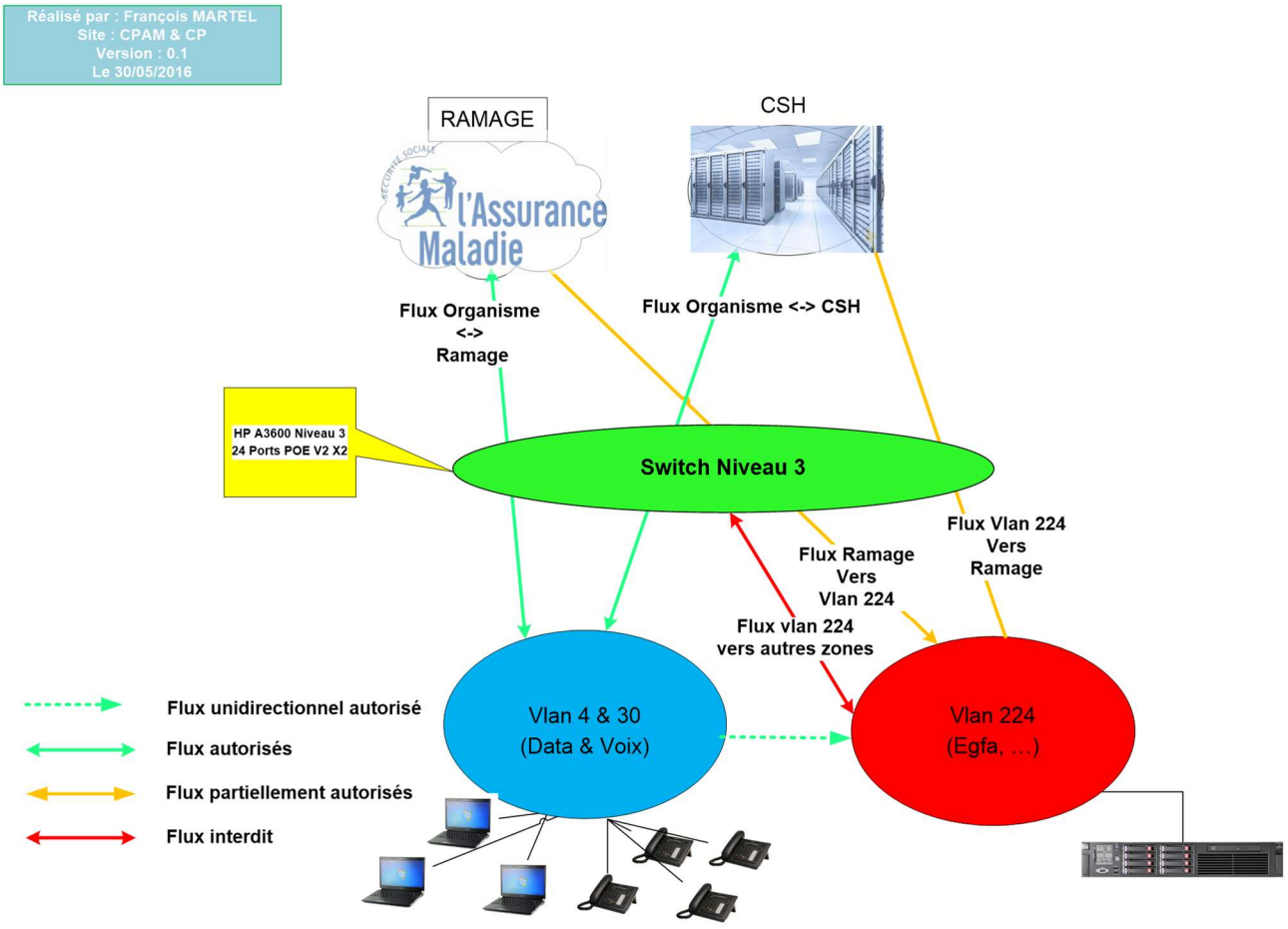
Voir : https://www.cngr.cnamts.fr/contenu/symfony/162

Une ACL (ACL 322X) sera mise en place permettant de filtrer les communications entre les matériels actifs isolés dans le VLAN 22x **« zone partenaire »** et les machines hébergés sur le LAN local des organismes dans **« la zone RAMAGE »**

Les ACL à appliquer seront décrites dans une procédure sur le portail du DR : https://www.cngr.cnamts.fr/
Pour des besoins locaux (hors projets nationaux), les équipements doivent être intégrés dans le VLAN 224.

2.11.7.1 VLAN 224 – VLAN-ACCES-PART

2.11.7.1.1 ACL EGFA : principe



2.11.7.1.2 Le VLAN et l'interface VLAN :

Vlan 224
name VLAN-ACCES-PART

interface Vlan-interface224
description INT-VLAN-ACCES-PART
ip address 55.X.224.1 255.255.255.128

2.11.7.1.3 ACL pour EGFA en SIEGE :

A appliquer sur le **switch fédérateur de niveau 3** du site et seulement sur ce switch.

Dans les ACL, les masques de sous-résaux sont exprimés en « wildcard ». En siège, le masque doit être 255.255.255.128. Le wildcard doit donc être 0.0.0.127.

ACL - Remplacer le X par votre octet d'organisme :

```
acl number 3224 name Acces-Part-vers-autres-Vlan

 rule 10 permit ip source 55.X.224.0 0.0.0.127 destination 55.227.1.20 0 logging
 rule 10 comment Autorisation dialogue vlan 224 / partenaires via CSH

 rule 20 permit ip source 55.X.224.0 0.0.0.127 destination 55.227.1.21 0 logging
 rule 20 comment Autorisation Proxy Egfa 1

 rule 30 permit ip source 55.X.224.0 0.0.0.127 destination 55.225.59.20 0 logging
 rule 30 comment Autorisation Proxy Egfa 2

 rule 40 permit ip source 55.X.224.0 0.0.0.127 destination 55.X.224.0 0.0.0.127 logging
 rule 40 comment Autorisation Flux interne Vlan Partenaires

 rule 50 permit ip source 55.X.224.0 0.0.0.127 destination 55.14.0.0 0.0.255.255 logging
 rule 50 comment Autorisation Csn Caen

 rule 100 deny ip logging
 rule 100 comment Interdiction tout autre flux
```

Application sur l'interface VLAN 224 :

```
interface Vlan-interface224
 description INT-VLAN-ACCES-PART
 ip address 55.X.224.1 255.255.255.128
 packet-filter 3224 inbound
```

L'ACL bloque tout flux en provenance des autres VLAN du site y compris les administrateurs informatiques. Pour permettre cet accès, il faut ajouter la règle 60 :

```
rule 60 permit ip source 55.X.224.0 0.0.0.127 destination 55.X.Y.Z 0 logging
rule 60 comment Autorisation flux legitime
```

55.X.Y.Z = Adresse IP du PMF autorisé. Ajouter autant de règles (61, 62…) que de PC à autoriser.

2.11.7.1.4 Ajout de l'accès d'un autre partenaire dans le VLAN-ACCES-PART en SIEGE :

Lors de votre demande d'interconnexion d'un partenaire, il vous est fournie une adresse IP par le SOC. Cette adresse IP est l'adresse IP entrante de **ce partenaire** : elle est de la forme 55.227.X.Y – 255.255.255.255.

Pour ajouter l'accès de partenaire au VLAN 224, ajouter une règle (par exemple 70) à l'ACL 3224 :

```
rule 70 permit ip source 55.X.224.0 0.0.0.127 destination 55.227.X.Y 0 logging
rule 70 comment Autorisation PARTENAIRE « nom du partenaire »
```

2.11.7.1.5 ACL pour EGFA en AGENCE :

Comme indiqué dans le référentiel LAN des agences : « les CP utiliseront un des sous-réseaux suivants pour le VLAN 224. Il s'agit de choisir un sous-réseau par CP. Si le nombre d'adresses est insuffisant pour un site, veuillez adapter le masque de sous-réseau. »

Dans les ACL, le masque est « inversé » : on parle de WILDCARD (en vert dans l'exemple : première règle) dans les configurations ci-dessous. En fonction du masque utilisé, veuillez adapter le wildcard.

Masque		Wildcard
255.225.255.248	/29	0.0.0.7
255.255.255.240	/28	0.0.0.15
255.255.255.224	/27	0.0.0.31
…etc.		

Comme listé de manière exhaustive dans le référentiel LAN des agences, le plan d'adressage est le suivant (masque à adapter en fonction du besoin) :

CP	subnet	Masque	Première @	Dernière @	Int vlan 224 Switch N3	Disponibles pour clients				
1	55.X.246.0	255.255.255.248 (/29)	1	6	1	4	5	6	2	3
2	55.X.246.8	255.255.255.248 (/29)	9	14	9	12	13	14	10	11
3	55.X.246.16	255.255.255.248 (/29)	17	22	17	20	21	22	18	19
4	55.X.246.24	255.255.255.248 (/29)	25	30	25	28	29	30	26	27
5	55.X.246.32	255.255.255.248 (/29)	33	38	33	36	37	38	34	35
…etc……										
61	55.X.247.224	255.255.255.248 (/29)	225	230	225	228	229	230	226	227
62	55.X.247.232	255.255.255.248 (/29)	233	238	233	236	237	238	234	235
63	55.X.247.240	255.255.255.248 (/29)	241	246	241	244	245	246	242	243
64	55.X.247.248	255.255.255.248 (/29)	249	254	249	252	253	254	250	251

Il faut adapter l'ACL au plan d'adressage IP du site et remplacer le X par votre octet d'organisme.

ACL - Remplacer le X par votre octet d'organisme :

Dans la configuration ci-dessous, nous utilisons le cas du CP n° 1 (55.X.246.0 /29) :

acl number 3224 name Acces-Part-vers-autres-Vlan

rule 10 permit ip source 55.X.246.**0 0.0.0.7** destination 55.227.1.20 0 logging
rule 10 comment Autorisation dialogue vlan 224 / partenaires via CSH

rule 20 permit ip source 55.X.246.0 0.0.0.7 destination 55.227.1.21 0 logging
rule 20 comment Autorisation Proxy Egfa 1

rule 30 permit ip source 55.X.246.0 0.0.0.7 destination 55.225.59.20 0 logging
rule 30 comment Autorisation Proxy Egfa 2

rule 40 permit ip source 55.X.246.0 0.0.0.7 destination 55.X.246.0 0.0.0.7 logging
rule 40 comment Autorisation Flux interne Vlan Partenaires

rule 50 permit ip source 55.X.246.0 0.0.0.7 destination 55.14.0.0 0.0.255.255 logging
rule 50 comment Autorisation Csn Caen

rule 100 deny ip logging
rule 100 comment Interdiction tout autre flux

L'ACL bloque tout flux en provenance des autres VLAN du site y compris les administrateurs informatiques. Pour permettre cet accès, il faut ajouter la règle 60 :

rule 60 permit ip source 55.X.246.0 0.0.0.7 destination 55.X.Y.Z 0 logging
rule 60 comment Autorisation flux legitime

55.X.Y.Z = Adresse IP du PMF autorisé. Ajouter autant de règles (61, 62…) que de PC à autoriser.

Application sur l'interface VLAN 224 :

interface Vlan-interface224
description INT-VLAN-ACCES-PART
ip address 55.X.246.1 255.255.255.248
packet-filter 3224 inbound

2.11.7.1.6 Ajout de l'accès d'un autre partenaire dans le VLAN-ACCES-PART en AGENCE

Lors de votre demande d'interconnexion d'un partenaire, il vous est fournie une adresse IP par le SOC. Cette adresse IP est l'adresse IP entrante de **ce partenaire** : elle est de la forme 55.227.X.Y – 255.255.255.255.

Pour ajouter l'accès de partenaire au VLAN 224, ajouter une règle (par exemple 70) à l'ACL 3224 :

rule 70 permit ip source 55.X.246.0 0.0.0.7 destination 55.227.X.Y 0 logging
rule 70 comment Autorisation PARTENAIRE « nom du partenaire »

2.11.7.2 VLAN 226 (VLAN-IMPRIMANTES)

1/ Déclaration du vlan 226

<>system-view
Vlan 226
name VLAN-IMPRIMANTES

2/ Déclaration de la vlan interface 226:

Pour un SIEGE :

<>system-view
int vlan 226
description INT-VLAN-IMPRIMANTES
ip address 55.xxx.248.1 255.255.255.128 | pour un siège voir le référentiel LAN-SIEGES plus haut
packet-filter 3226 inbound | voir le paragraphe « Sécurité »

Pour une AGENCE :

<>system-view
int vlan 226
description INT-VLAN-IMPRIMANTES
ip address 55.xxx.249.137 255.255.255.248 | pour une agence/établissement voir le référentiel LAN-Agences plus haut
packet-filter 3226 inbound | voir le paragraphe « Sécurité »

2.11.7.3 VLAN 227 (VLAN-IMPRIMANTES-MEDICAL)

1/ Déclaration du vlan 227

```
<>system-view
Vlan 227
name VLAN-IMPRIMANTES-MEDICAL
```

2/ Déclaration de la vlan interface 227:

Pour une CPAM

```
<>system-view
int vlan 227
description  INT-VLAN-IMPRIMANTES-MEDICAL
ip address 55.2xx.248.1* 255.255.255.128          | pour un siège voir le référentiel LAN-SIEGES plus haut
```

Pour un Centre de Paiement

```
<>system-view
int vlan 227
description  INT-VLAN-IMPRIMANTES-MEDICAL
ip address 55.2xx.249.137 255.255.255.248         | pour un siège voir le référentiel LAN-SIEGES plus haut
```

2.11.8 Suppression du VLAN 249 VISIO

Pour supprimer le VLAN 249 « VISIO » sur tous vos switches :

- Supprimer le VLAN 249 et l'interface VLAN 249 :
  undo vlan 249

- Si le terminal visio était connecté sur un switch d'extrémité, il faut supprimer le vlan 249 sur les aggrégats de tous les switches traversés :

  Interface Bridge-Agregation X
  undo port trunk permit vlan 249

2.12 CONFIGURATION DES INTERFACES

2.12.1 Interfaces non utilisées



Pour respecter les consignes de la PSSI MCAS, <u>au moins dans les lieux sensibles comme les accueils</u>… (Possibilité pour un inconnu de se connecter au réseau sur une prise dans les lieux ouverts au public, possibilité de connecter un PC « non PLC » ou un hub ou un switch ou un sniffer sur une prise libre dans son bureau….) :

- ⇨ **<u>il est demandé de mettre à « shutdown »</u> <u>toutes les interfaces Ethernet, GigaEthernet et TenGigaEthernet non utilisées</u>.**

```
[351-sw-et-redon-n3-1-3600-GigabitEthernet3/0/49]default                    | remise en conf usine
This command will restore the default settings. Continue? [Y/N]:y

[351-sw-et-redon-n3-1-3600-GigabitEthernet3/0/49]shut                       | shut de l'interface Giga
[351-sw-et-redon—n3-1-3600--GigabitEthernet3/0/49]description SHUTDOWN
```

2.12.2 Description des interfaces

La description des interfaces doit être renseignée. Celles des routeurs opérateurs sont normalisées:

description ROUTEUR-BTE
description ROUTEUR-NXO

2.12.3 Speed / Duplex

<u>RAPPEL :</u>

1/ Configurer l'interface sans s'occuper des « speed et duplex » : laisser en auto par défaut

2/ Entre des « hosts » (PMF, téléphone, serveurs) et des switches, <u>lorsque</u> :
- **le débit négocié est inférieur à celui escompté**
- **un quelconque problème apparaît (lenteurs, accès à des ressources…)**
- **des erreurs sont constatées sur les interfaces**

⇨ **il faut forcer les speed et duplex côté switch <u>et</u> côté « host » (si possible).**

Les exemples ci-dessous correspondent aux VLAN utilisés en organismes. Des descriptions sont données en exemple.

Les 5XXX sont utilisés pour la connexion de serveurs et d'autres switches (essentiellement). Il ne sera pas indiqué dans ce guide la configuration des interfaces de connexion des PMF et des téléphones IP. Reportez-vous pour cela au guide de configuration des HP 3600-v2 où la méthode de déploiement de la ToIP et la configuration des interfaces des switches est décrite.

2.12.4 Routeurs opérateurs RV6 (RAMAGE)

Seuls les HP 5510 et 5520 peuvent accueillir des routeurs opérateurs. Les HP 5130 ne sont pas compatibles avec Ramage v6.

2.12.4.1 Les fonctions associées aux ports des routeurs opérateurs

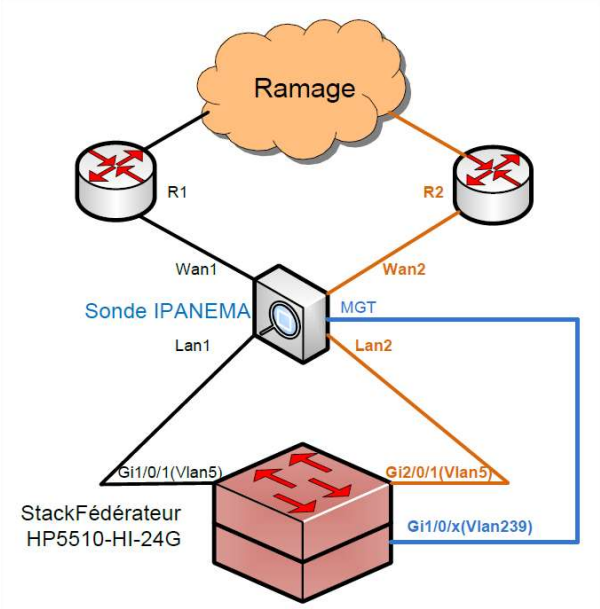
- **Description ROUTEUR-BTE (Routeur Bouygues Telecom)**
- **Description ROUTEUR-NXO (Routeur NextiraOne)**
- **port access vlan 5 (connectés au VLAN5 d'intercowan)**
- **undo stp enable** (**désactivation du spanning tree**)

Le VLAN 5 aura été créé au préalable.

2.12.4.2 Sonde IPANEMA

Dans le cas où une sonde est à installer sur le site, elle s'intercale entre les switches fédérateurs et les routeurs RAMAGE :

Schéma de principe :



Configuration de l'interface MGT :

Vlan et interface VLAN:

```
vlan 239
 description MGT-IPANEMA
 name MGT-IPANEMA
#
interface Vlan-interface239
 description MGT-IPANEMA
 ip address 55.239.X.Y 255.255.255.248
```

Connexion de l'interface MGT :

➔ choisir un port disponible sur le fédérateur **MASTER OBLIGATOIREMENT !!**

```
interface GigabitEthernet1/0/x
 description MGT-IPANEMA
 port link-type access
 port access vlan 239
 speed 100
 duplex full
 stp edged-port
```

Les valeurs de **X** et de **Y** sont uniques pour chaque sonde. Cette information adaptée à votre site, est disponible sur le portail du CNGR.

La configuration des interfaces VLAN 5 côté switch est la même que lorsqu'il n'y a pas de sonde.

2.12.4.3 Les ports normalisés des routeurs opérateurs

Accès Ramage v6 SANS FTTH

Cas d'un switch N3 seul

			Interfaces normalisées sur le switch pour la connexion des routeurs		
			Switches HP à ports RJ45	Switches HP à ports Fibre	Description
PROFILS	Gammes de switches ==>		5510-24G ou 48G-POE	5510-24G-SFP	-
Profils 1, 2 et 3	port 1 Routeur BTE		GI 1/0/1	GI 1/0/24	ROUTEUR-BTE
(2 opérateurs)	Port 5 routeur NXO		GI 1/0/2	GI 1/0/23	ROUTEUR-NXO
Profil 4	Profil 4a (BTE)	port 1 Routeur BTE	GI 1/0/1	GI 1/0/24	ROUTEUR-BTE
(1 opérateur)	Profil 4b (NXO)	Port 5 routeur NXO	GI 1/0/2	GI 1/0/23	ROUTEUR-NXO

Cas d'un stack N3

			Interfaces normalisées sur le STACK de N switches pour la connexion des routeurs		
			5510-24G ou 48G-POE	Switches HP à ports Fibre	Description
PROFILS	Gammes de switches ==>		5510-24G	5510-24G-SFP	-
Profils 1, 2 et 3	port 1 Routeur BTE		GI 1/0/1	GI 1/0/24	ROUTEUR-BTE
(2 opérateurs)	Port 5 routeur NXO		GI N/0/1	GI N/0/24	ROUTEUR-NXO
Profil 4	Profil 4a (BTE)	port 1 Routeur BTE	GI 1/0/1	GI 1/0/24	ROUTEUR-BTE
(1 opérateur)	Profil 4b (NXO)	Port 5 routeur NXO	GI N/0/1	GI N/0/24	ROUTEUR-NXO

N = numéro du dernier switch du stack

Accès Ramage v6 AVEC FTTH

Cas d'un switch N3 seul

			Interfaces normalisées sur le switch pour la connexion des routeurs		
			Switches HP à ports RJ45	Switches HP à ports Fibre	Description
PROFILS	Gammes de switches ==>		5510-24G ou 48G-POE	5510-24G-SFP	-
Profils 2 et 3	Un des 2 opérateurs	port 1 Routeur BTE	GI 1/0/1	GI 1/0/24	ROUTEUR-BTE
(2 opérateurs)	est en FTTH	Port 5 routeur NXO	GI 1/0/2	GI 1/0/23	ROUTEUR-NXO
Profil 4	Profil 4a (BTE)	port 1 Routeur BTE FTTH	GI 1/0/1	GI 1/0/24	ROUTEUR-BTE
(1 opérateur)	Profil 4b (NXO)	Port 5 routeur NXO FTTH	GI 1/0/2	GI 1/0/23	ROUTEUR-NXO

Cas d'un stack N3

			Interfaces normalisées sur le STACK de N switches pour la connexion des routeurs		
			Switches HP à ports RJ45	Switches HP à ports Fibre	Description
PROFILS	Gammes de switches ==>		5510-24G ou 48G-POE	5510-24G-SFP	-
Profils 2 et 3	Un des 2 opérateurs	port 1 Routeur BTE	GI 1/0/1	GI 1/0/24	ROUTEUR-BTE
(2 opérateurs)	est en FTTH	Port 5 routeur NXO	GI N/0/1	GI N/0/24	ROUTEUR-NXO
Profil 4	Profil 4a (BTE)	port 1 Routeur BTE FTTH	GI 1/0/1	GI 1/0/24	ROUTEUR-BTE
(1 opérateur)	Profil 4b (NXO)	Port 5 routeur NXO FTTH	GI N/0/1	GI N/0/24	ROUTEUR-NXO

N = numéro du dernier switch du stack

Dans certains sites, une sonde IPANEMA sera intercalée entre le routeur et le stack fédérateur.

2.12.4.4 La configuration

Switch fédérateur maître :	**Switch fédérateur secours :**
<>system-view **#** **interface GigabitEthernet1/0/1➔si HP 5xx0** **ou** **interface GigabitEthernet1/0/24➔si HP 5xx0-SFP** **description ROUTEUR-BTE** **port link-type access*** **port access vlan 5** **speed 100 ou 1000 si FTTH** **duplex full** **undo stp enable**	**<>system-view** **#** **interface GigabitEthernet2/0/1➔si HP 5xx0** **ou** **interface GigabitEthernet2/0/24➔ si HP 5xx0-SFP** **description ROUTEUR-NXO** **port link-type access*** **port access vlan 5** **speed 100 ou 1000 si FTTH** **duplex full** **undo stp enable**

* Commande n'apparaissant pas en « *display current configuration* »

Si la commande « stp edged-port enable » est présente, il faut la retirer avec « stp edged-port disable ». La désactivation du spanning-tree sur ces interfaces ne provoque aucune coupure (« stp-edged-port disable» et « undo stp enable »).

Les descriptions « ROUTEUR-BTE » et « ROUTEUR-NXO » sont normalisées.

Si un cas n'est pas décrit dans le tableau précédent vous pouvez consulter les référentiels plus haut pour plus de précision ou poster une demande au DR via le PSN.

2.12.5 Routeurs opérateurs SDWAN (RAMAGE)

2.12.5.1 La configuration SDWAN

Switch fédérateur maître (BTE) :	**Switch fédérateur secours (NXO) :**
<>system-view **#** **interface GigabitEthernet1/0/24** **port link-mode bridge** **description SDWAN-OP1** **port link-type trunk** **undo port trunk permit vlan 1** **port trunk permit vlan 172** **undo stp enable**	**<>system-view** **#** **interface GigabitEthernet2/0/24** **port link-mode bridge** **description SDWAN-OP2** **port link-type trunk** **undo port trunk permit vlan 1** **port trunk permit vlan 172** **undo stp enable**

Si la commande « stp edged-port enable » est présente, il faut la retirer avec « stp edged-port disable ». La désactivation du spanning-tree sur ces interfaces ne provoque aucune coupure (« stp-edged-port disable» et « undo stp enable »).

Les descriptions « SDWAN-OP1» et « SDWAN-OP2» sont normalisées et ne doivent pas être modifiées.

Si un cas n'est pas décrit dans le tableau précédent vous pouvez consulter les référentiels plus haut pour plus de précision ou poster une demande au DR via le PSN.

2.12.5.2 Connexion du routeur 4G

- **Switch ou Stack HP 5510 ou HP 5520 … CUIVRE (24 ou 48 ports RJ45) :**

► Le ROUTEUR-4G est à connecter :
- SI STACK : sur le port 1/0/2 du fédérateur maitre
- SI SWICH SEUL et pas de routeur secours : sur le port 1/0/2 du switch
- SI SWICH SEUL et routeur secours : sur le port 1/0/3 du switch

- Stack de HP 5510 ou 5140G-24-SFP-EI FIBRE OPTIQUE (24 ports SFP ou 16 ports SFP +8 ports RJ45) :

► Le ROUTEUR-4G est à connecter :
- SI STACK : sur le port 1/0/23 (RJ45) du fédérateur maitre
- SI SWITCH SEUL et pas de routeur secours : sur le port 1/0/23 du switch
- SI SWITCH SEUL et routeur secours : sur le port 1/0/22 du switch

Configuration : Il existe plusieurs contextes … Veuillez-vous référer à la documentation spécifique sur le portail du DR (rubrique Infrastructure / WAN / Offre 4G).

2.12.6 Box Evasion Internet

```
interface GigabitEthernet1/0/x
description BOX-EVASION-INTERNET
port link-mode bridge
port access vlan 17
```

2.12.7 Serveur physique (non VMWARE)

```
interface GigabitEthernet1/0/1
description SERVEUR PHYSIQUE
port link-mode bridge
 stp enable                                | cette commande n'apparaît pas en « display current-configuration »
 stp edged-port
 port link-type access                     | cette commande n'apparaît pas en « display current-configuration »
 port access vlan 4
 loopback-detection enable vlan all        | action détection des boucles
 loopback-detection action shutdown        | action détection des boucles
 multicast-suppression 20                  | limitation à 20% maxi du trafic multicast sur le port
 broadcast-suppression 20                  | limitation à 20% maxi du trafic broadcast sur le port
 [speed 1000]                              | Si négociation différente 1Gb
 [duplex full]                             | Si négociation différente 1Gb
 description serveur intranet
```

2.12.8 PMF + TEL

Nous préconisons l'interconnexion des PMF avec les switches HP **via des ports trunk.** Les commandes spécifiques associées aux ports trunk+PMF sont les suivantes:

- poe enable (Alimentation du port)
- Vlan 4
- voice-vlan 30 enable (force le téléphone à démarrer dans le vlan30)

```
#
voice-vlan mac-address 0080-9f00-0000 mask ffff-ff00-0000  (autoriser le constructeur à faire du voice vlan, ici ALCATEL)
#
interface GigabitEthernet1/0/2
port link-mode bridge
description PMF TEL
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 4 30
 port trunk pvid vlan 4                                | Force le vlan par défaut à 4 (VLAN-DATA)
 undo voice-vlan mode auto                             | Force le boot du tel sur le vlan 30
 voice-vlan 30 enable                                  | Force le boot du tel sur le vlan 30
 broadcast-suppression 20                              | limitation à 20% maxi du trafic multicast sur le port
 multicast-suppression 20                              | limitation à 20% maxi du trafic multicast sur le port
 stp edged-port
 stp port bpdu-protection enable
 poe enable
 loopback-detection enable vlan 1 to 4099              | action détection des boucles
 loopback-detection action shutdown                    | action détection des boucles
```

Cette configuration est la configuration standard pour la connexion des téléphones IP de CETIAM.

2.12.9 PMF + TEL pour SERVICE MEDICAUX

Les PMF Service medical doivent être isolés dans un vlan spécifique le VLAN3 car ils font parti des services hébergés par l'assurance maladie.
Nous préconisons l'interconnexion des PMF du service medical avec les switches HP **via des ports trunk.** Les commandes spécifiques associées aux ports trunk+PMF sont les suivantes:

- poe enable (Alimentation du port)
- Vlan 3
- Voice-vlan 30 enable (force le téléphone à démarrer dans le vlan30)

```
voice-vlan mac-address 0080-9f00-0000 mask ffff-ff00-0000  (autoriser le constructeur à faire du voice vlan, ici ALCATEL)
#
interface GigabitEthernet1/0/2
port link-mode bridge
description SERVICE MEDICAL+TEL
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 3 30
 port trunk pvid vlan 3                          | Force le vlan par défaut à 4 (vlan DATA)
 undo voice-vlan mode auto                       | Force le boot du tel sur le vlan 30
 voice-vlan 30 enable                            | Force le boot du tel sur le vlan 30
 broadcast-suppression 20                        | limitation à 20% maxi du trafic multicast sur le port
 multicast-suppression 20                        | limitation à 20% maxi du trafic multicast sur le port
 stp edged-port
 stp port bpdu-protection enable
 poe enable
 loopback-detection enable vlan 1 to 4099        | action détection des boucles
 loopback-detection action shutdown              | action détection des boucles
```

2.12.10 Equipement e-GFA

- Port access
- Vlan 224

```
interface gi1/0/X
port link-mode bridge
description e-GFA
stp enable                                       | n'apparait pas en display current-configuration
stp edged-port
port link-type access                            | n'apparait pas en display current-configuration
port access vlan 224
speed 100                                        | préconisé – vérifiez avec « dis counters [inbound] [outbound] interface
duplex full                                      | préconisé – vérifiez avec « dis counters [inbound] [outbound] interface
loopback-detection enable vlan 1 to 4094         | détection des boucles
loopback-detection action shutdown               | action détection des boucles
multicast-suppression 20                         | limitation à 20% maxi du trafic multicast sur le port
broadcast-suppression 20                         | limitation à 20% maxi du trafic broadcast sur le port
```

2.12.11 Imprimante

- Port access
- Vlan 226

```
interface gi1/0/X
 port link-mode bridge
 description IMPRIMANTE-XX
 stp enable                                  | n'apparait pas en display current-configuration
 stp edged-port
 port link-type access                       | n'apparait pas en display current-configuration
 port access vlan 226
 loopback-detection enable vlan 1 to 4094    | détection des boucles
 loopback-detection action shutdown          | action détection des boucles
 multicast-suppression 20                    | limitation à 20% maxi du trafic multicast sur le port
 broadcast-suppression 20                    | limitation à 20% maxi du trafic broadcast sur le port
```

2.12.12 Imprimante SERVICE MEDICAL

- Port access
- Vlan 227

```
interface gi1/0/X
 port link-mode bridge
 description IMPRIMANTE-MEDICAL
 stp enable                                  | n'apparait pas en display current-configuration
 stp edged-port
 port link-type access                       | n'apparait pas en display current-configuration
 port access vlan 227
 loopback-detection enable vlan 1 to 4094    | détection des boucles
 loopback-detection action shutdown          | action détection des boucles
 multicast-suppression 20                    | limitation à 20% maxi du trafic multicast sur le port
 broadcast-suppression 20                    | limitation à 20% maxi du trafic broadcast sur le port
```

2.12.13 Serveur Virtuel (VMWARE) mono ou multi-Vlan

Nous préconisons l'interconnexion des serveurs virtuels VMWARE avec les switches HP **via des agrégats.**
Attention, dans ce cas, ne pas utiliser les commandes suivantes:

- Mad enable (Par défaut la commande n'est pas appliquée)
- Link-aggregation mode dynamique. (Par défaut la commande n'est pas appliquée)

La procédure est disponible sur le **portail réseaux et Télécom du CNGR / rubrique LAN**.

```
interface Bridge-Aggregation10
description Esx-xxxx-10
port link-type trunk
undo port trunk permit vlan 1
port trunk permit vlan 4 16 30
dhcp snooping trust
#
interface GigabitEthernet1/0/21
description Esx-xxxx-10-Eth1
port link-type trunk
undo port trunk permit vlan 1
port trunk permit vlan 4 16 30
stp edged-port
broadcast-suppression 20          | limitation à 20% maxi du trafic multicast sur le port
multicast-suppression 20          | limitation à 20% maxi du trafic multicast sur le port
port link-aggregation group 10
```

```
#
interface GigabitEthernet2/0/21
description Esx-xxxx-10-Eth2
port link-type trunk
undo port trunk permit vlan 1
port trunk permit vlan 4 16 30
stp edged-port
broadcast-suppression 20          | limitation à 20% maxi du trafic multicast sur le port
multicast-suppression 20          | limitation à 20% maxi du trafic multicast sur le port
port link-aggregation group 10
#
interface GigabitEthernet3/0/1
description CONSOLE-SERVEUR
stp enable                        | cette commande n'apparaît pas en « display current-configuration »
stp edged-port
port link-type access             | cette commande n'apparaît pas en « display current-configuration »
port access vlan 216
```

2.12.14 Borne wifi

```
interface gi1/0/X
 description normalisée           | obligatoire : voir les référentiels
 stp enable                       | n'apparait pas en display current-configuration
 stp edged-port
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 50 54 901 902   | voir doc wifi (028NT001)
```

2.12.15 Contrôleur wifi

```
interface Bridge-AggregationX     | X = Id de l'interface Bridge-Aggregation
 description normalisée           | obligatoire : voir les référentiels
 port link-type trunk
 stp enable                       | n'apparait pas en display current-configuration
 undo port trunk permit vlan 1
 port trunk permit vlan 50 54 902
 port trunk pvid vlan 902
 link-aggregation mode dynamic
 dhcp snooping trust

interface Ethernet1/0/X
 description normalisée           | obligatoire : voir les référentiels
 description Contrôleur wifi
 stp enable                       | n'apparait pas en display current-configuration
 stp edged-port
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 50 54 902
 port trunk pvid vlan 902         | voir doc wifi (028NT001)
 port link-aggregation group X

interface Ethernet1/0/X
 description normalisée           | obligatoire : voir les référentiels
 description Contrôleur wifi
 stp enable                       | n'apparait pas en display current-configuration
 stp edged-port
 port link-type trunk
 undo port trunk permit vlan 1
```

port trunk permit vlan 50 54 902
port trunk pvid vlan 902 | voir doc wifi (028NT001)
port link-aggregation group X

2.12.16 Boitier pour portail captif wifi

(exemple « Ucopia »)

Il y a une interface à connecter sur le LAN :

interface GigabitEthernet1/0/X
description UCOPIA-IN
undo port trunk permit vlan 1
port trunk permit vlan 54 900 | Vlan 54 - voir doc wifi (409NT058)
port trunk pvid vlan 900 | Vlan 900 - voir doc wifi (409NT058)
loopback-detection enable vlan all
loopback-detection action shutdown
broadcast-suppression 20
multicast-suppression 20
dhcp snooping trust
stp enable | n'apparait pas en display current-configuration
stp edged-port

2.12.17 IPBX (hors Cetiam)

interface GigabitEthernet1/0/11
description IPBX-CONSTRUCTEUR
port link-mode bridge
port access vlan 30
undo voice vlan mode auto
[speed 100 ou 1000] | A adapter en fonction de l'IPBX et des observations
[duplex full] | A adapter en fonction de l'IPBX et des observations
loopback-detection enable vlan all
loopback-detection action shutdown
broadcast-suppression 20
multicast-suppression 20
stp edged-port

2.12.18 Passerelle « Audiocodes » (hors Cetiam)

interface GigabitEthernet1/0/11
description AUDIOCODE1 (ou 2 …)
port link-mode bridge
port access vlan 30
undo voice vlan mode auto
speed 100
duplex full
loopback-detection enable vlan all
loopback-detection action shutdown
broadcast-suppression 20
multicast-suppression 20
stp edged-port

2.12.19 Passerelle « CETIAM »

Les passerelles (ou Gateway) CETIAM sont à connecter dans le vlan 230 en 58.X.230.Y /29 (255.255.255.248) **SUR LE FEDERATEUR AUTANT QUE POSSIBLE**. Voir les référentiels LAN et les documentations de la téléphonie. Le plan d'adressage de vos passerelles (si besoin) vous sera communiqué dans le cadre du projet CETIAM. Exemples :

VLAN 230 - NOM "GW-CETIAM"									
Organisme	Site	Sous-réseau	Masque	Interface vlan 230	Passerelle1	Passerelle2	Passerelle3	Passerelle4	Passerelle5
PROTOTYPE	CPAM 901	58.230.0.0	255.255.255.248	58.230.0.1	58.230.0.2	58.230.0.3	58.230.0.4	58.230.0.5	58.230.0.6
PROTOTYPE	CP 901	58.230.0.8	255.255.255.248	58.230.0.9	58.230.0.10	58.230.0.11	58.230.0.12	58.230.0.13	58.230.0.14
PROTOTYPE	CP 902	58.230.0.16	255.255.255.248	58.230.0.17	58.230.0.18	58.230.0.19	58.230.0.20	58.230.0.21	58.230.0.22
CPAM Alpes-de-Haute-Provence	SIEGE DIGNE	58.230.0.24	255.255.255.248	58.230.0.25	58.230.0.26	58.230.0.27	58.230.0.28	58.230.0.29	58.230.0.30
CPAM Alpes-de-Haute-Provence	Manosque	58.230.0.32	255.255.255.248	58.230.0.33	58.230.0.34	58.230.0.35	58.230.0.36	58.230.0.37	58.230.0.38
CPAM Alpes-de-Haute-Provence	...etc.	58.230.0.40	255.255.255.248	58.230.0.41	58.230.0.42	58.230.0.43	58.230.0.44	58.230.0.45	58.230.0.46

La passerelle sera pré-configurée par l'intégrateur avec l'une des adresses IP du vlan 230 réservé au site.

1°/ Dans le fédérateur N3 : création du vlan 230 avec son nom

system-view
#
vlan 230
name VLAN-GW-CETIAM
#
interface vlan 230
des INT-VLAN-GW-CETIAM
ip address 58.230.0.X 255.255.255.248
#

2°/ Interface sur le switch de connexion de chaque passerelle

system-view
#
interface x/0/y (exemple Gi1/0/10)
description GWX-CETIAM (exemple GW1-CETIAM)
port link-mode bridge
port link-type access
port access vlan 230
loopback-detection enable
loopback-detection action shutdown
broadcast-suppression 20
multicast-suppression 20
#
Save force

2.12.20 Interconnexion des switches

Les HP 5510 et HP 5520 servent principalement à l'interconnexion des switches d'extrémité, l'ensemble des interfaces vont être utilisées à cet effet (avec éventuellement quelques serveurs). Il va donc falloir configurer des trunks en veillant à ne permettre (« permit vlan x y … ») que les VLAN nécessaires, sans oublier le vlan 901 d'administration. Cas classiques :

- Entre 55X0 HI et 3600 : VLAN 4, 30 ,901 et 902
- Entre 55X0 HI et 51X0 : VLAN 4 901 et 902

Dans les architectures « Full HP » normalisées des sièges d'Organismes (cf Référentiels), les interconnexions des 5510 ou 5520 et des 3600 ou 5130 ou 5140 est à faire via des liens agrégés. La suite donne la configuration des trunks d'interconnexion AVEC ou SANS agrégation (si besoin).



Pas de « stp edged-port» sur les trunks d'interconnexion de switches !!!!!!

2.12.21 Règles de nommage

Description des agrégats ou de liens trunks simples

Le nommage des agrégats et des trunk est normalisé :

[]description [Type]-[Num]-[Niv]-[MOD]-*[DESCRIPTION]*

[type] = type de lien sur 3 digits (AGG; LIEN; ...)
[num] = numéro de l'agrégat (Num = 10, 20, 30,… (Suggestion 10 : 1er étage, 20 : 2ème étage...)
[niv] = vers un Niveau du switch (N2, N3)
[mod] = modèle de switch (3600)
[description] = optionnel ➔ répartiteur ou baie ou étage ou @IP du switch distant

Veuillez consulter les référentiels pour les détails. Le nommage se fait via la commande « description » sur l'interface « Bridge-Aggregation ».

Exemples :

Interface Bridge-Aggregation10
description AGG-010-N2-5130-ETAGE1 | Agrégat n° 10 vers niveau2 de type HP 5130 du 1er ETAGE

Interface Bridge-Aggregation11
description AGG-011-N2-5510-RG | Agrégat n° 11 vers niveau 3 de type HP 5510 du Répartiteur Général

Autres possibilités :
AGG-010-N2-5130-SW-020 | Agrégat numéro 10 vers niveau2 de type HP 5130 d'@ip 55.xx.221.20
LIEN-010-N2-5130-ETAGE | Lien simple numéro 10 vers niveau2 de type HP 5130 du 1er ETAGE

Lien trunk placé dans un agrégat :

[]description [Type]-[Num]-[Niv]-[MOD]-*[DESCRIPTION]*-[LIEN n°]

Exemples :

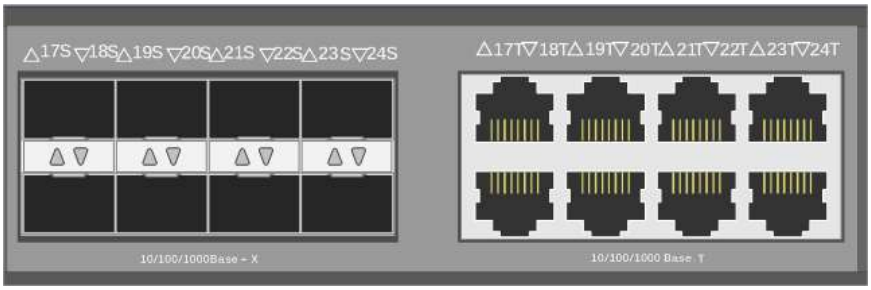
Interface TenGigabitEthernet1/0/25
description AGG-010-N2-5130-ETAGE1-LIEN1 | description du 1er lien de l'agrégat 10

Interface TenGigabitEthernet1/0/25
description AGG-010-N2-5130-ETAGE1-LIEN2 | description du 2ème lien de l'agrégat 10

2.12.22 Utilisation des ports « combo »

Les switches **HP 5510_HI-24G-SFP-4SFP et HP 5130-24G-SFP**-4SFP disposent de 8 ports (ou interfaces) gigabits « combo » **de 17 à 24**; ils sont entourés de gris clair : les ports « cuivre » **sont actifs par défaut** et sont couplés avec un port « SFP ».

HP 5510_HI-24G-SFP-4SFP & HP 5130-24G-SFP-4SFP EI :



Par exemple: si le port 17S «SFP» est utilisé, le port «cuivre» 17T ne peut pas être utilisé en même temps et VIS-VERSA.

Pour activer le port fibre de l'interface 17Sd'un HP 5xx0-24G-SFP :

```
<>system-view
#
interface GigabitEthernet X/0/17          | X dépend de la position du 5120 dans le stack
 combo enable fiber                       | l'interface physique X/0/17S  passe active
```

Pour activer le port cuivre de l'interface 17T d'un HP 5xx0-24G-SFP :

```
<>system-view
#
interface GigabitEthernet X/0/17          | X dépend de la position du 5120 dans le stack
 combo enable copper                      | l'interface physique X/0/17T passe active
```

2.12.23 Interconnexion de switches AVEC AGREGATION

2.12.23.1 Présentation

A quoi ça sert ?

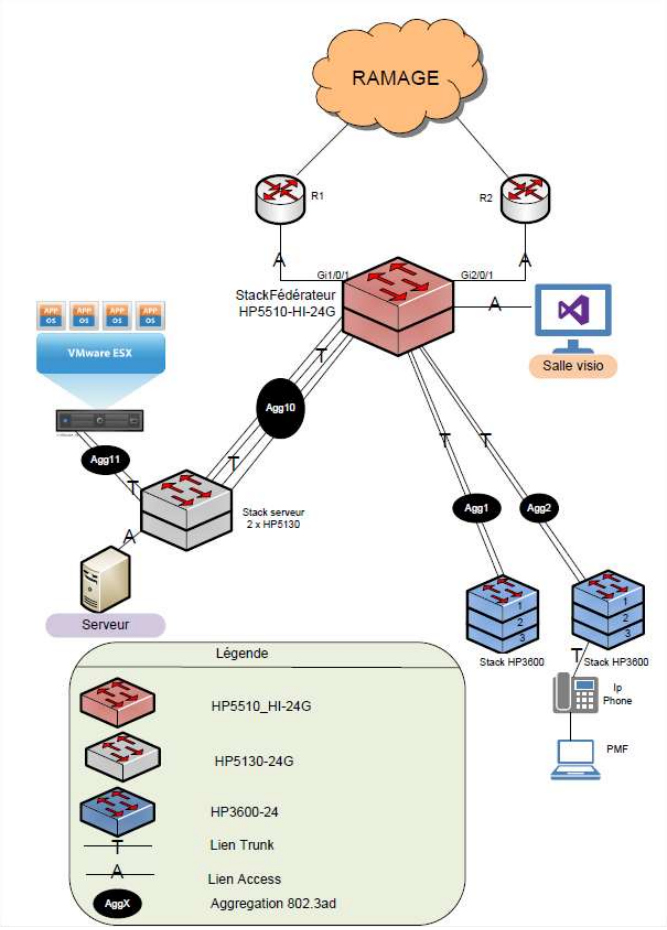
Un agrégat est une association de liens entre deux switches. Lorsque les deux switches sont proches (même baie ou même répartiteur) ou que le pré câblage d'immeuble met plusieurs rocades (cuivre ou fibre) à disposition, il est intéressant de multiplier les liens entre les switches. Ainsi, au lieu de monter une interconnexion de switches à 1 Gb/s, on monte par exemple deux liens à 1 Gb/s (et non un lien à 2 Gb/s). Le trafic est réparti automatiquement par les switches sur les « n » liens. Cette technologie est standardisée (IEEE 802.3ad). Si le nombre d'interfaces disponibles et le pré câblage le permettent, il est possible d'ajouter … jusqu'à 8 interfaces. Il est conseillé d'agréger les liens par paire (2, 4, 6 ou 8 et pas 3, 5 ou 7).

Du coup, comme expliqué dans les Référentiels LAN, il faut configurer des agrégats au niveau de toutes les interconnexions de switches HP (si le pré câblage le permet).

ATTENTION : il s'agit des agrégats inter-switches – PAS les agrégats Serveurs VMWare ➔ switches.

2.12.23.2 Architectures

ARCHITECTURES NORMALISEES :
Cas d'un siège d'organisme : interconnexion du stack 5510 avec des stacks 3600 et 5130 en agrégation :



Les stacks de 3600 et de 5130 doivent être interconnectés au stack fédérateur de 5510 via un agrégat à 2Gb/s ou 4Gb/s.

Interface à utiliser :

Pour les 3600 ➔ interfaces 25T ou 25S :

GigabitEthernet1/0/25 (Membre1 du stack)
GigabitEthernetX/0/25 (dernier Membre (X) du stack)

Pour les 5510:
Utiliser une interface sur chaque membre du stack de **manière symétrique (même numéro)**, cuivre ou fibre selon le type de pré câblage.

interface GigabitEthernet1/0/x (Membre 1 du stack)
interface GigabitEthernet2/0/x (Membre 2 du stack)

2.12.23.3 Configuration des agrégats inter-switch

Méthode :

Il est indispensable de renseigner strictement les mêmes paramètres au niveau de l'interface « Bridge-Aggregation » et au niveau des interfaces agrégées. Pour cela, la méthode suivante facilite la configuration :

1°/ Créer l'interface « Bridge-Aggregation »
2°/ Attacher les 2 ou N interfaces à agréger à l'interface « Bridge-Aggregation »
3°/ Configurer les autres paramètres sur l'interface « Bridge-Aggregation » :
Ils seront automatiquement reportés sur les interfaces attachées.

Attention, pour les trunks :

1/ Il ne faut pas oublier le *VLAN 901 d'Admin-Réseau.*
2/ **Pas de** « stp edged-port enable » !

Exemple en siège d'organisme avec les vlan 4 Data et 30 Voix, 902 Admin-wifi sans oublier le VLAN 901 d'ADMIN-RESEAU – Cas d'un agrégat entre un stack de 2 HP 5130, un stack de « n » HP 3600:

Deux nouvelles commandes associées aux liens inter switch :

- Description **AGG-010**-N2-5130-ETAGE1
- made enable | Optimise le fonctionnement inter IRF
- Link-aggregation mode dynamique | Activation du lacp en mode dynamique

***si la description contient AGG-010 : le lien sera automatiquement supervisé dans CENTREON**

2.12.23.4 Exemple de configuration

Côté fédérateur 5510 :

```
<>system-view
#
interface Bridge-Aggregation 1                  | N° de l'agrégat
 description AGG-010-N2-5130- ETAGE1            | description de l'agrégat vers le switch distant
 link-aggregation mode dynamic                  | Activation du protocole LACP
#
interface GigabitEthernet1/0/5                  | Par exemple Gi1/0/5
 description AGG-010-N2-5130-ETAGE1-LIEN1       | description du 1er lien de l'agregat
 port link-aggregation group 1
 broadcast-suppression 20
 multicast-suppression 20
#
Interface GigabitEthernet2/0/5                  | Par exemple Gi2/0/5
 description AGG-010-N2-5130-ETAGE1-LIEN2       | description du 2éme lien de l'agrégat
 port link-aggregation group 1
 broadcast-suppression 20
 multicast-suppression 20
#
interface Bridge-Aggregation 1                  | N° de l'agrégat ci-dessus
 stp enable
 port link-type trunk
 port trunk permit vlan 4 30 901 902
 undo port trunk permit vlan 1
 link-aggregation mode dynamic
 mad enable          | ATTENTION : avant de taper « MAD ENABLE », il faut être sûr d'avoir renseigné un n° d'IRF-DOMAIN !!!
 stp root-protection |Evite attaques et dysfonctionnements
```

Côté niveau 2 HP 5130 :

```
<>system-view
#
interface Bridge-Aggregation 1                  | N° de l'agrégat
 description AGG-010-N3-5510-ETAGE1             | description de l'agrégat
 link-aggregation mode dynamic
#
interface GigabitEthernet1/0/25                 | interface normalisée 1er élément du stack
 description AGG-010-N3-5510-ETAGE1-Lien1       | description du 1er lien de l'agrégat
 port link-aggregation group 1
 broadcast-suppression 20
 multicast-suppression 20
#
Interface GigabitEthernetn/0/25                 | interface normalisée n dernier élément du stack
 description AGG-010-N3-5510-ETAGE1-LienN       | description du nème lien l'agrégat
 port link-aggregation group 1
 broadcast-suppression 20
 multicast-suppression 20
#
interface Bridge-Aggregation 1                  | N° de l'agrégat ci-dessus
 description AGG-010-N3-5510-ETAGE1             | description du nème lien l'agrégat
 stp enable
 port link-type trunk
 port trunk permit vlan 4 30 901 902
 link-aggregation mode dynamic
 undo port trunk permit vlan 1
 mad enable                  | ATTENTION: avant de taper « MAD ENABLE », il faut être sûr d'avoir renseigné un numéro d'IRF-DOMAIN !!!
 stp loop-protection         | Evite attaques et dysfonctionnements ➔ voir $ 5.4
```

Contrôle:

```
[SIEGE-N3-HP 5510-xxxxx]interface Bridge-Aggregation 1
[SIEGE-N3-HP 5510-xxxxx-Bridge-Aggregation1]dis this
#
interface Bridge-Aggregation1
 description AGG-010-N2-5130- ETAGE1
 port link-type trunk
 port trunk permit vlan 4 30 901 902
 link-aggregation mode dynamic
 stp root-protection
 mad enable
```

2.12.23.5 Ajout d'une interface dans un agrégat existant

Sur la base de l'agrégat configuré ci-dessus (côté 5510). Il est conseillé de faire des agrégats avec un nombre paire d'interfaces de chaque côté.

1/ Mettre l'interface en configuration usine si besoin :

```
<>system-view
#
interface GigabitEthernet1/0/6                  | par exemple
 default
```

2/ Ajouter l'interface dans l'agrégat

```
interface GigabitEthernet1/0/6                | par exemple
description AGG-010-N3-5510-ETAGE1-LienN      | description du nème lien l'agrégat
 port link-aggregation group 1                | N° de l'agrégat
 broadcast-suppression 20
 multicast-suppression 20
```

3/ Renvoyer la configuration complète de l'interface bridge-aggrégation (copié – collé)

```
interface Bridge-Aggregation 1                | N° de l'agrégat de l'exemple
 stp enable
 port link-type trunk
 port trunk permit vlan 4 30 901 902
 undo port trunk permit vlan 1
 link-aggregation mode dynamic
 mad enable                                   | Optimise les dialogues inter-stacks - au prompt, le domain IRF est proposé – vérifier que c'est le bon et valider (sinon CTRL C)
 [stp loop-protection]                        | Côté switch N2 ➔ voir $ 5.4
 [stp roop-protection]                        | Côté switch N3➔ voir $ 5.4
```

2.12.23.6 Contrôle des agrégats

Une fois la configuration effectuée, il faut connecter les interfaces avec les câbles adéquats. La commande suivante permet alors de vérifier le fonctionnement.

<>Display link-aggregation verbose

Exemple pour un agrégat de 2 ports sur un stack de 5510 :

```
<>dis link-aggregation verbose
Loadsharing Type: Shar -- Loadsharing, NonS -- Non-Loadsharing
Port Status: S -- Selected, U -- Unselected
Flags:  A -- LACP_Activity, B -- LACP_Timeout, C -- Aggregation,
        D -- Synchronization, E -- Collecting, F -- Distributing,
        G -- Defaulted, H -- Expiresd

Aggregation Interface: Bridge-Aggregation1
Aggregation Mode: Dynamic
Loadsharing Type: Shar
System ID: 0x8000, 3822-d609-8306
Local:
  Port             Status  Priority Oper-Key  Flag
--------------------------------------------------------------------------------
  GE1/0/1          S       32768    1         {ACDEF}
  GE1/0/2          S       32768    1         {ACDEF}
Remote:
  Actor            Partner Priority Oper-Key  SystemID               Flag
--------------------------------------------------------------------------------
  GE1/0/1          26      32768    1         0x8000, 3822-d610-f396 {ACDEF}
  GE1/0/2          27      32768    1         0x8000, 3822-d610-f396 {ACDEF}
```

Vérifiez que les "flags" soient bien tous a "ACDEF".

Autre commande :

<>Display link-aggregation summary

```
<5500>dis link-aggregation summary
Aggregation Interface Type:
BAGG -- Bridge-Aggregation, RAGG -- Route-Aggregation
Aggregation Mode: S -- Static, D -- Dynamic
Loadsharing Type: Shar -- Loadsharing, NonS -- Non-Loadsharing
Actor System ID: 0x8000, 7848-59a2-9a58

AGG          AGG       Partner ID              Select Unselect   Share
Interface    Mode                              Ports  Ports      Type
--------------------------------------------------------------------------------
BAGG1        D         0x8000, 7848-59a8-714c  2      0          Shar
BAGG2        D         0x8000, 7848-5997-a9cc  2      0          Shar
BAGG3        D         0x8000, bcea-fa3b-2efe  2      0          Shar
BAGG4        D         0x8000, 7848-5997-b044  2      0          Shar
BAGG5        D         0x8000, 7848-5997-ac54  2      0          Shar
BAGG6        D         0x8000, bcea-fa3b-3216  2      0          Shar
BAGG7        D         0x8000, d07e-28f3-7060  2      0          Shar
BAGG8        D         0x8000, 7848-5981-8b12  2      0          Shar
BAGG9        D         0x8000, 7848-5997-b284  2      0          Shar
BAGG10       D         0x8000, bcea-fa3b-1c6e  2      0          Shar
BAGG11       D         0x8000, 7848-5997-a93c  2      0          Shar
BAGG12       D         0x8000, 7848-5997-ab34  2      0          Shar
BAGG13       D         0x8000, bcea-fa3b-2eb6  1      1          Shar
BAGG14       D         0x8000, 7848-5953-6c98  2      0          Shar
<5500>
```

⇨ **Vérifier que le mode est bien « D » (Dynamique) pour les agrégats d'interconnexion de switches** ***(les agrégats vers des serveurs ESX doivent être en « S » (statique) ➔ voir doc plus haut.)***

2.12.24 Interconnexion de switches SANS AGREGATION

Si l'architecture du bâtiment ne permet pas de faire d'agrégation, vous devez créer un lien trunk simple.

Exemple: Lien dans un organisme entre un switch N3 et un stack N2 à l'étage 1.
(trunk qui dessert des IP-Phones dans le VLAN 30, des PMF dans les VLAN 4, du WIFI dans le VLAN wifi 902, l'administration réseau dans le VLAN 901)

Côté Fédérateur :

```
<>system-view
#
interface GigabitEthernet1/0/X
 description LIEN-010-N2-5130- ETAGE1          | description du lien vers le switch distant
 stp enable                                    | cette commande n'apparaît pas en « display current-configuration »
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 4 30 901 902
 stp root-protection                           | Evite attaques et dysfonctionnements ➔ voir $ 5.3
 broadcast-suppression 20
 multicast-suppression 20
```

Côté switch niveau 2 :

```
<>system-view
#
interface GigabitEthernet1/0/25               | Interface normalisée
 description LIEN-010-N3-5510- ETAGE1          | description du lien vers le switch distant
 stp enable                                    | cette commande n'apparaît pas en « display current-configuration »
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 4 30 901 902
 stp loop-protection                           | Evite attaques et dysfonctionnements ➔ voir $ 5.3
 broadcast-suppression 20
 multicast-suppression 20
```

Attention, pour les trunks :

Il ne faut pas oublier le *VLAN 901 d'Admin-Réseau.*
Pas de « stp edged-port enable » !

2.13 CONFIGURATION DU DHCP

DHCP peut être utilisé au niveau des réseaux locaux pour distribuer les adresses IP automatiquement vers les clients (PMF et téléphones). Veuillez suivre les recommandations de la procédure CNGR NA-072-001 :

Préconisations DHCP
La procédure est disponible sur le **portail réseaux et Télécom du CNGR / rubrique Produits ➔ DHCP**.

Préconisation Cnam : le serveur DHCP pour les téléphones et les PMF est le contrôleur Windows (local (serveur de proximité en CP) ou distant (celui du siège)).

2.13.1 DHCP RELAIS



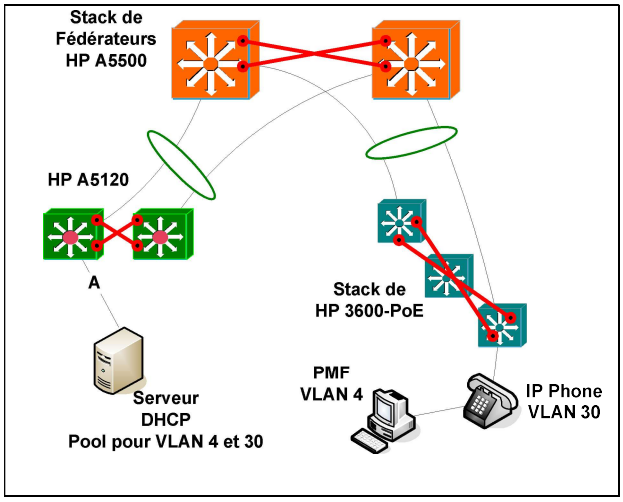
A quoi ça sert ?

Au démarrage (et ensuite périodiquement) les clients (PMF ou téléphones) émettent un broadcast (requête émise vers toutes les adresses d'un (sous-)réseau) pour trouver le serveur DHCP. Les broadcasts sont des trames qui ne sont pas transmises en dehors du (sous-)réseau d'où il est émis : ils ne traversent pas les routeurs et ne sont pas propagés non plus vers les autres VLAN. Pourtant, on peut avoir des clients dans des VLAN différents (cas des PMF et des téléphones) mais un seul serveur DHCP positionné dans un le VLAN 4. Les clients se trouvant dans le même VLAN vont le trouver grâce au broadcast mais ceux des autres VLAN devront trouver un relais vers le serveur DHCP.

IL FAUT DONC UN RELAIS POUR TOUTES LES INTERFACES VLAN CLIENTES du DHCP Y COMPRIS POUR LE WIFI (VLAN 50).

En siège d'organisme, ce sont les switches fédérateurs niveau 3 qui gèrent les interfaces VLAN. La configuration suivante est donc à mettre en œuvre sur le stack de niveau 3 seulement.

Le serveur DHCP est sur l'interface 1/0/X du stack 5120 dans le VLAN 4, il faut donc mettre en place le relais pour le VLAN 30 :



La configuration se fait au niveau de l'interface VLAN :

```
<>system-view
#
dhcp enable
#
interface Vlan-interface30
 description INT-VLAN-VOIX
 ip address 58.X.226.1 24
 dhcp select relay
 dhcp relay server-address 55.x.x.x                    | Adresse IP du serveur DHCP
```

Ne pas configurer le DHCP-Relais sur l'interface-VLAN du VLAN dans lequel se trouve le serveur dhcp :
1/ c'est inutile
2/ cela peut générer des problèmes techniques

2.13.2 DHCP SNOOPING

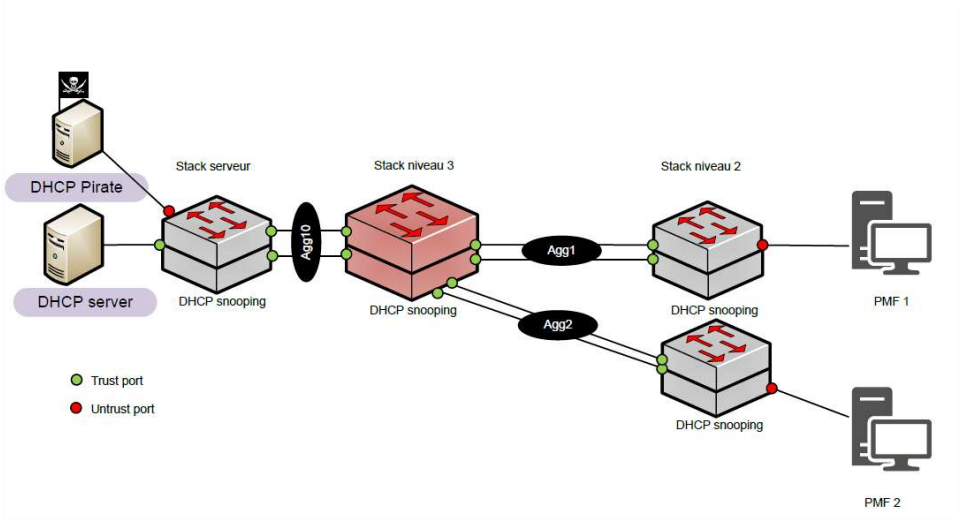
A quoi ça sert ?

DHCP-Snooping est utilisé pour éviter la mise en œuvre d'un serveur DHCP pirate en sécurisant la fonction DHCP sur un réseau. Veuillez consulter la procédure 072NA001_Preconisations_DHCP sur l'intranet du CNGR pour plus d'explications.

Les commandes ci-dessous sont donc à configurer sur tous les switches du réseau utilisant un serveur DHCP, 2 cas se présentent:

- **Serveur DHCP local (avec ou sans secours distant): appliquer les points 1,2 et 3.**
- **Serveur DHCP distant (pas de serveur local): appliquer les points 2 et 3.**

Attention respecter l'ordre ci-dessous (❶ Serveur DHCP, ❷ Trunks, ❸ Global)



DHCP-snooping : Schéma de principe

1/ Interface « Access » sur laquelle est connecté le serveur DHCP (si présent localement) :
Exemple sur un stack de HP 5130:

```
<>system-view
#
interface GigabitEthernet1/0/6
 port link-mode bridge
 description Serveur DHCP
 port access vlan 4
 stp enable                                  | n'apparait pas en display current-configuration
 stp edged-port enable
 dhcp snooping trust
```

2/ Toutes les interfaces par lesquels la réponse du serveur DHCP doit arriver :

- Toutes les interfaces « Trunk » d'interconnexion de switches
- Toutes les interfaces « bridge-aggregation »
- **Pas** sur les autres trunks !

Exemples sur un 5510 :

```
<>system-view
#
int GigabitEthernet 1/0/9
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 4 30 901 902
 dhcp snooping trust
```

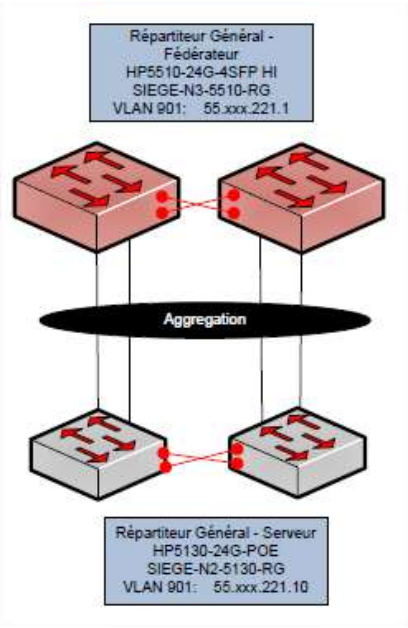
Agrégats :

```
<>system-view
#
interface Bridge-Aggregation1
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 4 30 901 902
 link-aggregation mode dynamic
 dhcp snooping trust
```

3/ En Global sur tous les switches :

```
<>system-view
#
Dhcp snooping enable
 DHCP Snooping is enabled.
```

2.13.3 Routage dans les HP 5130 et 5140 niveau 2 d'extrémité



Ces switches sont connectés en niveau 2. Mais il est nécessaire d'entrer une route pour assurer la communication entre les HP 5130 et les fédérateurs HP 5510 HI.

<>system-view
#
ip route-static 0.0.0.0 0.0.0.0 *@IP-Interface-vlan-Admin-Reseau-switch-fédérateur*

où :

@IP-Interface-vlan-Admin-Reseau-switch-fédérateur est l'adresse IP de l'interface VLAN 901 sur le stack fédérateur.

2.14 AUTRES CONFIGURATIONS

2.14.1 LLDP : découverte



LLDP (Lync Layer Discovery Protocol) est le protocole standard de communication entre les switches et les hosts qui implémentent ce protocole (téléphones IP par exemple). Il permet la découverte d'informations sur les équipements connectés sur les interfaces Ethernet. Cisco a développé son propre protocole : CDP.

L'activation de LLDP permettra de visualiser de nombreuses informations sur les switches et serveurs connectés sur les interfaces du 5XXX :

<>system-view
#
lldp global enable

Exemple de commandes de visualisation : <>dis lldp neighbor-information …

2.14.2 NTP: Tous à la même heure

Une seule adresse IP de référence : 55.223.10.8. Voir la nouvelle version des procédures 027NA001 et 027NT002 sur l'intranet du CNGR.

ATTENTION :
il se peut que l'implémentation de la version 3 de NTP soit nécessaire sur certains serveurs Linux :

➔ **mettre :** *server @ip-serveur-NTP version 3* **dans** */etc/ntp.conf*
➔ **relancer le process NTP :** */usr/sbin/ntpd –c /usr/ntp.conf*

Configuration sur tous les switches avec changement automatique heure d'été / heure d'hiver :

➔ **Préciser la source NTP pour les swiths Comware V7**

```
<>system-view
#
clock timezone PARIS add 01:00:00
clock summer-time PARIS 02:00:00 03/27 03:00:00 10/30 01:00:00
#
ntp-service enable
ntp-service unicast-server 55.223.10.8                | adresse unique pour tous
ntp-service source Vlan-interface 901                 | si site avec une interface vlan 901
ou
ntp-service source Loopback1                          | si site avec une interface Loopback1
```

Vérification du bon fonctionnement :

<>display ntp status

```
Clock status: synchronized
Clock stratum: 3
Reference clock ID: 55.223.10.8
Nominal frequency: 100.0000 Hz
Actual frequency: 100.0000 Hz
Clock precision: 2^17
Clock offset: 0.0000 ms
Root delay: 10.64 ms
Root dispersion: 0.27 ms
Peer dispersion: 3.23 ms
Reference time: 09:16:02.999 UTC Apr 5 2013(D50914D2.FFE30878)
```

2.14.3 Wake On LAN : réveil des PMF à distance



A quoi ça sert ?

Les paquets WoL sont envoyés sous forme de broadcast à travers le réseau pour allumer les PC à distance. Pour que les équipements de niveau 3 laissent passer ce broadcast (nativement bloqué), il est nécessaire de le préciser dans la configuration. Une ACL permet en outre de limiter ce type de flux à la seule initiative du module PULSE des serveurs GEDIFF. La configuration est à appliquer sur les interfaces VLAN des PMF dans le dernier switch N3 traversé (vlan 4, 3 18 …).

Les serveurs GEDIFF sont centralisés au CSH-GE.

UNE ACL (3002) est à configurer pour n'autoriser que GEDIFF à traiter le WOL.



Le WOL est à configurer sur les fédérateurs,
pas sur les switches d'extrémité.

➔ pas de commande en global

Configuration sur les fédérateurs :

```
<>system-view
#
acl number 3002 name GEDIFF
 rule 1 permit udp source 55.245.4.0 0.0.3.255
#
```

N° d'ACL normalisé

GDIFF centralisé en CSH

Application sur l'interface VLAN 4 (par exemple) :

```
Interface Vlan-interface4
 ip forward-broadcast acl 3002
```

2.14.4 QoS pour la voix et la videoconference

Ce paragraphe explique la configuration des commutateurs HP permettant d'appliquer une QoS (Qualité de Service) minimum sur les LAN des Organismes (hors CSH) qui le nécessiteraient. Elle permet le traitement prioritaire des flux **voix** (Téléphonie sur IP) **et vidéo** (visioconférence sur PMF) par les switches en cas de congestion.

L'application de cette QoS n'est pas obligatoire mais elle doit être appliquée lorsque des lenteurs sont observées avant d'ouvrir un ticket d'incident.

Ces blocs de configuration sont à appliquer sur tous les switches du LAN :

En global sur les switches HP N2 et N3 :

```
System-view
#
qos map-table dscp-dot1p
 import 38 export 5
 import 46 export 6
```

Sur les interfaces :

- **interfaces trunks d'interconnexion de switches (commande non acceptée sur agrégats),**
- **interfaces de connexion des routeurs Ramage,**
- **des éventuels serveurs de téléphonie locaux (IPBX),**
- **interfaces de connexion des téléphones et/ou PMF.**

Exemples avec Gi1/0/10 et Gi1/0/25 :

```
System-view
#
Interface Gi1/0/10
 Qos trust dscp
#
Interface Gi1/0/25
 Qos trust dscp
```

La QoS est appliquée même s'il n'y a pas de congestion sur une interface. Les traces suivantes ont cependant été réalisées en passant un appel téléphonique pendant qu'un flux saturant (FTP) était envoyé (avec un générateur de trafic) vers le PMF connecté derrière le téléphone. Cela afin de montrer que les paquets supprimés (droppés) sont ceux des classes de priorité moindre.

Pour visualiser les résultats nous utilisons la commande **« display qos queue-statistics … ».**

2.15 L'EXPLOITATION

2.15.1 Ping

➔ **Préciser la source du ping pour les swiths Comware V7**

[011-sw-cp-ain-001-n3-5510-baie4]ping -a 55.xx.221.1 ns.cnamts.fr **|préciser l'adresse source source**
Ping ns.cnamts.fr (55.223.10.1) from 55.40.221.1: 56 data bytes, press CTRL+C to break
56 bytes from 55.223.10.1: icmp_seq=0 ttl=251 time=14.456 ms
56 bytes from 55.223.10.1: icmp_seq=1 ttl=251 time=46.407 ms

2.15.2 Mirroring d'interface

Exemple : mirroring du port 2/0/14 sur 1/0/6 (même stack) :

```
<>system-view
#
mirroring-group 1 local
mirroring-group 1 mirroring-port GigabitEthernet 2/0/14 both
mirroring-group 1 monitor-port GigabitEthernet 1/0/6
```

Résultat (display current) :

```
mirroring-group 1 local
#
interface GigabitEthernet1/0/6
 port link-mode bridge
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 6 30 901
 mirroring-group 1 monitor-port
#
interface GigabitEthernet2/0/14
 port link-mode bridge
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 6 30 901
 mirroring-group 1 mirroring-port both                    | ou inbound ou outbound
```

```
display mirroring-group 1
mirroring-group 1:
   type: local
   status: active
   mirroring port:
      GigabitEthernet2/0/14  both
   mirroring CPU:
   monitor port: GigabitEthernet1/0/6
```

➔ **Connecter l'analyseur sur le port 1/0/6.**

2.15.3 Sauvegardes

Tous les switches ou les stacks installés sur RAMAGE sont à déclarer dans le SI. Ils sont alors automatiquement sauvegardés. La sauvegarde contient la configuration de l'ensemble du stack. NCM permet de visualiser les différentes modifications effectuées sur les équipements.

Seuls les équipements déclarés dans le SI seront dépannés et pris en charge par le CNGR.

Si vous disposez d'un serveur tftp en local

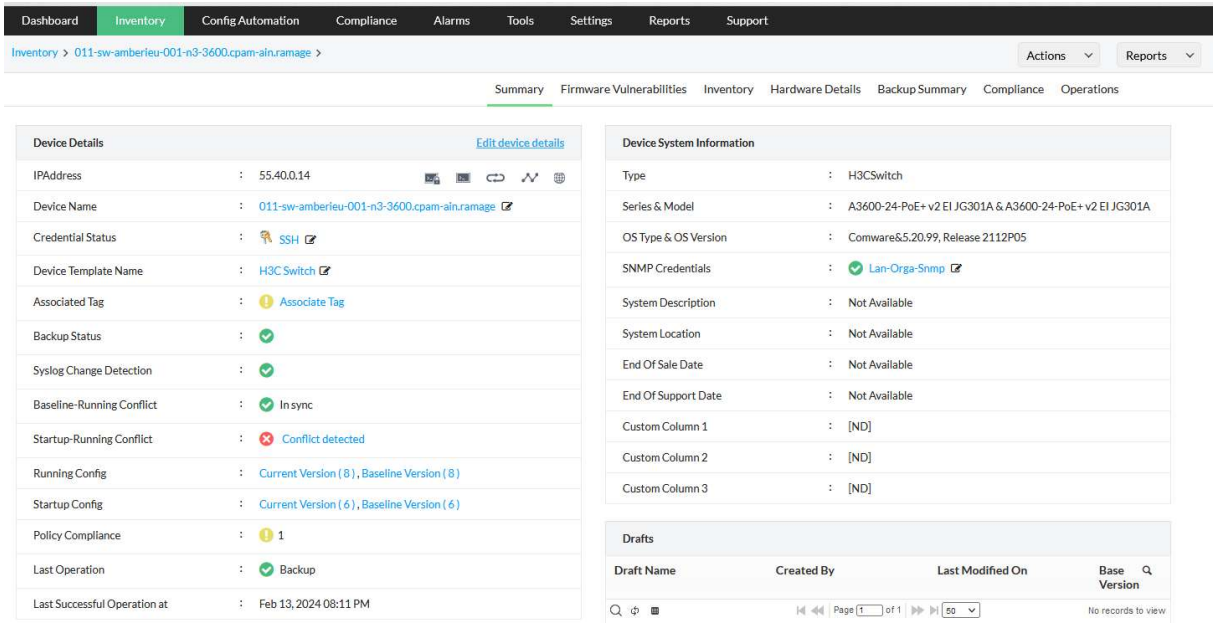
<sysname>tftp @ip_tftp put startup.cfg

```
Press CTRL+C to abort.
 % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                Dload  Upload   Total   Spent    Left  Speed
100 16615    0     0  100 16615     0  12017  0:00:01  0:00:01 --:--:-- 12483
```

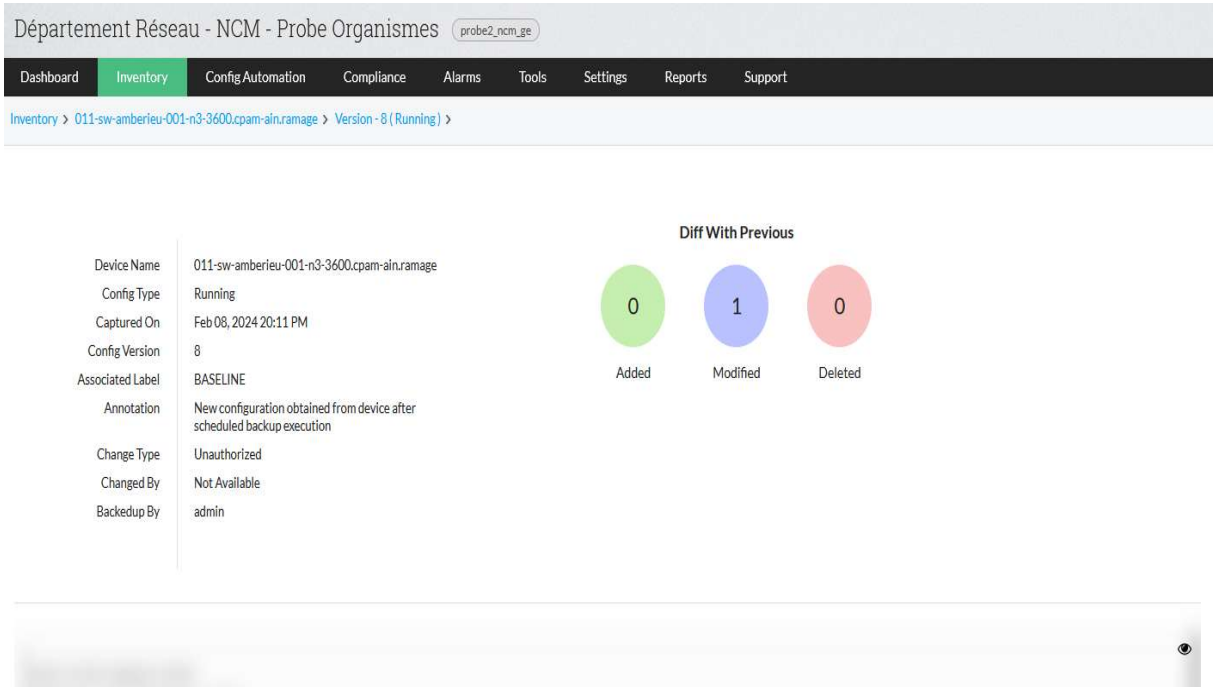
2.15.4 Restaurations

2.15.4.1 Depuis l'outil NCM (Méthode 1)

Se placer sur l'équipement souhaité dans l'inventaire du logiciel Network Configuration Manager :

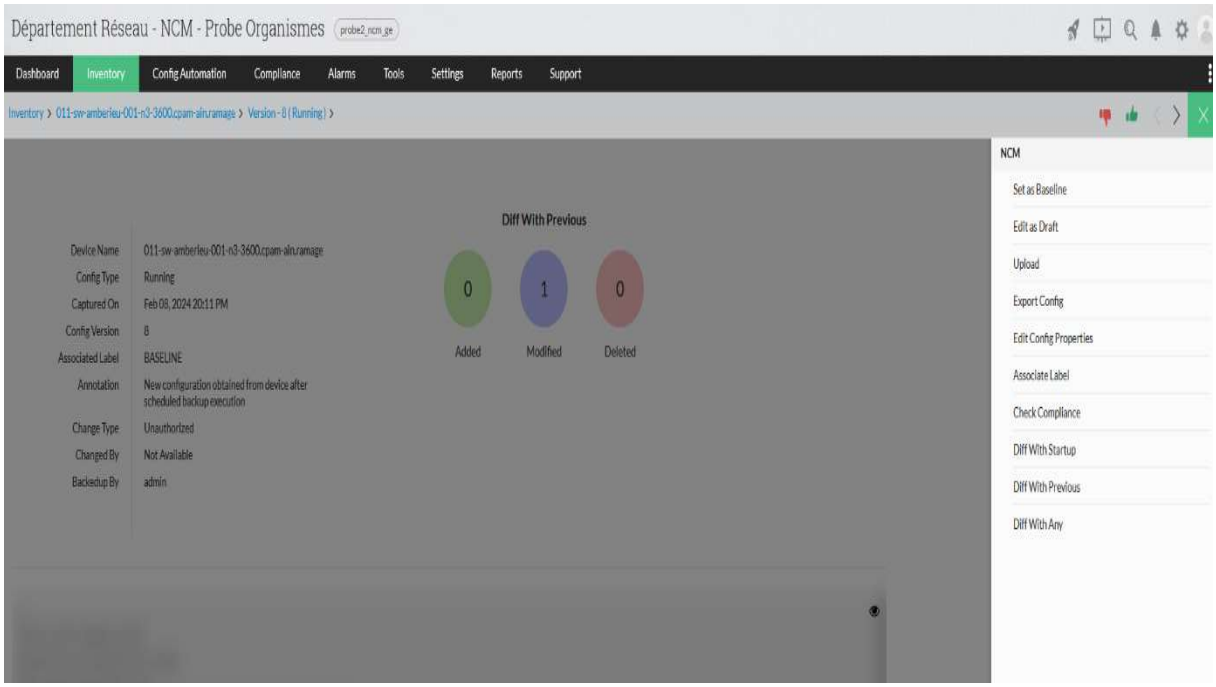


Cliquer sur la dernière version de la configuration « Current Version de la « Running Config » :

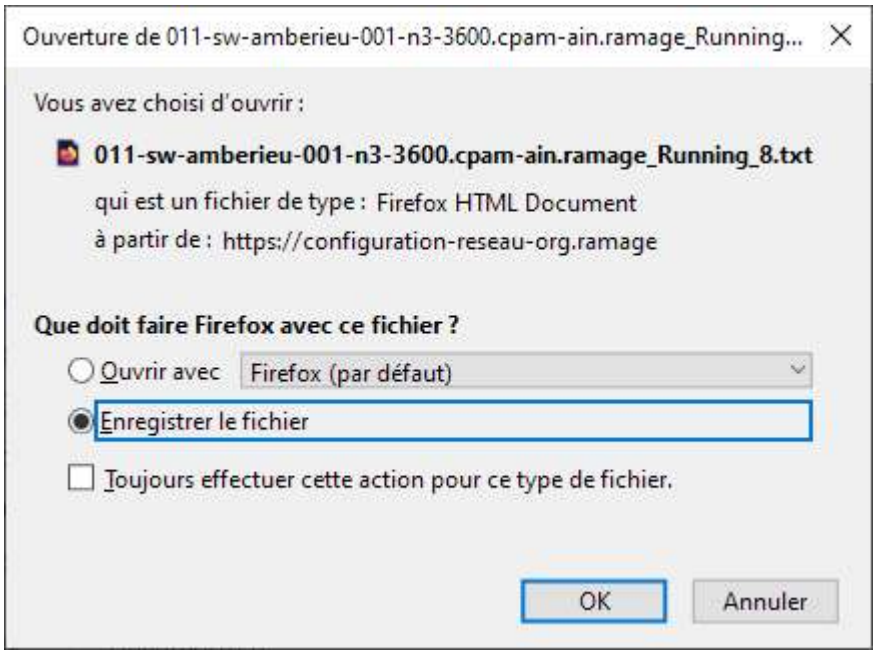


Cliquer sur le bouton en haut à droite 

Cliquer sur « Exporter la configuration » :



Enregistrer le fichier dans le dossier de votre choix :



Vous devez renommer le fichier de .txt à .cfg

Mettre votre fichier à la racine du dossier de votre serveur TFTP et vous pouvez faire la restauration de configuration :

Commande :

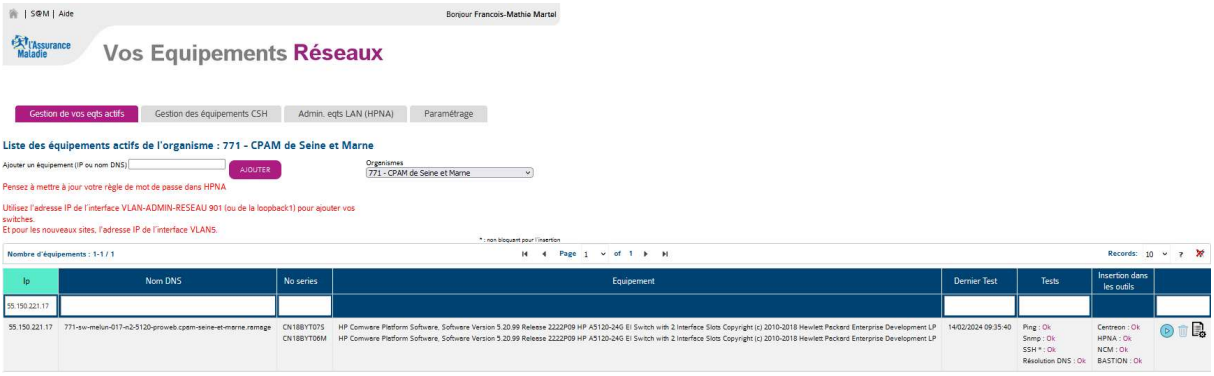
<>restore startup-configuration from *@IP-serveur-TFTP* ***fichier.cfg***
<>Reboot **(sans sauvegarder : lisez bien les questions posées).**
Dans l'exemple du § précédent, la commande aurait été :
<>restore startup-configuration from *@IP-serveur-TFTP* ***stack.cfg***

2.15.4.2 Depuis le portail du SI (Méthode 2)

Se connecter à la page suivante sur le portail du DR :

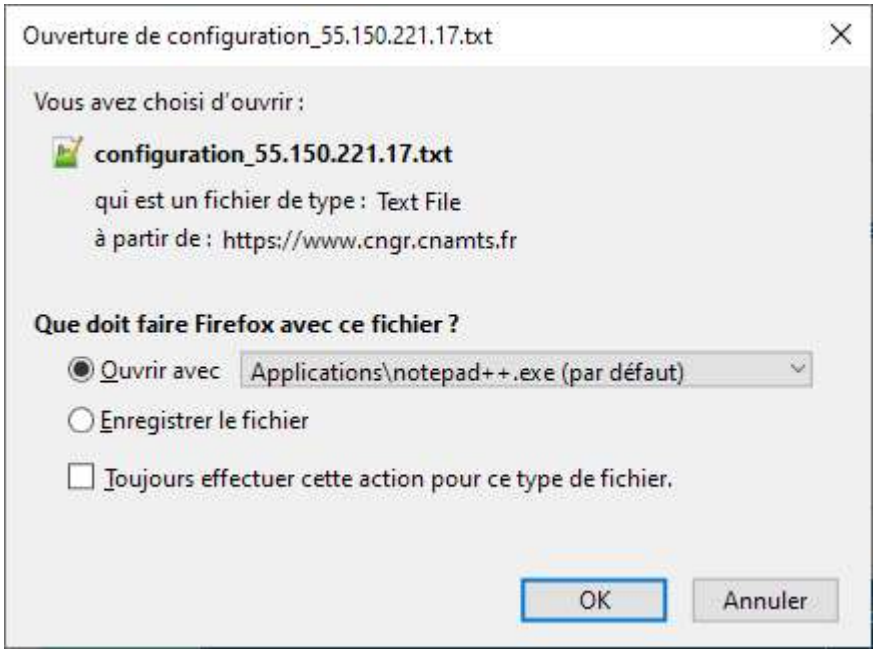
https://www.cngr.cnamts.fr/supervision/equipementActif/

Rechercher votre équipement via son adresse IP ou son nom dns :



Cliquer sur le bouton  pour télécharger la configuration de votre équipement.

Une fenêtre de téléchargement va apparaitre :



Vous devez renommer le fichier de .txt à .cfg

Mettre votre fichier à la racine du dossier de votre serveur TFTP et vous pouvez faire la restauration de configuration :

Commande :

```
<>restore startup-configuration from @IP-serveur-TFTP fichier.cfg
<>Reboot (sans sauvegarder : lisez bien les questions posées).
Dans l'exemple du § précédent, la commande aurait été :
<>restore startup-configuration from @IP-serveur-TFTP stack.cfg
```

2.15.5 Remplacement d'un switch non maitre en panne dans un stack

- Ouvrez un ticket d'incident au PSN (http://www.support-national.cnamts.fr/) pour obtenir un switch identique de remplacement (voir « que faire en cas de panne dans le référentiel »).
- Assurez-vous que ce switch est en configuration usine
- Connectez-vous en console
- mettre le même sysname que celui du stack dont on veut remplacer un switch
- Configurez la partie stackage pour un switch « N » (la config du switch « N » en entier)
- récupérez la sauvegarde dans NCM
- Avec un copier – coller reportez la configuration de toutes les interfaces sauf celles utilisées pour le stackage. Ne reportez pas le reste de la configuration.
- Vous n'avez plus qu'à placer ce switch dans le stack en remplacement du switch en panne dans le stack. Le stack sera reconstruit à l'identique.

2.15.6 Remplacement d'un switch maitre en panne dans un stack

Le switch 1 du stack est maitre. Le **routeur BTE** peut être connecté l'interface gi1/0/1 (normalisé). Si le switch 1 tombe en panne, le site bascule sur le secours. Connectez-vous au stack et configurez une interface libre sur le 2 pour recevoir la connexion du nominal :

```
interface Gi2/0/X
 port link-mode bridge
 description ROUTEUR-BTE
 port access vlan 5
 speed 100
 duplex full
 stp disable
```

Si le site n'a pas de **routeur NXO**, il faut se déplacer …où avoir prévu une interface de secours préconfigurée.

- Ouvrez un ticket d'incident au PSN pour obtenir un switch identique de remplacement (voir « que faire en cas de panne dans le référentiel).
- récupérez la sauvegarde du stack dans NCM (aller sur le stack puis sur view-configuration et cliquez « download text-file »).

Le maitre d'un stack est celui qui a la priorité la plus haute : c'est la configuration de ce switch qui va être mutualisée aux autres switches.

1/ Sur le stack où le maitre est HS, un nouveau switch est devenu maitre : le switch 2 (normalement car il a la priorité 30). Pour vérifier, taper « display irf » sur le stack :

```
<35-CN-RENNES-Sw-Buro-86-Fd>display irf
Switch  Role   Priority  CPU-Mac        Description
 *+2    Master  30       b8af-6770-ccec  -----
-------------------------------------------------------
```

2/ passer la priorité du maitre (le 2) à 32 – cela ne génère pas de coupure :

```
Irf member 2 priority 32
Save force (sauvegarde)
```

On obtient :

```
<35-CN-RENNES-Sw-Buro-86-Fd>display irf
Switch  Role   Priority  CPU-Mac        Description
 *+2    Master  32       b8af-6770-ccec  -----
-------------------------------------------------------
```

3/ Préparer le switch de remplacement du switch en panne :

- Assurez-vous que ce switch est en configuration usine
- Connectez-vous en console
- Donner au switch le même sysname que celui du stack dont vous remplacez l'unité 1
- Configurez la partie stackage pour un switch « 1 » (toute la séquence – NE PAS OUBLIER LE NUMERO DE « DOMAIN ») mais avec :

Irf member 1 priority 30

Cela donne (exemple avec un 24 port) :

```
<>System-view
#
irf domain YY
irf member 1 priority 30
#
interface range Ten-GigabitEthernet1/0/27 to Ten-GigabitEthernet1/0/28
 shutdown
 quit
#
irf-port 1/1
 port group interface Ten-GigabitEthernet 1/0/27
 quit
#
irf-port 1/2
 port group interface tenGigabitEthernet 1/0/28
 quit
#
irf-port-configuration active
#
interface range Ten-GigabitEthernet1/0/27 to Ten-GigabitEthernet1/0/28
 undo shutdown
 description STACKAGE
 quit
#
<>save force
```

4/ Placer ce switch dans le stack en remplacement du switch en panne dans le stack. Le switch n°1 que vous avez inséré va rebooter s'insérer au stack et prendre la configuration fournie par le numéro 2.
Le stack sera reconstruit à l'identique, les interfaces du n°1 aussi. Au cas où vous pouvez les reconfigurer en faisant un copier-coller à partir du fichier de sauvegarde (seulement les interfaces de 1/01 à 1/0/26 (ou 1/0/50)).

5/ Repasser la priorité du switch à 30 et celui du switch 1 à 32 :

Irf member 2 priority 31
Irf member 1 priority 32
Irf member 2 priority 30
Save force (sauvegarde)

2.15.7 Remplacement d'un stack complet

- Ouvrez un ticket d'incident au PSN (http://www.support-national.cnamts.fr/) pour obtenir des switches identiques de remplacement (voir « que faire en cas de panne dans le référentiel »
- Assurez-vous que ces switches sont en configuration usine
- Connectez-vous en console sur les switches et reconstruisez le stack
- Restaurez la configuration sauvegardée dans NCM

2.15.8 Ajout d'un switch dans un stack (en production)

Exemple : on veut ajouter un 3ème switch 5500 dans un stack existant (cas rare). Méthode sans coupure :
1/ Préparer un switch avec la même version que la stack
2/ Lui attribuer le même nom (sysname) que celui du stack
3/ Lui attribuer le numéro 3 (cf configuration stackage IRF) + sysname
4/ Déconnecter le lien IRF entre le port 2 du 2ème et le port 1 du 1er
5/ Mettre le switch 3 en baie et le démarrer
6/ Connecter le port 2 du 2ème au port 1 du 3ème et le port 1 du 3ème au port 2 du 1er

Le switch n° 3 redémarre et s'insère dans le stack.

2.15.9 Mise à jour de la version des HP 5510, 5520, 5130, 5140

2.15.9.1 Prérequis: Appliquer la version courante sur la partition backup

Appliquer la version courante sur la partition de backup, il faut saisir la commande ci-dessous :

```
<HPE>dis boot
<CSM-CESTIF-N3-5130>dis boot
Software images on slot 1:
Current software images:
  flash:/5130ei-cmw710-boot- r3111p02.bin                (version courante)
  flash:/5130ei-cmw710-system- r3111p02.bin              (version courante)
Main startup software images:
  flash:/5130ei-cmw710-boot- r3111p02.bin                (version courante)
  flash:/5130ei-cmw710-system- r3111p02.bin              (version courante)
Backup startup software images:
  flash:/5130ei-cmw710-boot- r3111p01.bin                (version précédente)
  flash:/5130ei-cmw710-system- r3111p01.bin              (version précédente)
Software images on slot 2:
Current software images:
  flash:/5130ei-cmw710-boot- r3111p02.bin
  flash:/5130ei-cmw710-system- r3111p02.bin
Main startup software images:
  flash:/5130ei-cmw710-boot- r3111p02.bin
  flash:/5130ei-cmw710-system- r3111p02.bin
Backup startup software images:
  flash:/5130ei-cmw710-boot- r3111p01.bin                (version précédente)
  flash:/5130ei-cmw710-system- r3111p01.bin              (version précédente)
```

boot-loader file boot flash:/5130ei-cmw710-**boot**-r3111p02.bin system flash:/5130ei-cmw710-**system**-r3111p02.bin all backup
This command will set the backup startup software images. Continue? [Y/N]:**y**

The images that have passed all examinations will be used as the backup startup software images at the next reboot on slot 1.

File flash:/5130ei-cmw710-boot-r3111p02.bin already exists on slot 2.
Do you want to overwrite the file?
Y: Overwrite the file.
N: Not overwrite the file.
A: From now on, overwrite or not overwrite without prompt.

Please make a choice. [Y/N/A]:y

Loading.....%Jan 1 01:04:47:004 2013 HPE DEV/4/BOARD_LOADING: Board in slot 2 is loading software images.
.....%Jan 1 01:04:53:767 2013 HPE DEV/5/LOAD_FINISHED: Board in slot 2 has finished loading software images.
.....Done.

File flash:/5130ei-cmw710-system- r3506p06.bin already exists on slot 2.
Do you want to overwrite the file?

Y: Overwrite the file.
N: Not overwrite the file.
A: From now on, overwrite or not overwrite without prompt.

Please make a choice. [Y/N/A]:y

Loading.....%Jan 1 01:05:35:497 2013 HPE DEV/4/BOARD_LOADING: Board in slot 2 is loading software images.
.....%Jan 1 01:06:03:651 2013 HPE DEV/5/LOAD_FINISHED: Board in slot 2 has finished loading software images.
.....Done.
Verifying the file flash:/5130ei-cmw710-boot- r3506p06.bin on slot 2.....Done.
Verifying the file flash:/5130ei-cmw710-system- r3506p06.bin on slot 2.....Done.
The images that have passed all examinations will be used as the backup startup software images at the next reboot on slot 2.

Vérification de la prise en compte de la version de backup :

<HPE>dis boot
Software images on slot 1:
Current software images:
flash:/5130ei-cmw710-boot-r3111p02.bin
flash:/5130ei-cmw710-system-r3111p02.bin
Main startup software images:
flash:/5130ei-cmw710-boot- r3111p02.bin

flash:/5130ei-cmw710-system- r3111p02.bin
Backup startup software images:
flash:/5130ei-cmw710-boot- r3111p02.bin
flash:/5130ei-cmw710-system-r3111p02.bin
Software images on slot 2:
Current software images:
flash:/5130ei-cmw710-boot-r3111p02.bin
flash:/5130ei-cmw710-system-r3111p02.bin
Main startup software images:
flash:/5130ei-cmw710-boot- r3111p02.bin
flash:/5130ei-cmw710-system- r3111p02.bin
Backup startup software images:
flash:/5130ei-cmw710-boot-r3111p02.bin
flash:/5130ei-cmw710-system-r3111p02.bin

2.15.9.2 Prérequis : Vérifier qu'il y a de la place sur les flashs du stack

<>dir /all

```
<SIEGE-N3-1-5130-SS>dir /all
Directory of flash:
  0 -rw-    7172096 Mar 25 2021 11:32:42   5510hi-cmw710-boot-r3506p06.bin
  1 -rw-   83632128 Mar 25 2021 11:33:34   5510hi-cmw710-system-r3506p06.bin
  2 -rw-      10873 Feb 22 2018 09:31:23   NA_running.cfg
  3 -rw-     142805 Feb 22 2018 09:31:23   NA_running.mdb
  4 drw-          - Jan 01 2013 01:00:29   diagfile
  5 -rw-        735 Jan 01 2013 05:30:35   hostkey
  6 -rw-       1924 Feb 22 2018 09:31:22   ifindex.dat
  7 drw-          - Jan 01 2013 01:00:32   license
  8 drw-          - Jan 02 2013 01:00:22   logfile
  9 drw-          - Jan 01 2013 05:28:56   pki
 10 drw-          - Jan 01 2013 01:00:29   seclog
 11 -rw-        591 Jan 01 2013 05:30:36   serverkey
 12 -rw-      10873 Jan 31 2018 18:50:06   startup.cfg
 13 -rw-     142805 Jan 31 2018 18:50:06   startup.mdb
 14 drw-          - Jan 01 2013 01:00:36   versionInfo
 15 -rwh         20 Jan 01 2013 05:56:13   .snmpboots

524288 KB total (452408 KB free)
```

Ici 90 Mo suffisant pour une future version à 83 Mo + 7 Mo = 90 Mo

Si nécessaire supprimer des fichiers pour faire de la place:

A/ Suppression de fichiers dans la flash (pas assez de place) de manière non définitive :

<>delete flash:/***fichier***

OU:

<>delete slot2#flash:/***fichier***

➔ Les fichiers sont visibles entre crochets si on fait un **dir /all**
➔ Pour les supprimer définitivement, il faut vider la corbeille :

<>reset recycle-bin /force

B/ Suppression de fichiers dans la flash (pas assez de place) de manière définitive :

<>delete /unreserved #flash:/***fichier***
<>delete /unreserved slot2#flash:/***fichier***

2.15.9.3 Début de la procédure: Résumé des commandes

❶ **<HPE> tftp *@IP-du-PMF* get 5130EI-CMW710-R35606p06.ipe ou via USB** | Nouvelle version à installer
❷ **<HPE> boot-loader file flash:/5130EI-CMW710- R35606p06.ipe slot 1 main**
❸ **<HPE> boot-loader file flash:/5130EI-CMW710- R35606p06.ipe slot 2 main**
❹ **<HPE>boot-loader file boot flash:/5510hi-cmw710-boot-r3506p06.bin system flash:/5510hi-cmw710-system-r3606p06.bin all backup**
❺ **<HPE> reboot <HPE> schedule reboot at 23:00**

2.15.9.4 Procédure de mise à jour détaillée

2.15.9.4.1 Téléchargement de la version en USB

Il est possible de transférer la version (fichier .ipe) récupérée sur le portail du DR **en USB dans les switch**es de la **gamme 5510** :

- Insérer la clé USB dans le switch (en haut à droite)
- Sur le switch en console ou en accès à distance transférez le fichier .ipe de la clé USB vers la flash :

<HPE>cd usba0:/
<HPE>dir
Directory of usba0:
1 -rw- 91821056 Jun 26 2020 00:21:22 5510HI-CMW710-R3506P06.ipe
2 drw- - Sep 25 2020 08:10:40 System Volume Information

7920608 KB total (7752168 KB free)

<HPE>copy 5510HI-CMW710-R3506P06.ipe flash:/

Copy usba0:/5510HI-CMW710-R3506P06.ipe to flash:/5510HI-CMW710-R3506P06.ipe? [Y/N]**:y**
Copying file usba0:/5510HI-CMW710-R3506P06.ipe to flash:/5510HI-CMW710-R3506P06.ipe..... Done.
<HPE>
<HPE>cd flash:/
<HPE>dir
Directory of flash:
0 -rw- 91821056 Jan 01 2013 00:26:50 5510HI-CMW710-R3506P06.ipe
1 drw- - Jan 01 2013 00:00:17 diagfile
2 -rw- 866 Jan 01 2013 01:55:00 ifindex.dat
3 -rw- 255 Jan 01 2013 00:25:13 lauth.dat
4 drw- - Jan 01 2013 00:00:24 license
5 drw- - Jan 01 2013 01:32:11 logfile
6 drw- - Jan 01 2013 00:00:49 pki
7 drw- - Jan 01 2013 00:00:17 seclog
8 drw- - Jan 01 2013 00:00:50 versionInfo

524288 KB total (433392 KB free)

2.15.9.4.2 Téléchargement de la version en TFTP

La version des switches HP 5130 est composée de 2 fichiers binaires : boot.bin et system.bin.
Ces deux fichiers sont regroupés dans un fichier *.ipe.

Pour réaliser l'upgrade des HP 5130, il faut donc télécharger le fichier *.ipe.

<HPE>dis boot
Software images on slot 1:
Current software images:
flash:/5130ei-cmw710-**boot**-**r3606p06**.bin
flash:/5130ei-cmw710-**system**-**r3606p06**.bin

Chargement la nouvelle version via TFTP :
Connectez votre PMF (ayant un serveur TFTP) dans un VLAN, vérifiez que vous "pinguez" le switch et tapez la commande suivante (adaptez le nom du fichier) :

❶ **<HPE> tftp *@IP-du-PMF* get 5130EI-CMW710-R3606P06.ipe**

2.15.9.4.3 Appliquer la nouvelle version sur le membre 1

Application de la version sur le membre 1

Pour mettre à jour le membre 1 du stack tapez la commande ci-dessous:

❷ <HPE> **boot-loader file flash:/5130EI-CMW710-R3606P06.ipe slot 1 main**

Les messages ci-dessous apparaissent :
Verifying the file flash:/5130ei-cmw710-r3606p06.ipe on slot 1.....Done.
HPE 5130-24G-4SFP+ EI Switch images in IPE:
5130ei-cmw710-boot- r3606p06.bin
5130ei-cmw710-system- r3606p06.bin
This command will set the main startup software images. Continue? [Y/N]:**y**
➔ Saisir « Y » pour valider l'application de la version *.ipe.

Add images to slot 1.
Decompressing file 5130ei-cmw710-system-r3606p06.bin to flash:/5130ei-cmw710-system-r3113p05.bin.....
Decompressing file 5130ei-cmw710-boot-r3606p06.bin to flash:/5130ei-cmw710-boot-r3113p05.bin.....Done.
Decompression completed.

You are recommended to delete the .ipe file after you set startup software images for all slots.
Do you want to delete flash:/5130ei-cmw710-r3606p06.ipe now? [Y/N]:**N**

*!!!!!!! Si vous faite « **Y** » pour supprimer le fichier * .ipe, vous ne pourrez pas exécuter la commande « **boot-loader file flash:/5130EI-CMW710-R3606p06.ipe slot 2 main** » sur le membre 2. Cependant, il sera possible de synchroniser avec le slot 1 (à jour) avec la commande ci-dessous :*
boot-loader update slot 2

N.B : Les fichiers 5130ei-cmw710-boot-r3606p06.bin et 5130ei-cmw710-system-r3113p05.bin ont automatiquement été décompressés.

Verifying the file flash:/5130ei-cmw710-boot-r3606p06.bin on slot 1...Done.
Verifying the file flash:/5130ei-cmw710-system-r3606p06.bin on slot 1.....Done.
The images that have passed all examinations will be used as the main startup software images at the next reboot on slot 1.

Vérification

<HPE>dis boot
Software images on slot 1:
Current software images:
flash:/5130ei-cmw710-boot-r3111p02.bin
flash:/5130ei-cmw710-system-r3111p02.bin
Main startup software images:
flash:/5130ei-cmw710-**boot-r3606p06**.bin (nouvelle version)
flash:/5130ei-cmw710-**system-r3606p06**.bin (nouvelle version)
Backup startup software images:
flash:/5130ei-cmw710-boot-r3111p02.bin
flash:/5130ei-cmw710-system-r3111p02.bin
Software images on slot 2:
Current software images:
flash:/5130ei-cmw710-boot-r3111p02.bin
flash:/5130ei-cmw710-system-r3111p02.bin
Main startup software images:
flash:/5130ei-cmw710-boot-r3111p02.bin
flash:/5130ei-cmw710-system-r3111p02.bin
Backup startup software images:
flash:/5130ei-cmw710-boot-r3111p02.bin
flash:/5130ei-cmw710-system-r3111p02.bin

La version n'est installée que sur le membre 1 pour le moment.

2.15.9.4.4 Mettre à jour le membre 2

❸ <HPE> boot-loader file flash:/5130EI-CMW710-R3606p06.ipe slot 2 main

This command will update the specified standby MPU. Continue? [Y/N]:**y**
Updating. Please wait...
Verifying the file flash:/5130ei-cmw710-boot-r3606p06.bin on slot 1...Done.
Verifying the file flash:/5130ei-cmw710-system-r33606p06.bin on slot 1.....Done.
Copying main startup software images to slot 2. Please wait...
Done.
Setting copied images as main startup software images for slot 2...
The images that have passed all examinations will be used as the main startup software images at the next reboot on slot 2.
Done.
Successfully updated the startup software images of slot 2.

You are recommended to delete the .ipe file after you set startup software images for all slots.
Do you want to delete flash:/5130ei-cmw710-r3606p06.ipe now? [Y/N]:**Y**

Dans la dernière version cela n'est pas forcément demandé : pensez à supprimer le fichier.ipe du slot 1 :
> delete /u flash:/ 5130EI-xxxxxxxx.ipe

Vérification :

<HPE>dis boot
Software images on slot 1:
Current software images:
flash:/5130ei-cmw710-boot-r3111p02.bin
flash:/5130ei-cmw710-system-r3111p02.bin
Main startup software images:
flash:/5130ei-cmw710-boot-r3606p06.bin
flash:/5130ei-cmw710-system-r3606p06.bin
Backup startup software images:
None
Software images on slot 2:
Current software images:
flash:/5130ei-cmw710-boot-r3111p02.bin
flash:/5130ei-cmw710-system-r3111p02.bin
Main startup software images:
flash:/5130ei-cmw710-**boot-r3606p06**.bin (nouvelle version)
flash:/5130ei-cmw710-**system-r3606p06**.bin (nouvelle version)
Backup startup software images:
flash:/5130ei-cmw710-boot-r3111p02.bin
flash:/5130ei-cmw710-system-r3111p02.bin

La version est installée sur le membre 2.

2.15.9.4.5 Reboot des switches

Pour mettre en œuvre la nouvelle version, il faut rebooter les switches.

❹ **<HPE> reboot**
Ou
<HPE> schedule reboot at 23:00

Après le reboot, voici l'état du boot :

<HPE>dis boot
Software images on slot 1:
Current software images:
flash:/5130ei-cmw710-boot-r3606p06.bin (nouvelle version)
flash:/5130ei-cmw710-system-r3606p06.bin (nouvelle version)
Main startup software images:
flash:/5130ei-cmw710-boot-r3606p06.bin (nouvelle version)
flash:/5130ei-cmw710-system-r3606p06.bin (nouvelle version)
Backup startup software images:
flash:/5130ei-cmw710-boot-r3111p02.bin (ancienne version)
flash:/5130ei-cmw710-system-r3111p02.bin (ancienne version)
Software images on slot 2:
Current software images:
flash:/5130ei-cmw710-boot-r3606p06.bin (nouvelle version)
flash:/5130ei-cmw710-system-r3606p06.bin (nouvelle version)
Main startup software images:
flash:/5130ei-cmw710-boot-r3606p06.bin (nouvelle version)
flash:/5130ei-cmw710-system-r3606p06.bin (nouvelle version)

Backup startup software images:
flash:/5130ei-cmw710-boot-r3111p02.bin (ancienne version)
flash:/5130ei-cmw710-system-r3111p02.bin (ancienne version)

2.15.10 Récupération d'un switch sans version

La méthode étant la même pour les HP 3600 V1, V2, 5500 et 5120, les écrans ci-dessous sont des copies de la procédure 3600 V1. Veuillez évidemment adapter avec les bons fichiers de version. Rappel : les versions sont disposées sur le site intranet du CNGR.

```
**************************************************************
*                                                            *
*        H3C S3600-28P-PWR-EI BOOTROM, Version 606           *
*                                                            *
**************************************************************

Copyright(c) 2004-2010 Hangzhou H3C Technologies Co., Ltd.
Creation date    : Sep 25 2010, 11:30:43
CPU Clock Speed  : 200MHz
BUS Clock Speed  : 33MHz
Memory Size      : 64MB
Mac Address      : 3ce5a689835e

Press Ctrl-B to enter Boot Menu... 0
Auto-booting...

No correct default file to boot!
-
```

Il faut dans un premier temps entrer dans le Boot Menu par Ctrl + B

Password : **(pas de password par défaut)**

BOOT MENU

1. Download application file to flash
2. Select application file to boot
3. Display all files in flash
4. Delete file from flash
5. Modify bootrom password
6. Enter bootrom upgrade menu
7. Skip current configuration file
8. Set bootrom password recovery
9. Set switch startup mode
0. Reboot

Choisir le 1. Download application file to flash

1. Set TFTP protocol parameters
2. Set FTP protocol parameters
3. Set XMODEM protocol parameters
0. Return to boot menu

Choisir le 1 Set TFTP protocol parameters

Au préalable, il faut connecter le PMF sur une interface du switch et choisir un adressage cohérant entre le switch et le PMF.
Sur ce PMF, il faut ouvrir un serveur tftp avec les fichiers à télécharger.

```
Enter your choice(0-3): 1
Load File name          :s3600ei-cmw310-R1702p28-s168.bin
Switch IP address       :55.16.221.232
Server IP address       :55.16.221.234
Are you sure you want to download file to flash? Yes or No [Y/N] y
Loading.....................................................................
.....................done
Free flash Space: 4834304 bytes
Writing flash.....................................................................
.....................................................................
.....................................................................
.....................................................done!

Please input the file attribute (main/backup/none):main
```

On vérifie si le ficheir a bien été pris en compte.

```
 BOOT  MENU

1. Download application file to flash
2. Select application file to boot
3. Display all files in flash
4. Delete file from flash
5. Modify bootrom password
6. Enter bootrom upgrade menu
7. Skip current configuration file
8. Set bootrom password recovery
9. Set switch startup mode
0. Reboot

Enter your choice(0-9): 3
File Number    File Size(bytes)     File Name
================================================================================
1           195268            s3600
2(*)         882249             h3c-http3.1.9-0014.web
3           2211              config.def
4           4589776            test
5           151               private-data.txt
6           195268            s3600_n.btm
7           2304              default_file
8           302080            boot_n
9(*)        4679012           s3600ei-cmw310-R1702p28-s168.bin
10          2392              config.cfg
Free Space: 154624 bytes
The current application file is s3600ei-cmw310-R1702p28-s168.bin
(*)-with main attribute
(b)-with backup attribute
(*b)-with both main and backup attribute

 BOOT  MENU

1. Download application file to flash
2. Select application file to boot
3. Display all files in flash
4. Delete file from flash
5. Modify bootrom password
6. Enter bootrom upgrade menu
7. Skip current configuration file
8. Set bootrom password recovery
9. Set switch startup mode
0. Reboot
```

```
Enter your choice(0-9): 2

Select application file to boot
1. Set application files
2. Set configuration files
3. Set web files
0. Return

Enter your choice(0-3): 1
File Number    File Size(bytes)     File Name
================================================================================
1(*)          4679012            s3600ei-cmw310-R1702p28-s168.bin
Free Space: 154624 bytes
(*)-with main attribute
(b)-with backup attribute
(*b)-with both main and backup attribute
Please input the file number to change: 1
Please input the file attribute (main/backup):main
Do you want to run s3600ei-cmw310-R1702p28-s168.bin now? Yes or No [Y/N] y
Decompress Image.....................................................................
.....................................................................
.....................................................................
.....................................................................
.....................................................................
.....................................OK!
Starting at 0x80100000...

        Board checking.....................LSJ1LTSH
        SDRAM fast selftest.....................OK!
        Flash fast selftest.....................OK!
        CPLD selftest.....................OK!
        Switch chip selftest.....................OK!
        Port 1 has no module
        Port 2 has no module
        Port 3 has no module
        Port 4 has 1000_BASE_T_AN_SFP module
        PHY selftest.....................OK!
        Please check port leds.....FINISHED!

Startup configuration is skipped.
User interface aux0 is available.
```

2.15.11 Remettre un switch en configuration usine

2.15.11.1 Retour usine complet (avec changement de n° d'unité)

Sur un « master » (tête de stack) :

<>**reset saved-configuration** ➔ **Y**
<>**reboot** (sans sauvegarde) ➔ **N puis Y**

Sur un « slave » (exemple avec member = 2) :

<>system-view
#
irf member 2 renumber 1 ➔ **Y**
save
reboot ➔ **Y**

puis :

<>**reset saved-configuration** ➔ **Y**
<>**reboot** (sans sauvegarde) ➔ **N puis Y**

2.15.11.2 Retour usine sans changement de n° d'unité

Rebooter le switch et en console taper CTRL B lorsque cela est proposé. Ensuite, validez : Il n'y a normalement pas de « bootrom password » pour entrer dans le menu de boot :

BOOT MENU

1. Download application file to flash
2. Select application file to boot
3. Display all files in flash
4. Delete file from flash
5. Modify bootrom password
6. Enter bootrom upgrade menu
7. Skip current configuration file
8. Set bootrom password recovery
9. Set switch startup mode
0. Reboot

Choisir "4. Delete file from flash" et choisissez le ou les fichiers « .cfg » pour les supprimer tous.
Choisir ensuite «0. Reboot ».

2.15.12 Accéder à la console du switch sans authentification

En cas de perte du mot de passe de l'équipement, il est possible de reprendre la main en console en contournant l'authentification du switch.

Pour cela, il faut suivre la procédure ci-dessous lors du reboot du switch :

Using the EXTENDED-BOOTWARE menu

To access the EXTENDED-BOOTWARE menu, press **Ctrl+B** within three seconds after the "Press Ctrl+B to access EXTENDED-BOOTWARE MENU..." prompt message appears. If you fail to do this, the system starts decompressing the Comware software.

```
System is starting...
Press Ctrl+D to access BASIC-BOOTWARE MENU...
Press Ctrl+T to start memory test
Booting Normal Extended BootWare
The Extended BootWare is self-decompressing........Done.

********************************************************************************
*                                                                              *
*                    HPE Routers BootWare, Version 2.05                        *
*                                                                              *
********************************************************************************
Copyright (c) 2010-2017 Hewlett Packard Enterprise Development LP.

Compiled Date       : Jan 18 2016
CPU Type            : P2020
CPU L1 Cache        : 32KB
CPU Clock Speed     : 1000MHz
Memory Type         : DDR3 SDRAM
Memory Size         : 2048MB
Memory Speed        : 800MHz
BootWare Size       : 1024KB
Flash Size          : 8MB
NVRAM Size          : 128KB
BASIC CPLD Version  : 3.0
EXTENDED CPLD Version: 2.0
PCB Version         : Ver.B

BootWare Validating...
Press Ctrl+B to access EXTENDED-BOOTWARE MENU...
```

The following is the EXTENDED-BOOTWARE menu:

```
Password recovery capability is enabled.
Note: The current operating device is flash
Enter < Storage Device Operation > to select device.

==========================<EXTENDED-BOOTWARE MENU>==========================
|<1> Boot System                                                           |
|<2> Enter Serial SubMenu                                                  |
|<3> Enter Ethernet SubMenu                                                |
|<4> File Control                                                          |
|<5> Restore to Factory Default Configuration                              |
|<6> Skip Current System Configuration                                     |
|<7> BootWare Operation Menu                                               |
|<8> Skip Authentication for Console Login                                 |
|<9> Storage Device Operation                                              |
|<0> Reboot                                                                |
============================================================================
Ctrl+Z: Access EXTENDED ASSISTANT MENU
Ctrl+F: Format File System
Ctrl+C: Display Copyright
Enter your choice(0-9):
```

Puis, choisir 1 ou 0 dans l'extended-bootware menu.

2.15.13 Annexe : exemple complet de configuration

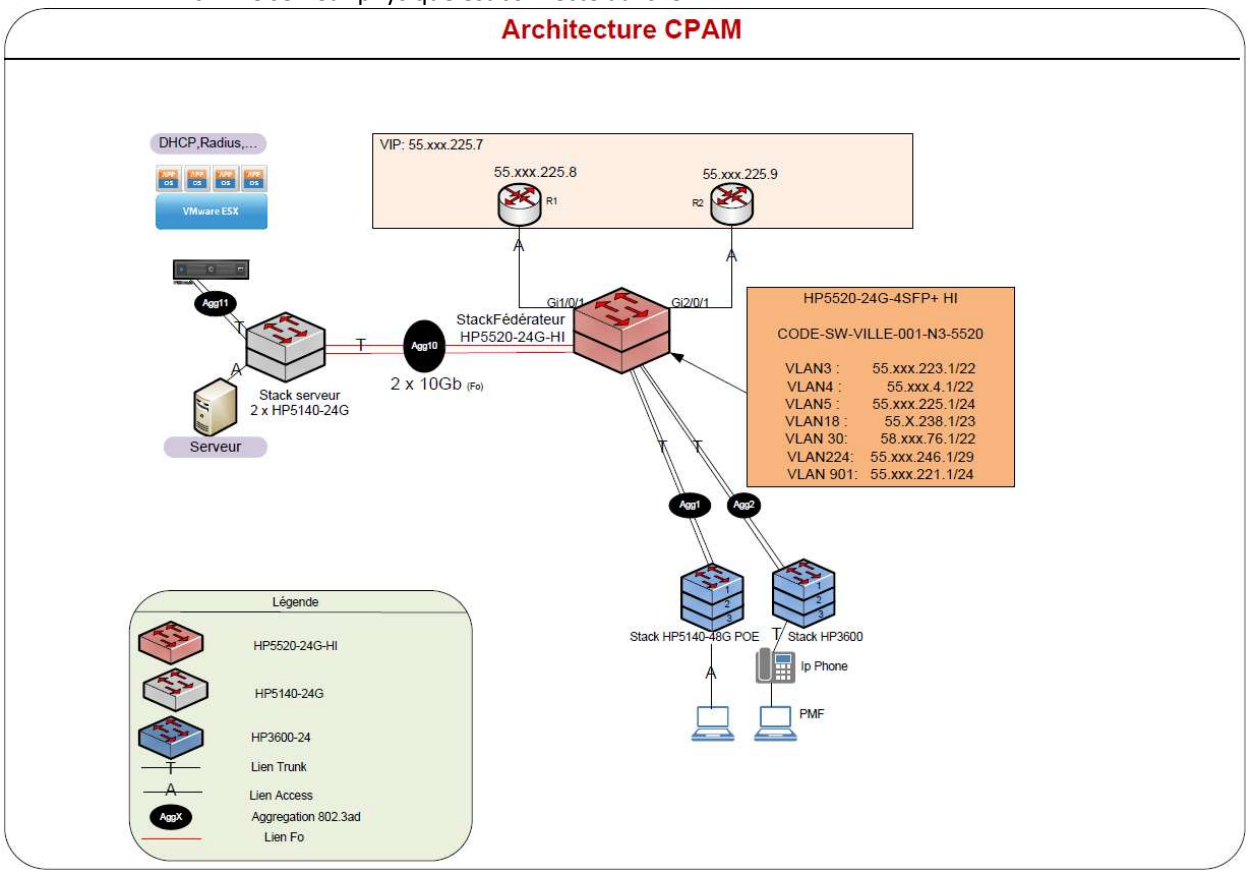
Dans ce chapitre, nous allons donner des exemples complets de configuration à partir d'architectures normalisées, en fonction des types de sites.

Ci-dessous l'exemple d'un siège d'Organisme de type CPAM. On retrouve une architecture classique :

- Un accès RAMAGE avec 2 routeurs opérateurs **BTE et NXO**
- Un stack fédérateur de 2 x HP 5510-24G-4SFP HI
  - agrégat 4 Gb vers un stack de HP 5130
  - 4 agrégats de 2 Gb vers des stacks HP 3600-24G POE V2

L'ensemble des stacks de 3600-24-PoE-v2 sont connectés en cuivre.L'interconnexion normalisée s'effectue via les interfaces Gi1/0/25 et Gi3/0/25 ou Gi1/0/25 et Gi2/0/25.

- Des équipements connectés au stack de 2 x HP 5130-24G (Stack serveur)
  - Un ESX connecté via un agrégat
  - Le serveur physique est connecté dans le VLAN 4



Plan d'adressage IP **(exemple)** :

- VLAN 5 – VLAN-INTERCOWAN : 55.X.225.0 /28: 55.X.225.1
- VLAN 4 – VLAN-DATA : 55.X.4.0 /22 – interface VLAN 4 : 55.X.4.1
- VLAN 30 – VLAN-VOIX : 58.X.4.0 /22 – interface VLAN 30 : 58.X.4.1
- VLAN 3 – VLAN-MEDICAL : 55.X.223.0 /24 – interface VLAN 3 : 55.X.223.1
- VLAN 18 – VLAN-PFS : 55.X.238.0 /23 – interface VLAN 18 : 55.X.238.1
- VLAN 901 – VLAN-ADMIN-RESEAU : 55.X.221.0 /24 – Interface VLAN 901 : 55.X.221.1
  - ⇨ stack de 3600 en 55.X.221.11.

- Serveurs GEDIFF :
  - National : 55.245.4.0
- Adresse IP du serveur DHCP : 55.X.4.60 (VLAN 4) qui distribue les adresses aux PMF et aux téléphones
- Les postes du service medical sont connectés sur les interfaces 10 à 24 du switch 3 du stack 3600

Configurations des 5510

Résultat d'un « display current » : certaines commandes par défaut non entrées en configuration apparaissent, d'autres, entrées n'apparaissent pas (stp enable sur interfaces par ex).

2.15.13.1 STACK 5510-24G-SFP 4SFP N3 (Niveau3)

```
#
############ MultiConfigPart Running configuration
#
 version 7.1.070, Release 3506P06
#
 sysname 191-SW-VILLE-001-N3-5510
#
 clock timezone PARIS add 01:00:00
 clock summer-time PARIS 01:00:00 March last Sunday 02:00:00
October last Sunday 02:00:00
#
 irf domain 1
 irf mac-address persistent timer
 irf auto-update enable
 undo irf link-delay
 irf member 1 priority 32
 irf member 2 priority 30
#
 ip unreachables enable
 ip ttl-expires enable
#
 dhcp enable
#
 dhcp snooping enable
#
 dns domain cnamts.fr
 dns server 55.223.10.1
#
 lldp global enable
#
 loopback-detection global enable vlan 1 to 4094
 loopback-detection global action shutdown
#
 password-recovery enable
#
vlan 1
#
vlan 4
 name VLAN-DATA
#
vlan 5
 name VLAN-INTERCOWAN
#
vlan 17
 name VLAN-EVASION-INTERNET
#
vlan 30
 name VLAN-VOIX
#
vlan 224
 name VLAN-ACCES-PART
#
vlan 226
 name VLAN-IMPRIMANTES
#
vlan 230
 name VLAN-GW-CETIAM
#
vlan 239
 name VLAN-MGT-IPANEMA
#
vlan 901
 name VLAN-ADMIN-RESEAU
#
irf-port 1/1
 port group interface Ten-GigabitEthernet1/0/27
#
irf-port 1/2
 port group interface Ten-GigabitEthernet1/0/28
#
irf-port 2/1
 port group interface Ten-GigabitEthernet2/0/27
#
irf-port 2/2
 port group interface Ten-GigabitEthernet2/0/28
#
qos map-table dscp-dot1p
 import 38 export 5
 import 46 export 6
#
 stp instance 0 priority 0
 stp mode rstp
 stp timer forward-delay 700
 stp timer max-age 1000
 stp bpdu-protection
 stp pathcost-standard dot1t
 stp global enable
#
interface Bridge-Aggregation1
 description 111901L020ESXI
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 4 30 226
#
interface Bridge-Aggregation2
 description 111901L060ESXI
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 4 30 226
#
interface Bridge-Aggregation3
 description 111901L050ESXI
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 4 30 226
#
interface Bridge-Aggregation4
 description ESXI 2022
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 4 30 226
 dhcp snooping trust
#
interface Bridge-Aggregation10
 description AGG-011-N2-3600
 port link-type trunk
```

```
 undo port trunk permit vlan 1
 port trunk permit vlan 4 30 226 901
 link-aggregation mode dynamic
 mad enable
 stp root-protection
 dhcp snooping trust
#
interface Bridge-Aggregation20
 description AGG-015-N2-3600
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 4 30 226 901
 link-aggregation mode dynamic
 mad enable
 stp root-protection
 dhcp snooping trust
#
interface Bridge-Aggregation30
 description AGG-019-N2-3600
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 4 30 226 901
 link-aggregation mode dynamic
 mad enable
 stp root-protection
 dhcp snooping trust
#
interface NULL0
#
interface LoopBack0
 description INT-LOOPBACK-BGP
 ip address 55.248.11.22 255.255.255.255
#
interface Vlan-interface4
 description INT-VLAN-DATA
 ip address 55.60.4.1 255.255.252.0
 ip forward-broadcast acl 3002
#
interface Vlan-interface5
 description INT-INTERCOWAN
 ip address 55.60.225.1 255.255.255.240
#
interface Vlan-interface17
 description INT-VLAN-EVASION-INTERNET
 ip address 192.168.1.4 255.255.255.0

#
interface Vlan-interface30
 description INT-VLAN-VOIX
 ip address 58.60.4.1 255.255.252.0
 dhcp select relay
 dhcp relay server-address 55.60.4.6
#
interface Vlan-interface224
 description INT-ACCES-ACCES-PART
 ip address 55.60.224.1 255.255.255.128
 packet-filter 3224 inbound
#
interface Vlan-interface226
 description INT-VLAN-IMPRIMANTES
 ip address 55.60.248.1 255.255.255.128
 packet-filter 3226 inbound
#
interface Vlan-interface230
 description INT-VLAN-GW-CETIAM
 ip address 58.230.3.153 255.255.255.248
#
interface Vlan-interface239
 description INT-VLAN-MGT-IPANEMA
 ip address 55.239.59.209 255.255.255.248
#
interface Vlan-interface901
 description INT-VLAN-ADMIN-RESEAU
 ip address 55.60.221.1 255.255.255.0


#
interface GigabitEthernet1/0/1
 port link-mode bridge
 description ROUTEUR-BTE
 port access vlan 5
 speed 100
 duplex full
 undo stp enable
 qos trust dscp
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 description MGT-IPANEMA
 port access vlan 239
 speed 100
 duplex full
 stp edged-port
#
interface GigabitEthernet1/0/3
 port link-mode bridge
 description EGFA AFFICHEUR TV 1
 port access vlan 224
 speed 100
 duplex full
 broadcast-suppression 20
 multicast-suppression 20
 stp edged-port
 loopback-detection enable vlan 1 to 4094
 loopback-detection action shutdown
#
interface GigabitEthernet1/0/4
 port link-mode bridge
 description EGFA DISTRIB TICKET PRISE VITALE
 port access vlan 224
 speed 100
 duplex full
 broadcast-suppression 20
 multicast-suppression 20
 stp edged-port
 loopback-detection enable vlan 1 to 4094
 loopback-detection action shutdown
#
interface GigabitEthernet1/0/5
 port link-mode bridge
 description W11190100SAV - ED 19
 port access vlan 4
 broadcast-suppression 20
 multicast-suppression 20
 stp edged-port
 loopback-detection enable vlan 1 to 4094
 loopback-detection action shutdown
#
interface GigabitEthernet1/0/6
 port link-mode bridge
 description 111901L030APP - ETH1 - EE03
 port access vlan 4
 broadcast-suppression 20
 multicast-suppression 20
 stp edged-port
 loopback-detection enable vlan 1 to 4094
 loopback-detection action shutdown
#
interface GigabitEthernet1/0/7
 port link-mode bridge
 description 111901L010AMBX - ED22
 port access vlan 4
```

```
 broadcast-suppression 20
 multicast-suppression 20
 stp edged-port
 loopback-detection enable vlan 1 to 4094
 loopback-detection action shutdown
#
interface GigabitEthernet1/0/8
 port link-mode bridge
 description 111901L090ESXI - EE11
 port access vlan 4
 broadcast-suppression 20
 multicast-suppression 20
 stp edged-port
 loopback-detection enable vlan 1 to 4094
 loopback-detection action shutdown
#
interface GigabitEthernet1/0/9
 port link-mode bridge
 shutdown
#
interface GigabitEthernet1/0/10
 port link-mode bridge
 shutdown
#
interface GigabitEthernet1/0/11
 port link-mode bridge
 shutdown
#
interface GigabitEthernet1/0/12
 port link-mode bridge
 shutdown
#
interface GigabitEthernet1/0/13
 port link-mode bridge
 shutdown
#
interface GigabitEthernet1/0/14
 port link-mode bridge
 shutdown
#
interface GigabitEthernet1/0/15
 port link-mode bridge
 shutdown
#
interface GigabitEthernet1/0/16
 port link-mode bridge
 shutdown
#
interface GigabitEthernet1/0/17
 port link-mode bridge
 shutdown
#
interface GigabitEthernet1/0/18
 port link-mode bridge
 description 111901L020ESXI - ETH1 - ED18
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 4 30 226
 broadcast-suppression 20
 multicast-suppression 20
 port link-aggregation group 1
#
interface GigabitEthernet1/0/19
 port link-mode bridge
 description 111901L060ESXI - ETH1 - ED13
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 4 30 226
 broadcast-suppression 20
 multicast-suppression 20
 port link-aggregation group 2
#
interface GigabitEthernet1/0/20
 port link-mode bridge
 description 111901L050ESXI - ETH1 - ED14
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 4 30 226
 broadcast-suppression 20
 multicast-suppression 20
 port link-aggregation group 3
#
interface GigabitEthernet1/0/21
 port link-mode bridge
 description 111901l030ESXI - ED 16
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 4 30 226
 broadcast-suppression 20
 multicast-suppression 20
 port link-aggregation group 4
 dhcp snooping trust
#
interface GigabitEthernet1/0/22
 port link-mode bridge
 description AGG-011-N2-3600–LIEN1
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 4 30 226 901
 broadcast-suppression 20
 multicast-suppression 20
 qos trust dscp
 port link-aggregation group 10
 dhcp snooping trust
#
interface GigabitEthernet1/0/23
 port link-mode bridge
 description AGG-015-N2-3600-LIEN1
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 4 30 226 901
 broadcast-suppression 20
 multicast-suppression 20
 qos trust dscp
 port link-aggregation group 20
 dhcp snooping trust
#
interface GigabitEthernet1/0/24
 port link-mode bridge
 description AGG-019-N2-3600-LIEN1
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 4 30 226 901
 broadcast-suppression 20
 multicast-suppression 20
 qos trust dscp
 port link-aggregation group 30
 dhcp snooping trust
#
interface GigabitEthernet2/0/1
 port link-mode bridge
 description ROUTEUR-NXO
 port access vlan 5
 speed 100
 duplex full
 undo stp enable
 qos trust dscp
#
interface GigabitEthernet2/0/2
 port link-mode bridge
 description GW1-CETIAM
 port access vlan 230
```

```
 broadcast-suppression 20
 multicast-suppression 20
 loopback-detection enable vlan 1 to 4094
 loopback-detection action shutdown
#
interface GigabitEthernet2/0/3
 port link-mode bridge
 description EGFA AFFICHEUR TV 2
 port access vlan 224
 speed 100
 duplex full
 broadcast-suppression 20
 multicast-suppression 20
 stp edged-port
 loopback-detection enable vlan 1 to 4094
 loopback-detection action shutdown
#
interface GigabitEthernet2/0/4
 port link-mode bridge
 description EGFA DISTRIB TICKET PRISE DISEO
 port access vlan 224
 speed 100
 duplex full
 broadcast-suppression 20
 multicast-suppression 20
 stp edged-port
 loopback-detection enable vlan 1 to 4094
 loopback-detection action shutdown
#
interface GigabitEthernet2/0/5
 port link-mode bridge
 description W11190100TIF - EE04
 port access vlan 4
 broadcast-suppression 20
 multicast-suppression 20
 stp edged-port
 loopback-detection enable vlan 1 to 4094
 loopback-detection action shutdown
#
interface GigabitEthernet2/0/6
 port link-mode bridge
 description 111901L030APP - ILO - EE01
 port access vlan 4
 broadcast-suppression 20
 multicast-suppression 20
 stp edged-port
 loopback-detection enable vlan 1 to 4094
 loopback-detection action shutdown
#
interface GigabitEthernet2/0/7
 port link-mode bridge
 description QUALIT-BOX
 port access vlan 5
 broadcast-suppression 20
 multicast-suppression 20
 stp edged-port
 loopback-detection enable vlan 1 to 4094
 loopback-detection action shutdown
#
interface GigabitEthernet2/0/8
 port link-mode bridge
 shutdown
#
interface GigabitEthernet2/0/9
 port link-mode bridge
 shutdown
#
interface GigabitEthernet2/0/10
 port link-mode bridge
 shutdown
#
interface GigabitEthernet2/0/11
 port link-mode bridge
 shutdown
#
interface GigabitEthernet2/0/12
 port link-mode bridge
 shutdown
#
interface GigabitEthernet2/0/13
 port link-mode bridge
 shutdown
#
interface GigabitEthernet2/0/14
 port link-mode bridge
 shutdown
#
interface GigabitEthernet2/0/15
 port link-mode bridge
 shutdown
#
interface GigabitEthernet2/0/16
 port link-mode bridge
 shutdown
#
interface GigabitEthernet2/0/17
 port link-mode bridge
 shutdown
#
interface GigabitEthernet2/0/18
 port link-mode bridge
 description 111901L020ESXI - ETH2
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 4 30 226
 broadcast-suppression 20
 multicast-suppression 20
 port link-aggregation group 1
#
interface GigabitEthernet2/0/19
 port link-mode bridge
 description 111901L060ESXI - ETH2 - ED12
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 4 30 226
 broadcast-suppression 20
 multicast-suppression 20
 port link-aggregation group 2
#
interface GigabitEthernet2/0/20
 port link-mode bridge
 description 111901L050ESXI - ETH2 - ED15
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 4 30 226
 broadcast-suppression 20
 multicast-suppression 20
 port link-aggregation group 3
#
interface GigabitEthernet2/0/21
 port link-mode bridge
 description 111901l030ESXI - ED 17
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 4 30 226
 broadcast-suppression 20
 multicast-suppression 20
 port link-aggregation group 4
 dhcp snooping trust
#
interface GigabitEthernet2/0/22
 port link-mode bridge
```

```
 description AGG-011-N2-3600-LIEN2
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 4 30 226 901
 broadcast-suppression 20
 multicast-suppression 20
 qos trust dscp
 port link-aggregation group 10
 dhcp snooping trust
#
interface GigabitEthernet2/0/23
 port link-mode bridge
 description AGG-015-N2-3600-LIEN2
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 4 30 226 901
 broadcast-suppression 20
 multicast-suppression 20
 qos trust dscp
 port link-aggregation group 20
 dhcp snooping trust
#
interface GigabitEthernet2/0/24
 port link-mode bridge
 description AGG-019-N2-3600-LIEN2
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 4 30 226 901
 broadcast-suppression 20
 multicast-suppression 20
 qos trust dscp
 port link-aggregation group 30
 dhcp snooping trust
#
interface M-GigabitEthernet0/0/0
 ip address dhcp-alloc
 ipv6 address auto
 ipv6 address dhcp-alloc
#
interface Ten-GigabitEthernet1/0/25
 port link-mode bridge
 shutdown
#
interface Ten-GigabitEthernet1/0/26
 port link-mode bridge
 shutdown
#
interface Ten-GigabitEthernet2/0/25
 port link-mode bridge
 shutdown
#
interface Ten-GigabitEthernet2/0/26
 port link-mode bridge
 shutdown
#
interface Ten-GigabitEthernet1/0/27
 description STACKAGE
#
interface Ten-GigabitEthernet1/0/28
 description STACKAGE
#
interface Ten-GigabitEthernet2/0/27
 description STACKAGE
#
interface Ten-GigabitEthernet2/0/28
 description STACKAGE
#
bgp 65005
 router-id 55.248.11.22
 timer keepalive 5 hold 15
 peer 55.60.225.8 as-number 65000
 peer 55.60.225.8 password cipher
$c$3$5gRQyxCo67T/9qyXRfamaABxf1gPW45ByXQvF58=
 peer 55.60.225.9 as-number 65003
 peer 55.60.225.9 password cipher
$c$3$jMjAACqffT8tPN30pT1UXNr2WVczVbZi4uvnQoE=
 #
 address-family ipv4 unicast
  preference 50 50 50
  import-route direct route-policy DIRECT-TO-BGP
  peer 55.60.225.8 enable
  peer 55.60.225.8 route-policy BGP-IN import
  peer 55.60.225.8 route-policy BGP-OUT-BTEL export
  peer 55.60.225.8 advertise-community
  peer 55.60.225.9 enable
  peer 55.60.225.9 route-policy BGP-IN import
  peer 55.60.225.9 route-policy BGP-OUT-NXO export
  peer 55.60.225.9 advertise-community
#
route-policy BGP-IN permit node 10
 if-match community name LP500
 apply community no-advertise additive
 apply local-preference 500
#
route-policy BGP-IN permit node 20
 if-match community name LP400
 apply community no-advertise additive
 apply local-preference 400
#
route-policy BGP-IN permit node 30
 if-match community name LP300
 apply community no-advertise additive
 apply local-preference 300
#
route-policy BGP-IN permit node 40
 if-match community name LP200
 apply community no-advertise additive
 apply local-preference 200
#
route-policy BGP-IN permit node 50
 if-match community name LP100
 apply community no-advertise additive
 apply local-preference 100
#
route-policy BGP-IN permit node 60
 if-match community name LP50
 apply community no-advertise additive
 apply local-preference 50
#
route-policy BGP-IN permit node 70
 if-match community name LP10
 apply community no-advertise additive
 apply local-preference 10
#
route-policy BGP-OUT-BTEL permit node 10
 apply community 65005:110
#
route-policy BGP-OUT-NXO permit node 10
 apply community 65005:210
#
route-policy DIRECT-TO-BGP permit node 10
 if-match ip address acl 2922
#
 ip community-list basic LP10 permit 65005:1
 ip community-list basic LP100 permit 65005:10
 ip community-list basic LP200 permit 65005:20
 ip community-list basic LP300 permit 65005:30
 ip community-list basic LP400 permit 65005:40
 ip community-list basic LP50 permit 65005:5
 ip community-list basic LP500 permit 65005:50
#
 scheduler logfile size 16
```

```
#
line class aux
 user-role network-admin
#
line class vty
 user-role network-operator
#
line aux 0 1
 authentication-mode scheme
 user-role network-admin
#
line vty 0 63
 authentication-mode scheme
 user-role network-admin
 user-role network-operator
 protocol inbound ssh
#
info-center loghost source Vlan-interface 901
info-center loghost slog-reseau-org.ramage.
#
 snmp-agent
 snmp-agent local-engineid
800063A2804CAEA3D300C200000001
 snmp-agent community write Snmp-Cp@m19 acl 2099
 snmp-agent community read TOKTBAT22! acl 2099
 snmp-agent sys-info contact Departement Informatique
 snmp-agent sys-info location Salle Info RDC
 snmp-agent sys-info version v2c v3
 snmp-agent trap enable arp
 snmp-agent trap enable radius
#
 ssh server enable
 ssh user admin service-type stelnet authentication-type
password
#
 ntp-service enable
 ntp-service unicast-server 55.223.10.8
#
acl number 2099
 description SNMP RW ACCESS POUR CNGR
 rule 0 permit source 55.60.0.0 0.0.255.255
 rule 1 permit source 55.18.0.0 0.0.255.255
 rule 2 permit source 55.245.0.0 0.0.255.255
 rule 3 permit source 55.244.0.0 0.0.255.255
#
acl number 2922
 rule 0 permit source 55.0.0.0 0.255.255.255
 rule 5 permit source 58.0.0.0 0.255.255.255
#
acl number 3002
 description WOL
 rule 1 permit udp source 55.245.0.0 0.0.255.255
#
acl number 3224
 description ACCESS-PART
 rule 10 permit ip source 55.60.224.0 0.0.0.127 destination
55.227.1.20 0 logging
 rule 10 comment AUTORISATION DIALOGUE VLAN 224 /
PARTENAIRES VIA CSH
 rule 20 permit ip source 55.60.224.0 0.0.0.127 destination
55.227.1.21 0 logging
 rule 20 comment AUTORISATION PROXY EGFA 1
 rule 30 permit ip source 55.60.224.0 0.0.0.127 destination
55.225.59.20 0 logging
 rule 30 comment AUTORISATION PROXY EGFA 2
 rule 40 permit ip source 55.60.224.0 0.0.0.127 destination
55.60.224.0 0.0.0.127 logging
 rule 40 comment AUTORISATION FLUX INTERNE VLAN
PARTENAIRES
 rule 50 permit ip source 55.60.224.0 0.0.0.127 destination
55.14.0.0 0.0.255.255 logging
 rule 50 comment AUTORISATION CSN CAEN
 rule 60 permit ip source 55.60.224.0 0.0.0.127 destination
55.60.0.0 0.0.255.255 logging
 rule 60 comment AUTORISATION CPAM VLAN 4
 rule 100 deny ip logging
 rule 100 comment INTERDICTION TOUT AUTRE FLUX
#
radius scheme system
 user-name-format without-domain
#
domain system
#
 domain default enable system
#
role name level-0
 description Predefined level-0 role
#
role name level-1
 description Predefined level-1 role
#
role name level-2
 description Predefined level-2 role
#
role name level-3
 description Predefined level-3 role
#
role name level-4
 description Predefined level-4 role
#
role name level-5
 description Predefined level-5 role
#
role name level-6
 description Predefined level-6 role
#
role name level-7
 description Predefined level-7 role
#
role name level-8
 description Predefined level-8 role
#
role name level-9
 description Predefined level-9 role
#
role name level-10
 description Predefined level-10 role
#
role name level-11
 description Predefined level-11 role
#
role name level-12
 description Predefined level-12 role
#
role name level-13
 description Predefined level-13 role
#
role name level-14
 description Predefined level-14 role
#
user-group system
#
local-user admin class manage
 password hash
$h$6$Mj9PWOvtT20Hogli$nmaIgHJEZ288nGykA2siw5Ii6r/ZrPa
BEdBi1jYVvvcDjvxE7HojwJxj6wYpaHnoTXMpLpe8r4SFRMY3yFW
LIQ==
 service-type https ssh terminal
 authorization-attribute user-role network-admin
 authorization-attribute user-role network-operator
#
Fin de la configuration du HP 5510
```

2.15.13.2 STACK 5130-24G-4SPF N2 siège (Niveau2)

```
#
version 7.1.070, Release 1309
#
 sysname 111-SW-SIEGE-N2-25-5130-MULTISERVICE
#
 clock timezone PARIS add 01:00:00
 clock summer-time PARIS 01:00:00 March last Sunday 02:00:00 October
last Sunday 02:00:00
#
voice vlan mac-address XXXX-XXXX-XXXXX mask ffff-ff00-0000 description
Postes Constructeur
voice-vlan mac-address 0080-9f00-0000 mask ffff-ff00-0000 description
Postes Alcatel
 voice-vlan mac-address 0008-7b00-0000 mask ffff-ff00-0000 description
Bornes IP-DECT Alcatel
 voice-vlan mac-address 0018-2700-0000 mask ffff-ff00-0000 description
Bornes IP-DECT Alcatel
 voice-vlan mac-address 0021-0400-0000 mask ffff-ff00-0000 description
Gigaset Alcatel
 voice-vlan mac-address 0026-8b00-0000 mask ffff-ff00-0000 description
Postes Alcatel
 voice-vlan mac-address 14b3-7000-0000 mask ffff-ff00-0000 description
Gigaset Alcatel
 voice-vlan mac-address 487a-5500-0000 mask ffff-ff00-0000 description
Postes Alcatel-2018
 voice-vlan mac-address 589e-c600-0000 mask ffff-ff00-0000 description
Gigaset Alcatel
 voice-vlan mac-address 7881-0200-0000 mask ffff-ff00-0000 description
Postes Alcatel
 voice-vlan mac-address 7c2f-8000-0000 mask ffff-ff00-0000 description
Gigaset Alcatel
#
irf domain 25
 irf mac-address persistent timer
 irf auto-update enable
 undo irf link-delay
 irf member 1 priority 32
 irf member 2 priority 30
 irf member 3 priority 28
 irf member 4 priority 26
#
 ip unreachables enable
 ip ttl-expires enable
#
 dhcp snooping enable
#
 dns domain cnamts.fr
 dns server 55.223.10.1
#
 lldp global enable
#
 loopback-detection global enable vlan 1 to 4094
 loopback-detection global action shutdown

#
 password-recovery enable
#
vlan 1
#
vlan 4
name VLAN-DATA
#
vlan 30
name VLAN-VOIX
#
vlan 901
name VLAN-ADMIN-RESEAU
#
irf-port 1/1
 port group interface Ten-GigabitEthernet1/0/27
#
irf-port 1/2
 port group interface Ten-GigabitEthernet1/0/28
#
irf-port 2/1
 port group interface Ten-GigabitEthernet2/0/27
#
irf-port 2/2
 port group interface Ten-GigabitEthernet2/0/28
#
irf-port 3/1
 port group interface Ten-GigabitEthernet3/0/27
#
irf-port 3/2
 port group interface Ten-GigabitEthernet3/0/28
#
irf-port 4/1
 port group interface Ten-GigabitEthernet4/0/27
#
irf-port 4/2
 port group interface Ten-GigabitEthernet4/0/28

#
 stp mode rstp
 stp bpdu-protection
 stp pathcost-standard dot1t
 stp global enable
#
interface Bridge-Aggregation10
 description AGG-010-5510-N3-RDC-NORD
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 4 30 901
 link-aggregation mode dynamic
 mad enable
 stp loop-protection
 dhcp snooping trust
#
interface NULL0
#
interface Vlan-interface901
 description ADMIN-RESEAU
 ip address 55.167.222.45 255.255.255.0
#
interface GigabitEthernet1/0/1
 description DATA-VOIP
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 4 30
 port trunk pvid vlan 4
 undo voice-vlan mode auto
 voice-vlan 30 enable
 broadcast-suppression 20
 multicast-suppression 20
 stp edged-port
 stp port bpdu-protection enable
 poe enable
 loopback-detection enable vlan 1 to 4094
 loopback-detection action shutdown
#
interface GigabitEthernet1/0/2
 description DATA-VOIP
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 4 30
 port trunk pvid vlan 4
 undo voice-vlan mode auto
 voice-vlan 30 enable
 broadcast-suppression 20
 multicast-suppression 20
 stp edged-port
```

```
 stp port bpdu-protection enable
 poe enable
 loopback-detection enable vlan 1 to 4094
 loopback-detection action shutdown
#
interface GigabitEthernet1/0/3
 description DATA-VOIP
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 4 30
 port trunk pvid vlan 4
 undo voice-vlan mode auto
 voice-vlan 30 enable
 broadcast-suppression 20
 multicast-suppression 20
 stp edged-port
 stp port bpdu-protection enable
 poe enable
 loopback-detection enable vlan 1 to 4094
 loopback-detection action shutdown
#
interface GigabitEthernet1/0/4
 description DATA-VOIP
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 4 30
 port trunk pvid vlan 4
 undo voice-vlan mode auto
 voice-vlan 30 enable
 broadcast-suppression 20
 multicast-suppression 20
 stp edged-port
 stp port bpdu-protection enable
 poe enable
 loopback-detection enable vlan 1 to 4094
 loopback-detection action shutdown
#
interface GigabitEthernet1/0/5
description DATA-VOIP
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 4 30
 port trunk pvid vlan 4
 undo voice-vlan mode auto
 voice-vlan 30 enable
 broadcast-suppression 20
 multicast-suppression 20
 stp edged-port
 stp port bpdu-protection enable
 poe enable
 loopback-detection enable vlan 1 to 4094
 loopback-detection action shutdown
#
interface GigabitEthernet1/0/6
description DATA-VOIP
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 4 30
 port trunk pvid vlan 4
 undo voice-vlan mode auto
 voice-vlan 30 enable
 broadcast-suppression 20
 multicast-suppression 20
 stp edged-port
 stp port bpdu-protection enable
 poe enable
 loopback-detection enable vlan 1 to 4094
 loopback-detection action shutdown
#
interface GigabitEthernet1/0/7
 description DATA-VOIP
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 4 30
 port trunk pvid vlan 4
 undo voice-vlan mode auto
 voice-vlan 30 enable
 broadcast-suppression 20
 multicast-suppression 20
 stp edged-port
 stp port bpdu-protection enable
 poe enable
 loopback-detection enable vlan 1 to 4094
 loopback-detection action shutdown
#
interface GigabitEthernet1/0/8
description DATA-VOIP
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 4 30
 port trunk pvid vlan 4
 undo voice-vlan mode auto
 voice-vlan 30 enable
 broadcast-suppression 20
 multicast-suppression 20
 stp edged-port
 stp port bpdu-protection enable
 poe enable
 loopback-detection enable vlan 1 to 4094
 loopback-detection action shutdown
#
interface GigabitEthernet1/0/9
 description DATA-VOIP
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 4 30
 port trunk pvid vlan 4
 undo voice-vlan mode auto
 voice-vlan 30 enable
 broadcast-suppression 20
 multicast-suppression 20
 stp edged-port
 stp port bpdu-protection enable
 poe enable
 loopback-detection enable vlan 1 to 4094
 loopback-detection action shutdown
#
interface GigabitEthernet1/0/10
 description DATA-VOIP
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 4 30
 port trunk pvid vlan 4
 undo voice-vlan mode auto
 voice-vlan 30 enable
 broadcast-suppression 20
 multicast-suppression 20
 stp edged-port
 stp port bpdu-protection enable
 poe enable
 loopback-detection enable vlan 1 to 4094
 loopback-detection action shutdown

#
interface GigabitEthernet1/0/11
description DATA-VOIP
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 4 30
 port trunk pvid vlan 4
 undo voice-vlan mode auto
 voice-vlan 30 enable
 broadcast-suppression 20
 multicast-suppression 20
 stp edged-port
 stp port bpdu-protection enable
```

```
 poe enable
 loopback-detection enable vlan 1 to 4094
 loopback-detection action shutdown
#
interface GigabitEthernet1/0/12
 description DATA-VOIP
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 4 30
 port trunk pvid vlan 4
 undo voice-vlan mode auto
 voice-vlan 30 enable
 broadcast-suppression 20
 multicast-suppression 20
 stp edged-port
 stp port bpdu-protection enable
 poe enable
 loopback-detection enable vlan 1 to 4094
 loopback-detection action shutdown
#
interface GigabitEthernet1/0/13
description DATA-VOIP
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 4 30
 port trunk pvid vlan 4
 undo voice-vlan mode auto
 voice-vlan 30 enable
 broadcast-suppression 20
 multicast-suppression 20
 stp edged-port
 stp port bpdu-protection enable
 poe enable
 loopback-detection enable vlan 1 to 4094
 loopback-detection action shutdown
#
interface GigabitEthernet1/0/14
 description DATA-VOIP
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 4 30
 port trunk pvid vlan 4
 undo voice-vlan mode auto
 voice-vlan 30 enable
 broadcast-suppression 20
 multicast-suppression 20
 stp edged-port
 stp port bpdu-protection enable
 poe enable
 loopback-detection enable vlan 1 to 4094
 loopback-detection action shutdown
#
interface GigabitEthernet1/0/15
description DATA-VOIP
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 4 30
 port trunk pvid vlan 4
 undo voice-vlan mode auto
 voice-vlan 30 enable
 broadcast-suppression 20
 multicast-suppression 20
 stp edged-port
 stp port bpdu-protection enable
 poe enable
 loopback-detection enable vlan 1 to 4094
 loopback-detection action shutdown
#
interface GigabitEthernet1/0/16
description DATA-VOIP
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 4 30
 port trunk pvid vlan 4
 undo voice-vlan mode auto
 voice-vlan 30 enable
 broadcast-suppression 20
 multicast-suppression 20
 stp edged-port
 stp port bpdu-protection enable
 poe enable
 loopback-detection enable vlan 1 to 4094
 loopback-detection action shutdown
#
interface GigabitEthernet1/0/17
description DATA-VOIP
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 4 30
 port trunk pvid vlan 4
 undo voice-vlan mode auto
 voice-vlan 30 enable
 broadcast-suppression 20
 multicast-suppression 20
 stp edged-port
 stp port bpdu-protection enable
 poe enable
 loopback-detection enable vlan 1 to 4094
 loopback-detection action shutdown
#
interface GigabitEthernet1/0/18
 description PC & Tel
port link-type trunk
undo port trunk permit vlan 1
port trunk permit vlan 4 30
port trunk pvid vlan 4
undo voice-vlan mode auto
voice-vlan 30 enable
broadcast-suppression 20
multicast-suppression 20
stp edged-port
stp port bpdu-protection enable
poe enable
loopback-detection enable vlan 1 to 4094
loopback-detection action shutdown
#
interface GigabitEthernet1/0/19
description PC & Tel
port link-type trunk
undo port trunk permit vlan 1
port trunk permit vlan 4 30
port trunk pvid vlan 4
undo voice-vlan mode auto
voice-vlan 30 enable
broadcast-suppression 20
multicast-suppression 20
stp edged-port
stp port bpdu-protection enable
poe enable
loopback-detection enable vlan 1 to 4094
loopback-detection action shutdown
#
interface GigabitEthernet1/0/20
 description PC & Tel
port link-type trunk
undo port trunk permit vlan 1
port trunk permit vlan 4 30
port trunk pvid vlan 4
undo voice-vlan mode auto
voice-vlan 30 enable
broadcast-suppression 20
multicast-suppression 20
stp edged-port
stp port bpdu-protection enable
poe enable
loopback-detection enable vlan 1 to 4094
```

```
loopback-detection action shutdown
#
interface GigabitEthernet1/0/21
description PC & Tel
port link-type trunk
undo port trunk permit vlan 1
port trunk permit vlan 4 30
port trunk pvid vlan 4
undo voice-vlan mode auto
voice-vlan 30 enable
broadcast-suppression 20
multicast-suppression 20
stp edged-port
stp port bpdu-protection enable
poe enable
loopback-detection enable vlan 1 to 4094
loopback-detection action shutdown
#
interface GigabitEthernet1/0/22
 description PC & Tel
port link-type trunk
undo port trunk permit vlan 1
port trunk permit vlan 4 30
port trunk pvid vlan 4
undo voice-vlan mode auto
voice-vlan 30 enable
broadcast-suppression 20
multicast-suppression 20
stp edged-port
stp port bpdu-protection enable
poe enable
loopback-detection enable vlan 1 to 4094
loopback-detection action shutdown
#
interface GigabitEthernet1/0/23
description PC & Tel
port link-type trunk
undo port trunk permit vlan 1
port trunk permit vlan 4 30
port trunk pvid vlan 4
undo voice-vlan mode auto
voice-vlan 30 enable
broadcast-suppression 20
multicast-suppression 20
stp edged-port
stp port bpdu-protection enable
poe enable
loopback-detection enable vlan 1 to 4094
loopback-detection action shutdown
#
interface GigabitEthernet1/0/24
 description PC & Tel
port link-type trunk
undo port trunk permit vlan 1
port trunk permit vlan 4 30
port trunk pvid vlan 4
undo voice-vlan mode auto
voice-vlan 30 enable
broadcast-suppression 20
multicast-suppression 20
stp edged-port
stp port bpdu-protection enable
poe enable
loopback-detection enable vlan 1 to 4094
loopback-detection action shutdown
#
.
.
.
#
interface GigabitEthernet3/0/24
 description PC & Tel
port link-type trunk
undo port trunk permit vlan 1
port trunk permit vlan 4 30
port trunk pvid vlan 4
undo voice-vlan mode auto
voice-vlan 30 enable
broadcast-suppression 20
multicast-suppression 20
stp edged-port
stp port bpdu-protection enable
poe enable
loopback-detection enable vlan 1 to 4094
loopback-detection action shutdown
#
interface GigabitEthernet4/0/1
port link-mode bridge
port access vlan 4
 broadcast-suppression 20
 multicast-suppression 20
 stp edged-port
 loopback-detection enable vlan 1 to 4094
 loopback-detection action shutdown
#
interface GigabitEthernet4/0/2
port link-mode bridge
port access vlan 4
 broadcast-suppression 20
 multicast-suppression 20
 stp edged-port
 loopback-detection enable vlan 1 to 4094
 loopback-detection action shutdown
#
interface GigabitEthernet4/0/3
port link-mode bridge
port access vlan 4
 broadcast-suppression 20
 multicast-suppression 20
 stp edged-port
 loopback-detection enable vlan 1 to 4094
 loopback-detection action shutdown
#
interface GigabitEthernet4/0/4
port link-mode bridge
port access vlan 4
 broadcast-suppression 20
 multicast-suppression 20
 stp edged-port
 loopback-detection enable vlan 1 to 4094
 loopback-detection action shutdown
#
interface GigabitEthernet4/0/5
 port link-mode bridge
 port access vlan 4
 broadcast-suppression 20
 multicast-suppression 20
 stp edged-port
 loopback-detection enable vlan 1 to 4094
 loopback-detection action shutdown
#
interface GigabitEthernet4/0/6
 port link-mode bridge
 port access vlan 4
 broadcast-suppression 20
 multicast-suppression 20
 stp edged-port
 loopback-detection enable vlan 1 to 4094
 loopback-detection action shutdown
#
interface GigabitEthernet4/0/7
 port link-mode bridge
 port access vlan 4
 broadcast-suppression 20
 multicast-suppression 20
 stp edged-port
```

```
 loopback-detection enable vlan 1 to 4094
 loopback-detection action shutdown
#
interface GigabitEthernet4/0/8
 port access vlan 4
 broadcast-suppression 20
 multicast-suppression 20
 stp edged-port
 loopback-detection enable vlan 1 to 4094
 loopback-detection action shutdown
#
interface GigabitEthernet4/0/9
 port access vlan 4
 broadcast-suppression 20
 multicast-suppression 20
 stp edged-port
 loopback-detection enable vlan 1 to 4094
 loopback-detection action shutdown
#
interface GigabitEthernet4/0/10
 port access vlan 4
 broadcast-suppression 20
 multicast-suppression 20
 stp edged-port
 loopback-detection enable vlan 1 to 4094
 loopback-detection action shutdown
#
interface GigabitEthernet4/0/11
 port link-mode bridge
port access vlan 4
 broadcast-suppression 20
 multicast-suppression 20
 stp edged-port
 loopback-detection enable vlan 1 to 4094
 loopback-detection action shutdown
#
interface GigabitEthernet4/0/12
 port link-mode bridge
 port access vlan 4
 broadcast-suppression 20
 multicast-suppression 20
 stp edged-port
 loopback-detection enable vlan 1 to 4094
 loopback-detection action shutdown
#
interface GigabitEthernet4/0/13
 port link-mode bridge
port access vlan 4
 broadcast-suppression 20
 multicast-suppression 20
 stp edged-port
 loopback-detection enable vlan 1 to 4094
 loopback-detection action shutdown
#
interface GigabitEthernet4/0/14
 port link-mode bridge
 port access vlan 4
 broadcast-suppression 20
 multicast-suppression 20
 stp edged-port
 loopback-detection enable vlan 1 to 4094
 loopback-detection action shutdown
#
interface GigabitEthernet4/0/15
 port link-mode bridge
 port access vlan 4
 broadcast-suppression 20
 multicast-suppression 20
 stp edged-port
 loopback-detection enable vlan 1 to 4094
 loopback-detection action shutdown
#
interface GigabitEthernet4/0/16
 port link-mode bridge
 port access vlan 4
 broadcast-suppression 20
 multicast-suppression 20
 stp edged-port
 loopback-detection enable vlan 1 to 4094
 loopback-detection action shutdown
#
interface GigabitEthernet4/0/17
 port link-mode bridge
 port access vlan 4
 broadcast-suppression 20
 multicast-suppression 20
 stp edged-port
 loopback-detection enable vlan 1 to 4094
 loopback-detection action shutdown
#
interface GigabitEthernet4/0/18
 port link-mode bridge
port access vlan 4
 broadcast-suppression 20
 multicast-suppression 20
 stp edged-port
 loopback-detection enable vlan 1 to 4094
 loopback-detection action shutdown
#
interface GigabitEthernet4/0/19
 port link-mode bridge
 port access vlan 4
 broadcast-suppression 20
 multicast-suppression 20
 stp edged-port
 loopback-detection enable vlan 1 to 4094
 loopback-detection action shutdown
#
interface GigabitEthernet4/0/20
 port link-mode bridge
port access vlan 4
 broadcast-suppression 20
 multicast-suppression 20
 stp edged-port
 loopback-detection enable vlan 1 to 4094
 loopback-detection action shutdown
#
interface GigabitEthernet4/0/21
 port link-mode bridge
port access vlan 4
 broadcast-suppression 20
 multicast-suppression 20
 stp edged-port
 loopback-detection enable vlan 1 to 4094
 loopback-detection action shutdown
#
interface GigabitEthernet4/0/22
 port link-mode bridge
port access vlan 4
 broadcast-suppression 20
 multicast-suppression 20
 stp edged-port
 loopback-detection enable vlan 1 to 4094
 loopback-detection action shutdown
#
interface GigabitEthernet4/0/23
 port link-mode bridge
port access vlan 4
 broadcast-suppression 20
 multicast-suppression 20
 stp edged-port

 loopback-detection enable vlan 1 to 4094
 loopback-detection action shutdown
#
interface GigabitEthernet4/0/24
```

```
 port link-mode bridge
port access vlan 4
 broadcast-suppression 20
 multicast-suppression 20
 stp edged-port
 loopback-detection enable vlan 1 to 4094
 loopback-detection action shutdown
#
interface Ten-GigabitEthernet1/0/25
description AGG-010-5510-N3-RDC-NORD-LIEN1
port link-type trunk
undo port trunk permit vlan 1
port trunk permit vlan 4 30 901
port link-aggregation group 1
#
interface Ten-GigabitEthernet1/0/26
#
interface Ten-GigabitEthernet2/0/25
description AGG-010-5510-N3-RDC-NORD- LIEN2
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 4 30 901
 port link-aggregation group 1
#
interface Ten-GigabitEthernet2/0/26
#
interface Ten-GigabitEthernet3/0/25
#
interface Ten-GigabitEthernet3/0/26
#
interface Ten-GigabitEthernet4/0/25
#
interface Ten-GigabitEthernet4/0/26
#
interface Ten-GigabitEthernet1/0/27
 description STACKAGE
#
interface Ten-GigabitEthernet1/0/28
 description Stackage
#
interface Ten-GigabitEthernet2/0/27
 description STACKAGE
#
interface Ten-GigabitEthernet2/0/28
 description STACKAGE
#
interface Ten-GigabitEthernet3/0/27
 description STACKAGE
#
interface Ten-GigabitEthernet3/0/28
 description STACKAGE
#
interface Ten-GigabitEthernet4/0/27
 description STACKAGE
#
interface Ten-GigabitEthernet4/0/28
 description STACKAGE
#
 scheduler logfile size 16
#
line class aux
 user-role network-admin
#
line class vty
 user-role network-operator
#
line aux 0 3
 authentication-mode scheme
 user-role network-admin
#
line vty 0 63
 authentication-mode scheme
 user-role network-operator
 protocol inbound ssh
#
 ip route-static 0.0.0.0 0 55.144.221.1
#
info-center loghost source Vlan-interface 901
info-center loghost slog-reseau-org.ramage
#
 snmp-agent
 snmp-agent local-engineid 800063A28040B93C7B152900000001
 snmp-agent community read TOKTBAT22! acl 2099
 snmp-agent community write xxx acl 2099
 snmp-agent sys-info contact Francois PIGNON
 snmp-agent sys-info location Salle Serveurs 3eme etage
 snmp-agent sys-info version v2c v3
 snmp-agent target-host trap address udp-domain PARIS-
CAL.smarts.cnamts.fr params securityname TOKTBAT22! v2c
 snmp-agent trap enable arp
 snmp-agent trap enable radius
 snmp-agent trap enable stp
#
 ssh server enable
undo ssh server compatible-ssh1x enable
 ssh user admin service-type stelnet authentication-type password
#
 ntp-service enable
 ntp-service unicast-server 55.223.10.8
#
acl number 2099
 description SNMP RW ACCESS POUR CNGR
 rule 0 permit source 55.144.0.0 0.0.255.255
 rule 1 permit source 55.18.0.0 0.0.255.255
 rule 2 permit source 55.245.4.0 0.0.0.255
 rule 3 permit source 55.244.0.0 0.0.255.255
#
radius scheme system
 user-name-format without-domain
#
domain system
#
 domain default enable system
#
role name level-0
 description Predefined level-0 role
#
role name level-1
 description Predefined level-1 role
#
role name level-2
 description Predefined level-2 role
#
role name level-3
 description Predefined level-3 role
#
role name level-4
 description Predefined level-4 role
#
role name level-5
 description Predefined level-5 role
#
role name level-6
 description Predefined level-6 role
#
role name level-7
 description Predefined level-7 role

#
role name level-8
 description Predefined level-8 role
#
role name level-9
 description Predefined level-9 role
#
role name level-10
```

```
 description Predefined level-10 role
#
role name level-11
 description Predefined level-11 role
#
role name level-12
 description Predefined level-12 role
#
role name level-13
 description Predefined level-13 role
#
role name level-14
 description Predefined level-14 role
#
user-group system
#
local-user admin class manage
 password hash
$h$6$1SAgEH0R/54bmaML$h+o3OyfmB4m4SiiN4+bFn4gxFCX98ZLTq3oEa
NabYEQTgro5lJpRMM2DiL+i5JTeGnB9UEjkxZnmzkeyTmAsFg==
 service-type ssh terminal
 authorization-attribute user-role network-admin
 authorization-attribute user-role network-operator
#
public-key peer 55.244.111.45
 public-key-code begin

30820120300D06092A864886F70D0101010500038201 0D0030820108028
2010100CBC968F2
E881F38ED7AA40E410342A5A1EC6B5112018D615D183105D1890048319
462E8CF4D529E04C

355503D8F8F1621E10A156D494E76ABFBA56930BDA4EFD06AB7C941B31
F78CF2CA0C23D303

AE9813EC865C2BC2F5FD71309042F2258E5D496D88FA1CF185AA8BAC12
910F7F6EF0AE6804

8553950989754B86C11AD6A4F8FEA5D5A20111451E89F94172A30BDA91
CE8661445EA09E7C

08C8E9DE4499245ABAE04A39E1747BEA7E4C49B8E36FE5C7E337EB42A96
D1A769D0CE48842

65F8383B7BBBC4A22F53BCA61FC1E11B8A602D767BA7B31B554250C08F
1C3054C1717075EE

A56E2BD00457F4E924A3F1E8D383E755A848C4206BE92BE287B4603D6A7
D020123
 public-key-code end
 peer-public-key end
#
```

Fin de la configuration du HP 5130-24G N2

3 GUIDE DE CONFIGURATION DES HP 3600-V2IMPORTANT : ORDRE DE CONFIGURATION SUGGERE.

Nous conseillons de configurer les HP 3600-v2 dans l'ordre suivant.

1/ Commencer par vérifier la version du switch et appliquer la mise à jour si nécessaire

⇨ Voir sur le site du DR

2/ Si un stackage est envisagé, configurer la partie stackage

3/ Configurer les accès (SSH…) et bannière

4/ Configurer le Spanning-tree

5/ Configurer SNMP / SYSLOG

6/ Configurer les VLAN et les interfaces VLAN

7/ Configurer les interfaces (access, trunk)

8/ Configurer les routages (sur les switches niveau 2)

9/ Configurer la partie DHCP (relais et snooping)

10/ Configurer NTP, LLDP, WAKE ON LAN

Dans la suite du document, la plupart des lignes ou blocs de lignes de commandes peuvent être copiés-collés. Dans ces blocs de commandes :

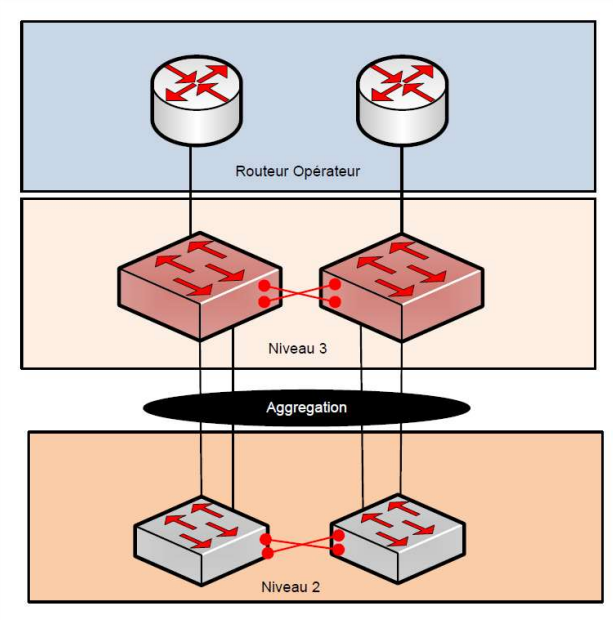
- les paramètres à personnaliser sont en rouge
- les explications sur certaines commandes sont en vert
- les « commentaires » du switch en réponse aux commandes sont en bleu et en italique
- les paramètres optionnels sont mis entre crochet (ex : [speed 100])

Toute la suite du document (après l'introduction de présentation) est rédigée dans le même ordre pour faciliter la compréhension et la configuration.

3.2 DIFFERENCE ENTRE SWITCH NIVEAU 2 ET SWITCH NIVEAU 3

Un **switch niveau 2** établit et met à jour dynamiquement une table d'adresses MAC, qui lui indique sur quels ports diriger les trames destinées à une adresse MAC donnée. Un switch niveau 2 ne fait que de la commutation au niveau des adresses MAC (niveau 2). Si vous créez plusieurs VLAN, chaque VLAN sera isolé.

Un **switch niveau 3** permet en plus d'assigner une adresse IP par Vlan et de pouvoir faire communiquer des machines connectées à différents vlans. Il réalise ainsi le routage Inter Vlan. Il permet aussi de mettre en œuvre les politiques de sécurité entre les vlan via des ACL (access list). Enfin, Il est connecté aux routeurs opérateurs pour accéder aux réseaux externes à l'organisme (réseau public (internet), réseau csh (applications nationales)…).



3.3 LA GAMME HP A3600 V2

Ne pose aucun problème pour le WoL. Il peut donc être utilisé :
- au niveau 2
- et à l'extrémité dans tout site ayant un autre modèle de switch N3, HP ou Cisco (siège de CPAM, MEDICAL…)
- au niveau 3 et en tête de réseau dans toutes les agences de type CP

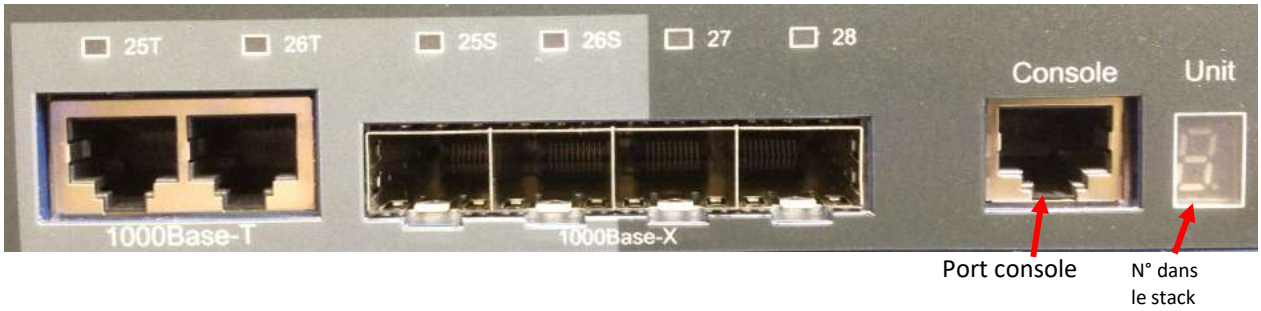
Il existe 2 modèles :
- 3600-24-EI v2 PoE
- 3600-48-EI v2 PoE

Photo d'un 3600-24 v2 PoE :



24 ports 10/100 Mb/s RJ45 PoE ou non — 2 ports 10/100/1000 — 4 ports SFP pour SPF SX : 1000 Mb/s Fibre optique, SFP TX : 1000 Mb/s Cuivre RJ45 Ou stackage

Zoom sur les ports 25 /26 et SFP :



L'entourage gris clair signifie que les ports 25T, 26T, 25S et 26S sont des ports « combo » deux à deux : si le port 25T est utilisé, le port 25S est inhibé ; idem pour les ports 26T et 26S.

- Les ports 25T et 26T :
  - au siège : serviront à la connexion avec les fédérateurs en cuivre 10/100/1000 (pour le premier et le dernier de chaque stack).
  - en CP : peuvent servir à la connexion de serveurs en 10/100/1000 ou à l'interconnexion en cuivre d'autres switches situés dans d'autres répartiteurs. Si aucun port gigabit n'est nécessaire dans ce CP, ces ports peuvent aussi servir au stackage via des cordons de brassage cat 6 lorsque les switches sont éloignés (voir plus loin).

- Les ports 25S et 26S :
  - au siège : serviront à la connexion avec les fédérateurs en fibre (pré-câblage local fibre) ➔ il faut prévoir 2 SPF SX par stack. Dans ce cas, les ports 25T et 26T sont inhibés.
  - En CP, ces ports peuvent servir au stackage via des jarretières en fibre optique lorsque les switches sont éloignés (voir plus loin).

- **Ports 27 et 28 : serviront exclusivement au stackage (voir § 3).**

Pour un 3600-48, les ports respectifs sont 49(T/S), 50(T/S), 51 et 52 :



- Les ports 49T et 50T :
  - au siège : serviront à la connexion avec les fédérateurs en cuivre 10/100/1000 (pour le premier et le dernier de chaque stack).
  - en CP : peuvent servir à la connexion de serveurs en 10/100/1000 ou à l'interconnexion en cuivre d'autres switches situés dans d'autres répartiteurs. Si aucun port gigabit n'est nécessaire dans ce CP, ces ports peuvent aussi servir au stackage via des cordons de brassage cat 6 lorsque les switches sont éloignés (voir plus loin).

- Les ports 49S et 50S :
  - au siège : serviront à la connexion avec les fédérateurs en fibre (pré-câblage local fibre) ➔ il faut prévoir 2 SPF SX par stack. Dans ce cas, les ports 49T et 50T sont inhibés.
  - en CP, ces ports peuvent servir au stackage via des jarretières en fibre optique lorsque les switches sont éloignés (voir plus loin).

- **Ports 51 et 52 : serviront exclusivement au stackage (voir § 3).**

3.3.1 Prise en main

La connexion aux switches se fait via le câble bleu fourni dans le carton d'emballage du switch que l'on connecte sur le port série d'un PC. Ensuite, la prise en main se fait via « Putty » ou « Hyperterminal » par exemple.

Pour passer les commandes, il faut être en mode « configuration ». Pour cela, il faut taper « system-view » au prompt de base (>). Le prompt change pour un # . C'est l'équivalent du « conf t » de Cisco, et comme pour Cisco :

```
<sw-buro-86>system-view
System View: return to User View with Ctrl+Z.
```

Le Ctrl+Z permet de revenir au prompt initial hors mode configuration.
Le « ? » permet de visualiser les commandes disponibles à l'endroit où on se trouve.
La touche tabulation permet de compléter automatiquement une commande commencée.
La commande « save » permet de sauvegarder la configuration (« write memory » de Cisco – voir § « Sauvegarde »).

Dans la suite du document, par défaut les commandes à passer sont en mode de configuration « system-view » (prompt []). Sinon, le symbole <> placé devant la commande signifiera qu'il faut revenir au prompt initial (hors configuration). Pour revenir à ce prompt initial, tapez CTRL+z.

3.3.2 Commandes de base

<> = Mode sans privilège (Prompt de base)
[] = Mode System-View

<>display current-configuration (di cu) : voir la configuration courante

<>display interface brief : voir le status des interfaces

<>display interface ethernet… : informations importantes sur les interfaces (erreurs, CRC…)

[]display lldp neighbor-information […] voir les voisins lldp

[]display gvrp […] voir la diffusion des vlans

[]display ntp-service status voir le serveur ntp

[]display cpu history voir le pourcentage de cpu utilisé

<>dir [/all ou slotN#flash:] voir les fichiers de la flash

<>schedule reboot at 00:00 : rebooter le switch à une heure donnée

<>display vlan [static) ou [dynamic]

[]interface range int eth1/0/1 to eth1/0/24 eth2/0/1 to eth2/0/24 eth3/0/1 to eth3/0/24 etc…. : configuration de groupes d'interfaces.

Limites : il faut entrer les commandes une à une (le copier-coller de plusieurs lignes ne fonctionne pas)

<>display counters inbound interface : statistiques sur les interfaces en entrée

<>display counters outbound interface : statistiques sur les interfaces en sortie

<>display logbuffer : affiche les logs

Les commandes « reset counters interface » et « reset logbuffer » remettent les compteurs ci-dessus à zéro.

<>display device manuinfo : affichage d'information **dont le n° de série**

En configuration sur une interface, la commande « default » permet de remettre l'interface en configuration usine.

<> ou [] save : sauvegarde de la configuration (switch / stack) avec demande de confirmation

<> ou [] save force : Forcer une sauvegarde, sans avoir à répondre « yes », aux questions intermédiaires

[sur l'interface] shutdown : éteindre une interface

[sur l'interface] undo shutdown : allumer une interface

[sur l'interface] poe enable : activer le PoE sur une interface

[sur l'interface] undo poe enable : désactiver le PoE sur une interface

3.3.3 Alias

Permet de renommer des commandes HP "à la mode Cisco". Exemple : display ←→ show :

System-view
#
command-alias mapping display show

Suppression:

System-view
#
undo command-alias show

Il semble qu'un alias ne soit pas complété automatiquement lorsqu'on « tabule » (touche « TAB »)…

3.4 STACKAGE (IRF)

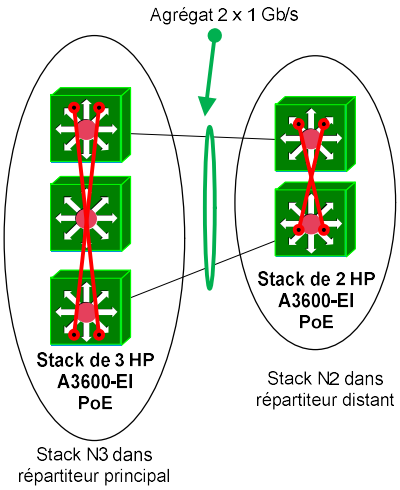
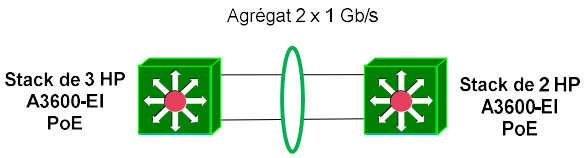
3.4.1 Présentation



A quoi ça sert ?

Le stackage est une technique propriétaire permettant de transformer plusieurs switches physiques en un seul switch logique en utilisant des éléments de connectique particuliers (fournis par le DR avec les switches lorsqu'un stackage est prévu). La configuration globale est alors commune et les interfaces s'additionnent.

Il est donc possible de réaliser des agrégats entre des groupes de switches stackés. Exemple :

Ainsi :	Equivaut à :
	

3600 24 ports :

Ports de stackage par défaut via câbles spécifiques fournis : 27 et 28 en croisant les câbles.

Lorsqu'il sera envisagé de monter un stack entre des 3600 situés dans des répartiteurs différents, on pourra construire le stack avec au choix les interfaces :

- 25T et 26T via des rocades en cuivre
- 25S et 26S via des rocades en fibre optique

3600 48 ports :

Ports de stackage par défaut via câbles spécifiques fournis : 51 et 52 en croisant les câbles.

Lorsqu'il sera envisagé de monter un stack entre des 3600 situés dans des répartiteurs différents, on pourra construire le stack avec au choix les interfaces :

- 49T et 50T via des rocades en cuivre
- 49S et 50S via des rocades en fibre optique

Préconisation DR : les 3600 doivent être stackés en priorité en utilisant les câbles de stackage fournis et les ports 27 et 28 pour les 3600 24 ports, 51 et 52 pour les 48 ports :



Le stack ainsi constitué est un vrai stack : les switches stackés entre eux sont vus comme **un seul switch logique** : toute la configuration est commune, le stack n'ayant qu'une seule adresse IP.

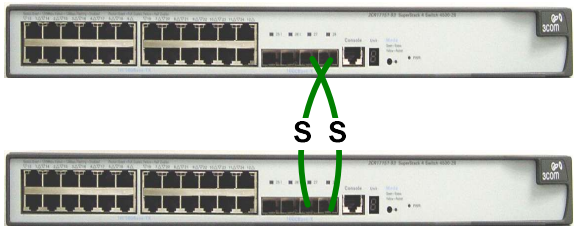
On peut stacker des 24 ports avec des 48 ports… **MAIS PAS des 3600-v2 avec des 5120, 5130 ou des 5500.**

Limites recommandées par les experts HP : 6 au maximum. Au-delà, le temps nécessaire au redémarrage d'un stack peut être (trop) long. Cependant, nous avons fait des tests au DR qui n'ont pas montré de problèmes… Il est donc possible de stacker jusqu'à 9 switches 3600 lorsque cela est nécessaire. Il faut dans ce cas veiller à agréger plusieurs liens vers les fédérateurs.

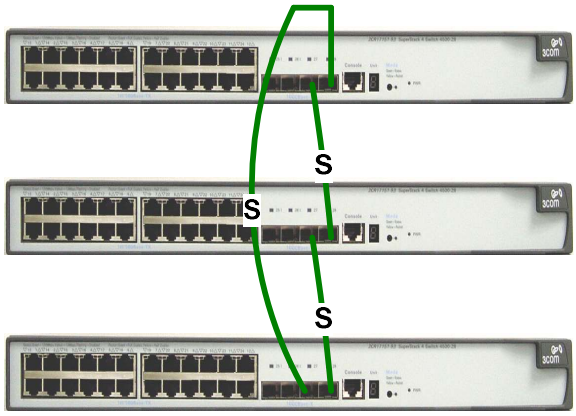
La version doit être identique sur les switches d'une même stack.

➔ CAS du STACKAGE DE 2 switches HP A3600 – exemple avec les ports 27 et 28 :

- 3600-24 : port 27 du 1er sur 28 du 2ème et 28 du 1er sur 27 du 2ème
- 3600-48 : port 51 du 1er sur 52 du 2ème et 52 du 1er sur 51 du 2ème



➔ CAS DU STACKAGE de n switches HP A3600 – exemple avec les ports 27 et 28 - : prévoir n Kits de stackage – exemple avec n=3 :



Ne pas s'occuper du nom (sysname = « HP » par défaut) des switches avant le stackage car ils doivent être identiques sur tous les switches que l'on veut stacker ensembles. Mieux vaut donc laisser le nom par défaut (« HP »). Le changement de nom pourra être fait une seule fois pour le stack (voir plus bas § « Définir le nom d'un switch ou d'un stack »).

3.4.2 Configuration

Un stack ne peut être construit qu'avec des switches en configuration usine. Pour ajouter un switch dans un stack, il faut qu'il soit en configuration usine (voir § « remettre en configuration usine).

Ne pas connecter les câbles. Il faut d'abord configurer les switches que l'on veut stacker UN à UN.

Switch N° 1 :

Commandes en ligne à appliquer sur le commutateur « Master » (le premier). On paramétrera par défaut l'unité 1 en tant que master (priorité maximum). Par défaut, le switch est member 1 et priorité 1, on va passer la priorité à 32 pour le forcer à être maître :

```
<>System-view
#                                  | NE GENERE PAS DE COUPURE si fait après un stackage déjà opérationnel
irf domain YY                      | remplacer YY par la fin de l'@IP du stack – ex : 11 pour 55.X.221.11
irf member 1 priority 32           | TOUJOURS 32 pour le premier
#
interface range GigabitEthernet1/0/27 to GigabitEthernet1/0/28
 shutdown
 quit
#
irf-port 1/1
 port group interface GigabitEthernet 1/0/27
 quit
#
irf-port 1/2
 port group interface GigabitEthernet 1/0/28
 quit
#
irf-port-configuration active
#
interface range GigabitEthernet1/0/27 to GigabitEthernet1/0/28
 undo shutdown
 description STACKAGE
 quit
#
<>save force
```

Switch N° 2 :

```
<>system-view
#
irf domain YY                      | remplacer YY par le même nombre que pour le 1er switch (dans notre ex : 11)
irf member 1 renumber 2            ➔ répondre « Y »
#
<>Save force
<>reboot                           ➔ répondre « Y »
```

Suite au redémarrage :

```
<>system-view
#                                  | NE GENERE PAS DE COUPURE si fait après un stackage déjà opérationnel
irf member 2 priority 30           | priorité du précédent -2 (ici 32 – 2 = 30)
interface range GigabitEthernet2/0/27 to GigabitEthernet2/0/28
 shutdown
 quit
#
irf-port 2/1
 port group interface GigabitEthernet 2/0/27
 quit
#
irf-port 2/2
 port group interface GigabitEthernet 2/0/28
 quit
#
irf-port-configuration active
#
```

```
interface range GigabitEthernet2/0/27 to GigabitEthernet2/0/28
 undo shutdown
 description STACKAGE
 quit
```

PUIS :

```
<>Save force
```

Switch N :

```
<>system-view
#                                  | NE GENERE PAS DE COUPURE si fait après un stackage déjà opérationnel
irf domain YY                      | remplacer YY par le même nombre que pour le 1er switch (dans notre ex : 11)
irf member 1 renumber N            ➔ répondre « Y»
#
<>Save force
<>reboot                           ➔ répondre « Y »
```

Suite au redémarrage:

```
<>system-view
#                                  | NE GENERE PAS DE COUPURE si fait après un stackage déjà opérationnel
irf member N priority YY           | priorité du précédent -2 (ex : si N=3 ici ➔ priorité YY = 32 - 2 - 2 = 28)
interface range GigabitEthernetN/0/27 to GigabitEthernetN/0/28
 shutdown
 quit
  #
  irf-port N/1
   port group interface GigabitEthernet N/0/27
   quit
  #
  irf-port N/2
   port group interface GigabitEthernet N/0/28
   quit
  #
  irf-port-configuration active
  #
  interface range GigabitEthernetN/0/27 to GigabitEthernetN/0/28
   undo shutdown
   description STACKAGE
   quit
  #
```

PUIS :

```
<>Save force
```

EXEMPLE POUR UN STACK DE 6 SWITCHES :

```
<>dis irf
Switch  Role   Priority  CPU-Mac        Description
 *+1    Master  32       b8af-67ad-3918  -----
  2     Slave   30       b8af-6770-ccec  -----
  3     Slave   28       b8af-6771-184c  -----
  4     Slave   26       b8af-6772-a9f3  -----
  5     Slave   24       b8af-6770-c47c  -----
  6     Slave   22       b8af-67ac-80e0  -----
-------------------------------------------------
```

Vous pouvez désormais connecter les câbles en les croisant (voir schéma ci-dessus). Les switches 2 à N redémarrent automatiquement.



Photo des voyants pour un stackage réussi
➔ les voyants des ports 27 et 28 s'allument en vert

3.4.3 Cas d'un switch seul (non stacké)

Dans le cas où un switch est seul à l'extrémité, il est recommandé de configurer aussi un numéro de domaine.

```
<>system-view
#
irf domain YY                | remplacer YY par la fin de l'@IP du stack – ex : 11 pour 55.X.221.11
```

3.4.4 Vérification

Commandes d'affichage pour vérification :

<>dis irf

Exemple d'un stack de 5 switches :

```
<sw-buro-86>dis irf
Switch   Role    Priority  CPU-Mac         Description
 *+1    Master   32        b8af-67ad-3918  -----
   2    Slave    30        b8af-6770-ccec  -----
   3    Slave    28        b8af-6771-184c  -----
   4    Slave    26        b8af-6772-a9f3  -----
   5    Slave    24        b8af-6770-c47c  -----
-------------------------------------------------

 * indicates the device is the master.
 + indicates the device through which the user logs in.

 The Bridge MAC of the IRF is: b8af-67ad-3917
 Auto upgrade               : yes
 Mac persistent             : 6 min
 Domain ID                  : 0
```

<>dis irf topology

Exemple d'un stack de 5 switches :

```
<sw-buro-86>dis irf topology
                          Topology Info
 ------------------------------------------------------------------------
              IRF-Port1                IRF-Port2
 Switch    Link       neighbor      Link       neighbor    Belong To
 1         UP         2             UP         5           b8af-67ad-3918
 2         UP         3             UP         1           b8af-67ad-3918
 3         UP         4             UP         2           b8af-67ad-3918
 4         UP         5             UP         3           b8af-67ad-3918
 5         UP         1             UP         4           b8af-67ad-3918
```

<>display irf configuration

Exemple d'un stack de 5 switches :

```
<sw-buro-86>dis irf configuration
 MemberID NewID    IRF-Port1                       IRF-Port2
  1       1        GigabitEthernet1/0/27           GigabitEthernet1/0/28
  2       2        GigabitEthernet2/0/27           GigabitEthernet2/0/28
  3       3        GigabitEthernet3/0/27           GigabitEthernet3/0/28
  4       4        GigabitEthernet4/0/27           GigabitEthernet4/0/28
  5       5        GigabitEthernet5/0/27           GigabitEthernet5/0/28
```

3.5 NOMMER LE SWITCH

Le nommage des switches est normalisé : voir le § « Nommage des switches » plus haut dans ce document.

La commande à utiliser est « sysname ».

Exemples : Etablissement Redon

[] sysname 351-sw-et-redon-001-n3-3600-RG

3.6 CONFIGURATION DES ACCES

3.6.1 Règle de construction du mot de passe

- **Taille :** le mot de passe doit avoir au moins 12 caractères
- **Complexité :** le mot de passe doit contenir au moins 4 types de caractères différents, et au moins 2 caractères pour chaque type

Exemple de mot de passe :

Exemple : « 12ABcd$!12AB »
2 x Caractères spéciaux : $!
2x Majuscules : AB
2x Minuscules : cd
2x Nombres : 12

3.6.2 Accès console, SSH et HTTP

A appliquer sur un switch seul (non stacké) ou sur le stack. Cela est valable pour tous les switches HP.
Ces commandes permettront de paramétrer un accès au switch ou au stack en console, ssh et http via le login « admin » et un mot de passe (à personnaliser). Le mot clé « cipher » signifie que le mot de passe sera crypté lors des visualisations de configuration :

```
<>system-view
#
local-user admin
 password cipher motdepasse          | remplacer «motdepasse» par le vôtre
 service-type ssh terminal           | si présent enlever « telnet » : undo service-type telnet
 service-type web
 authorization-attribute level 3
#
undo ip http enable                  | Suppression de l'accès HTTP
undo ip https enable                 | Suppression de l'accès HTTPS
#
user-interface aux 0 X               | où x = NB de switches dans la stack – 1 (ex : stack de 3, x=2)
 authentication-mode scheme
#
user-interface vty 0 15
 authentication-mode scheme
 protocol inbound ssh
#public-key local create rsa
        The range of public key size is (512 ~ 2048).
        NOTES: If the key modulus is greater than 512,
```

```
It will take a few minutes.
Press CTRL+C to abort.
Input the bits of the modulus[default = 1024]:2048          (puis valider avec la touché "Entrée")
Generating Keys...
        +++++
        ++++++++++++++++++++++
        ++++++++++
        ++++
```

ssh server enable
ssh user admin service-type stelnet authentication-type password
ip ttl-expires enable | validation de la réponse au « traceroute »
ip unreachables enable | validation de l'envoi de paquet ICMP destination injoignable

undo ssh server compatible-ssh1x | Interdire ssh v1 (n'apparait pas en lecture de conf (dis cu))

Sauvegarder le switch (ou stack) :

<>Save force

Remarque:

✶**Controle de la désactivation ssh1x**

```
[35N-SW-CNGR-N2-012-5510]dis ssh server status
 Stelnet server: Enable
 SSH version : 2.0                          (la version 1 est bien désactivée)
 SSH authentication-timeout : 60 second(s)
 SSH server key generating interval : 0 hour(s)
 SSH authentication retries : 3 time(s)
 SFTP server: Disable
 SFTP Server Idle-Timeout: 10 minute(s)
 NETCONF server: Disable
 SCP server: Disable
```

3.6.3 Bannière

OBLIGATION OSE :

Une bannière de mise en garde doit être configurée sur tous les switches. Voici la configuration. Commencez et finissez avec le même caractère (ici %)

Ne pas donner d'information de localisation de l'équipement (@ip, adresse physique, type de matériel, nom organisme…) **et utiliser obligatoirement et uniquement la bannière suivante** :

```
System-view
#
header shell %
****************************************
*             ! Attention !            *
*                                      *
*    Acces reserve aux personnels du   *
*         service informatique         *
*                                      *
*  Toutes les activites sur ce systeme *
*          sont enregistrees           *
*                                      *
*    Toutes preuves d activites non    *
*   autorisees seront traitees par les *
*    autorites competentes             *
*                                      *
*     Toute intrusion sur un systeme   *
*   informatique est interdite par les *
*     articles 323-2 du code penal     *
*                                      *
****************************************
%
```

3.6.4 Résolution DNS

Nouveauté v2.3 : pour permettre l'utilisation de nom DNS au lieu d'adresses IP (ex : syslog), il est nécessaire d'entrer ces commandes :

dns resolve
dns server 55.223.10.1
dns domain cnamts.fr

3.7 CONFIGURATION DU SPANNING-TREE



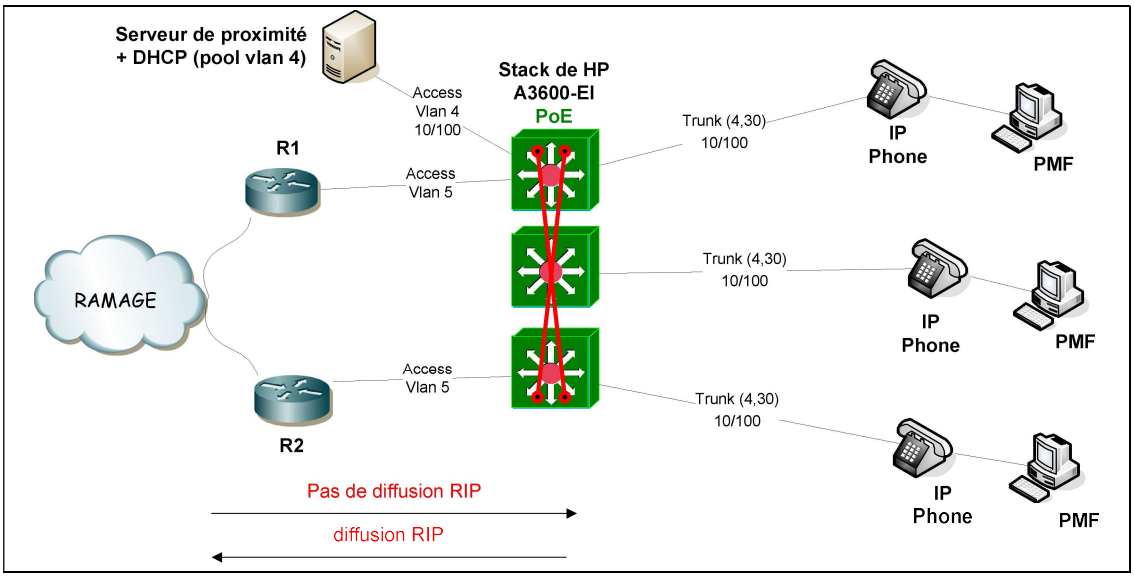
A quoi ça sert ?

Le spanning-tree est un protocole utilisant un algorithme de détection des boucles de niveau 2 sur un LAN. Une adresse MAC (celle d'un PMF par exemple) ne doit être apprise que par un seul chemin. Sur la base d'une structure d'arbre, les branches redondantes sont bloquées. Le sommet de l'arbre est le « root-bridge ».

3.7.1 Spanning-tree : mode et root-bridge

3.7.1.1 Cas 1 : 3600 seul ou en stack au niveau 3 (fédérateur) en agence

Exemple :



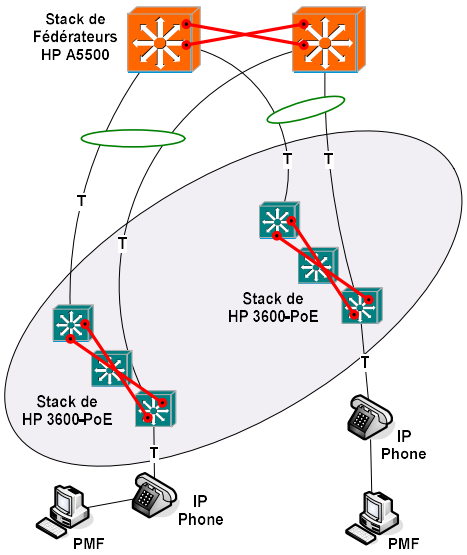
<>system-view
#
stp enable
stp mode rstp
stp instance 0 priority 0 | ce switch ou stack sera toujours root-bridge
loopback-detection enable | détection des boucles
loopback-detection multi-port-mode enable | détection des boucles
stp bpdu-protection | Blocage des interfaces edge-port recevant des BPDU* à
| tort actif sur les interfaces stp edge-port enable

stp pathcost-standard dot1t | optimisation standard du STP
stp bridge-diameter 2 **QUE SUR LE STACK N3** | optimisation des temps de convergence STP

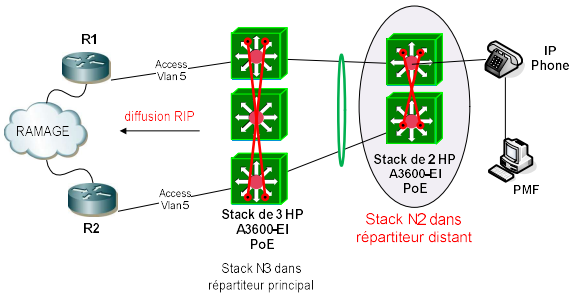
Remarque : une fois tapée, cette commande engendre automatiquement les suivantes :
stp timer forward-delay 700
stp timer max-age 1000

3.7.1.2 Cas 2 : 3600 seul ou en stack au niveau 2 à l'extrémité

Au niveau 2 à l'extrémité en siège :



Au niveau 2 à l'extrémité en agence :



stp enable
stp mode rstp
loopback-detection enable | détection des boucles
loopback-detection multi-port-mode enable | détection des boucles
stp pathcost-standard dot1t | optimisation standard du STP
stp bpdu-protection | Blocage des interfaces recevant des BPDU* à tort

Les BPDU sont des messages de spanning-tree. Une interface connectée à un hôte final (PMF, imprimante, téléphone…) ne doit recevoir aucun BPDU. Si c'est le cas, cela signifie qu'un switch est connecté (à tort) ou qu'il y a une boucle niveau 2 sur le LAN.* ***Cette commande bloquera toute interface configurée avec « stp edge- port enable » pour éviter les boucles.*

3.7.2 Spanning-tree au niveau des interfaces

Se reporter au § « Configuration des interfaces ».

Une fois configuré en global, le spanning-tree est validé de base sur toutes les interfaces. La commande « stp enable » est implicitement active au niveau des interfaces même si elle n'apparaît pas lors d'un « display current-configuration ».

Il faudra ajouter la commande « stp edged-port enable » sur les interfaces suivantes :
- Interfaces connectées à des téléphones IP, téléphones IP+PMF, PMF, imprimantes…
- Interfaces connectées à des serveurs

PAS SUR LES INTERFACES SUIVANTES :
- **Trunks d'interconnexion de switches**
- **Routeurs RAMAGE**

Cette commande allège l'algorithme du Spanning-tree et, associée à la commande globale « stp bpdu-protection », permet le blocage de l'interface recevant du trafic Spannig-tree (BPDU*) à tort.

Exemple pour une interface eth1/0/6 utilisée pour un Téléphone + PMF :
interface Ethernet1/0/6
stp enable **| n'apparaît pas en « display current-configuration »**
stp edged-port enable
etc…

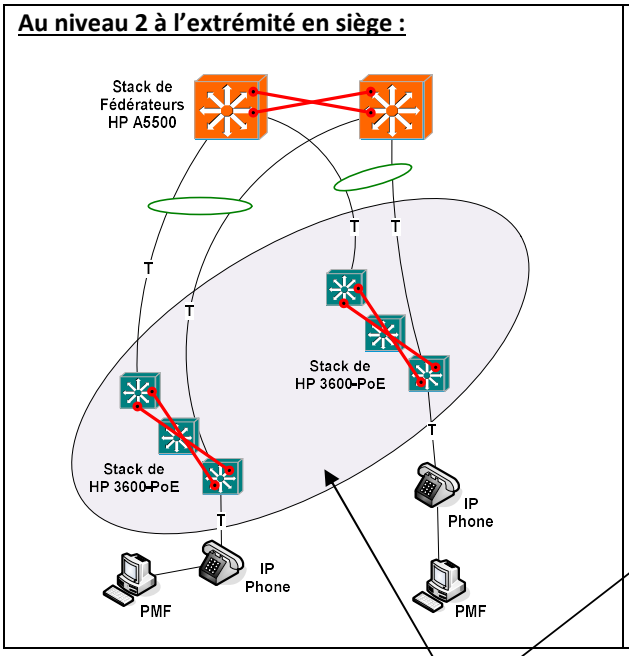
3.7.3 Protéger le root-bridge, limter les boucles, broadcasts et multicasts

Afin d'éviter des pannes provoquées par des problèmes de spanning-tree (boucles de niveau 2, changement de root-bridge…), nous demandons la mise en œuvre de mécanismes de protection en utilisant des commandes **sur certaines interfaces, dans certains cas** :

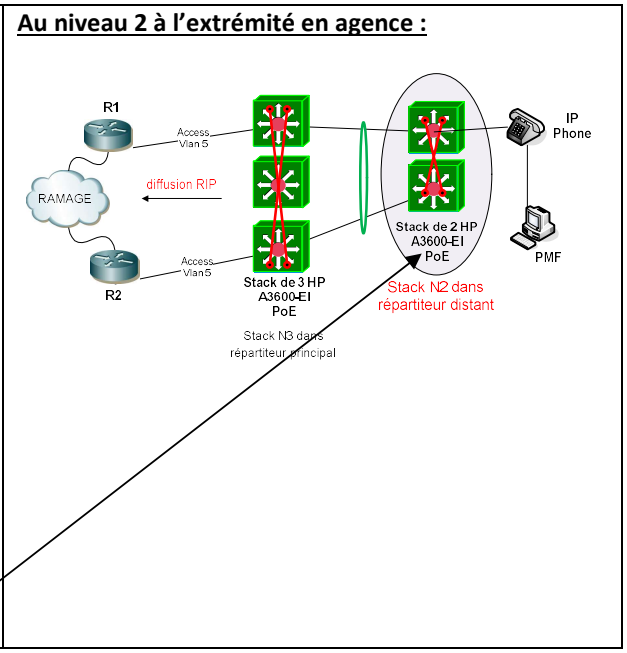
- stp loop-protection
- stp root protection
- loopback-detection enable
- loopback-detection action shutdown
- loopback-detection enable
- loopback-detection per-vlan enable
- multicast-suppression 20
- broadcast-suppression 20

stp loop-protection (protection anti-boucles) :

Au niveau 2 à l'extrémité en siège :



Au niveau 2 à l'extrémité en agence :



A appliquer sur les **switches niveau 2** ➔ ce guide de configuration concerne les 3600 ➔ HP 3600 niveau 2 d'extrémité en siège ou en agence. PAS SUR LES 3600 FEDERATEURS niveau 3 en agence.

Cette commande doit être appliquée :

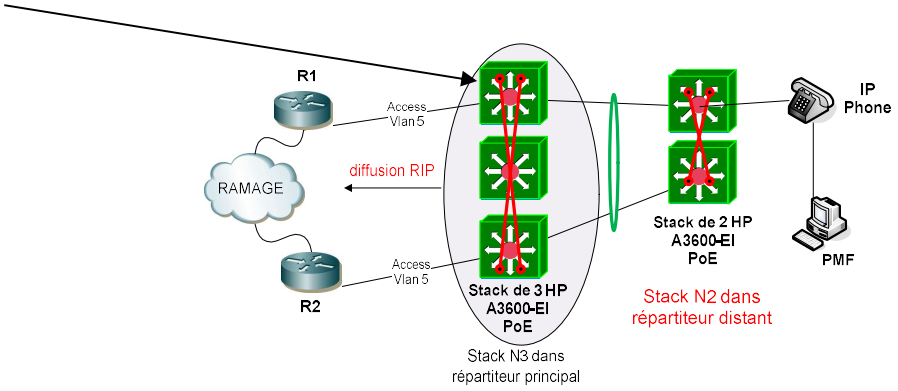
- sur les toutes les interfaces « bridge-agregation » des 3600 N2 vers des fédérateurs 5500 ou 3600 N3
- sur les interfaces trunks des 3600 N2 connectés en non agrégées et apparaissant « root » ou « alternate » avec la commande « display stp brief » :

```
<3600-N2>display stp brief
 MSTID      Port                        Role  STP State     Protection
   0        Bridge-Aggregation5         ROOT  FORWARDING    LOOP
   0        Ethernet1/0/3               DESI  FORWARDING    BPDU
   0        Ethernet1/0/4               DESI  FORWARDING    BPDU
   0        Ethernet1/0/5               DESI  FORWARDING    BPDU
```

loop-protection appliquée

stp root-protection (protection du root-bridge) :

Au niveau 3 à l'extrémité en agence :



A appliquer sur les **switches niveau 3** ➔ ce guide de configuration concerne les 3600 ➔ sont concernés par ce cas, les 3600 seuls ou les stacks de 3600 N3 en tête de réseau d'une petite agence

Cette commande doit être appliquée :

- sur les toutes les interfaces « bridge-agregation » côté 3600 N3 – **ATTENTION pas sur les aggrégats vers des serveurs ESX !!!**

- sur les interfaces trunks des 3600 N3 connectés en non agrégées à des 3600 N2 apparaissant « designated » avec la commande « display stp brief » :

```
<3600-N3>display stp brief
 MSTID      Port                        Role  STP State     Protection
   0        Bridge-Aggregation1         DESI  FORWARDING    ROOT
   0        GigabitEthernet1/0/26       DESI  FORWARDING    NONE
   0        GigabitEthernet2/0/26       DESI  FORWARDING    NONE
<3600-N3>
```

root-protection appliquée

root-protection non appliquée car l'interface n'est pas utilisée (shut)

loopback-detection enable et loopback-detection action shutdown :

Sont deux commandes à appliquer sur toutes les interfaces :

- port-link-type access ➔ serveurs non vmware, PMF seuls…
- port link-type trunk de connexion « TELEPHONE + PMF » **UNIQUEMENT**

multicast-suppression 20 et broadcast-suppression 20

Sont deux commandes à appliquer sur toutes les interfaces :

- port-link-type access ➔ serveurs non vmware, PMF seuls …
- port link-type trunk de connexion « TELEPHONE + PMF » **UNIQUEMENT**
- port link-type trunk d'agrégation

⇨ **Reportez-vous au § « Configuration des Interfaces »**

3.8 SNMP / SYSLOG

3.8.1 SNMP

Il est indispensable de configurer cette partie SNMP sur tous les switches pour deux raisons :

1/ Les switches fournis par le DR (Cnam) font l'objet d'un contrôle d'inventaire
2/ Les outils d'exploitation : Centréon, Netlix.

⇨ **Inventaire :** Veuillez prendre connaissance de la procédure : « Commandes à passer pour mettre à jour l'inventaire.pdf » : voir sur le site du DR.

Une access-list va permettre de définir quels sites sont autorisés à lancer des requêtes SNMP en lecture (polling) vers le switch (ou stack) ; ce sont notamment les serveurs du DR en CSH ou au DR.

"**COM_SNMP**" est le mot de passe de la communauté en écriture, que vous aurez paramétré dans chacun de vos switches, et que vous aurez transmis au DR. En effet, sans la connaissance de ce nom de communauté, le DR ne pourra pas mettre à jour son inventaire comptable, de façon automatique.

Ne pas oublier de configurer la « Résolution DNS » au préalable (voir plus haut).

```
acl number 2099                                  | n° d'ACL normalisé
 description SNMP RW ACCESS POUR DR              | Description
 rule 0 permit source 55.X.0.0 0.0.255.255       | Si besoin en local, adaptez à votre plan d'adressage
 rule 1 permit source 55.18.0.0 0.0.255.255      | DR
 rule 2 permit source 55.245.0.0 0.0.255.255     | CSH GE
 rule 3 permit source 55.244.0.0 0.0.255.255     | CSH SUD

snmp-agent
snmp-agent community read TOKTBAT22! acl 2099    | ➔ UNIQUE pour serveurs de polling
snmp-agent community write COM_SNMP acl 2099     | ➔ remplacez « COM_SNMP » par votre nom de communauté
snmp-agent sys-info contact François Pignon      | nom d'un contact)
snmp-agent sys-info location RG                  | nom du répartiteur et/ou de la baie
snmp-agent sys-info version v2c                  | version SNMP
snmp-agent trap enable                           | Envoi des traps
```

3.8.2 SYSLOG

SYSLOG : Il s'agit d'un serveur national qui recueille les logs des switches dans le cadre des outils IRMA. Cette commande est à entrer dans tous les switches car elle conditionne le bon fonctionnement de HP-NA :

```
<>system-view
#
info-center loghost source Vlan-interface 901        | dans le cas de la présence du vlan 901
info-center loghost source loopback1                 | dans le cas de la présence de la loopback 1 (switch ou stack seul)
info-center loghost slog-reseau-org.ramage           | adresse unique valable pour tous – résolution DNS à paramétrer avant !!
```

Ces modifications n'entrainent pas de coupure. Le CNGR pourra les déclencher en automatique à partir de NCM (avec votre accord).

Pour retirer le ou les anciens serveur syslog qui existaient, utiliser la commande :
« undo info-center loghost ….. »

Vérification de la configuration :

« display current-configuration | include info » (ou « di cu | i info ».

3.9 SECURITE

3.9.1 ACL 3224 pour le VLAN 224

Voir ci-dessous dans le chapitre suivant « VLAN 224 – VLAN-ACCES-PART.

3.9.2 ACL 2099 pour SNMP

```
acl number 2099                                  | n° d'ACL normalisé
 description SNMP RW ACCESS POUR CNGR            | Description
 rule 0 permit source 55.X.0.0 0.0.255.255       | Si besoin : plan d'adressage de votre organisme
 rule 1 permit source 55.18.0.0 0.0.255.255      | CNGR
 rule 2 permit source 55.245.0.0 0.0.255.255     | CSH GE
 rule 3 permit source 55.244.0.0 0.0.255.255     | CSH SUD
```

3.9.3 ACL 3002 WOL

```
acl number 3002                                  | n° d'ACL normalisé
 description WOL                                 | Description
 rule 1 permit udp source 55.245.0.0 0.0.255.255 | CSH GE
```

3.9.4 Fonction packet-filter

Cette commande permet d'appliquer une ACL sur un VLAN.

[*SYSNAME*-Vlan-interface224]packet-filter 3224 inbound |Application pour le vlan 224

Visualisation des statistiques :

[*SYSNAME*] dis packet-filter statistics sum inbound **XXXX** |Contrôle de la fonction. XXXX = n°ACL

3.10 CONFIGURATION DES VLAN



A quoi ça sert ?

Les Vlans permettent de gérer des domaines de broadcast distincts. Ils présentent les intérêts suivants:

- **Améliorer la gestion du réseau**
- **Optimiser la bande passante**
- **Séparer les flux**
- **Fragmentation: réduire la taille d'un domaine de broadcast**
- **Sécurité: permet de créer un ensemble logique isolé pour améliorer la sécurité.**

Vous pouvez gérer vos vlans de 2 façons :

- Soit statiquement : Déclaration manuelle des vlans sur les équipements niveau 3 et niveau 2
- Soit dynamiquement en utilisant le protocole GVRP (pas recommandé par la Cnam)

Nous conseillons donc de créer les VLAN manuellement sur tous les switches et de ne pas utiliser GVRP.

3.10.1 Nommage des Vlan et des interfaces VLAN

Le nommage des VLAN et des interfaces vlan est **normalisé et obligatoire**. Il faut consulter la dernière les référentiels ci-dessus.

3.10.2 Déclarer les VLAN (niveau 2)

Exemple avec le VLAN 30 :

CREATION	SUPPRESSION
<>system-view # vlan 30 **name VLAN-VOIX**	<>system-view # undo vlan 30

⇨ **Appliquez le nommage normalisé !**

3.10.3 Création des interfaces VLAN (niveau 3)

Seuls les 3600 fédérateurs niveau 3 possèdent plusieurs interfaces VLAN. Les 3600 d'extrémité n'ont qu'une seule interface VLAN : VLAN 901 (VLAN-ADMIN-RESEAU).

Ne configurez que celle dont vous avez besoin (en phase avec vos VLAN).

La VLAN-interface 1 doit être supprimée. Les autres VLAN-interfaces ont une adresse.

Ne pas oublier d'appliquer les descriptions normalisées OBLIGATOIRES.

Nous donnons ici **pour exemple** les interfaces VLAN et leur adressage en **AGENCES** : pour connaître les plans d'adressage IP à utiliser, reportez-vous aux référentiels LAN.

```
<>system-view
#
undo interface Vlan-interface 1
#
interface Vlan-interface 4
 description INT-VLAN-DATA
 ip address 55.X.12.1 255.255.252.0                | ou ip address 55.X.4.1 22
#
interface Vlan-interface 30
 description INT-VLAN-VOIX
 ip address 58.X.12.1 255.255.252.0                | ou ip address 58.X.4.1 22
 dhcp select relay
 dhcp relay server-address 55.x.4.y                 | ou ip address du serveur dns
#
interface Vlan-interface 5
 description INT-INTERCOWAN
 ip address 55.X.240.1 255.255.255.248              | ou ip address 55.X.225.1 29
#
interface Vlan-interface 17
 description INT-VLAN-EVASION-INTERNET
 ip address 192.168.1.4 255.255.255.0               | ou ip address 192.168.1.4 24
#
interface Vlan-interface224
 description INT-VLAN-ACCESS-PART
 ip address 55.X.246.1 255.255.255.248              | ou ip address 55.X.224.1 29
 packet-filter 3224 inbound   (*)
#
interface Vlan-interface 901
 description INT-VLAN-ADMIN-RESEAU
 ip address 55.X.221.1 255.255.255.0                | ou ip address 55.X.221.1 24
```

…etc.

(*) : Voir paragraphe « Sécurité »

3.10.4 VLAN 901 (ADMIN-RESEAU) en AGENCES



Attention à la coupure réseau

Principe : L'interface VLAN 1 ou VLAN4 doit être supprimée et remplacée par l'interface VLAN 901.

A partir de 2021 et Ramage V6, le VLAN 901 sera à déclarer sur tous les sites de l'assurance maladie, car tous les sites seront niveau 3.

Pour connaître les plans d'adressage IP à utiliser, reportez-vous aux référentiels.

	Agence avec 1 stack	Agence avec 1 switch	Agence avec plusieurs switches ou stacks
Déclaration vlan 901 Niveau 2	Non	Non	Oui
Déclaration Vlan interface 901	Non	Non	Oui
Déclaration loopback 1	Oui	Oui	Non

3.10.4.1 Cas ou l'agence dispose de plusieurs stacks

-Seuls les fédérateurs ont plusieurs interfaces VLAN alors que switches ou les stacks d'extrémité n'en n'ont qu'une seule : l'interface VLAN 901.

Consultez les tableaux dans le référentiel LAN des agences d'extrémité des organismes.

```
<>system-view
#
interface Vlan-interface901
 Description INT-VLAN-ADMIN-RESEAU
 Ip address première-adresse-du-sous-réseau                | Pour le fédérateur
#
interface Vlan-interface901
 Description INT-VLAN-ADMIN-RESEAU
 Ip address adresse2-du-sous-réseau                        | Pour le 1ère Stack d'extrémité
#
interface Vlan-interface901
 Description INT-VLAN-ADMIN-RESEAU
 Ip address adresse3-du-sous-réseau                        | Pour le 2ème Stack d'extrémité
```

Etc …➔ Voir le Référenciel-LAN-AGENCES 9.X (vous pouvez déclarer 13 stacks par site).

Attention : : Dans les 3600 d'extrémité, ne pas oublier de modifier la route vers le fédérateur (Coupure à prévoir / Opération en HNO) : 0.0.0.0 .0.0.0.0 @IP interface-VLAN-901-du-fédérateur.

Connectez-vous en port console sur chaque switch.

3.10.4.2 Cas d'un site avec une seule stack de switch : Loopback1

Vous ne pouvez pas configurer un VLAN d'ADMIN-RESEAU puisque vous ne disposez que d'un seul switch ou d'une seule stack (stack) : comme aucun équipement n'est connecté dans ce VLAN, il resterait « DOWN ».

Vous allez donc déclarer une adresse de loopback qui sera diffusée sur le réseau RAMAGE via votre interface VLAN 5. Cette loopback doit être la loopback1 et doit avoir comme adresse IP la dernière du sous-réseau : consultez les tableaux dans le référentiel LAN des agences.

Pour connaître les plans d'adressage IP à utiliser, reportez-vous aux référentiels.

```
<>system-view
#
interface LoopBack1                          | Respecter le n° d'interface de loopback 1
 description INT-LOOPBACK-ADMIN-RESEAU       | DESCRIPTION NORMALISEE OBLIGATOIRE
 ip address 55.X.0.241 255.255.255.255       | Voir le référentiel des agences. La masque de la loopback1 est /32)
```

Exemples :

```
Interface loopback1
 Ip address 55.X.0.14

Interface loopback1
 Ip address 55.X.0.30

Interface loopback1
 Ip address 55.X.1.126
```

3.10.5 VLAN 902 (ADMIN-RESEAU-WIFI) en AGENCES

Le VLAN 902 sera déclaré sur tous les sites de l'assurance maladie, il correspond au vlan VLAN-ADMIN-RESEAU-WIFI qui aujourd'hui était confondu avec le vlan 901 VLAN-ADMIN-RES.

1/ Déclaration Vlan niveau 2

```
#
vlan 902
name VLAN-ADMIN-WIFI (à renseigner obligatoirement si wifi sur site)
```

2/Déclaration Vlan interface niveau 3

```
#
interface Vlan-interface 902
 description INT-VLAN-ADMIN-WIFI             | A renseigner obligatoirement si wifi sur site
 ip address 55.X.2.1 255.255.255.240         | voir les référentiels éférentiels
```

3.10.6 VLAN 22X

Tous les VLAN 22X permettront d'isoler des équipements pouvant être accédés à distance par un partenaire extérieur.

Ils doivent répondre à <u>un projet national</u> validé par la DS (la demande sera postée travers le psn).

Voir : https://www.cngr.cnamts.fr/contenu/symfony/162

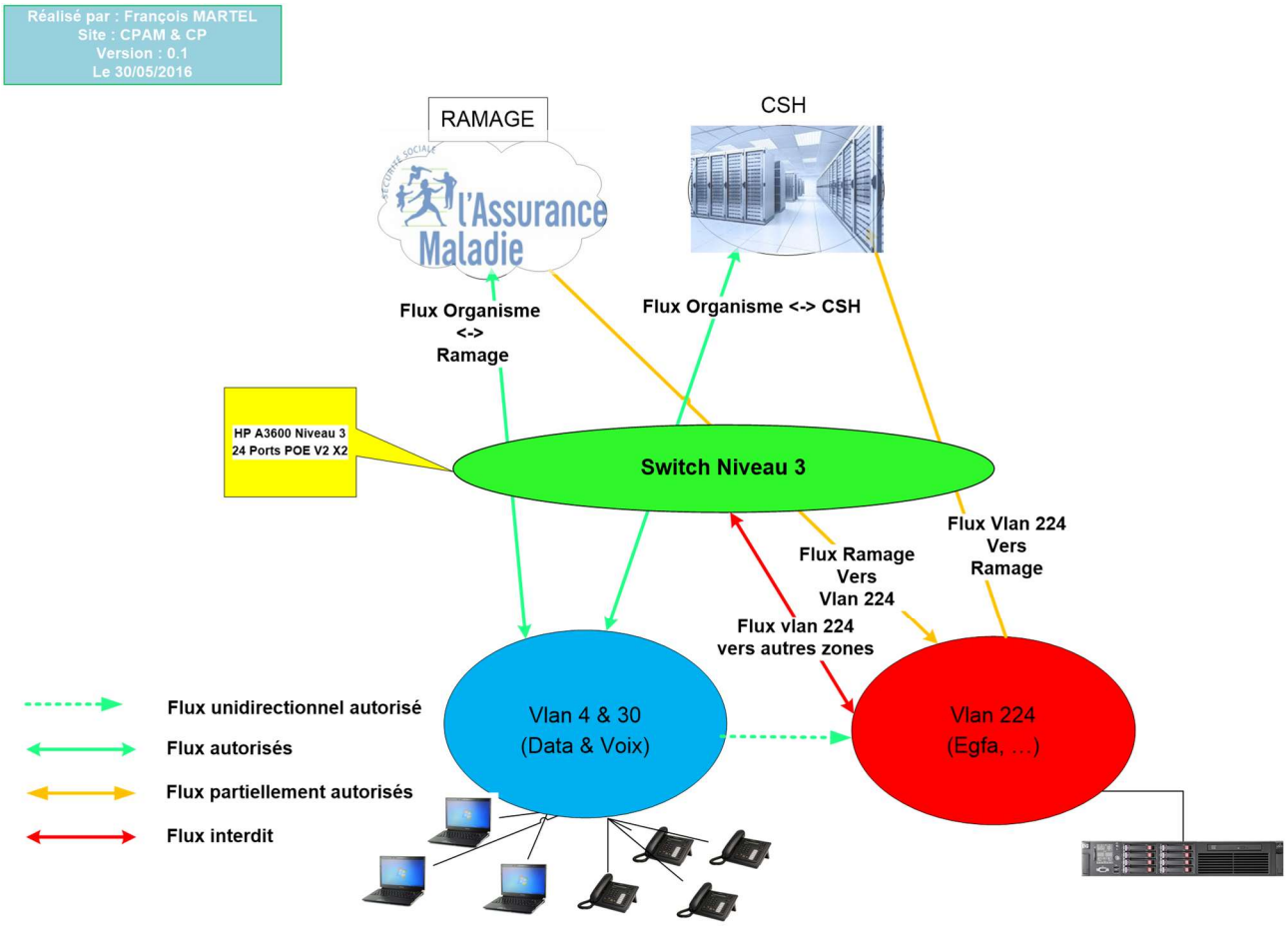
Une ACL (ACL 322X) sera mise en place permettant de filtrer les communications entre les matériels actifs isolés dans le VLAN 22x **<u>« zone partenaire »</u>** et les machines hébergés sur le LAN local des organismes dans **<u>« la zone RAMAGE »</u>**

Les ACL à appliquer seront décrites dans une procédure sur le portail du DR : https://www.cngr.cnamts.fr/
Pour des besoins locaux (hors projets nationaux), les équipements doivent être intégrés dans le VLAN 224.

3.10.6.1 VLAN 224 – VLAN-ACCES-PART

Le VLAN 224 est utilsé depuis le projet EGFA : il est nommé VLAN-ACCES-PART. Il doit être utilisé aussi en cas de connexion de partenaire(s) en SIEGE dans les cas de besoins **hors projets nationaux**.

<u>ACL EGFA : principe</u>



Le VLAN et l'interface VLAN

Vlan 224
name VLAN-ACCES-PART

interface Vlan-interface224
description INT-VLAN-ACCES-PART
ip address 55.X.224.1 255.255.255.128

3.10.6.1.1 ACL pour EGFA en SIEGE

A appliquer sur le **switch fédérateur de niveau 3** du site et seulement sur ce switch.

Dans les ACL, les masques de sous-résaux sont exprimés en « wildcard ». En siège, le masque doit être 255.255.255.128. Le wildcard doit donc être 0.0.0.127.

ACL - Remplacer le X par votre octet d'organisme :

acl number 3224 name Acces-Part-vers-autres-Vlan

rule 10 permit ip source 55.X.224.0 0.0.0.127 destination 55.227.1.20 0 logging
rule 10 comment Autorisation dialogue vlan 224 / partenaires via CSH

rule 20 permit ip source 55.X.224.0 0.0.0.127 destination 55.227.1.21 0 logging
rule 20 comment Autorisation Proxy Egfa 1

rule 30 permit ip source 55.X.224.0 0.0.0.127 destination 55.225.59.20 0 logging
rule 30 comment Autorisation Proxy Egfa 2

rule 40 permit ip source 55.X.224.0 0.0.0.127 destination 55.X.224.0 0.0.0.127 logging
rule 40 comment Autorisation Flux interne Vlan Partenaires

rule 50 permit ip source 55.X.224.0 0.0.0.127 destination 55.14.0.0 0.0.255.255 logging
rule 50 comment Autorisation Csn Caen

rule 100 deny ip logging
rule 100 comment Interdiction tout autre flux

Application sur l'interface VLAN 224 :

interface Vlan-interface224
description INT-VLAN-ACCES-PART
ip address 55.X.224.1 255.255.255.128
packet-filter 3224 inbound

L'ACL bloque tout flux en provenance des autres VLAN du site y compris les administrateurs informatiques. Pour permettre cet accès, il faut ajouter la règle 60 :

rule 60 permit ip source 55.X.224.0 0.0.0.127 destination 55.X.Y.Z 0 logging
rule 60 comment Autorisation flux legitime

55.X.Y.Z = Adresse IP du PMF autorisé. Ajouter autant de règles (61, 62…) que de PC à autoriser.

3.10.6.1.2 Ajout de l'accès d'un autre partenaire dans le VLAN-ACCES-PART en SIEGE

Lors de votre demande d'interconnexion d'un partenaire, il vous est fournie une adresse IP par le SOC. Cette adresse IP est l'adresse IP entrante de **ce partenaire** : elle est de la forme 55.227.X.Y – 255.255.255.255.

Pour ajouter l'accès de partenaire au VLAN 224, ajouter une règle (par exemple 70) à l'ACL 3224 :

rule 70 permit ip source 55.X.224.0 0.0.0.127 destination 55.227.X.Y 0 logging
rule 70 comment Autorisation PARTENAIRE « nom du partenaire »

3.10.6.1.3 ACL pour EGFA en AGENCE

Comme indiqué dans le référentiel LAN des agences : « les CP utiliseront un des sous-réseaux suivants pour le VLAN 224. Il s'agit de choisir un sous-réseau par CP. Si le nombre d'adresses est insuffisant pour un site, veuillez adapter le masque de sous-réseau. »

Dans les ACL, le masque est « inversé » : on parle de WILDCARD (en vert dans l'exemple : première règle) dans les configurations ci-dessous. En fonction du masque utilisé, veuillez adapter le wildcard.

Masque		Wildcard
255.225.255.248	/29	0.0.0.7
255.255.255.240	/28	0.0.0.15
255.255.255.224	/27	0.0.0.31
…etc.		

Comme listé de manière exhaustive dans le référentiel LAN des CP et agences, le plan d'adressage est le suivant (masque à adapter en fonction du besoin) :

CP	subnet	Masque	Première @	Dernière @	Int vlan 224 Switch N3	Disponibles pour clients				
1	55.X.246.0	255.255.255.248 (/29)	1	6	1	4	5	6	2	3
2	55.X.246.8	255.255.255.248 (/29)	9	14	9	12	13	14	10	11
3	55.X.246.16	255.255.255.248 (/29)	17	22	17	20	21	22	18	19
4	55.X.246.24	255.255.255.248 (/29)	25	30	25	28	29	30	26	27
5	55.X.246.32	255.255.255.248 (/29)	33	38	33	36	37	38	34	35
…etc……										
61	55.X.247.224	255.255.255.248 (/29)	225	230	225	228	229	230	226	227
62	55.X.247.232	255.255.255.248 (/29)	233	238	233	236	237	238	234	235
63	55.X.247.240	255.255.255.248 (/29)	241	246	241	244	245	246	242	243
64	55.X.247.248	255.255.255.248 (/29)	249	254	249	252	253	254	250	251

Il faut adapter l'ACL au plan d'adressage IP du site et remplacer le X par votre octet d'organisme.

ACL - Remplacer le X par votre octet d'organisme :

Dans la configuration ci-dessous, nous utilisons le cas de l'agence n° 1 (55.X.246.0 /29) :

acl number 3224 name Acces-Part-vers-autres-Vlan

rule 10 permit ip source 55.X.246.0 0.0.0.7 destination 55.227.1.20 0 logging
rule 10 comment Autorisation dialogue vlan 224 / partenaires via CSH

rule 20 permit ip source 55.X.246.0 0.0.0.7 destination 55.227.1.21 0 logging
rule 20 comment Autorisation Proxy Egfa 1

rule 30 permit ip source 55.X.246.0 0.0.0.7 destination 55.225.59.20 0 logging
rule 30 comment Autorisation Proxy Egfa 2

rule 40 permit ip source 55.X.246.0 0.0.0.7 destination 55.X.246.0 0.0.0.7 logging
rule 40 comment Autorisation Flux interne Vlan Partenaires

rule 50 permit ip source 55.X.246.0 0.0.0.7 destination 55.14.0.0 0.0.255.255 logging
rule 50 comment Autorisation Csn Caen

rule 100 deny ip logging
rule 100 comment Interdiction tout autre flux

L'ACL bloque tout flux en provenance des autres VLAN du site y compris les administrateurs informatiques. Pour permettre cet accès, il faut ajouter la règle 60 :

rule 60 permit ip source 55.X.224.0 0.0.0.7 destination 55.X.Y.Z 0 logging
rule 60 comment Autorisation flux legitime

55.X.Y.Z = Adresse IP du PMF autorisé. Ajouter autant de règles (61, 62…) que de PC à autoriser.

Application sur l'interface VLAN 224 :

interface Vlan-interface224
description INT-VLAN-ACCES-PART
ip address 55.X.246.1 255.255.255.248
packet-filter 3224 inbound

3.10.6.1.4 Ajout de l'accès d'un autre partenaire dans le VLAN-ACCES-PART en AGENCE

Lors de votre demande d'interconnexion d'un partenaire, il vous est fournie une adresse IP par le SOC. Cette adresse IP est l'adresse IP entrante de **ce partenaire** : elle est de la forme 55.227.X.Y – 255.255.255.255.

Pour ajouter l'accès de partenaire au VLAN 224, ajouter une règle (par exemple 70) à l'ACL 3224 :

rule 70 permit ip source 55.X.246.0 0.0.0.7 destination 55.227.X.Y 0 logging
rule 70 comment Autorisation PARTENAIRE « nom du partenaire »

3.10.6.2 Cas du VLAN « IMPRIMANTES » n° 226

1/ Déclaration du vlan 226

```
<>system-view
Vlan 226
name VLAN-IMPRIMANTES
```

2/ Déclaration de la vlan interface 226:

Pour un SIEGE :

```
<>system-view
int vlan 226
description  INT-VLAN-IMPRIMANTES
ip address 55.xxx.248.1 255.255.255.128          | pour un Siège, consultez le Référentiel-SIEGES ci-dessus
```

Pour une AGENCE

```
<>system-view
int vlan 226
description  INT-VLAN-IMPRIMANTES
ip address 55.xxx.249.137 255.255.255.248        | pour une Agence/Etablissement, consultez le Référentiel-Agences ci-dessus
```

3.10.6.3 Cas du VLAN « IMPRIMANTES-MEDICAL » n° 227

1/ Déclaration du vlan 227

```
<>system-view
Vlan 227
name VLAN-IMPRIMANTES-MEDICAL
```

2/ Déclaration de la vlan interface 227:

Pour un SIEGE :

```
<>system-view
int vlan 227
description INT-VLAN-IMPRIMANTES-MEDICAL
ip address 55.2xx.248.1* 255.255.255.128         | pour un Siège, consultez le Référentiel-SIEGES ci-dessus
```

***** : Le plan est à déterminer en collaboration avec la MEDICAL hébergée.

Pour une AGENCE

```
<>system-view
int vlan 227
description INT-VLAN-IMPRIMANTES-MEDICAL
ip address 55.2xx.249.137 255.255.255.248        | pour une Agence/Etablissement, consultez le Référentiel-Agences ci-dessus
```

3.10.7 Suppression du VLAN 249 « VISIO »

Pour supprimer le VLAN 249 « VISIO » sur tous vos switches :

- Supprimer le VLAN 249 et l'interface VLAN 249 : `undo vlan 249`

- Si le terminal visio était connecté sur un switch d'extrémité, il faut supprimer le vlan 249 sur les aggrégats de tous les switches traversés :

```
Interface Bridge-Agregation X
 undo port trunk permit vlan 249
```

3.11 CONFIGURATION DES INTERFACES DES 3600

3.11.1 Interfaces non utilisées



Pour respecter les consignes de la PSSI MCAS, au moins dans les lieux sensibles comme les accueils… (Possibilité pour un inconnu de se connecter au réseau sur une prise dans les lieux ouverts au public, possibilité de connecter un PC « non PLC » ou un hub ou un switch ou un sniffer sur une prise libre dans son bureau….) :

⇨ **il est demandé de mettre à « shutdown » toutes les interfaces Ethernet et GigaEthernet non utilisées.**

[351-sw-et-redon-n3-1-3600-GigabitEthernet3/0/49] **default** | remise en conf usine
This command will restore the default settings. Continue? [Y/N]: **y**
[351-sw-et-redon-n3-1-3600-GigabitEthernet3/0/49] **shut** | shut de l'interface
[351-sw-et-redon—n3-1-3600--GigabitEthernet3/0/49] **description SHUTDOWN**

3.11.2 Description des interfaces

La description des interfaces doit être renseignée. Celles des routeurs opérateurs sont normalisées :

description ROUTEUR-BTE
description ROUTEUR-NXO

3.11.3 Speed / Duplex

RAPPEL :

1/ Configurer l'interface sans s'occuper des « speed et duplex » : laisser en auto par défaut

2/ Entre des « hosts » (PMF, téléphone, serveurs) et des switches, lorsque :
- **le débit négocié est inférieur à celui escompté**
- **un quelconque problème apparaît (lenteurs, accès à des ressources…)**
- **des erreurs sont constatées sur les interfaces**

⇨ **il faut forcer les speed et duplex côté switch et côté « host » (si possible).**

Les exemples ci-dessous correspondent aux VLAN utilisés en siège d'Organisme. Des descriptions sont données en exemple.

3.11.4 Routeurs opérateurs (RAMAGE)

3.11.4.1 Les fonctions associées aux ports des routeurs opérateurs

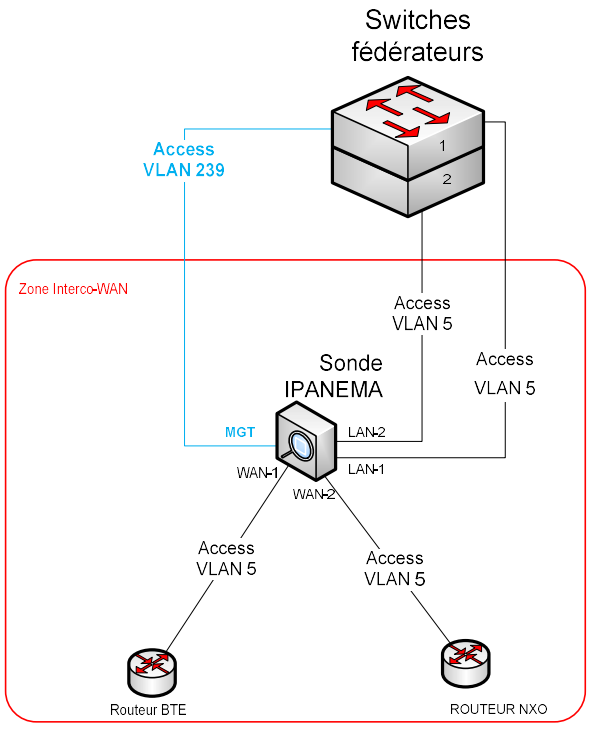
- **Description ROUTEUR-BTE (Routeur Bouygues Telecom)**
- **Description ROUTEUR-NXO (Routeur NextiraOne)**
- **port access vlan 5 (connectés au VLAN5 d'intercowan)**
- **undo stp enable (désactivation du spanning tree)**

Le VLAN 5 aura été créé au préalable.

3.11.4.2 Sonde IPANEMA

Dans le cas où une sonde est à installer sur le site, elle s'intercale entre les switches fédérateurs et les routeurs RAMAGE. Remarque : il est rare de trouver une sonde dans des sites dont les fédérateurs sont des 3600…

Schéma de principe :



Configuration pour l'interface MGT :

Vlan et interface VLAN:

```
vlan 239
 description MGT-IPANEMA
 name VLAN-MGT-IPANEMA
#
interface Vlan-interface239
 description INT-MGT-IPANEMA
 ip address 55.239.X.Y 255.255.255.248
```

Connexion de l'interface MGT :

➔ choisir un port disponible sur le fédérateur **MASTER OBLIGATOIREMENT !!**

```
interface Ethernet1/0/?
 description MGT-IPANEMA
 port link-type access
 port access vlan 239
 speed 100
 duplex full
 stp edged-port enable
```

Les valeurs de **X** et de **Y** sont uniques pour chaque sonde. Cette information adaptée à votre site, est disponible sur le portail du DR.

La configuration des interfaces VLAN 5 côté switch est la même que lorsqu'il n'y a pas de sonde (cf § ci-dessous).

3.11.4.3 Les ports normalisés des routeurs opérateurs

La connexion des routeurs doit être faite sur les ports de switches normalisés.

Accès Ramage v6 SANS FTTH

Cas d'un switch N3 seul

			Interfaces normalisées sur le switch pour la connexion des routeurs	
			Switches HP à ports RJ45	Description
PROFILS	**Gammes de switches ==>**		**3600 (24 ou 48)**	-
Profils 1, 2 et 3	port 1 Routeur BTE		ET 1/0/1	ROUTEUR-BTE
(2 opérateurs)	Port 5 routeur NXO		ET 1/0/2	ROUTEUR-NXO
Profil 4	Profil 4a (BTE)	port 1 Routeur BTE	ET 1/0/1	ROUTEUR-BTE
(1 opérateur)	Profil 4b (NXO)	Port 5 routeur NXO	ET 1/0/2	ROUTEUR-NXO

Cas d'un stack N3

			Interfaces normalisées sur le STACK de N switches pour la connexion des routeurs	
			Switches HP à ports RJ45	Description
PROFILS	**Gammes de switches ==>**		**3600 (24 ou 48)**	-
Profils 1, 2 et 3	port 1 Routeur BTE		ET 1/0/1	ROUTEUR-BTE
(2 opérateurs)	Port 5 routeur NXO		ET N/0/1	ROUTEUR-NXO
Profil 4	Profil 4a (BTE)	port 1 Routeur BTE	ET 1/0/1	ROUTEUR-BTE
(1 opérateur)	Profil 4b (NXO)	Port 5 routeur NXO	ET N/0/1	ROUTEUR-NXO

N = numéro du dernier switch du stack

Configuration :

<>system-view # interface Ethernet1/0/1 **description ROUTEUR-BTE** port access vlan 5 port link-type access* speed 100 duplex full stp disable	<>system-view # interface EthernetN/0/1 *ou* 2/0/1 **description ROUTEUR-NXO** port access vlan 5 port link-type access* speed 100 duplex full stp disable

* Commande n'apparaissant pas en « *display current configuration* »

Si la commande « stp edged-port enable » est présente, il faut la retirer avec « stp edged-port disable ».

NB : La désactivation du spanning-tree sur ces interfaces ne provoque aucune coupure (« stp-edged-port disable» et « stp disable »).

Accès Ramage v6 AVEC FTTH

FTTH avec BTE :

Cas d'un switch N3 seul

			Interfaces normalisées sur le switch pour la connexion des routeurs		
			Switches HP à ports RJ45		Description
PROFILS	Gammes de switches ==>		3600-24	3600-48	-
Profils 2 et 3 (2 opérateurs)	port 1 routeur BTE FTTH		GI 1/0/25	GI 1/0/49	ROUTEUR-BTE
	Port 5 routeur NXO		ETH 1/0/2	ETH 1/0/2	ROUTEUR-NXO
Profil 4	Profil 4a (BTE)	port 1 Routeur BTE FTTH	GI 1/0/25	GI 1/0/49	ROUTEUR-BTE

Cas d'un stack N3

			Interfaces normalisées sur le STACK de N switches pour la connexion des routeurs		
			Switches HP à ports RJ45		Description
PROFILS	Gammes de switches ==>		3600-24	3600-48	-
Profils 2 et 3 (2 opérateurs)	port 1 routeur BTE FTTH		GI 1/0/25	GI 1/0/49	ROUTEUR-BTE
	Port 5 routeur NXO		ETH N/0/1	ETH N/0/1	ROUTEUR-NXO
Profil 4	Profil 4a (BTE)	port 1 Routeur BTE FTTH	GI 1/0/25	GI 1/0/49	ROUTEUR-BTE

N = numéro du dernier switch du stack

FTTH avec NXO :

Cas d'un switch N3 seul

			Interfaces normalisées sur le switch pour la connexion des routeurs		
			Switches HP à ports RJ45		Description
PROFILS	Gammes de switches ==>		3600-24	3600-48	-
Profils 2 et 3 (2 opérateurs)	port 1 routeur BTE		ETH 1/0/1	ETH 1/0/1	ROUTEUR-BTE
	Port 5 routeur FTTH NXO		GI 1/0/26	GI 1/0/50	ROUTEUR-NXO
Profil 4	Profil 4b (NXO)	Port 5 routeur FTTH NXO	GI 1/0/26	GI 1/0/50	ROUTEUR-NXO

Cas d'un stack N3

			Interfaces normalisées sur le STACK de N switches pour la connexion des routeurs		
			Switches HP à ports RJ45		Description
PROFILS	Gammes de switches ==>		3600-24	3600-48	-
Profils 2 et 3 (2 opérateurs)	port 1 routeur BTE		ETH 1/0/1	ETH 1/0/1	ROUTEUR-BTE
	Port 5 routeur FTTH NXO		GI N/0/26	GI N/0/50	ROUTEUR-NXO
Profil 4	Profil 4b (NXO)	Port 5 routeur FTTH NXO	GI N/0/26	GI N/0/50	ROUTEUR-NXO

N = numéro du dernier switch du stack

3.11.4.4 La configuration

Switch fédérateur maître :	**Switch fédérateur secours :**
<>system-view **#** **interface Ethernet1/0/1** **description ROUTEUR-BTE** **port link-type access*** **port access vlan 5** **speed 100** **duplex full** **undo stp enable** **Si FTTH :** **interface GigaEthernet1/0/25** **description ROUTEUR-BTE** **port link-type access*** **port access vlan 5** **speed 1000** **duplex full** **undo stp enable**	**<>system-view** **#** **interface EthernetN/0/2** **description ROUTEUR-NXO** **port link-type access*** **port access vlan 5** **speed 100 ou 1000** **duplex full** **undo stp enable** **Si FTTH :** **interface GigaEthernetN/0/26** **description ROUTEUR-BTE** **port link-type access*** **port access vlan 5** **speed 1000** **duplex full** **undo stp enable**

* Commande n'apparaissant pas en « *display current configuration* »

Si la commande « stp edged-port enable » est présente, il faut la retirer avec « stp edged-port disable ». La désactivation du spanning-tree sur ces interfaces ne provoque aucune coupure (« stp-edged-port disable» et « undo stp enable »).

Les descriptions « ROUTEUR-BTE » et « ROUTEUR-NXO » sont normalisées.

Si un cas n'est pas décrit dans le tableau précédent vous pouvez consulter les référentiels plus haut dans ce document pour plus de précision ou contacter le DR via une demande PSN.

3.11.4.5 Connexion des routeurs 4G

- **Switch ou Stack HP 3600-v2 CUIVRE (24 ou 48 ports RJ45) :**

► Le ROUTEUR-4G est à connecter :
- SI STACK : sur le port 1/0/2 du fédérateur maitre
- SI SWICH SEUL et pas de routeur secours : sur le port 1/0/2 du switch
- SI SWICH SEUL et routeur secours : sur le port 1/0/3 du switch

3.11.5 Téléphone + PMF : standard CETIAM

3.11.5.1 Pré-requis important

IMPORTANT : L'installation de la ToIP dans un CP (ou petite agence) entraine la création de VLAN dédiés à la donnée ou à la voix (4 et 30) et **la création spécifique du VLAN 5 d'interconnexion avec l'opérateur : les routeurs RAMAGE vont devoir changer d'adresse IP ➔ il faut que vous commandiez un « MOD-CONF ».**

➔ Reportez-vous au « Référentiel LAN des CP et agences d'extrémité » - chapitre « **A faire avant le déploiement de la ToIP : le MOD-CONF » :** la procédure est disponible sur le **portail réseaux et Télécom du DR / rubrique LAN**.

Pensez aussi à consulter les documentations liées à la téléphonie (voir portail du DR).

Rappel :

Préconisations Cnam : le serveur DHCP pour les téléphones et les PMF est le contrôleur Windows du siège.

3.11.5.2 Déploiement des téléphones

Sauf exception (certains modèles de téléphones anciens), voici comment fonctionne un téléphone au démarrage :

Pré-requis : le « voice vlan » est défini sur le switch selon le range des adresses MAC des téléphones*

1/ le téléphone neuf et vierge de toute configuration est connecté au switch (port LAN)

2/ le PMF est connecté au téléphone (port PC)

3/ le téléphone est alimenté par le PoE : il démarre

4/ l'adresse MAC du téléphone est détectée comme appartenant au « voice vlan » via LLDP

5/ le téléphone démarre sur le vlan 30 (vlan voix)

6/ il trouve le serveur DHCP dans le VLAN 30

7/ il lui est attribuée une adresse IP dans le VLAN 30

8/ le DHCP lui indique que le serveur TFTP qui stocke sa configuration est une adresse IP dans le VLAN 30 (l'IPBX)

9/ le téléphone contacte le serveur TFTP et charge sa configuration

10/ le téléphone redémarre et fonctionne dans le VLAN 30

11/ le PMF fonctionne sur le VLAN 4 natif.

*** Renseignez-vous auprès de l'intégrateur qui réalise l'installation de votre téléphonie. Les documentations de configuration des options DHCP pour la téléphonie sont sur le site du DR.**

3.11.5.3 Configuration

PRECONISATION DR : comme pour tout host (sauf les routeurs RAMAGE), il est demandé de configurer les interfaces LAN des téléphones IP en mode auto-négociation et de laisser les interfaces de swiches en mode auto (par défaut). Ensuite, il faut vérifier :

- **que la négociation s'est correctement déroulée et que les interfaces sont à 100 FULL**
- **qu'il n'y a aucune erreur sur les interfaces**

➔ ***Les commandes de vérification de ces paramètres sont indiquées plus bas.***

<u>En global sur tous les 3600 ou stack de 3600</u> :

```
<>system-view
#
voice vlan mac-address 0080-9f00-0000 mask ffff-ff00-0000** description ALCATEL**
#
** Exemple d'Alcatel ➔ veuillez adapter à votre contexte et ajouter toutes les plages d'adresses MAC nécessaires !!
```

<u>Sur les interfaces</u> :

```
<>system-view
#
interface Ethernet1/0/X
 description Phone+PMF François Pignon
 poe enable
 stp enable*
 stp edged-port enable
 [speed 100]
 [duplex full]
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 4 30
 port trunk pvid vlan 4
 undo voice vlan mode auto
 voice vlan 30 enable
 loopback-detection enable                    | détection des boucles
 loopback-detection action shutdown           | action suite détection des boucles
 loopback-detection enable                    | détection de boucles
 loopback-detection per-vlan enable           | détection de boucles
 multicast-suppression 20                     | limitation à 20% maxi du trafic multicast sur le port
 broadcast-suppression 20                     | limitation à 20% maxi du trafic broadcast sur le port
```

3.11.5.4 Vérifications

NEGOCIATION CORRECTE

<>display interface brief

```
The brief information of interface(s) under route mode:
Link: ADM - administratively down; Stby - standby
Protocol: (s) - spoofing
Interface         Link Protocol Main IP       Description
NULL0             UP   UP(s)   --
Vlan901           UP   UP      55.X.221.11

The brief information of interface(s) under bridge mode:
Link: ADM - administratively down; Stby - standby
Speed or Duplex: (a)/A - auto; H - half; F - full
Type: A - access; T - trunk; H - hybrid
Interface     Link Speed   Duplex Type PVID Description
Eth1/0/1      UP   100M    F      A    5    ROUTEUR          | ➔ (Access) forcé à 100 FULL
Eth1/0/2      UP   100M(a) F(a)   T    4    Tel + PMF        | auto-négo ➔ (Trunk)100 FULL OK
Eth1/0/3      DOWN auto    A      T    4    Libre            | Port libre prêt pour un Tel+PMF
```

…ETC.

NEGOCIATION NON CORRECTE

<>display interface brief

```
The brief information of interface(s) under route mode:
Link: ADM - administratively down; Stby - standby
Protocol: (s) - spoofing
Interface         Link Protocol Main IP       Description
NULL0             UP   UP(s)   --
Vlan901           UP   UP      55.X.221.11

The brief information of interface(s) under bridge mode:
Link: ADM - administratively down; Stby - standby
Speed or Duplex: (a)/A - auto; H - half; F - full
Type: A - access; T - trunk; H - hybrid
Interface     Link Speed   Duplex Type PVID Description
Eth1/0/1      UP   100M    F      A    5    ROUTEUR          | ➔ (Access) forcé à 100 FULL
Eth1/0/2      UP   100M(a) H(a)   T    4    Tel + PMF        | auto-négo ➔ (Trunk)100 HALF pas OK
Eth1/0/3      UP   10M(a)  F(a)   T    4    Tel + PMF        | auto-négo ➔ (Trunk)10 FULL : à vérifier
```

* Il peut arriver que des équipements aient une carte à 10 Mb/s…

…ETC.

ETAT DES INTERFACES CORRECT

CAS 1 : L'interface LAN du téléphone est en auto-négociation, l'interface du switch aussi :

<>display interface Ethernet 1/0/14

```
Ethernet1/0/14 current state: UP
IP Packet Frame Type: PKTFMT_ETHNT_2, Hardware Address: b8af-67ad-3949
Description: D. FAUCHEUX-1023/A
Loopback is not set
Media type is twisted pair
Port hardware type is  100_BASE_TX
100Mbps-speed mode, full-duplex mode
Link speed type is autonegotiation, link duplex type is autonegotiation
Flow-control is not enabled
The Maximum Frame Length is 10000
Broadcast MAX-ratio: 100%
Unicast MAX-ratio: 100%
Multicast MAX-ratio: 100%
Allow jumbo frame to pass
```

PVID: 6
Mdi type: auto
Port link-type: trunk
VLAN passing : 4, 30
VLAN permitted: 4, 30
Trunk port encapsulation: IEEE 802.1q
Port priority: 0
Last clearing of counters: 14:59:16 Wed 09/03/2014
Peak value of input: 4493263 bytes/sec, at 2014-09-17 13:13:13
Peak value of output: 5253181 bytes/sec, at 2014-09-11 12:12:49
Last 300 seconds input: 1 packets/sec 314 bytes/sec 0%
Last 300 seconds output: 11 packets/sec 1351 bytes/sec 0%
Input (total): 26843753 packets, 33468193849 bytes
26651301 unicasts, 144799 broadcasts, 47653 multicasts, 0 pauses
Input (normal): 26843753 packets, - bytes
26651301 unicasts, 144799 broadcasts, 47653 multicasts, 0 pauses
Input: 0 input errors, 0 runs, 0 giants, 0 throttles
0 CRC, 0 frame, - overruns, 0 aborts
- ignored, - parity errors
Output (total): 30962890 packets, 11241140965 bytes
19160039 unicasts, 8373963 broadcasts, 3428888 multicasts, 0 pauses
Output (normal): 30962890 packets, - bytes
19160039 unicasts, 8373963 broadcasts, 3428888 multicasts, 0 pauses
Output: 0 output errors, - underruns, - buffer failures
0 aborts, 0 deferred, 0 collisions, 0 late collisions
0 lost carrier, - no carrier

CAS 2 : L'interface LAN du téléphone est forcée à 100 FULL, l'interface du switch aussi :

<>display interface Ethernet 1/0/14
Ethernet1/0/14 current state: UP
IP Packet Frame Type: PKTFMT_ETHNT_2, Hardware Address: b8af-67ad-3949
Description: D. FAUCHEUX-1023/A
Loopback is not set
Media type is twisted pair
Port hardware type is 100_BASE_TX
100Mbps-speed mode, full-duplex mode
Link speed type is force link, link duplex type is force link
Flow-control is not enabled
The Maximum Frame Length is 10000
Broadcast MAX-ratio: 100%
Unicast MAX-ratio: 100%
Multicast MAX-ratio: 100%
Allow jumbo frame to pass
PVID: 6
Mdi type: auto
Port link-type: trunk
VLAN passing : 4, 30
VLAN permitted: 4, 30
Trunk port encapsulation: IEEE 802.1q
Port priority: 0
Last clearing of counters: 11:53:19 Thu 09/18/2014
Peak value of input: 86 bytes/sec, at 2014-09-18 11:53:36
Peak value of output: 176 bytes/sec, at 2014-09-18 11:53:36
Last 300 seconds input: 0 packets/sec 86 bytes/sec 0%
Last 300 seconds output: 1 packets/sec 176 bytes/sec 0%
Input (total): 391 packets, 45011 bytes
365 unicasts, 25 broadcasts, 1 multicasts, 0 pauses
Input (normal): 391 packets, - bytes
365 unicasts, 25 broadcasts, 1 multicasts, 0 pauses
Input: 0 input errors, 0 runs, 0 giants, 0 throttles
0 CRC, 0 frame, - overruns, 0 aborts
- ignored, - parity errors
Output (total): 629 packets, 75546 bytes
364 unicasts, 164 broadcasts, 101 multicasts, 0 pauses
Output (normal): 629 packets, - bytes
364 unicasts, 164 broadcasts, 101 multicasts, 0 pauses
Output: 0 output errors, - underruns, - buffer failures
0 aborts, 0 deferred, 0 collisions, 0 late collisions
0 lost carrier, - no carrier

ETAT DES INTERFACES NON CORRECT

CAS 3 : L'interface LAN du téléphone est forcée à 100 FULL, l'interface du switch en auto-négociation :

```
<>display interface Ethernet 1/0/14
Ethernet1/0/14 current state: UP
IP Packet Frame Type: PKTFMT_ETHNT_2, Hardware Address: b8af-67ad-3949
Description: D. FAUCHEUX-1023/A
Loopback is not set
Media type is twisted pair
Port hardware type is  100_BASE_TX
100Mbps-speed mode, half-duplex mode
Link speed type is autonegotiation, link duplex type is autonegotiation
Flow-control is not enabled
The Maximum Frame Length is 10000
Broadcast MAX-ratio: 100%
Unicast MAX-ratio: 100%
Multicast MAX-ratio: 100%
Allow jumbo frame to pass
PVID: 6
Mdi type: auto
Port link-type: trunk
 VLAN passing  : 4, 30
 VLAN permitted: 4, 30
 Trunk port encapsulation: IEEE 802.1q
Port priority: 0
Last clearing of counters:  14:59:16 Wed 09/03/2014
Peak value of input: 4493263 bytes/sec, at 2014-09-17 13:13:13
Peak value of output: 5253181 bytes/sec, at 2014-09-11 12:12:49
Last 300 seconds input:  35 packets/sec 3608 bytes/sec 0%
Last 300 seconds output:  34 packets/sec 3964 bytes/sec 0%
Input (total):  26857026 packets, 33469730552 bytes
     26663459 unicasts, 145697 broadcasts, 47870 multicasts, 0 pauses
Input (normal):  26857026 packets, - bytes
     26663459 unicasts, 145697 broadcasts, 47870 multicasts, 0 pauses
Input:  0 input errors, 0 runts, 0 giants, 0 throttles
     0 CRC, 0 frame, - overruns, 0 aborts
     - ignored, - parity errors
Output (total): 30983640 packets, 11243822858 bytes
     19170467 unicasts, 8380844 broadcasts, 3432329 multicasts, 0 pauses
Output (normal): 30983640 packets, - bytes
     19170467 unicasts, 8380844 broadcasts, 3432329 multicasts, 0 pauses
Output: 14 output errors, - underruns, - buffer failures
     0 aborts, 2 deferred, 8 collisions, 4 late collisions
     0 lost carrier, - no carrier
```

3.11.6 PMF seul

Un PMF seul (sans téléphone) peut être configuré comme suit **mais vous pouvez aussi le configurer comme ci-dessus, il sera ainsi prêt si un téléphone est un jour intercalé** :

```
<>system-view
#
interface Ethernet1/0/X                    | par exemple
 description PMF François Pignon
 undo poe enable
 stp enable                                | n'apparait pas en display current-configuration
 stp edged-port enable
 port link-type access                     | n'apparait pas en display current-configuration
 port access vlan 4
 [speed 100]
 [duplex full]
 loopback-detection enable                 | détection des boucles
 loopback-detection action shutdown        | action suite détection des boucles
 multicast-suppression 20                  | limitation à 20% maxi du trafic multicast sur le port
 broadcast-suppression 20                  | limitation à 20% maxi du trafic broadcast sur le port
```

3.11.7 Serveurs

Au siège, sauf exception, il n'est pas prévu de connecter des serveurs sur des 3600.
En agence, la connexion de serveur(s) devra être effectuée sur des ports 10/100/1000 si possible.

3.11.7.1 Serveur Physique (non VMWARE)

```
interface GigabitEthernet2/0/26                | par exemple
 description serveur intranet
 undo poe enable
 stp enable                                    | n'apparait pas en display current-configuration
 stp edged-port enable
 port link-type access                         | n'apparait pas en display current-configuration
 port access vlan 4
 [speed 1000]                                  | Si suffisamment de port Gb disponible
 [duplex full]
 loopback-detection enable                     | détection des boucles
 loopback-detection action shutdown            | action suite détection des boucles
 multicast-suppression 20                      | limitation à 20% maxi du trafic multicast sur le port
 broadcast-suppression 20                      | limitation à 20% maxi du trafic broadcast sur le port
```

3.11.7.2 Serveur Virtuel mono ou multi-Vlan

Nous préconisons l'interconnexion des serveurs virtuels VMWARE avec les switches HP **via des agrégats.**
Attention : dans ce cas, ne pas utiliser la commande « made enable » et mettre l'agrégat en mode statique. La procédure est disponible sur le **portail réseaux et Télécom du DR / rubrique LAN**.

3.11.8 Equipement e-GFA

```
interface Ethernet1/0/X
 description ….e-GFA…
 undo poe enable
 stp enable                                    | n'apparait pas en display current-configuration
 stp edged-port enable
 port link-type access                         | n'apparait pas en display current-configuration
 port access vlan 224
 speed 100                                     | préconisé – vérifiez avec « dis counters [inbound] [outbound] interface
 duplex full                                   | préconisé – vérifiez avec « dis counters [inbound] [outbound] interface
 loopback-detection enable                     | détection des boucles
 loopback-detection action shutdown            | action suite détection des boucles
 multicast-suppression 20                      | limitation à 20% maxi du trafic multicast sur le port
 broadcast-suppression 20                      | limitation à 20% maxi du trafic broadcast sur le port
```

3.11.9 Imprimante

```
interface Ethernet1/0/X
 description IMPRIMANTE-1
 undo poe enable
 stp enable                                  | n'apparait pas en display current-configuration
 stp edged-port enable
 port link-type access                       | n'apparait pas en display current-configuration
 port access vlan 226 (ou 227)                       | 227 pour Les services medicaux
 loopback-detection enable                   | détection des boucles
 loopback-detection action shutdown          | action suite détection des boucles
 multicast-suppression 20                    | limitation à 20% maxi du trafic multicast sur le port
 broadcast-suppression 20                    | limitation à 20% maxi du trafic broadcast sur le port
```

3.11.10 BOX « Evasion internet »

Le port d'interconnexion entre le switch de tête et la BOX ORANGE sera de type ACCESS sur le VLAN 17. La vitesse de connexion est fixée à Duplex Full en 100 ou 1000 selon les switches.
Autant que possible, la BOX devra être connectée directement sur le switch fédérateur (stack de tête connecté à RAMAGE).

```
 interface GigabitEthernet1/0/X
 description BOX-EVASION-INTERNET
 port link-mode bridge
 port access vlan 17
 [speed 1000 ou 100]                         | voir les documentations projet
 [duplex full]
```

REMARQUE : si la Box n'est pas connectée au fédérateur mais sur un switch d'extrémité, il faut ajouter le VLAN 17 en permit sur l'agrégat d'interconnexion côté fédérateur et côté extrémité sur tout le chemin :

```
interface Bridge-AggregationX
 description NORMALISEE
 port trunk permit vlan 17
```

3.11.11 Borne wifi

```
interface gi1/0/X
 description normalisée                      | obligatoire : voir les référentiels
 stp enable                                  | n'apparait pas en display current-configuration
 stp edged-port enable
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 50 54 902            | voir les documentations WIFI sur le portail du DR
 loopback-detection enable
 loopback-detection action shutdown
 broadcast-suppression 20
 multicast-suppression 20
 poe enable
```

3.11.12 Contrôleur wifi

```
interface Bridge-AggregationX                    | X = Id de l'interface Bridge-Aggregation
 description normalisée                          | obligatoire : voir les référentiels
 stp enable                                      | n'apparait pas en display current-configuration
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 50 54 902                | voir doc wifi (409NT0050 sur le portail du DR)
 port trunk pvid vlan 902
 link-aggregation mode dynamic
 dhcp-snooping trust
#
interface GigabitEthernet1/0/7
 description normalisée                          | obligatoire : voir les référentiels
 port link-mode bridge
 stp enable                                      | n'apparait pas en display current-configuration
 description Contrôleur wifi
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 50 54 902                | voir doc wifi (409NT0050)
 port trunk pvid vlan 902
 port link-aggregation group X                   | X = Id de l'interface Bridge-Aggregation
#
interface GigabitEthernet2/0/7
 description normalisée                          | obligatoire : voir les référentiels
 port link-mode bridge
 stp enable                                      | n'apparait pas en display current-configuration
 description Contrôleur wifi
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 50 54 902                | voir doc wifi (409NT0050)
 port trunk pvid vlan 902
 port link-aggregation group X                   | X = Id de l'interface Bridge-Aggregation
```

3.11.13 Boitier pour portail captif wifi

(exemple « Ucopia »)

Il y a une interface à connecter sur le LAN :

```
interface GigabitEthernet1/0/X
description UCOPIA-IN
undo port trunk permit vlan 1
port trunk permit vlan 54 900                   |Vlan 54 - voir doc wifi (409NT058)
port trunk pvid vlan 900                        | Vlan 900  - voir doc wifi (409NT058)
loopback-detection enable
loopback-detection action shutdown
broadcast-suppression 20
multicast-suppression 20
dhcp-snooping trust
stp enable                                      | n'apparait pas en display current-configuration
stp edged-port enable
```

3.11.14 Passerelle CETIAM

Les passerelles (ou Gateway) CETIAM sont à connecter dans le vlan 230 en 58.X.230.Y /29 (255.255.255.248) **SUR LE FEDERATEUR AUTANT QUE POSSIBLE**. Voir les référentiels LAN et les documentations de la téléphonie. Le plan d'adressage de vos passerelles (si besoin) vous sera communiqué dans le cadre du projet CETIAM. Exemples :

VLAN 230 - NOM "GW-CETIAM"									
Organisme	Site	Sous-réseau	Masque	Interface vlan 230	Passerelle1	Passerelle2	Passerelle3	Passerelle4	Passerelle5
PROTOTYPE	CPAM 901	58.230.0.0	255.255.255.248	58.230.0.1	58.230.0.2	58.230.0.3	58.230.0.4	58.230.0.5	58.230.0.6
PROTOTYPE	CP 901	58.230.0.8	255.255.255.248	58.230.0.9	58.230.0.10	58.230.0.11	58.230.0.12	58.230.0.13	58.230.0.14
PROTOTYPE	CP 902	58.230.0.16	255.255.255.248	58.230.0.17	58.230.0.18	58.230.0.19	58.230.0.20	58.230.0.21	58.230.0.22
CPAM Alpes-de-Haute-Provence	SIEGE DIGNE	58.230.0.24	255.255.255.248	58.230.0.25	58.230.0.26	58.230.0.27	58.230.0.28	58.230.0.29	58.230.0.30
CPAM Alpes-de-Haute-Provence	Manosque	58.230.0.32	255.255.255.248	58.230.0.33	58.230.0.34	58.230.0.35	58.230.0.36	58.230.0.37	58.230.0.38
CPAM Alpes-de-Haute-Provence	...etc.	58.230.0.40	255.255.255.248	58.230.0.41	58.230.0.42	58.230.0.43	58.230.0.44	58.230.0.45	58.230.0.46

La passerelle sera pré-configurée par l'intégrateur avec l'une des adresses IP du vlan 230 réservé au site.

1°/ Dans le fédérateur N3 : création du vlan 230 avec son nom

```
system-view
#
vlan 230
name VLAN-GW-CETIAM
#
interface vlan 230
des INT-VLAN-GW-CETIAM
ip address 58.230.0.X 255.255.255.248
#
```

2°/ Interface sur le switch de connexion de chaque passerelle

```
system-view
#
interface Et (ou Gi) x/0/y (exemple Et1/0/10)
 description GWX-CETIAM (exemple GW1-CETIAM)
 port link-mode bridge
 port link-type access
 port access vlan 230
 loopback-detection enable
 loopback-detection action shutdown
 broadcast-suppression 20
 multicast-suppression 20
#
Save force
```

3.11.15 IPBX (hors Cetiam)

Si un IPBX doit être connecté sur un 3600, le connecter de préférence sur un port giga.

```
interface Ethernet1/0/11
 port link-mode bridge
 description IPBX-CONSTRUCTEUR
 port access vlan 30
 undo voice vlan mode auto
 [speed 100 ou 1000]          | A adapter en fonction de l'IPBX et des observations
 [duplex full]                | A adapter en fonction de l'IPBX et des observations
 loopback-detection enable
 broadcast-suppression 20
 multicast-suppression 20
 stp edged-port enable
```

3.11.16 Passerelle « Audiocodes » (hors Cetiam)

```
interface Ethernet1/0/11
 port link-mode bridge
 description AUDIOCODE1 (ou 2 …)
 port access vlan 30
 undo voice vlan mode auto
 speed 100
 duplex full
 loopback-detection enable
 broadcast-suppression 20
 multicast-suppression 20
 stp edged-port enable
```

3.12 INTERCONNEXION DES SWITCHES

Dans les sièges, les HP 3600 sont placés à l'extrémité du réseau et connectés au cœur : les fédérateurs HP 5500. Il va donc falloir configurer des trunks d'interconnexion sur des interfaces en veillant à n'autoriser que les VLAN nécessaires à transiter (« permit vlan x y … »). En effet, sur les interfaces des 3600, on ne trouve que des téléphones ou des PMF : seuls les vlan 4 et 30 sont utiles sur ces trunks d'interco – sans oublier le VLAN 901 pour permettre l'administration.

Dans les architectures « Full HP » normalisées des sièges d'Organismes (cf Référentiels), les interconnexions des 5510 ou 5520 et des 3600 sont à faire via des liens agrégés. Vous trouverez ci-dessous la configuration des trunks d'interconnexion AVEC ou SANS agrégation (si besoin).



Pas de « stp edged-port enable » sur les trunks d'interconnexion de switches !!!

3.12.1 Règles de nommage

Description des agrégats ou de liens trunks simples

Le nommage des agrégats et des trunk est normalisé :

[]description [Type]-[Num]-[Niv]-[MOD]-*[DESCRIPTION]*

[type] = type de lien sur 3 digits (AGG; LIEN; ...)
[num] = numéro de l'agrégat (Num = 10, 20, 30,… (Suggestion 10 : 1er étage, 20 : 2ème étage...)
[niv] = vers un Niveau du switch (N2, N3)
[mod] = modèle de switch (3600)
[description] = optionnel ➔ répartiteur ou baie ou étage ou @IP du switch distant

Le nommage se fait via la commande « description » sur l'interface « Bridge-Aggregation ».

Exemples :

Interface Bridge-Aggregation10
description AGG-010-N2-3600-ETAGE1 | Agrégat n° 10 vers niveau2 de type HP 3600 du 1er ETAGE

Interface Bridge-Aggregation11
description AGG-011-N3-3600-RG | Agrégat n° 11 vers niveau3 de type HP 3600 du Répartiteur Général

Autres possibilités :
AGG-010-N2-3600-SW-020 | Agrégat numéro 10 vers niveau2 de type HP 3600 d'@ip 55.xx.221.20
LIEN-010-N2-3600-ETAGE1 | Lien simple numéro 10 vers niveau2 de type HP 3600 du 1er ETAGE

Lien trunk placé dans un agrégat :

[]description [Type]-[Num]-[Niv]-[MOD]-*[DESCRIPTION]*-[LIEN n°]

Exemples :

Interface GigabitEthernet1/0/25
description AGG-010-N2-3600-ETAGE1-LIEN1 | description du 1er lien de l'agrégat 10

Interface GigabitEthernet1/0/25
description AGG-010-N2-3600-ETAGE1-LIEN2 | description du 2ème lien de l'agrégat 10

3.12.2 Utilisation des ports « combo »

Les 3600-v2 disposent de ports gigabits utilisables pour l'interconnexion :
- les ports 25T, 25S, 26T et 26S pour le modèle 3600-24
- les ports 49T, 49S, 50T et 50S pour le modèle 3600-48

Les ports T sont « combo » avec les ports S : soit c'est le port 10/100/1000 cuivre « T » qui est actif, soit c'est le port SFP « S » qui est actif (ne peuvent pas être actifs en même temps) :

3600-48 v2 :	3600-24 v2 :
	

Les ports « combo » sont entourés de gris clair. **Par défaut, ce sont les ports cuivre 10/100/1000 (T) qui sont actifs. Pour activer l'un ou l'autre, il faut utiliser les commandes « combo enable… ».**

Exemples avec le port 25 :

Pour activer le port « S » (fibre optique) :

interface GigabitEthernet1/0/25
combo enable fiber

Pour activer le port « T » (cuivre) :

interface GigabitEthernet1/0/25
combo enable copper

Pour les modèles à 48 ports le principe est le même, seul le numéro des interfaces change, évidemment.

3.12.3 Interconnexion de switches AVEC AGREGATION

3.12.3.1 Présentation



A quoi ça sert ?

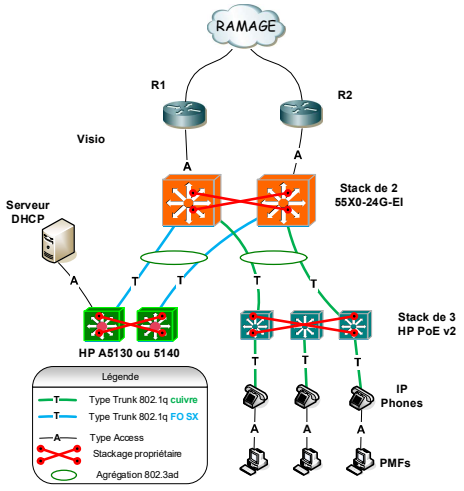
Un agrégat est une association de liens entre deux switches. Lorsque les deux switches sont proches (même baie ou même répartiteur) ou que le pré câblage d'immeuble met plusieurs rocades (cuivre ou fibre) à disposition, il est intéressant de multiplier les liens entre les switches. Ainsi, au lieu de monter une interconnexion de switches à 1 Gb/s, on monte par exemple deux liens à 1 Gb/s (et non un lien à 2 Gb/s). Le trafic est réparti automatiquement par les switches sur les « n » liens. Cette technologie est standardisée (IEEE 802.3ad) ; en terminologie Cisco, on appelle ça un « Etherchannel ». Si le nombre d'interfaces disponibles et le pré câblage le permettent, il est possible d'ajouter … jusqu'à 8 interfaces. Il est conseillé d'agréger les liens par paire (2, 4, 6 ou 8 et pas 3, 5 ou 7).

Du coup, comme expliqué dans les Référentiels LAN, on va pouvoir configurer des agrégats au niveau de toutes les interconnexions de switches HP (si le pré câblage le permet). Un stack étant vu comme un seul switch logique (une seule adresse MAC), la configuration d'un agrégat entre deux stacks est possible.

3.12.3.2 Architectures

ARCHITECTURES NORMALISEES :

Cas d'un siège d'organisme : interconnexion du stack 55X0 et des stacks 3600 et de 51X0 en agrégation :



Les stacks de 3600 et de 5130 (ou 5140) doivent être interconnectés aux stack fédérateur de 5500 via un agrégat à 2 x 1 Gb/s.

Interface à utiliser :

3600 ➔ interfaces 25T ou 25S :

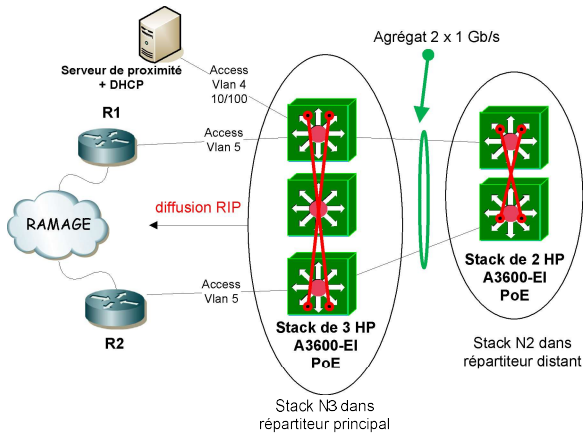
*GigabitEthernet**1**/0/25 du switch n°1 du stack*
*GigabitEthernet**X**/0/25 du dernier switch (X) du stack*

51X0 :
Utiliser une interface sur chaque 51X0, cuivre ou fibre selon la position des switches sur le réseau (répartiteur) et du pré câblage.

Cas d'un CP avec plusieurs stacks (plusieurs répartiteurs distants) :

Dans ce cas, on construira un stack de 3600 N3 en central interconnecté via des agrégats doubles à des stacks de 3600 N2. Il restera de nombreux ports 10/100/1000 Mb/s pour des serveurs (en orange sur l'exemple 2) :

Exemple 1 : un stack fédérateur N3 et un ou plusieurs stack distants N2 (autre répartiteur) :



Les stacks de 3600 N2 doivent être interconnectés au stack fédérateur de 3600 N3 via un agrégat à 2 x 1 Gb/s.

Interface à utiliser :

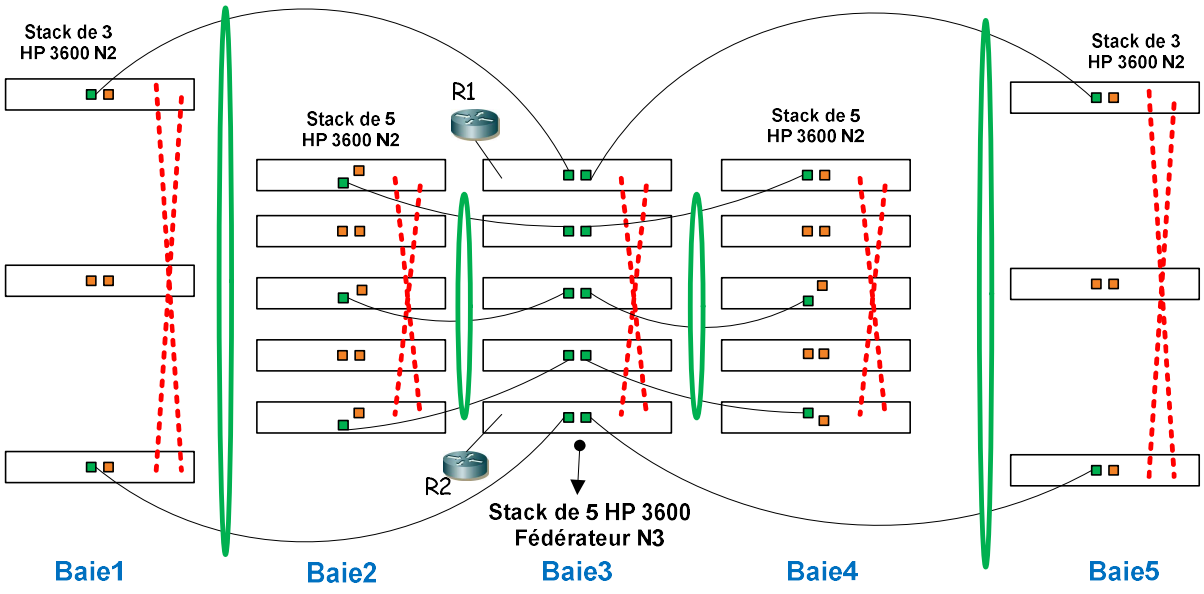
3600 ➔ interfaces 25T ou 25S :

*GigabitEthernet**1**/0/25 du switch n°1 du stack*
*GigabitEthernet**X**/0/25 du dernier switch (X) du stack*

S'il y a un deuxième stack de 3600 N2, utilisez de même les ports 26T ou 26S.

S'il y en plus, contactez le DR…

Exemple 2 : un stack N3 dans un répartiteur unique avec plusieurs baies :



On retrouve ce cas ci-dessus dans de grosses agences (ex : un des anciens sièges de CPAM fusionnées).

3.12.3.3 Configuration des agrégats

Méthode :

Il est indispensable de renseigner les mêmes paramètres au niveau de l'interface « Bridge-Aggregation » et au niveau des interfaces agrégées. Pour cela, utilisez la méthode suivante :

1°/ Créer l'interface « Bridge-Aggregation »

2°/ Attacher les 2 ou N (N paire de préférence et N = 8 max) interfaces à agréger à l'interface « Bridge-Aggregation » (port link-aggregation group 1). Vérifier qu'elles ne sont pas « shutdown ».

3°/ Configurer les autres paramètres sur l'interface « Bridge-Aggregation » : ils seront automatiquement reportés sur les interfaces attachées.



Attention, pour les trunks :
1/ Il ne faut pas oublier le *VLAN 901 d'Admin-Réseau.*
2/ **Pas de** « stp edged-port enable » !
3/ Ajouter le vlan 902 ADMIN-WIFI (si vous avez du wifi dans votre organisme)
4/ Ne pas oublier d'ajouter la description **normalisée**

Exemple en siège d'organisme avec les vlan 4 Data et 30 Voix, sans oublier le VLAN d'admin-reseau (901) – Cas d'un agrégat entre un stack de 2 HP 55X0 et un stack de « n » HP 3600 :

Côté 3600 – (en « system-view) :

```
interface Bridge-Aggregation 1                  | N° de l'agrégat
 link-aggregation mode dynamic
#
interface GigabitEthernet1/0/25                 | interface normalisée
 port link-aggregation group 1
#
Interface GigabitEthernetn/0/25                 | interface normalisée
 port link-aggregation group 1
#
interface Bridge-Aggregation 1                  | N° de l'agrégat ci-dessus
 stp enable
 port link-type trunk
 port trunk permit vlan 4 30 901 902
 undo port trunk permit vlan 1
 mad enable                  | Optimise les dialogues inter-stacks - au prompt, le domain IRF est proposé – vérifier que c'est le bon et valider (sinon CTRL C)
 stp loop-protection         | Evite attaques et dysfonctionnements ➔ voir $ 5.3
```

Côté 55X0 (fédérateur) - (en « system-view):

```
interface Bridge-Aggregation 1                  | N° de l'agrégat
 description NORMALISEE
 link-aggregation mode dynamic
#
interface GigabitEthernet1/0/5                  | par exemple
 port link-aggregation group 1
#
Interface GigabitEthernet2/0/5                  | par exemple
 port link-aggregation group 1
#
interface Bridge-Aggregation 1                  | N° de l'agrégat ci-dessus
 description NORMALISEE
 stp enable
 port link-type trunk
 port trunk permit vlan 4 30 901 902
 undo port trunk permit vlan 1
 mad enable                  | Optimise les dialogues inter-stacks - au prompt, le domain IRF est proposé – vérifier que c'est le bon et valider (sinon CTRL C)
 stp root-protection         | Evite attaques et dysfonctionnements ➔ voir $ 5.3
```

3.12.3.4 Ajout d'une interface dans un agrégat existant

Sur la base de l'agrégat configuré ci-dessus (côté 3600), en « system-view » :

1/ Mettre l'interface en configuration usine si besoin :

interface GigabitEthernet1/0/26 | par exemple
default

2/ Ajouter l'interface dans l'agrégat

interface GigabitEthernet1/0/26 | par exemple
description NORMALISEE
stp enable
port link-type trunk
port trunk permit vlan 4 30 901 902
undo port trunk permit vlan 1
port link-aggregation group 1 | N° de l'agrégat

3/ Renvoyer la configuration complète de l'interface bridge-aggrégation (copié – collé)

interface Bridge-Aggregation 1 | N° de l'agrégat de l'exemple
description NORMALISEE
stp enable
port link-type trunk
port trunk permit vlan 4 30 901 902
undo port trunk permit vlan 1
mad enable | Optimise les dialogues inter-stacks - au prompt, le domain IRF est proposé – vérifier que c'est le bon et valider (sinon CTRL C)
[stp loop-protection] | Côté switch N2 ➔ voir $ 5.3
[stp roop-protection] | Côté switch N3➔ voir $ 5.3

3.12.3.5 Vérification

Une fois la configuration effectuée, connecter les interfaces avec les câbles adéquats. La commande suivante permet alors de verifier le fonctionnement.

<>display link-aggregation verbose

Exemple pour un agrégat de 2 ports sur un stack de 5500 :

```
<>dis link-aggregation verbose
Loadsharing Type: Shar -- Loadsharing, NonS -- Non-Loadsharing
Port Status: S -- Selected, U -- Unselected
Flags:  A -- LACP_Activity, B -- LACP_Timeout, C -- Aggregation,
        D -- Synchronization, E -- Collecting, F -- Distributing,
        G -- Defaulted, H -- Expiresd

Aggregation Interface: Bridge-Aggregation1
Aggregation Mode: Dynamic
Loadsharing Type: Shar
System ID: 0x8000, 3822-d609-8306
Local:
  Port             Status  Priority Oper-Key  Flag
--------------------------------------------------------------------------------
  GE1/0/1          S       32768    1         {ACDEF}
  GE1/0/2          S       32768    1         {ACDEF}
Remote:
  Actor            Partner Priority Oper-Key  SystemID               Flag
--------------------------------------------------------------------------------
  GE1/0/1          26      32768    1         0x8000, 3822-d610-f396 {ACDEF}
  GE1/0/2          27      32768    1         0x8000, 3822-d610-f396 {ACDEF}
```

Vérifiez que les "flags" soient bien tous à "ACDEF".

Autre commande :

<>Display link-aggregation summary

```
<3600>dis link-aggregation summary
Aggregation Interface Type:
BAGG -- Bridge-Aggregation, RAGG -- Route-Aggregation
Aggregation Mode: S -- Static, D -- Dynamic
Loadsharing Type: Shar -- Loadsharing, NonS -- Non-Loadsharing
Actor System ID: 0x8000, 7848-59a2-9a58

AGG        AGG      Partner ID            Select Unselect   Share
Interface  Mode                          Ports  Ports      Type
--------------------------------------------------------------------------------
BAGG1      D        0x8000, 7848-59a8-714c  2     0        Shar
BAGG2      D        0x8000, 7848-5997-a9cc  2     0        Shar
BAGG3      D        0x8000, bcea-fa3b-2efe  2     0        Shar
BAGG4      D        0x8000, 7848-5997-b044  2     0        Shar
BAGG5      D        0x8000, 7848-5997-ac54  2     0        Shar
BAGG6      D        0x8000, bcea-fa3b-3216  2     0        Shar
BAGG7      D        0x8000, d07e-28f3-7060  2     0        Shar
BAGG8      D        0x8000, 7848-5981-8b12  2     0        Shar
BAGG9      D        0x8000, 7848-5997-b284  2     0        Shar
BAGG10     D        0x8000, bcea-fa3b-1c6e  2     0        Shar
BAGG11     D        0x8000, 7848-5997-a93c  2     0        Shar
BAGG12     D        0x8000, 7848-5997-ab34  2     0        Shar
BAGG13     D        0x8000, bcea-fa3b-2eb6  1     1        Shar
BAGG14     D        0x8000, 7848-5953-6c98  2     0        Shar
<3600>
```

⇨ **Vérifier que le mode est bien « D » (Dynamique) pour les agrégats d'interconnexion de switches** ***(les agrégats vers des serveurs ESX doivent être en « S » (statique) ➔ voir doc plus haut.)***

3.13 INTERCONNEXION DE SWITCHES SANS AGREGATION

Exemple en siège d'organisme d'un trunk entre un 55X0 fédérateur et un 3600 qui dessert des IP-Phones et des PMF dans les VLAN 4 Data, 30 Voix :

Côté 55X0 fédérateur - (en system-view) :

```
interface GigabitEthernet1/0/X
 stp enable                                  | n'apparaît pas en « display current-configuration »
 description NORMALISEE
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 4 30 901 902
```

Côté 3600 - (en system-view) :

```
interface GigabitEthernet1/0/25              | Interface normalisée
 description NORMALISEE
 stp enable                                  | n'apparaît pas en « display current-configuration »
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 4 30 901 902
```

Attention, pour les trunks :

Il ne faut pas oublier le *VLAN 901 d'Admin-Réseau.*
Pas de « stp edged-port enable » !

3.14 CONFIGURATION DU DHCP

DHCP peut être utilisé au niveau des réseaux locaux pour distribuer les adresses IP automatiquement vers les clients (PMF et téléphones). Veuillez suivre les recommandations de la procédure DR NA-072-001 : *Préconisations DHCP.*

La procédure est disponible sur le **portail réseaux et Télécom du DR / rubrique Produits ➔ DHCP**.

Préconisation Cnam : le serveur DHCP pour les téléphones et les PMF est le contrôleur Windows (local (serveur de proximité en CP) ou distant (celui du siege)).

1.1 DHCP-RELAY



A quoi ça sert ?

Au démarrage (et ensuite périodiquement) les clients (PMF ou téléphones) émettent un broadcast (requête émise vers toutes les adresses d'un (sous-)réseau) pour trouver le serveur DHCP. Les broadcasts sont des trames qui ne sont pas transmises en dehors du (sous-)réseau d'où il est émis : ils ne traversent pas les routeurs et ne sont pas propagés non plus vers les autres VLAN. Pourtant, on peut avoir des clients dans des VLAN différents (cas des PMF et des téléphones) mais un seul serveur DHCP positionné dans le VLAN 4. Les clients se trouvant dans le même VLAN vont le trouver grâce au broadcast mais ceux des autres VLAN devront trouver un relais vers le serveur DHCP. Ce relais doit être indiqué sur l'interface VLAN.

IL FAUT DONC UN RELAIS POUR TOUTES LES INTERFACES VLAN CLIENTES du DHCP Y COMPRIS POUR LE WIFI (VLAN 50).

MAIS : il ne faut pas configurer de relais sur l'interface VLAN du VLAN dans lequel se trouve le serveur DHCP (cela peut poser des problèmes techniques).

En siège d'organisme, les 3600 ne sont pas configurés au niveau 3, il n'est donc pas nécessaire de configurer cette partie dans les 3600. Reportez-vous au guide des HP 5XXX qui eux auront ce rôle à jouer.

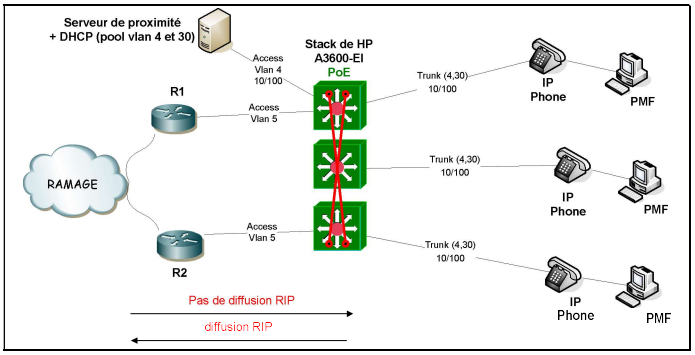
Le DHCP relais est à configurer dans les CP où on trouve des 3600 niveau 3 en stack.

Ne pas configurer le DHCP-Relay sur l'interface-VLAN du VLAN dans lequel se trouve le serveur dhcp :

1/ c'est inutile

2/ cela peut générer des problèmes techniques

CAS 1 : Le DHCP est local (serveur DHCP local) :



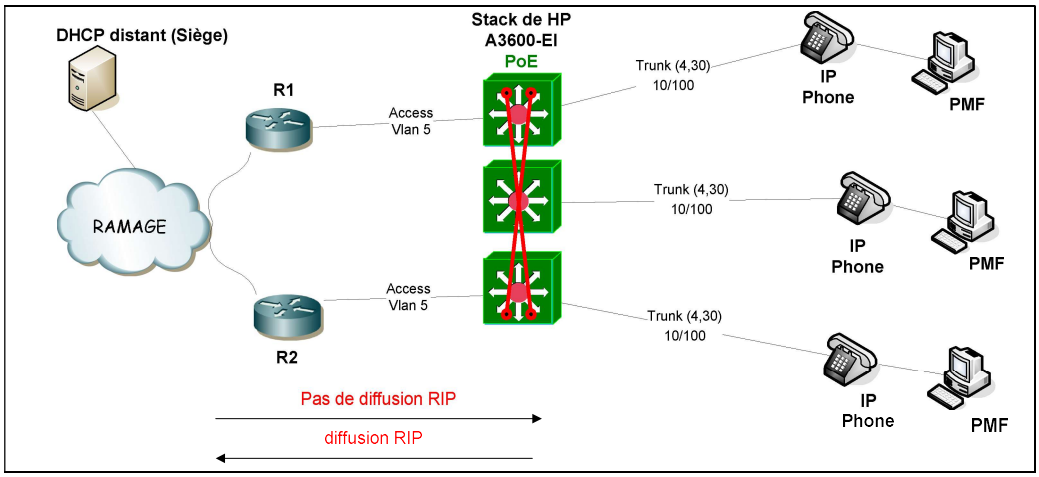
Le serveur DHCP est connecté sur l'interface Gi 1/0/25, en « access » dans le VLAN 4 :

- Diffusion aux PMF : pas de problème (même VLAN)
- Diffusion aux téléphones : il faut relayer la demande d'adresse vers le serveur qui se trouve dans un autre VLAN.

Configuration du CAS 1 :

```
<>system-view
#
dhcp enable
dhcp relay server-group 1 ip @IP-serveur-DHCP-local
#
interface Vlan-interface30
 description INT-VLAN-VOIX
 ip address 58.X.8.1 22
 dhcp select relay
 dhcp relay server-select 1
#
interface GigabitEthernet1/0/25
 port link-mode bridge
 description Serveur DHCP
 port access vlan 4
 stp enable                          | n'apparait pas en display current-configuration
 stp edged-port enable
 [dhcp-snooping trust]               | voir plus bas « DHCP snooping »
```

CAS 2 : Le DHCP est distant (au siège) : il faut appliquer les commandes de relais sur toutes les interfaces VLAN concernant des clients DHCP : les VLAN 4 et 30.

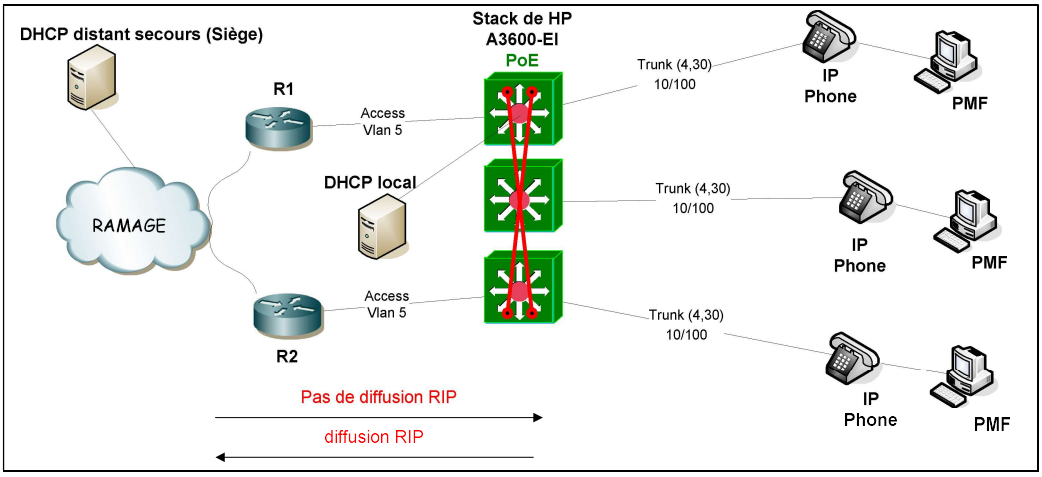


Configuration du CAS 2 :

```
<>system-view
#
dhcp enable
dhcp relay server-group 1 ip @IP-serveur-DHCP-backup-distant

interface Vlan-interface30
 description INT-VLAN-VOIX
 ip address 58.X.8.1 22
 dhcp select relay
 dhcp relay server-select 1
#
interface Vlan-interface4
 description INT-VLAN-DATA
 ip address 55.X.8.1 22
 dhcp select relay
 dhcp relay server-select 1
```

CAS 3 : Le DHCP est en local et un secours distant existe (au siège) : il faut appliquer les commandes de relais sur toutes les interfaces VLAN concernant des clients DHCP : les VLAN 4 et 30.



Dans ce cas, il faut créer sur les deux serveurs les pool DHCP de manière identique. Les deux serveurs DHCP sont sollicités par les clients (PMF, Téléphones …) et c'est le plus rapide à répondre (donc le local…) qui est utilisé. Si le serveur local est HS, le distant fera le travail, à l'expiration du bail.

Configuration du CAS 3 :

```
<>system-view
#
dhcp enable
dhcp relay server-group 1 ip @IP-serveur-DHCP-local
dhcp relay server-group 1 ip @IP-serveur-DHCP-backup-distant

interface Vlan-interface30
 description INT-VLAN-VOIX
 ip address 58.X.8.1 22
 dhcp select relay
 dhcp relay server-select 1
#
interface Vlan-interface4
 description INT-VLAN-DATA
 ip address 55.X.8.1 22
 dhcp select relay
 dhcp relay server-select 1
```

3.14.1 DHCP-Snooping



A quoi ça sert ?

DHCP-Snooping est utilisé pour éviter la mise en œuvre d'un serveur DHCP pirate en sécurisant la fonction DHCP sur un réseau. Veuillez consulter la procédure 072NA001_Préconisations_DHCP sur l'intranet du DR pour plus d'explications.

Les commandes ci-dessous sont donc à configurer sur tous les switches du réseau utilisant un serveur DHCP.

S'il y a serveur DHCP local (avec ou sans secours distant) : appliquer les points 1, 2 et 3.
Si le serveur DHCP est distant seulement (pas de serveur local) : appliquer les points 2 et 3.



Ne pas configurer le DHCP-snooping sur un LAN construit d'un mélange de Cisco et de HP.



Attention à respecter l'ordre ci-dessous (1/ Serveur DHCP, 2/ Trunks, 3/ Global)

1/ Interface « Access » sur laquelle est connecté le serveur DHCP (si présent localement) :

Exemple sur un 5120:

```
<>system-view
#
interface GigabitEthernet1/0/6
 port link-mode bridge
 description Serveur DHCP
 port access vlan 4
 stp enable                                  | n'apparait pas en display current-configuration
 stp edged-port enable
 dhcp-snooping trust
```

2/ Toutes les interfaces des 3600 par lesquels la réponse du serveur DHCP doit arriver :

- Toutes les interfaces « Trunk » d'interconnexion de switches
- Toutes les interfaces « bridge-aggregation »

Exemples :

Interfaces trunks :	**Agrégats :**
<>system-view # int GigabitEthernet 1/0/25 **description NORMALISEE** port link-type trunk undo port trunk permit vlan 1 port trunk permit vlan 4 30 901 **dhcp-snooping trust**	<>system-view # interface Bridge-Aggregation1 **description NORMALISEE** port link-type trunk undo port trunk permit vlan 1 port trunk permit vlan 4 30 901 link-aggregation mode dynamic **dhcp-snooping trust**

3/ En Global sur le switch :

```
<>system-view
#
dhcp-snooping
 DHCP Snooping is enabled.
```

3.15 ROUTAGE

3.15.1 Routage dans les fédérateurs niveau 3 TOUS SITES

La configuration du routage est EXCLUSIVEMENT gérée par le DR qui s'occupe de supprimer le RIP et mettre en œuvre le BGP.

NE JAMAIS MODIFIER !!

Pour information, voici les Masters de configuration du routage BGP configure par le DR en fonction des profils. IL NE FAUT PAS MODIFIER CES CONFIGURATIONS:

Profil 1 :	Profil 2 :
interface LoopBack0 ip address $LOOPBACK 255.255.255.255 # ip community-list basic LP500 permit 65005:50 ip community-list basic LP400 permit 65005:40 ip community-list basic LP300 permit 65005:30 ip community-list basic LP200 permit 65005:20 ip community-list basic LP100 permit 65005:10 ip community-list basic LP50 permit 65005:5 ip community-list basic LP10 permit 65005:1 # route-policy BGP-IN permit node 10 if-match community LP500 apply local-preference 500 apply community no-advertise additive route-policy BGP-IN permit node 20 if-match community LP400 apply local-preference 400 apply community no-advertise additive route-policy BGP-IN permit node 30 if-match community LP300 apply local-preference 300 apply community no-advertise additive route-policy BGP-IN permit node 40 if-match community LP200 apply local-preference 200 apply community no-advertise additive route-policy BGP-IN permit node 50 if-match community LP100 apply local-preference 100 apply community no-advertise additive route-policy BGP-IN permit node 60 if-match community LP50 apply local-preference 50 apply community no-advertise additive route-policy BGP-IN permit node 70 if-match community LP10 apply local-preference 10 apply community no-advertise additive route-policy BGP-OUT-BTEL permit node 10 apply community 65005:110 route-policy BGP-OUT-NXO permit node 10 apply community 65005:210 # bgp 65005 router-id $LOOPBACK preference 50 50 50 undo synchronization timer keepalive 5 hold 15 import-route direct peer $OP1 as-number $AS1 peer $OP1 route-policy BGP-IN import	interface LoopBack0 ip address $LOOPBACK 255.255.255.255 # ip community-list basic LP500 permit 65005:50 ip community-list basic LP400 permit 65005:40 ip community-list basic LP300 permit 65005:30 ip community-list basic LP200 permit 65005:20 ip community-list basic LP100 permit 65005:10 ip community-list basic LP50 permit 65005:5 ip community-list basic LP10 permit 65005:1 # route-policy BGP-IN permit node 10 if-match community LP500 apply local-preference 500 apply community no-advertise additive route-policy BGP-IN permit node 20 if-match community LP400 apply local-preference 400 apply community no-advertise additive route-policy BGP-IN permit node 30 if-match community LP300 apply local-preference 300 apply community no-advertise additive route-policy BGP-IN permit node 40 if-match community LP200 apply local-preference 200 apply community no-advertise additive route-policy BGP-IN permit node 50 if-match community LP100 apply local-preference 100 apply community no-advertise additive route-policy BGP-IN permit node 60 if-match community LP50 apply local-preference 50 apply community no-advertise additive route-policy BGP-IN permit node 70 if-match community LP10 apply local-preference 10 apply community no-advertise additive route-policy BGP-OUT-BTEL permit node 10 apply community 65005:120 route-policy BGP-OUT-NXO permit node 10 apply community 65005:221 # bgp 65005 router-id $LOOPBACK preference 50 50 50 undo synchronization timer keepalive 5 hold 15 import-route direct peer $OP1 as-number $AS1 peer $OP1 route-policy BGP-IN import

peer $OP1 route-policy BGP-OUT-BTEL export peer $OP1 advertise-community peer $OP1 password cipher $PWD1 peer $OP2 as-number $AS2 peer $OP2 route-policy BGP-IN import peer $OP2 route-policy BGP-OUT-NXO export peer $OP2 advertise-community peer $OP2 password cipher $PWD2	peer $OP1 route-policy BGP-OUT-BTEL export peer $OP1 advertise-community peer $OP1 password cipher $PWD1 peer $OP2 as-number $AS2 peer $OP2 route-policy BGP-IN import peer $OP2 route-policy BGP-OUT-NXO export peer $OP2 advertise-community peer $OP2 password cipher $PWD2

Profil 3 :	**Profil 4 :**
interface LoopBack0 ip address $LOOPBACK 255.255.255.255 # ip community-list basic LP500 permit 65005:50 ip community-list basic LP400 permit 65005:40 ip community-list basic LP300 permit 65005:30 ip community-list basic LP200 permit 65005:20 ip community-list basic LP100 permit 65005:10 ip community-list basic LP50 permit 65005:5 ip community-list basic LP10 permit 65005:1 # route-policy BGP-IN-ACTIF permit node 10 apply local-preference 400 apply community no-advertise additive route-policy BGP-IN-PASSIF permit node 10 apply community no-advertise additive route-policy BGP-OUT-BTEL permit node 10 apply community 65005:130 route-policy BGP-OUT-NXO permit node 10 apply community 65005:231 # bgp 65005 router-id $LOOPBACK preference 50 50 50 undo synchronization timer keepalive 5 hold 15 import-route direct peer $OP1 as-number $AS1 peer $OP1 route-policy BGP-IN-ACTIF import peer $OP1 route-policy BGP-OUT-BTEL export peer $OP1 advertise-community peer $OP1 password cipher $PWD1 peer $OP2 as-number $AS2 peer $OP2 route-policy BGP-PASSIF import peer $OP2 route-policy BGP-OUT-NXO export peer $OP2 advertise-community peer $OP2 password cipher $PWD2	interface LoopBack0 ip address $LOOPBACK 255.255.255.255 # route-policy BGP-OUT-BTEL permit node 10 apply community 65005:140 # bgp 65005 router-id $LOOPBACK preference 50 50 50 undo synchronization timer keepalive 5 hold 15 import-route direct peer $OP1 as-number $AS1 peer $OP1 route-policy BGP-OUT-BTEL export peer $OP1 advertise-community peer $OP1 password cipher $PWD1

3.15.2 Routage « Evasion Internet » dans les stacks niveau 3

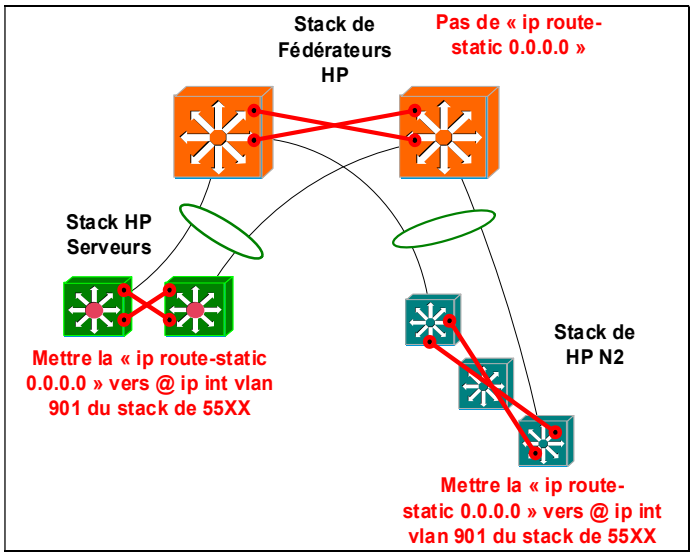
#
ip route-static 0.0.0.0 0.0.0.0 192.168.1.1
#

En Ramage v6 : l'ACL 2922 sera configurée par le DR avec le BGP

acl number 2922 name FILTER-DIRECT-NETWORK-RV6
rule 0 permit source 55.0.0.0 0.255.255.255
rule 5 permit source 58.0.0.0 0.255.255.255
#
route-policy DIRECT-TO-BGP permit node 10
if-match ip address acl 2922
#
bgp 65005
import-route direct route-policy DIRECT-TO-BGP
#

3.15.3 Routage dans les HP 3600 niveau 2 d'extrémité

Dans les sièges d'organismes (CPAM, ERSM, UGECAM…) les switches N2 d'extrémité (3600, 5130 ou 5140) sont configurés au niveau 2 sous la fédération des 55XX. Il est nécessaire de configurer une route statique pour assurer la communication entre les switches d'extrémité et les fédérateurs. Cela va être fait grâce à une route par défaut au niveau du VLAN d'admin (901) :



<>system-view
#
ip route-static 0.0.0.0 0.0.0.0 *@IP-Interface-vlan-901-stack-fédérateur*

A n'appliquer que sur switches N2 derrière le stack fédérateur N3 de HP 55XX.

3.15.4 Autres configurations

3.15.4.1 LLDP : découverte



A quoi ça sert ?

LLDP (Lync Layer Discovery Protocol) est le protocole standard de communication entre les switches et les hosts qui implémentent ce protocole (téléphones IP par exemple). Il permet la découverte d'informations sur les équipements connectés sur les interfaces Ethernet. Cisco a développé son propre protocole : CDP.

L'activation de LLDP permettra de visualiser de nombreuses informations sur les PMF, les téléphones, les serveurs… connectés sur les interfaces du 3600 et, via CDP de prendre en compte les Cisco :

<>system-view
#
lldp enable

Exemple de commandes de visualisation : <>dis lldp neighbor-information …

3.15.5 NTP : tous à la même heure

Une seule adresse IP de référence : 55.223.10.8. Voir la nouvelle version des procédures 027NA001 et 027NT002 sur l'intranet du DR.

ATTENTION : il se peut que l'implémentation de la version 3 de NTP soit nécessaire sur certains serveurs Linux :
- ➔ **mettre :** *server @ip-serveur-NTP version 3* **dans** */etc/ntp.conf*
- ➔ **relancer le process NTP :** */usr/sbin/ntpd –c /usr/ntp.conf*

Configuration sur tous les switches avec changement automatique heure d'été / heure d'hiver :

<>system-view
#
clock timezone PARIS add 01:00:00
clock summer-time PARIS repeating 02:00:00 03/27/2011 03:00:00 10/30/2011 01:00:00
#
ntp-service unicast-server **55.223.10.8** | adresse unique pour tous

Vérification du bon fonctionnement :

<>display ntp status
*Clock status: **synchronized***
Clock stratum: 3
Reference clock ID: 55.223.10.8
Nominal frequency: 100.0000 Hz
Actual frequency: 100.0000 Hz
Clock precision: 2^17
Clock offset: 0.0000 ms
Root delay: 10.64 ms
Root dispersion: 0.27 ms
Peer dispersion: 3.23 ms
Reference time: 09:16:02.999 UTC Apr 5 2013(D50914D2.FFE30878)

3.15.6 Wake On LAN : réveil des PMF à distance



A quoi ça sert ?

Les paquets WoL sont envoyés sous forme de broadcast à travers le réseau pour allumer les PC à distance. Pour que les équipements de niveau 3 laissent passer ce broadcast (nativement bloqué), il est nécessaire de le préciser dans la configuration. Une ACL permet en outre de limiter ce type de flux à la seule initiative du module PULSE des serveurs GEDIFF. La configuration est à appliquer sur l'interface VLAN des PMF dans le dernier switch N3 traversé (VLAN 4, 3, 18…).



Le WOL est à configurer sur les fédérateurs,
pas sur les switches d'extrémité.

Les serveurs GEDIFF sont centralisés au CSH-GE.

UNE ACL (3002) est à configurer pour n'autoriser que GEDIFF à traiter le WOL.

Configuration sur le ou les 3600 fédérateurs :

```
<>system-view
#
ip forward-broadcast
#
acl number 3002 name GEDIFF
 rule 1 permit udp source 55.245.0.0 0.0.255.255
```

N° d'ACL normalisé



GDIFF centralisé en CSH

Application sur l'interface VLAN 4 (par exemple) :

```
#
Interface Vlan-interface4
 ip forward-broadcast acl 3002
```

3.16 QOS POUR LA VOIX ET LA VIDEOCONFERENCE

Ce paragraphe explique la configuration des commutateurs HP permettant d'appliquer une QoS (Qualité de Service) minimum sur les LAN des Organismes (hors CSH) qui le nécessiteraient. Elle permet le traitement prioritaire des flux **voix** (Téléphonie sur IP) **et vidéo** (vidéoconférence sur PMF) par les switches en cas de congestion.

L'application de cette QoS n'est pas obligatoire mais elle doit être appliquée lorsque des lenteurs sont observées avant d'ouvrir un ticket d'incident.

Ces blocs de configuration sont à appliquer sur tous les switches du LAN.

En global sur les switches HP 3600 N2 et N3 :

```
System-view
#
qos map-table dscp-dot1p
 import 38 export 5
 import 46 export 6
```

Sur les interfaces :

- **interfaces trunks d'interconnexion de switches (commande non acceptée sur agrégats),**
- **interfaces de connexion des routeurs Ramage,**
- **des éventuels serveurs de téléphonie locaux (IPBX),**
- **interfaces de connexion des téléphones et/ou PMF.**

Exemples avec et1/0/10 et Gi1/0/25 :

```
System-view
#
Interface et1/0/10
 Qos trust dscp

Interface gi1/0/25
 Qos trust dscp
```

La QoS est appliquée même s'il n'y a pas de congestion sur une interface. Les traces suivantes ont cependant été réalisées en passant un appel téléphonique pendant qu'un flux saturant (FTP) était envoyé (avec un générateur de trafic) vers le PMF connecté derrière le téléphone. Cela afin de montrer que les paquets supprimés (droppés) sont ceux des classes de priorité moindre.

Pour visualiser les résultats nous utilisons la commande **« display qos queue-statistics … »** :

Commande pour les switches HP 3600 :

➔ **display qos queue-statistics interface Ethernet 1/0/X**

3.17 L'EXPLOITATION

3.17.1 Mirroring d'interface

Exemple : mirroring du port 3/0/14 sur 1/0/6 (même stack) :

```
<>system-view
#
mirroring-group 1 local
mirroring-group 1 mirroring-port Ethernet 1/0/14 both
mirroring-group 1 monitor-port Ethernet 1/0/6
```

Résultat (display current) :

```
mirroring-group 1 local
#
interface Ethernet1/0/6
 port link-mode bridge
 description ILE DE GROIX
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 6 30
 port trunk pvid vlan 6
 poe enable
 stp edged-port enable
 mirroring-group 1 monitor-port
#
interface Ethernet1/0/14
 port link-mode bridge
 description BURO
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 6 30
 port trunk pvid vlan 6
 poe enable
 mirroring-group 1 mirroring-port both                    | ou inbound ou outbound
```

```
display mirroring-group 1
mirroring-group 1:
   type: local
   status: active
   mirroring port:
      Ethernet1/0/14  both
   mirroring CPU:
   monitor port: Ethernet1/0/6
```

➔ **Connecter l'analyseur sur le port 1/0/6.**

3.17.2 Sauvegardes

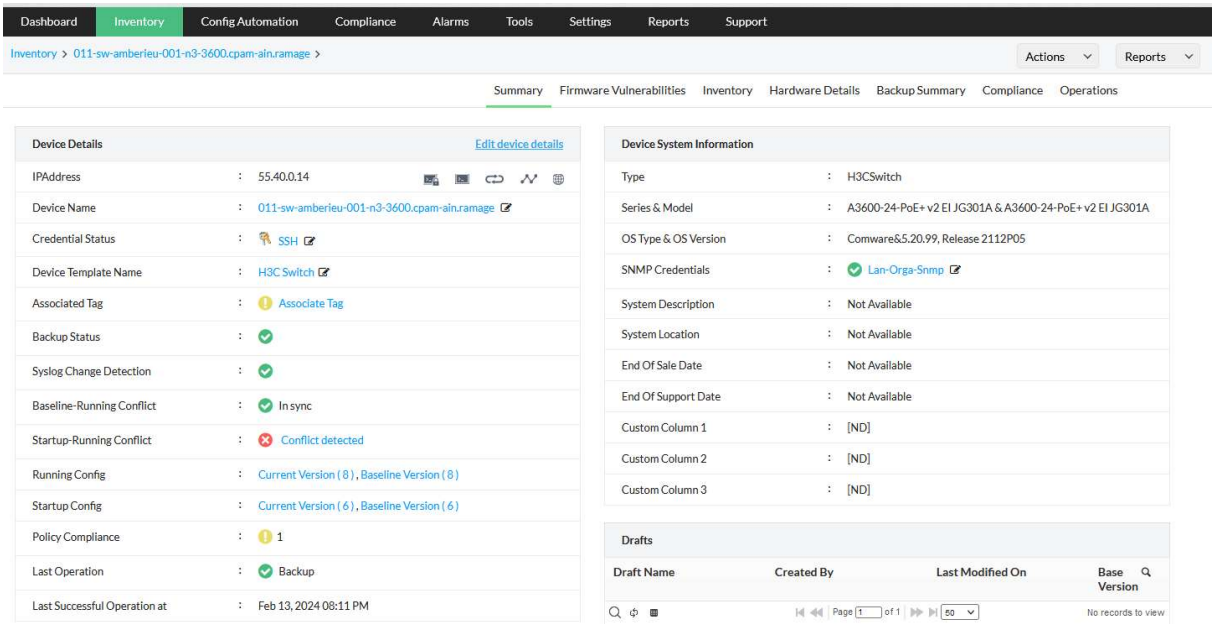
Tout switch ou stack installé sur RAMAGE doit être intégré au SI. Il est alors automatiquement sauvegardé dans NCM. La sauvegarde contient la configuration de l'ensemble du stack.

3.17.3 Restaurations

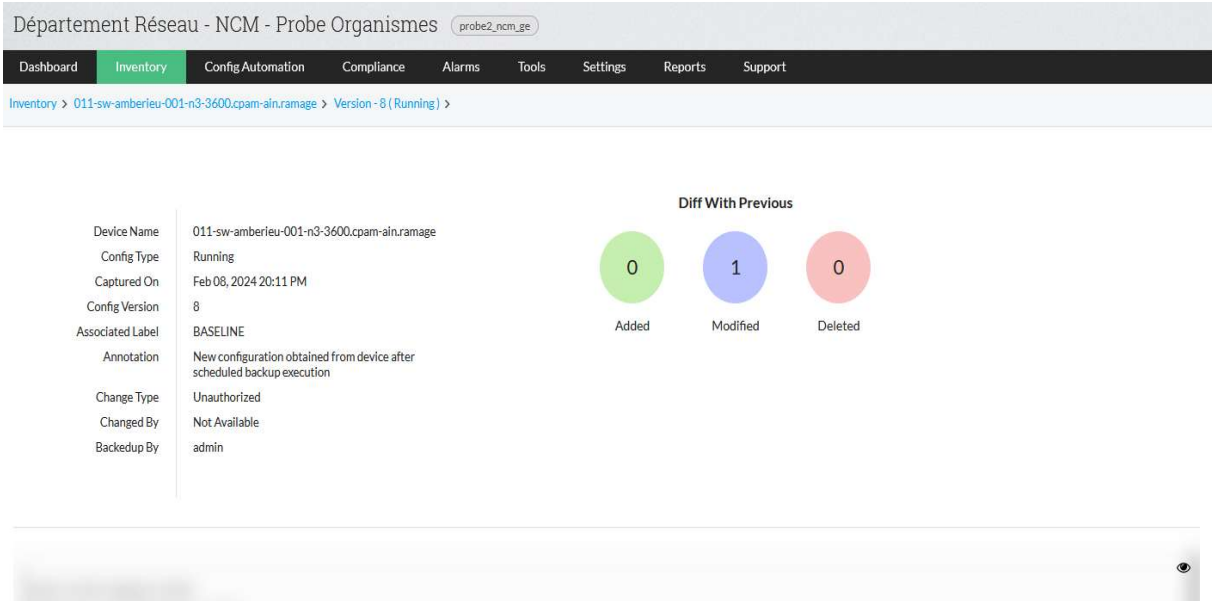
Tout switch ou stack installé sur RAMAGE étant sauvegardé dans NCM, il est possible de récupérer le fichier de sauvegarde via 2 méthodes :

3.17.3.1 Depuis l'outil NCM (Méthode 1)

Se placer sur l'équipement souhaité dans l'inventaire du logiciel Network Configuration Manager :

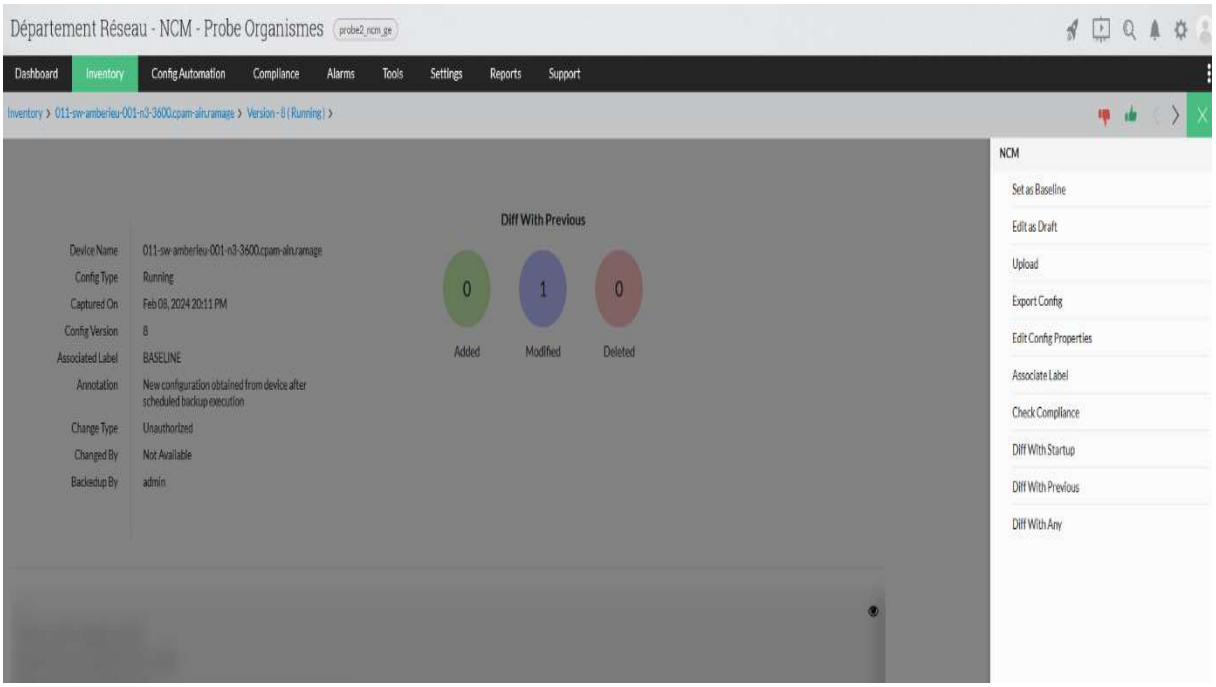


Cliquer sur la dernière version de la configuration « Current Version de la « Running Config » :

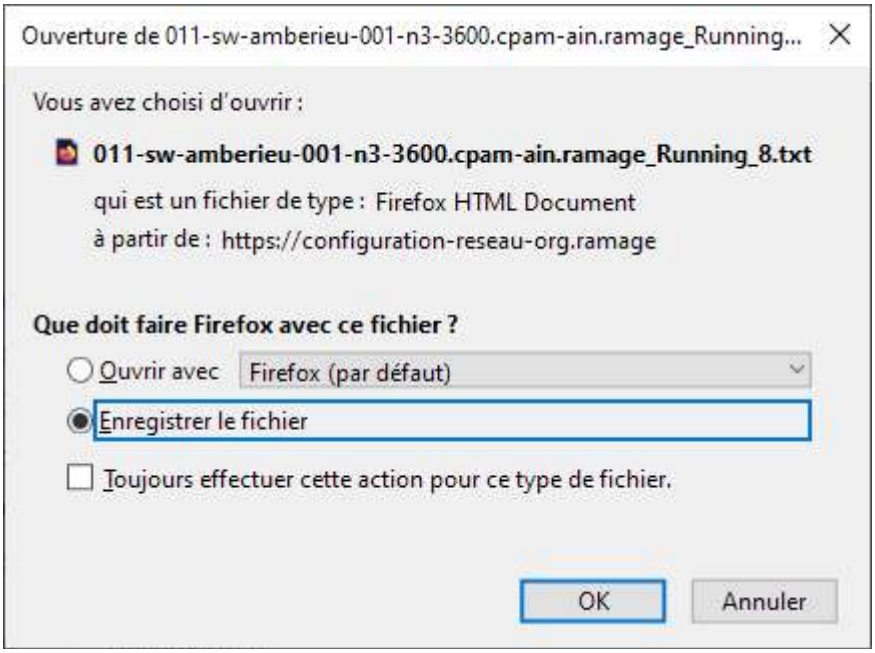


Cliquer sur le bouton en haut à droite 

Cliquer sur « Exporter la configuration » :



Enregistrer le fichier dans le dossier de votre choix :



Vous devez renommer le fichier de .txt à .cfg

Mettre votre fichier à la racine du dossier de votre serveur TFTP et vous pouvez faire la restauration de configuration :

Commande :

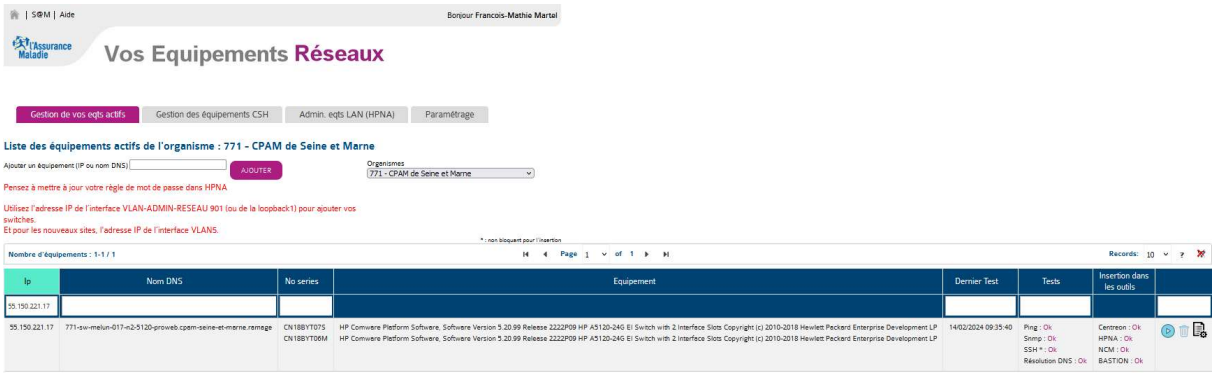
```
<>restore startup-configuration from @IP-serveur-TFTP fichier.cfg
<>Reboot (sans sauvegarder : lisez bien les questions posées).
Dans l'exemple du § précédent, la commande aurait été :
<>restore startup-configuration from @IP-serveur-TFTP stack.cfg
```

3.17.3.2 Depuis le portail du SI (Méthode 2)

Se connecter à la page suivante sur le portail du DR :

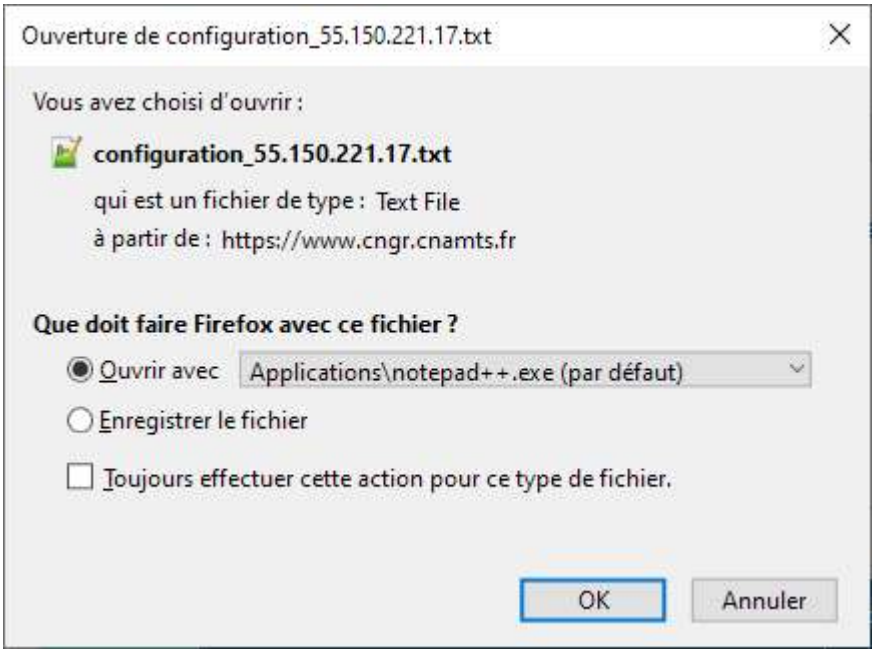
https://www.cngr.cnamts.fr/supervision/equipementActif/

Rechercher votre équipement via son adresse IP ou son nom dns :



Cliquer sur le bouton  pour télécharger la configuration de votre équipement.

Une fenêtre de téléchargement va apparaitre :



Vous devez renommer le fichier de .txt à .cfg

Mettre votre fichier à la racine du dossier de votre serveur TFTP et vous pouvez faire la restauration de configuration :

Commande :

```
<>restore startup-configuration from @IP-serveur-TFTP fichier.cfg
<>Reboot (sans sauvegarder : lisez bien les questions posées).
Dans l'exemple du $ précédent, la commande aurait été :
<>restore startup-configuration from @IP-serveur-TFTP stack.cfg
```

3.17.4 Remplacement d'un switch non maitre en panne dans un stack

- Ouvrez un ticket d'incident au PSN pour obtenir un switch identique de remplacement (voir « que faire en cas de panne dans le référentiel).
- Assurez-vous que ce switch est en configuration usine
- Connectez-vous en console
- Donner au switch le même nom « *sysname* » que celui du stack dont vous remplacez un des membres
- Configurez la partie stackage pour un switch « N » (toute la séquence)
- récupérez la sauvegarde du stack dans NCM (aller sur le stack puis sur view-configuration et cliquez « download text-file »).
- Avec un copier – coller reportez la configuration de toutes les interfaces sauf celles utilisées pour le stackage. Ne reportez pas le reste de la configuration.
- Vous n'avez plus qu'à placer ce switch dans le stack en remplacement du switch en panne dans le stack. Le stack sera reconstruit à l'identique.

3.17.5 Remplacement du switch maitre en panne dans un stack

Le switch 1 du stack est maitre. Le routeur principal est connecté l'interface et1/0/1 (normalisé). Si le switch 1 tombe en panne, le site bascule sur le secours. Connectez-vous au stack et configurez une interface libre sur le 2 pour recevoir la connexion du principal :

```
interface Et2/0/X
 port link-mode bridge
 description ROUTEUR-PROVISOIRE
 port access vlan 5
 speed 100
 duplex full
 stp disable
```

Si le site n'a pas de routeur secours, il faut se déplacer …où avoir prévu une interface de secours préconfigurée.

- Ouvrez un ticket d'incident au PSN pour obtenir un switch identique de remplacement (voir « que faire en cas de panne dans le référentiel).
- récupérez la sauvegarde du stack dans NCM (aller sur le stack puis sur view-configuration et cliquez « download text-file »).

Le maitre d'un stack est celui qui a la priorité la plus haute : c'est la configuration de ce switch qui va être mutualisée aux autres switches.

1/ Sur le stack où le maitre est HS, un nouveau switch est devenu maitre : le switch 2 (normalement car il a la priorité 30). Pour vérifier, taper « display irf » sur le stack :

```
<35-CN-RENNES-Sw-Buro-86-Fd>display irf
Switch   Role    Priority  CPU-Mac         Description
 *+2     Master  30        b8af-6770-ccec  -----
   3     Slave   28        b8af-6771-184c  -----
   4     Slave   26        b8af-6772-a9f3  -----
   5     Slave   24        b8af-6770-c47c  -----
   6     Slave   22        b8af-67ac-80e0  -----
   7     Slave   20        cc3e-5fb8-3d83  -----
-------------------------------------------------
```

2/ passer la priorité du maitre (le 2) à 32 – cela ne génère pas de coupure :

Irf member 2 priority 32
Save force (sauvegarde)

On obtient :

```
<35-CN-RENNES-Sw-Buro-86-Fd>display irf
Switch   Role    Priority  CPU-Mac         Description
 *+2     Master  32        b8af-6770-ccec  -----
   3     Slave   28        b8af-6771-184c  -----
   4     Slave   26        b8af-6772-a9f3  -----
   5     Slave   24        b8af-6770-c47c  -----
   6     Slave   22        b8af-67ac-80e0  -----
   7     Slave   20        cc3e-5fb8-3d83  -----
-------------------------------------------------
```

3/ Préparer le switch de remplacement du switch en panne :

- Assurez-vous que ce switch est en configuration usine
- Connectez-vous en console
- Donner au switch le même nom « *sysname* » que celui du stack dont vous remplacez l'unité 1
- Configurez la partie stackage pour un switch « 1 » (toute la séquence – NE PAS OUBLIER LE NUMERO DE « DOMAIN »)

mais avec :

Irf member 1 priority 30

Cela donne (exemple avec un 24 port) :

```
<>System-view
#
irf domain YY
irf member 1 priority 30
#
interface range GigabitEthernet1/0/27 to GigabitEthernet1/0/28
 shutdown
 quit
#
irf-port 1/1
 port group interface GigabitEthernet 1/0/27
 quit
#
irf-port 1/2
 port group interface GigabitEthernet 1/0/28
 quit
#
irf-port-configuration active
#
interface range GigabitEthernet1/0/27 to GigabitEthernet1/0/28
 undo shutdown
 description STACKAGE
 quit
#
<>save force
```

4/ Placer ce switch dans le stack en remplacement du switch en panne dans le stack. Le switch n°1 que vous avez inséré va rebooter s'insérer au stack et prendre la configuration fournie par le numéro 2.
Le stack sera reconstruit à l'identique, les interfaces du n°1 aussi. Au cas où vous pouvez les reconfigurer en faisant un copier-coller à partir du fichier de sauvegarde (seulement les interfaces de 1/01 à 1/0/26 (ou 1/0/50)).

5/ Repasser la priorité du switch à 30 et celui du switch 1 à 32 :

Irf member 2 priority 31
Irf member 1 priority 32
Irf member 2 priority 30
Save force (sauvegarde)

3.17.6 Remplacement d'un stack complet

- Ouvrez un ticket d'incident au PSN pour obtenir des switches identiques de remplacement (voir « que faire en cas de panne » dans le référentiel)
- Assurez-vous que ces switches sont en configuration usine
- Connectez-vous en console sur les switches et reconstrusez le stack
- Restaurez la configuration sauvegardée dans NCM (aller sur le stack puis sur view-configuration et cliquez « download text-file »).

3.17.7 Ajout d'un switch dans un stack (en production)

Exemple : on veut ajouter un 4ème switch dans un stack existant. Méthode sans coupure :
1/ Préparer un switch avec la bonne version
2/ Lui attribuer le même nom (sysname) que celui du stack
3/ Lui attribuer le numéro 4 (cf configuration stakage IRF)
4/ Déconnecter le lien IRF entre le port 27 du 3ème et le port 28 du 1er
5/ Mettre le switch 4 en baie et le démarrer
6/ Connecter le port 27 du 3ème au port 28 du 4ème et le port 27 du 4ème au port 28 du 1er

Le switch n° 4 rédémarre et s'insère dans le stack.

3.17.8 Mise à jour de la version

Méthode pour la mise à jour logicielle d'un switch 3600-v2 ou de tous les switches d'un stack.

Exemple d'un stack de 2 A3600-v2

1 - Vérifier qu'il y a de la place avec la commande « dir » :

<>dir /all

2 – Si nécessaire supprimer des fichiers pour faire de la place :

A/ Suppression de fichiers dans la flash (pas assez de place) de manière non définitive :

<>delete ***fichier***

OU :

<>delete slot2#flash:***fichier***

➔ les fichiers sont visibles entre crochets si on fait un **dir /all**

➔ Pour les supprimer définitivement, il faut vider la corbeille :

<>**reset recycle-bin /force**

B/ Suppression de fichiers dans la flash (pas assez de place) de manière définitive :

<>delete /unreserved ***fichier***
<>delete /unreserved slot2#flash:***fichier***

Si vous avez supprimé des fichiers de la version en cours (pour faire de la place),

NE PAS REBOOTER avant d'avoir appliqué la suite !!!

3 – Préparer un serveur TFTP + se connecter en SSH + lancer les transferts des fichiers :

En fonction des versions, le nombre de fichiers peut différer. **Au maximum**, il y aura :

- un fichier .btm
- un fichier .bin
- un fichier .web

Exemple :

<>tftp *@ip_serveur_TFTP* get *fichier***.btm**
<>tftp *@ip_serveur_TFTP* get *fichier***.bin**

Si un fichier ".web" fait partie des fichiers constituant la version, il faut le transférer aussi.

4 – Lancer la mise à jour :

D'abord le « .btm » :

Switch seul :

<>bootrom update file flash:/*fichier*.**btm** slot 1

Tout un stack :

<>bootrom update file flash:/*fichier*.**btm** slot 1 to **X**

x = n° d'unité du dernier switch du stack.

Ensuite le « .bin » :

Switch seul ou pour tout un stack :

<>boot-loader update file flash:/*fichier*.**bin** slot all main

Pour les 3600, possibilité de laisser l'ancienne version en backup :
<>boot-loader update file flash:/s5500ei-cmw520-R2207-s168.**bin** slot all backup
⇨ Cela permet de de revenir à cette version s'il y a un problem avec la nouvelle

Il n'y a rien à faire pour le fichier « .web » (si présent dans la version)

5 – Redémarrer le stack :

<>reboot

3.17.9 Récupération d'un switch sans version

La méthode étant la même pour les HP 3600-v2, les 55XX et les 51XX, les écrans ci-dessous sont des copies de la procédure 3600 v1. Veuillez évidemment adapter avec les bons fichiers de version. Rappel : les versions sont disposées sur le site intranet du DR.

```
**************************************************************
*                                                            *
*        H3C S3600-28P-PWR-EI BOOTROM, Version 606           *
*                                                            *
**************************************************************

Copyright(c) 2004-2010 Hangzhou H3C Technologies Co., Ltd.
Creation date    : Sep 25 2010, 11:30:43
CPU Clock Speed  : 200MHz
BUS Clock Speed  : 33MHz
Memory Size      : 64MB
Mac Address      : 3ce5a689835e

Press Ctrl-B to enter Boot Menu... 0
Auto-booting...

No correct default file to boot!
-
```

Il faut dans un premier temps entrer dans le Boot Menu par Ctrl + B

Password : **(pas de password par défaut)**

BOOT MENU

1. Download application file to flash
2. Select application file to boot
3. Display all files in flash
4. Delete file from flash
5. Modify bootrom password
6. Enter bootrom upgrade menu
7. Skip current configuration file
8. Set bootrom password recovery
9. Set switch startup mode
0. Reboot

Choisir le 1. Download application file to flash

1. Set TFTP protocol parameters
2. Set FTP protocol parameters
3. Set XMODEM protocol parameters
0. Return to boot menu

Choisir le 1. Set TFTP protocol parameters

Au préalable, il faut connecter le PMF sur une interface du switch et choisir un adressage cohérant entre le switch et le PMF. Sur ce PMF, il faut ouvrir un serveur tftp avec les fichiers à télécharger.

Enter your choice(0-3): 1
Load File name :s3600ei-cmw310-702p28-s168.bin
Switch IP address :55.16.221.232
Server IP address :55.16.221.234
Are you sure you want to download file to flash? Yes or No [Y/N] y

```
Loading.....................................................................
.....................done
Free flash Space: 4834304 bytes
Writing flash.....................................................................
.....................................................................
.....................................................................
.....................................................done!

Please input the file attribute (main/backup/none):main
```

On vérifie si le fichier a bien été pris en compte.

```
 BOOT  MENU

1. Download application file to flash
2. Select application file to boot
3. Display all files in flash
4. Delete file from flash
5. Modify bootrom password
6. Enter bootrom upgrade menu
7. Skip current configuration file
8. Set bootrom password recovery
9. Set switch startup mode
0. Reboot

Enter your choice(0-9): 3
File Number    File Size(bytes)     File Name
================================================================================
1           195268            s3600
2(*)         882249             h3c-http3.1.9-0014.web
3           2211              config.def
4           4589776             test
5           151               private-data.txt
6           195268              s3600_n.btm
7           2304              default_file
8           302080              boot_n
9(*)         4679012            s3600ei-cmw310-R1702p28-s168.bin
10          2392              config.cfg
Free Space: 154624 bytes
The current application file is s3600ei-cmw310-R1702p28-s168.bin
(*)-with main attribute
(b)-with backup attribute
(*b)-with both main and backup attribute

 BOOT  MENU

1. Download application file to flash
2. Select application file to boot
3. Display all files in flash
4. Delete file from flash
5. Modify bootrom password
6. Enter bootrom upgrade menu
7. Skip current configuration file
8. Set bootrom password recovery
9. Set switch startup mode
0. Reboot

Enter your choice(0-9): 2

Select application file to boot
1. Set application files
2. Set configuration files
3. Set web files
0. Return
```

```
Enter your choice(0-3): 1
File Number   File Size(bytes)     File Name
============================================================================
1(*)          4679012             s3600ei-cmw310-R1702p28-s168.bin
Free Space: 154624 bytes
(*)-with main attribute
(b)-with backup attribute
(*b)-with both main and backup attribute
Please input the file number to change: 1
Please input the file attribute (main/backup):main
Do you want to run s3600ei-cmw310-R1702p28-s168.bin now? Yes or No [Y/N] y
Decompress Image.....................................................
.....................................................................
.....................................................................
.....................................................................
.....................................................................
.....................................OK!
Starting at 0x80100000...


      Board checking.....................LSJ1LTSH
      SDRAM fast selftest.....................OK!
      Flash fast selftest.....................OK!
      CPLD selftest.....................OK!
      Switch chip selftest.....................OK!
      Port 1 has no module
      Port 2 has no module
      Port 3 has no module
      Port 4 has 1000_BASE_T_AN_SFP module
      PHY selftest.....................OK!
      Please check port leds.....FINISHED!

Startup configuration is skipped.
User interface aux0 is available.
```

3.17.10 Remettre un switch en configuration usine

3.17.10.1 Retour usine complet (avec changement de n° d'unité)

Sur un « master » (tête de stack) :

<>reset saved-configuration ➔ Y
<>reboot (sans sauvegarde) ➔ N puis Y

Sur un « slave » (exemple avec member = 2) :

<>system-view
#
irf member 2 renumber 1 ➔ Y
save force
#
<>reboot ➔ Y

puis :

<>reset saved-configuration ➔ Y
<>reboot (sans sauvegarde) ➔ N puis Y

3.17.10.2 Retour usine sans changement de n° d'unité

Rebooter le switch et en console taper CTRL B lorsque cela est proposé. Ensuite, validez : Il n'y a normalement pas de « bootrom password » pour entrer dans le menu de boot :

BOOT MENU

1. Download application file to flash
2. Select application file to boot
3. Display all files in flash
4. Delete file from flash
5. Modify bootrom password
6. Enter bootrom upgrade menu
7. Skip current configuration file
8. Set bootrom password recovery
9. Set switch startup mode
0. Reboot

Choisir "4. Delete file from flash" et choisissez le ou les fichiers « .cfg » pour les supprimer tous. Choisir ensuite «0. Reboot ».

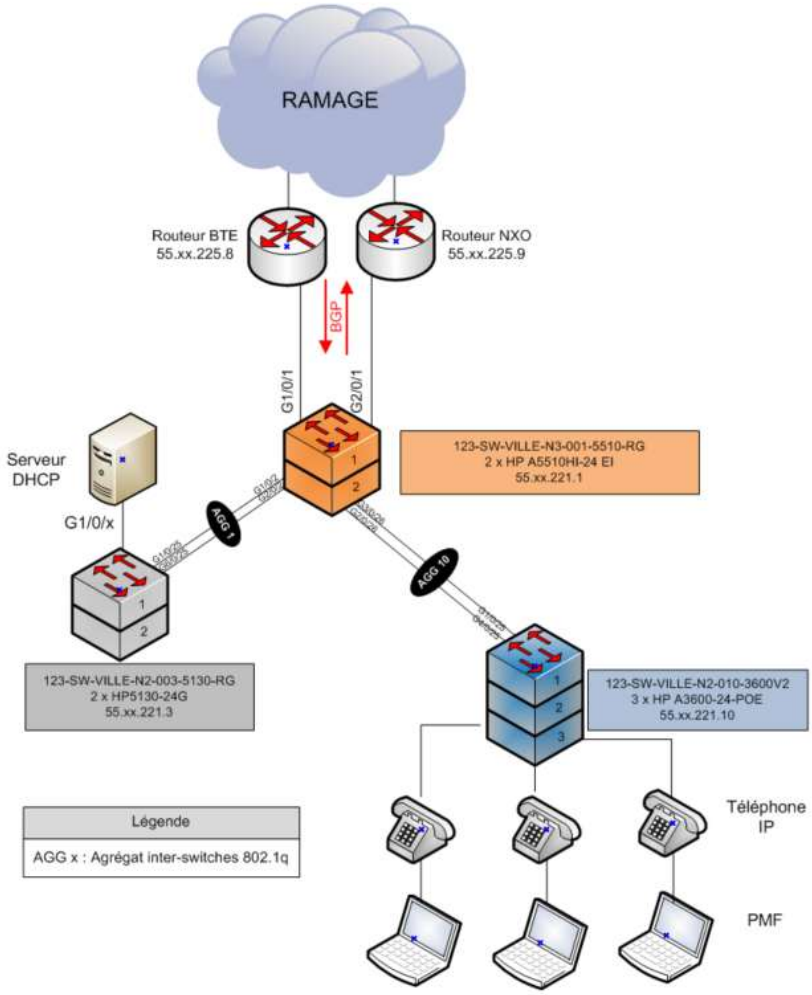
3.17.11 Annexes : exemples complets de configuration

Dans ce chapitre, nous allons donner des exemples complets de configuration à partir d'architectures normalisées, en fonction des types de sites.

3.17.11.1 Siège d'organisme

Ci-dessous l'exemple d'un siège d'Organisme de type CPAM. On retrouve une architecture classique :

- Un accès RAMAGE avec 2 routeurs opérateur
- Un stack fédérateur de 2 x 5510HI-24G-EI
- Un stack de 2 x HPE5130 pour les serveurs
- Un ensemble de stacks de 3 x HP 3600-24-PoE-v2 connectés en cuivre. Pour l'exemple, nous nous limiterons à un stack de 3 HP 3600 connectés en agrégat au stack de 5510 via les interfaces (normalisées) 1/0/25 et 3/0/25).
- La ToIP est en place migrée sur CETIAM
- Les postes du service medical sont connectés sur les interfaces 10 à 24 du switch 3 du stack 3600



- Plan d'adressage IP **(exemple)** :
  - *VLAN 5 – VLAN-INTERCOWAN : 55.X.225.0 /28 – Interface VLAN 5 : 55.X.225.1*

  ROUTEUR BTE : 55.X.225.8 ; ROUTEUR NXO : 55.X.225.9
  - *VLAN 4 – VLAN-DATA :55.X.4.0 /22 – interface VLAN 4 : 55.X.4.1*
  - *VLAN 30 – VLAN-VOIX : 58.X.4.0 /22 – interface VLAN 30 : 58.X.4.1*
  - *VLAN 3 – VLAN-MEDICAL : 55.X.223.0 /24 – interface VLAN 3 : 55.X.223.1*
  - *VLAN 18 – VLAN-PFS : 55.X.238.0 /23 – interface VLAN 18 : 55.X.238.1*
  - **VLAN 901 – VLAN-ADMIN-RESEAU : 55.X.221.0 /24 – Interface VLAN 901 : 55.X.221.1**
    - ⇨ **stack de 3600 en 55.X.221.10.**

Seul le VLAN 901 est a configurer dans le stack de 3600.

Configurations du stack de 3600

Résultat d'un « display current » : certaines commandes par défaut non entrées en configuration apparaissent, d'autres, entrées n'apparaissent pas (stp enable sur interfaces par ex).

La configuration des stacks de 5510 et de 5130 est fournie dans le guide de configuration des HPE 5510 et HPE5130.

STACK 3600 N2 siège

```
#
 sysname XXX-sw-cp-xxxxx-011-n2-3600-RG
#
 clock timezone PARIS add 01:00:00
 clock summer-time PARIS repeating 02:00:00 03/27/2011
03:00:00 10/30/2011  01:00:00
#
voice vlan mac-address XXXX-XXXX-XXXXX mask ffff-ff00-0000
description Postes Constructeur
#
 irf mac-address persistent timer
 irf auto-update enable
 undo irf link-delay
 irf domain 11
 irf member 1 priority 32
 irf member 2 priority 30
 irf member 3 priority 28
#
 domain default enable system
#
dns resolve
dns server 55.223.10.1
dns domain cnamts.fr
#
loopback-detection enable
loopback-detection multi-port-mode enable
#
undo ip http enable
undo ip http enable
#
ip ttl-expires enable
ip unreachables enable
#
acl number 2099
 description SNMP RO ACCESS FOR DR
 rule 0 permit source 55.18.0.0 0.0.255.255
 rule 1 permit source 55.36.0.0 0.0.255.255
rule 2 permit source 55.X.0.0 0.0.255.255
 rule 3 permit source 55.Y.0.0 0.0.255.255
 rule 4 permit source 55.245.4.0 0.0.0.255
#
vlan 1
#
vlan 3
 name VLAN-MEDICAL
#
vlan 4
 name VLAN-DATA
#
vlan 30
 name VLAN-VOIX
#
vlan 901
 name VLAN ADMIN-RESEAU
#
radius scheme system
 server-type extended
 primary authentication 127.0.0.1 1645
 primary accounting 127.0.0.1 1646
 user-name-format without-domain
#
domain system
 access-limit disable
 state active
 idle-cut disable
 self-service-url disable
#
user-group system
 group-attribute allow-guest
#
local-user admin
 password cipher MotDePasse
 authorization-attribute level 3
 service-type ssh terminal
 service-type web
#
 stp mode rstp
 stp bpdu-protection
 stp enable
 stp pathcost-standard dot1t
#
interface Bridge-Aggregation10
description vers AGG-010-N3-5510-MASTER
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 3 to 4 30 901
 link-aggregation mode dynamic
 dhcp-snooping trust
 mad enable
 stp loop-protection
#
interface NULL0
#
interface Vlan-interface901
description INT-VLAN-ADMIN-RESEAU
 ip address 55.X.221.10 255.255.255.0
#
interface Ethernet1/0/1
 port link-mode bridge
 description TEL+PMF
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 4 30
 port trunk pvid vlan 4
 undo voice vlan mode auto
 voice vlan 30 enable
 poe enable
 stp edged-port enable
 loopback-detection enable
 loopback-detection action shutdown
 loopback-detection enable
 loopback-detection per-vlan enable
 multicast-suppression 20
 broadcast-suppression 20
#
```

…Etc.

```
#
interface Ethernet1/0/24
 port link-mode bridge
 description IP-Phone+PMF
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 4 30
```

```
 port trunk pvid vlan 4
 undo voice vlan mode auto
 voice vlan 30 enable
 poe enable
 stp edged-port enable
 loopback-detection enable
 loopback-detection action shutdown
 loopback-detection enable
 loopback-detection per-vlan enable
 multicast-suppression 20
 broadcast-suppression 20
#
interface Ethernet2/0/1
 port link-mode bridge
 description IP-Phone+PMF
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 4 30
 port trunk pvid vlan 4
 undo voice vlan mode auto
 voice vlan 30 enable
 poe enable
 stp edged-port enable
 loopback-detection enable
 loopback-detection action shutdown
 loopback-detection enable
 loopback-detection per-vlan enable
 multicast-suppression 20
 broadcast-suppression 20
#
```

…Etc.

```
#
interface Ethernet2/0/24
 port link-mode bridge
 description IP-Phone+PMF
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 4 30
 port trunk pvid vlan 4
 undo voice vlan mode auto
 voice vlan 30 enable
 poe enable
 stp edged-port enable
 loopback-detection enable
 loopback-detection action shutdown
 loopback-detection enable
 loopback-detection per-vlan enable
 multicast-suppression 20
 broadcast-suppression 20
#
interface Ethernet3/0/1
 port link-mode bridge
 description IP-Phone+PMF
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 4 30
 port trunk pvid vlan 4
 undo voice vlan mode auto
 voice vlan 30 enable
 poe enable
 stp edged-port enable
 loopback-detection enable
 loopback-detection action shutdown
 loopback-detection enable
 loopback-detection per-vlan enable
 multicast-suppression 20
 broadcast-suppression 20
#
```

…Etc.

```
#
interface Ethernet3/0/11
 port link-mode bridge
 description IP-Phone+PMF-MEDICAL
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 3 30
 port trunk pvid vlan 3
 undo voice vlan mode auto
 voice vlan 30 enable
 poe enable
 stp edged-port enable
 loopback-detection enable
 loopback-detection action shutdown
 loopback-detection enable
 loopback-detection per-vlan enable
 multicast-suppression 20
 broadcast-suppression 20
#
interface Ethernet3/0/12
 port link-mode bridge
 description IP-Phone+ PMF-MEDICAL
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 3 30
 port trunk pvid vlan 3
 undo voice vlan mode auto
 voice vlan 30 enable
 poe enable
 stp edged-port enable
 loopback-detection enable
 loopback-detection action shutdown
 loopback-detection enable
 loopback-detection per-vlan enable
 multicast-suppression 20
 broadcast-suppression 20
#
interface Ethernet3/0/13
 port link-mode bridge
 description IP-Phone+ PMF-MEDICAL
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 3 30
 port trunk pvid vlan 3
 undo voice vlan mode auto
 voice vlan 30 enable
 poe enable
 stp edged-port enable
 loopback-detection enable
 loopback-detection action shutdown
 loopback-detection enable
 loopback-detection per-vlan enable
 multicast-suppression 20
 broadcast-suppression 20
#
```

…Etc.

```
#
interface Ethernet3/0/24
 port link-mode bridge
 description IP-Phone+ PMF-MEDICAL
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 3 30
 port trunk pvid vlan 3
 undo voice vlan mode auto
 voice vlan 30 enable
 poe enable
 stp edged-port enable
 loopback-detection enable
 loopback-detection action shutdown
```

```
 loopback-detection enable
 loopback-detection per-vlan enable
 multicast-suppression 20
 broadcast-suppression 20
#
interface GigabitEthernet1/0/25
 port link-mode bridge
 description vers AGG-010-N3-5500-MASTER-LIEN1
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 3 to 4 30 901
 port link-aggregation group 10
 dhcp-snooping trust
#
interface GigabitEthernet1/0/26
description SHUTDOWN
 shutdown
#
interface GigabitEthernet2/0/25
 description SHUTDOWN
port link-mode bridge
 shutdown
#
interface GigabitEthernet2/0/26
 description SHUTDOWN
port link-mode bridge
 shutdown
#
interface GigabitEthernet3/0/25
 port link-mode bridge
 description vers AGG-010-N3-5500-MASTER-LIEN2
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 3 to 4 30 901
 port link-aggregation group 10
 dhcp-snooping trust
#
interface GigabitEthernet3/0/26
 description SHUTDOWN
port link-mode bridge
 shutdown
#
interface GigabitEthernet1/0/27
 description STACKAGE
#
interface GigabitEthernet1/0/28
 description STACKAGE
#
interface GigabitEthernet2/0/27
 description STACKAGE
#
interface GigabitEthernet2/0/28
 description STACKAGE
#
interface GigabitEthernet3/0/27
 description STACKAGE
#
interface GigabitEthernet3/0/28
 description STACKAGE
#
 dhcp-snooping
#
 ip route-static 0.0.0.0 0.0.0.0 55.X.221.1
#
 info-center loghost source Vlan-interface 901
 info-center loghost slog-reseau-org.ramage
#
 snmp-agent
 snmp-agent local-engineid 800063A203B8AF67AC8A04
 snmp-agent community read TOKTBAT22! acl 2099
 snmp-agent community write xxxxxxxx acl 2099
 snmp-agent sys-info contact François Pignon
 snmp-agent sys-info location Local-RDC
 snmp-agent sys-info version v2c
 snmp-agent trap enable default-route
#
```

OBLIGATION OSE :

Une bannière de mise en garde doit être configurée sur tous les switches. Commencez et finissez avec le même caractère (ici %). Vous devez utiliser obligatoirement la bannière suivante :

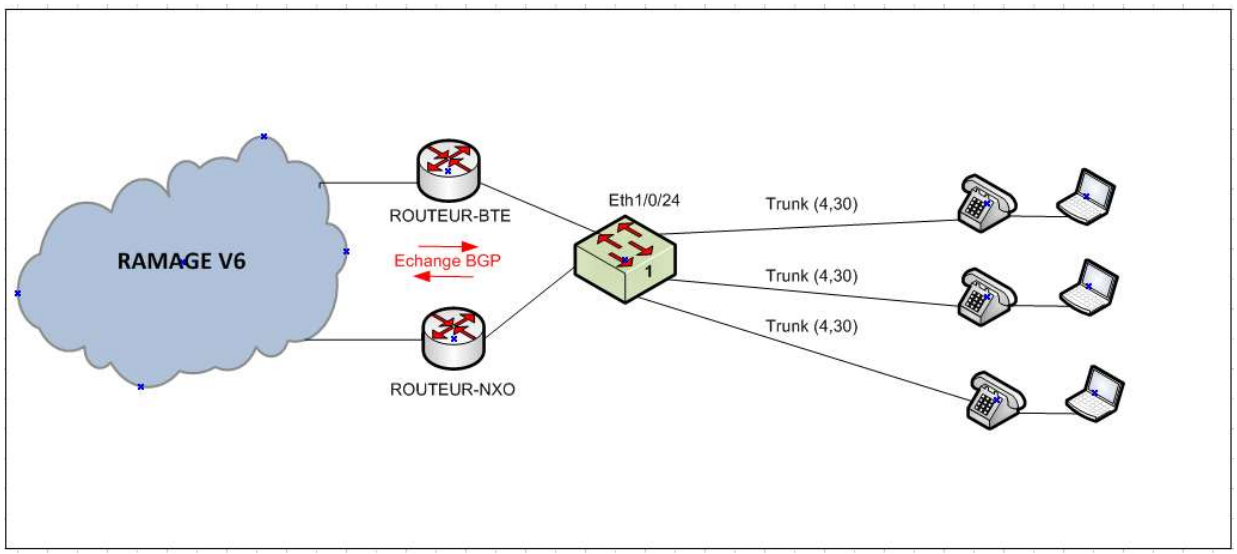
```
#
header shell %
****************************************
*             ! Attention !            *
*                                      *
*    Acces reserve aux personnels du   *
*         service informatique         *
*                                      *
*  Toutes les activites sur ce systeme *
*          sont enregistrees           *
*                                      *
*    Toutes preuves d activites non    *
*   autorisees seront traitees par les *
*    autorites competentes             *
*                                      *
*     Toute intrusion sur un systeme   *
*   informatique est interdite par les *
*     articles 323-2 du code penal     *
*                                      *
****************************************
%
#
 ntp-service unicast-server 55.223.10.8
#
 ssh server enable
undo ssh server compatible-ssh1x ssh
 user admin service-type stelnet authentication-type password
#
 load xml-configuration
#
 load tr069-configuration
#
user-interface aux 0 2
 authentication-mode scheme
user-interface vty 0 15
 authentication-mode scheme
 protocol inbound ssh
#
irf-port 1/1
 port group interface GigabitEthernet1/0/27
#
irf-port 1/2
 port group interface GigabitEthernet1/0/28
#
irf-port 2/1
 port group interface GigabitEthernet2/0/27
#
irf-port 2/2
 port group interface GigabitEthernet2/0/28
#
irf-port 3/1
 port group interface GigabitEthernet3/0/27
#
irf-port 3/2
 port group interface GigabitEthernet3/0/28
#
```

3.17.11.2 Agence / Etablissment

3.17.11.2.1 Avec un seul HP 3600

Ci-dessous l'exemple d'une agence de type CP. On retrouve une architecture classique **avec un seul stack ou un seul switch 3600-24-PoE-v2 car il n'y a qu'un seul répartiteur et environ 15 agents** :

- Un accès RAMAGE avec 2 routeurs opérateur
- Un stack de 1 xHP 3600-24-PoE-v2
- La ToIP est en place CETIAM (Projet national)
- Le serveur DHCP est en siège d'organisme



- Plan d'adressage IP **(exemple)** :
  - VLAN 5 – VLAN-INTERCOWAN : 55.X.240.1 /29
  - VLAN 4 : VLAN-DATA : 55.X.8.0 /22 – Interface VLAN 4 : 55.X.8.1
  - VLAN 30 : VLAN-VOIX : 58.X.8.0 /22 – Interface VLAN 30 : 58.X.8.1
  - INTERFACE LOOPBACK0 : 55.248.11.38 255.255.255.255 (INT-LOOPBACK-BGP / CNGR)
  - INTERFACE LOOPBACK1 : 55.xx.0.46 255.255.255.255 (INT-LOOPBACK-ADMIN-RES)

- Serveurs GEDIFF :
  - National : 55.245.4.0

- Adresse IP du serveur DHCP en siège d'organisme : 55.X.4.6 (VLAN 4) distribue les adresses aux PMF et aux téléphones – port 1/0/25T.

Configurations

Résultat d'un « display current » : certaines commandes par défaut non entrées en configuration apparaissent, d'autres, entrées n'apparaissent pas (stp enable sur interfaces par ex).
La partie routage e-BGP et la loopback0 est là à titre indicatif, il faut vous renseigner sur le profil de votre agence et récupérer la configuration BGP auprès de votre correspondant LAN

Pages suivantes…

HP 3600-24-POE N3 en CP :

```
version 5.20.99, Release 2112P05
#
 sysname XXX-sw-et-xxxxx-046-n3-3600
#
 clock timezone PARIS add 01:00:00
 clock summer-time PARIS repeating 02:00:00 03/27/2011
03:00:00 10/30/2011  01:00:00
#
 voice vlan mac-address 0008-7b00-0000 mask ffff-ff00-0000
description Bornes IP-DECT Alcatel
 voice vlan mac-address 0080-9f00-0000 mask ffff-ff00-0000
description telephone alcatel 2014
 voice vlan mac-address 487a-5500-0000 mask ffff-ff00-0000
description Postes Alcatel-2018
 voice vlan track lldp
#
 dhcp relay server-group 2 ip 55.xx.4.6
#
 irf domain 1
 irf mac-address persistent timer
 irf auto-update enable
 undo irf link-delay
 irf member 1 priority 32
#
 domain default enable system
#
 dns resolve
 dns server 55.223.10.1
 dns domain cnamts.fr
#
 ip ttl-expires enable
 ip unreachables enable
#
 loopback-detection enable
 loopback-detection multi-port-mode enable
#
 undo ip http enable
#
 password-recovery enable
#
 ip forward-broadcast
#
acl number 2099
 description SNMP RW ACCESS POUR CNGR
 rule 0 permit source 55.xx.0.0 0.0.255.255
 rule 1 permit source 55.18.0.0 0.0.255.255
 rule 2 permit source 55.245.0.0 0.0.255.255
 rule 3 permit source 55.244.0.0 0.0.255.255
acl number 2922
 description FILTER-DIRECT-NETWORK-RV6
 rule 0 permit source 55.0.0.0 0.255.255.255
 rule 5 permit source 58.0.0.0 0.255.255.255
#
acl number 3002 name gediff
 rule 0 permit udp source 55.8.1.185 0
 rule 1 permit udp source 55.245.4.0 0.0.3.255
 rule 5 permit udp source 55.8.1.186 0
#
vlan 1
#
vlan 4
 name VLAN-DATA
#
vlan 5
 name VLAN-INTERCOWAN
#
vlan 30
 name VLAN-VOIX
#
vlan 226
 name VLAN-IMPRIMANTES
#
#
 public-key peer 55.244.111.45
  public-key-code begin

308201B73082012C06072A8648CE3804013082011F02818100C
43E558E2D2482D1DDC7261A

195B47461C21E5372BB13EF5F83BE0B1ECCBFC8BC4E39746294
D642ECF7B29FDB1F4198290

B45B9EBEBA4D844CF634C2AB57CFC2C70D77DD4339C917A56
F3D51E0E1BA871BB264378AFF

E7DBA6F71648B87E30BC67FE5D9DD054FEA10ADD042FA64C2
6B00323DD05C072FEF36A5DA4

D865377D05021500CF36CC6588D3A172F425E22B1325C98A1D
B036250281810096CC0403DB

44BF43683F5E72ECAC3D26EC8382F619B137DFF1857E0090221
68EFCFB50A0CFB5B5F16619

B513C0C2C8BD83B2412B433C7950ED4D079EB59C639AA452C5
18731D01A6DF9863A3B1CF47

5C14007B9864FDACED7F6780D67D739B677A64E6E7A2EF973C
AF93ACABF58C58FA3D1E45B8

1121D9096CDE451CEC5D28AB03818400028180638C95D00EC4
34315B73DFC8ECAC07A41587

1585D6D446A775079FF3E92D157D8C0043AB2A19BD261AF4FB
3B3BF5D689C4FC0CFEA40BA0

1FEE14D60DA286E0C3AA9881E95BFCA3EE30873AC04DD7085A
F1878B6AE8E6944AFE5C1A1E

BCFF35DD7576C293FD1EA12C2A053FFB72CF26A581ADAF899C
7BD230FCEFFE250D4EF7B8
  public-key-code end
 peer-public-key end
#
qos map-table dscp-dot1p
 import 38 export 5
 import 46 export 6
#
user-group system
 group-attribute allow-guest
#
local-user admin
 password cipher
$c$3$KWCqqx4osnRmj3cusgpewVNx0v63AdMg7Rbd4FGMofL2
 authorization-attribute level 3
 service-type ssh terminal
 service-type web
#
 stp mode rstp
 stp instance 0 priority 0
 stp timer forward-delay 700
 stp timer max-age 1000
 stp bpdu-protection
 stp pathcost-standard dot1t
 stp enable
#
interface NULL0
#
```

```
interface LoopBack0
description INT-LOOPBACK-BGP
 ip address 55.248.11.38 255.255.255.255
#
interface LoopBack1
description INT-LOOPBACK-ADMIN-RESEAU
 ip address 55.xx.0.46 255.255.255.255
#
interface Vlan-interface4
 description INT-VLAN-DATA
 ip address 55.xx.8.1 255.255.252.0
 dhcp select relay
 dhcp relay server-select 2
 ip forward-broadcast acl 3002
#
interface Vlan-interface5
 description INT-VLAN-INTERCOWAN
 ip address 55.xx.240.1 255.255.255.248
#
interface Vlan-interface30
 description INT-VLAN-VOIX
 ip address 58.xx.8.1 255.255.252.0
 dhcp select relay
 dhcp relay server-select 2
#
interface Vlan-interface226
 description INT-VLAN-IMPRIMANTES
ip address 55.xx.249.1 255.255.255.248
#
interface Ethernet1/0/1
 port link-mode bridge
 description ROUTEUR-BTE
 port access vlan 5
 speed 100
 duplex full
 stp disable
 #
interface Ethernet1/0/2
 port link-mode bridge
 description ROUTEUR-NXO
 port access vlan 5
 speed 100
 duplex full
 stp disable
 #
interface Ethernet1/0/3
 port link-mode bridge
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 4 30
 port trunk pvid vlan 4
 undo voice vlan mode auto
 voice vlan 30 enable
 loopback-detection enable
 loopback-detection enable
 loopback-detection per-vlan enable
 loopback-detection action shutdown
 broadcast-suppression 20
 multicast-suppression 20
 poe enable
 stp edged-port enable
 qos trust dscp
#
interface Ethernet1/0/4
 port link-mode bridge
 description Telephone IP + PMF
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 4 30
 port trunk pvid vlan 4
 undo voice vlan mode auto
 voice vlan 30 enable
 loopback-detection enable
 loopback-detection enable
 loopback-detection per-vlan enable
 loopback-detection action shutdown
 broadcast-suppression 20
 multicast-suppression 20
 poe enable
 stp edged-port enable
 qos trust dscp
#
interface Ethernet1/0/5
 port link-mode bridge
 description Telephone IP + PMF
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 4 30
 port trunk pvid vlan 4
 undo voice vlan mode auto
 voice vlan 30 enable
 loopback-detection enable
 loopback-detection enable
 loopback-detection per-vlan enable
 loopback-detection action shutdown
 broadcast-suppression 20
 multicast-suppression 20
 poe enable
 stp edged-port enable
 qos trust dscp
#
interface Ethernet1/0/6
 port link-mode bridge
 description Telephone IP + PMF
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 4 30
 port trunk pvid vlan 4
 undo voice vlan mode auto
 voice vlan 30 enable
 loopback-detection enable
 loopback-detection enable
 loopback-detection per-vlan enable
 loopback-detection action shutdown
 broadcast-suppression 20
 multicast-suppression 20
 poe enable
 stp edged-port enable
 qos trust dscp
#
interface Ethernet1/0/7
 port link-mode bridge
 description Telephone IP + PMF
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 4 30
 port trunk pvid vlan 4
 undo voice vlan mode auto
 voice vlan 30 enable
 loopback-detection enable
 loopback-detection enable
 loopback-detection per-vlan enable
 loopback-detection action shutdown
 broadcast-suppression 20
 multicast-suppression 20
 poe enable
 stp edged-port enable
 qos trust dscp
#
interface Ethernet1/0/8
 port link-mode bridge
 description Telephone IP + PMF
```

```
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 4 30
 port trunk pvid vlan 4
 undo voice vlan mode auto
 voice vlan 30 enable
 loopback-detection enable
 loopback-detection enable
 loopback-detection per-vlan enable
 loopback-detection action shutdown
 broadcast-suppression 20
 multicast-suppression 20
 poe enable
 stp edged-port enable
 qos trust dscp
#
interface Ethernet1/0/9
 port link-mode bridge
 description Telephone IP + PMF
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 4 30
 port trunk pvid vlan 4
 undo voice vlan mode auto
 voice vlan 30 enable
 loopback-detection enable
 loopback-detection enable
 loopback-detection per-vlan enable
 loopback-detection action shutdown
 broadcast-suppression 20
 multicast-suppression 20
 poe enable
 stp edged-port enable
 qos trust dscp
#
interface Ethernet1/0/10
 port link-mode bridge
 description Telephone IP + PMF
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 4 30
 port trunk pvid vlan 4
 undo voice vlan mode auto
 voice vlan 30 enable
 loopback-detection enable
 loopback-detection enable
 loopback-detection per-vlan enable
 loopback-detection action shutdown
 broadcast-suppression 20
 multicast-suppression 20
 poe enable
 stp edged-port enable
 qos trust dscp
#
interface Ethernet1/0/11
 port link-mode bridge
 description Telephone IP + PMF
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 4 30
 port trunk pvid vlan 4
 undo voice vlan mode auto
 voice vlan 30 enable
 loopback-detection enable
 loopback-detection enable
 loopback-detection per-vlan enable
 loopback-detection action shutdown
 broadcast-suppression 20
 multicast-suppression 20
 poe enable
 stp edged-port enable
 qos trust dscp
#
interface Ethernet1/0/12
 port link-mode bridge
 description Telephone IP + PMF
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 4 30
 port trunk pvid vlan 4
 undo voice vlan mode auto
 voice vlan 30 enable
 loopback-detection enable
 loopback-detection enable
 loopback-detection per-vlan enable
 loopback-detection action shutdown
 broadcast-suppression 20
 multicast-suppression 20
 poe enable
 stp edged-port enable
 qos trust dscp
#
interface Ethernet1/0/13
 port link-mode bridge
 description Telephone IP + PMF
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 4 30
 port trunk pvid vlan 4
 undo voice vlan mode auto
 voice vlan 30 enable
 loopback-detection enable
 loopback-detection enable
 loopback-detection per-vlan enable
 loopback-detection action shutdown
 broadcast-suppression 20
 multicast-suppression 20
 poe enable
 stp edged-port enable
 qos trust dscp
#
interface Ethernet1/0/14
 port link-mode bridge
 description Telephone IP + PMF
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 4 30
 port trunk pvid vlan 4
 undo voice vlan mode auto
 voice vlan 30 enable
 loopback-detection enable
 loopback-detection enable
 loopback-detection per-vlan enable
 loopback-detection action shutdown
 broadcast-suppression 20
 multicast-suppression 20
 poe enable
 stp edged-port enable
 qos trust dscp
#
interface Ethernet1/0/15
 port link-mode bridge
 description Telephone IP + PMF
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 4 30
 port trunk pvid vlan 4
 undo voice vlan mode auto
 voice vlan 30 enable
 loopback-detection enable
 loopback-detection enable
 loopback-detection per-vlan enable
```

```
 loopback-detection action shutdown
 broadcast-suppression 20
 multicast-suppression 20
 poe enable
 stp edged-port enable
 qos trust dscp
#
interface Ethernet1/0/16
 port link-mode bridge
 description Telephone IP + PMF
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 4 30
 port trunk pvid vlan 4
 undo voice vlan mode auto
 voice vlan 30 enable
 loopback-detection enable
 loopback-detection enable
 loopback-detection per-vlan enable
 loopback-detection action shutdown
 broadcast-suppression 20
 multicast-suppression 20
 poe enable
 stp edged-port enable
 qos trust dscp
#
interface Ethernet1/0/17
 port link-mode bridge
 description Telephone IP + PMF
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 4 30
 port trunk pvid vlan 4
 undo voice vlan mode auto
 voice vlan 30 enable
 loopback-detection enable
 loopback-detection enable
 loopback-detection per-vlan enable
 loopback-detection action shutdown
 broadcast-suppression 20
 multicast-suppression 20
 poe enable
 stp edged-port enable
 qos trust dscp
#
interface Ethernet1/0/18
 port link-mode bridge
 description Telephone IP + PMF
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 4 30
 port trunk pvid vlan 4
 undo voice vlan mode auto
 voice vlan 30 enable
 loopback-detection enable
 loopback-detection enable
 loopback-detection per-vlan enable
 loopback-detection action shutdown
 broadcast-suppression 20
 multicast-suppression 20
 poe enable
 stp edged-port enable
 qos trust dscp
#
interface Ethernet1/0/19
 port link-mode bridge
 description Telephone IP + PMF
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 4 30
 port trunk pvid vlan 4
 undo voice vlan mode auto
 voice vlan 30 enable
 loopback-detection enable
 loopback-detection enable
 loopback-detection per-vlan enable
 loopback-detection action shutdown
 broadcast-suppression 20
 multicast-suppression 20
 poe enable
 stp edged-port enable
 qos trust dscp
#
interface Ethernet1/0/20
 port link-mode bridge
 description Telephone IP + PMF
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 4 30
 port trunk pvid vlan 4
 undo voice vlan mode auto
 voice vlan 30 enable
 loopback-detection enable
 loopback-detection enable
 loopback-detection per-vlan enable
 loopback-detection action shutdown
 broadcast-suppression 20
 multicast-suppression 20
 poe enable
 stp edged-port enable
 qos trust dscp
#
interface Ethernet1/0/21
 port link-mode bridge
 description Onduleur
 port access vlan 4
 undo voice vlan mode auto
 loopback-detection enable
 loopback-detection action shutdown
 broadcast-suppression 20
 multicast-suppression 20
 stp edged-port enable
#
interface Ethernet1/0/22
 port link-mode bridge
 description Telephone IP + PMF
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 4 30
 port trunk pvid vlan 4
 undo voice vlan mode auto
 voice vlan 30 enable
 loopback-detection enable
 loopback-detection enable
 loopback-detection per-vlan enable
 loopback-detection action shutdown
 broadcast-suppression 20
 multicast-suppression 20
 poe enable
 stp edged-port enable
 qos trust dscp
#
interface Ethernet1/0/23
 port link-mode bridge
 description Telephone IP + PMF
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 4 30
 port trunk pvid vlan 4
 undo voice vlan mode auto
 voice vlan 30 enable
 loopback-detection enable
```

```
 loopback-detection enable
 loopback-detection per-vlan enable
 loopback-detection action shutdown
 broadcast-suppression 20
 multicast-suppression 20
 poe enable
 stp edged-port enable
 qos trust dscp
#



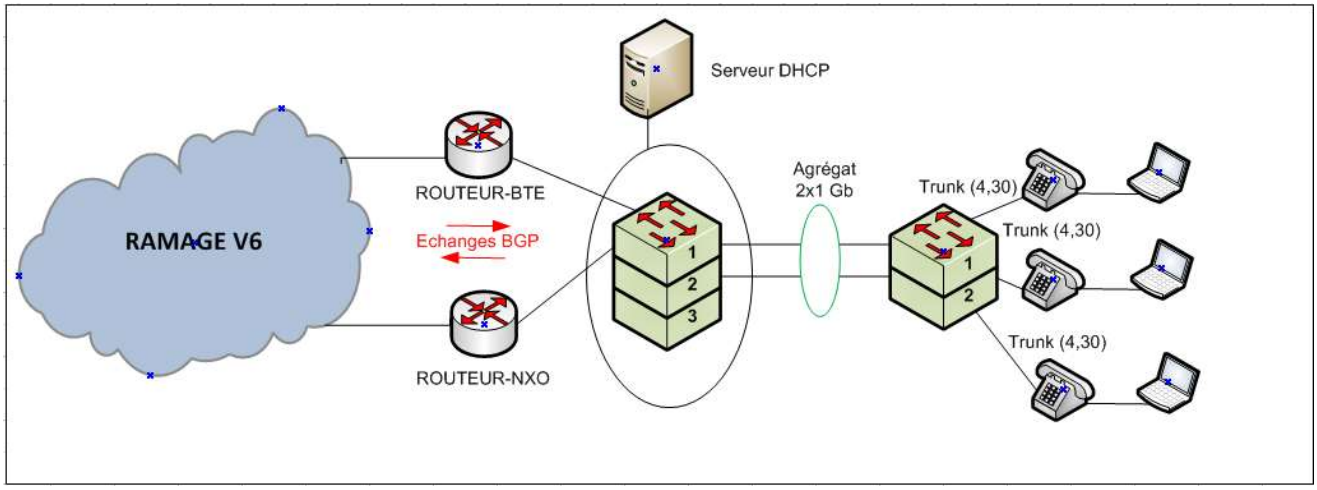
#
interface Ethernet1/0/24
port link-mode bridge
description Serveur
port access vlan 4
undo voice vlan mode auto
loopback-detection enable
loopback-detection action shutdown
broadcast-suppression 20
multicast-suppression 20
stp enable
stp edged-port enable
#
interface GigabitEthernet1/0/25
 port link-mode bridge
 description 111901L010ESXi - ETH1
 port access vlan 4
 loopback-detection enable
 broadcast-suppression 20
 multicast-suppression 20
 stp edged-port enable
#
interface GigabitEthernet1/0/26
port link-mode bridge
description SHUTDOWN
shutdown
#
interface GigabitEthernet1/0/27
 description STACKAGE
#
interface GigabitEthernet1/0/28
 description STACKAGE
#
bgp 65005
 router-id 55.248.11.38
 preference 50 50 50
 import-route direct route-policy DIRECT-TO-BGP
 undo synchronization
 timer keepalive 5 hold 15
 peer 55.xx.240.8 as-number 65000
 peer 55.xx.240.9 as-number 65003
 peer 55.xx.240.8 route-policy BGP-OUT-BTEL export
 peer 55.xx.240.8 route-policy BGP-IN import
 peer 55.xx.240.8 password cipher
$c$3$0UBTgQwbW3kDB9GjNu/Loq/oDvy5jMUSWWdOGMo=
 peer 55.xx.240.8 advertise-community
 peer 55.xx.240.9 route-policy BGP-OUT-NXO export
 peer 55.xx.240.9 route-policy BGP-IN import
 peer 55.xx.240.9 password cipher $c$3$+2HP
52iY0TTFfCiQKGMawsbd4mFy26Ahn0m5m+M=
 peer 55.60.240.9 advertise-community
#
rip 1
 undo summary
 version 2
 network 55.0.0.0
 network 58.0.0.0
 silent-interface all
 undo silent-interface Vlan-interface5
#
route-policy BGP-IN permit node 10
 if-match community LP500
 apply local-preference 500
 apply community no-advertise additive
route-policy BGP-IN permit node 20
 if-match community LP400
 apply local-preference 400
 apply community no-advertise additive
route-policy BGP-IN permit node 30
 if-match community LP300
 apply local-preference 300
 apply community no-advertise additive
route-policy BGP-IN permit node 40
 if-match community LP200
 apply local-preference 200
 apply community no-advertise additive
route-policy BGP-IN permit node 50
 if-match community LP100
 apply local-preference 100
 apply community no-advertise additive
route-policy BGP-IN permit node 60
 if-match community LP50
 apply local-preference 50
 apply community no-advertise additive
route-policy BGP-IN permit node 70
 if-match community LP10
 apply local-preference 10
 apply community no-advertise additive
route-policy BGP-OUT-BTEL permit node 10
 apply community 65005:121
route-policy BGP-OUT-NXO permit node 10
 apply community 65005:220
route-policy DIRECT-TO-BGP permit node 10
 if-match acl 2922
#
 ip community-list basic LP500 permit 65005:50
 ip community-list basic LP400 permit 65005:40
 ip community-list basic LP300 permit 65005:30
 ip community-list basic LP200 permit 65005:20
 ip community-list basic LP100 permit 65005:10
 ip community-list basic LP50 permit 65005:5
 ip community-list basic LP10 permit 65005:1
#
info-center loghost source loopback1
info-center loghost slog-reseau-org.ramage
#
 snmp-agent
 snmp-agent local-engineid 800063A203CC3E5FF17A63
 snmp-agent community read TOKTBAT22!  acl 2099
 snmp-agent community write snmp-private  acl 2099
 snmp-agent sys-info contact Departement Informatique /
CPAM VILLE
 snmp-agent sys-info location MSP Ussel - Rue Prouzergue
 snmp-agent sys-info version v2c v3
 snmp-agent target-host trap address udp-domain 55.18.4.89
params securityname Snmp-Cp@m19 v2c
 snmp-agent target-host trap address udp-domain 55.245.4.125
params securityname Snmp-Cp@m19 v2c
#
header shell %
**************************************
*             ! Attention !          *
*                                    *
*    Acces reserve aux personnels du *
*         service informatique       *
*                                    *
*  Toutes les activites sur ce systeme *
*           sont enregistrees        *
*                                    *
*    Toutes preuves d activites non  *
*   autorisees seront traitees par les *
```

```
*     autorites competentes              *
*                                        *
*      Toute intrusion sur un systeme    *
*    informatique est interdite par les  *
*      articles 323-2 du code penal      *
*                                        *
******************************************
%
#
 dhcp enable
#
 ntp-service unicast-server 55.223.10.8
#
 ssh server enable
 undo ssh server compatible-ssh1x
 ssh user admin service-type stelnet authentication-type
password
 ssh client authentication server 55.244.111.45 assign publickey
55.244.111.45
#
undo ip http enable
undo ip https enable
#
 load xml-configuration
#
 load tr069-configuration
#
user-interface aux 0
 authentication-mode scheme
user-interface vty 0 15
 authentication-mode scheme
 protocol inbound ssh
#
irf-port 1/1
 port group interface GigabitEthernet1/0/27
#
irf-port 1/2
 port group interface GigabitEthernet1/0/28
#
return
```

3.17.11.2.2 Avec un stack N3 et un stack N2

Ci-dessous l'exemple d'une agence (agence ou établissement). On retrouve une architecture construite **avec un stack fédérateur de 3 3600-24-PoE-v2 de niveau 3 et un stack de 2 3600-24-PoE-v2 de niveau 2 car il y a deux répartiteurs distants l'un de l'autre et environ 120 agents** :

- Un accès RAMAGE avec 2 routeurs opérateur
- Deux stacks de 3600-24-PoE-v2
- Les rocades entre les deux répartiteurs sont en cuivre permettant une redondance via un agrégat à 2 x 1 Gb/s entre les deux stacks via leurs interfaces 1/0/25 et N/0/25
- La ToIP est en place avec un IPBX distant (au siège de l'Organisme)
- Le serveur DHCP est local (sur serveur de proximité) et connecté à 1 Gb/s au port 26T du 1er 3600 du stack fédérateur.



- Plan d'adressage IP **(exemple)** :
  - VLAN 5 – VLAN-INTERCOWAN : 55.X.240.0 /29 – Interface VLAN 5 : 55.X.240.1
  - VLAN 4 – VLAN-DATA : 55.X.8.0 /22 – Interface VLAN 4 : 55.X.8.1
  - VLAN 30 – VLAN-VOIX : 58.X.8.0 /22 – Interface VLAN 30 : 58.X.8.1

- Serveurs GDIFF :
  - National : 55.245.4.0

- Adresse IP du serveur DHCP : 55.X.8.60 (VLAN 4) qui distribue les adresses aux PMF et aux téléphones – port 1/0/26T.

Configurations (pages suivantes)

Résultat d'un « display current » : certaines commandes par défaut non entrées en configuration apparaissent, d'autres, entrées n'apparaissent pas (stp enable sur interfaces par ex).

La partie routage e-BGP n'est pas indiquée, il faut vous renseigner sur le profil de votre agence et récupérer la configuration BGP auprès de votre correspondant LAN

STACK 3600 N3 :

```
sysname xxx-et-001-N3-3600-RG
#
 clock timezone PARIS add 01:00:00
 clock summer-time PARIS repeating 02:00:00 03/27/2011
03:00:00 10/30/2011  01:00:00
#
 dhcp relay server-group 1 ip 55.X.8.60
#
voice vlan mac-address XXXX-XXXX-XXXXX mask ffff-ff00-0000
description Postes Constructeur
#
irf mac-address persistent timer
 irf auto-update enable
 undo irf link-delay
 irf domain 1
irf member 1 priority 32
 irf member 2 priority 30
 irf member 3 priority 28
#
domain default enable system
dns resolve
dns server 55.223.10.1
dns domain cnamts.fr
#
loopback-detection enable
loopback-detection multi-port-mode enable
#
undo ip https enable
undo ip http enable
#
ip ttl-expires enable
ip unreachables enable
#
 ip forward-broadcast
#
acl number 2099
 description SNMP RO ACCESS FOR DR
 rule 0 permit source 55.18.0.0 0.0.255.255
 rule 1 permit source 55.36.0.0 0.0.255.255
 rule 2 permit source 55.X.0.0 0.0.255.255
 rule 3 permit source 55.Y.0.0 0.0.255.255
 rule 4 permit source 55.245.4.0 0.0.0.255
#
acl number 3002 name GEDIFF
 rule 1 permit udp source 55.245.4.0 0.0.3.255
#
vlan 1
#
vlan 4
 name VLAN-DATA
#
vlan 5
 name VLAN-INTERCOWAN
#
vlan 30
 name VLAN-VOIX
#
VLAN 901
 Name VLAN-ADMIN-RESEAU
#
radius scheme system
 server-type extended
 primary authentication 127.0.0.1 1645
 primary accounting 127.0.0.1 1646
 user-name-format without-domain
#
domain system
 access-limit disable
 state active
 idle-cut disable
 self-service-url disable
#
user-group system
 group-attribute allow-guest
#
local-user admin
 password cipher MotDePasse
 authorization-attribute level 3
 service-type ssh terminal
 service-type web
#
 stp mode rstp
 stp instance 0 priority 0
 stp enable
 stp bpdu-protection
stp bridge-diameter 2
 loopback-detection enable
 loopback-detection multi-port-mode enable
 stp pathcost-standard dot1t
#
interface Bridge-Aggregation1
description AGG-010-N2-3600
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 4 30
 link-aggregation mode dynamic
 dhcp-snooping trust
 mad nable
 stp root-protection
#
interface NULL0
#
interface Vlan-interface4
description INT-VLAN-DATA
 ip address 55.X.8.1 255.255.252.0
 ip forward-broadcast acl 3002
#
interface Vlan-interface5
description INT-VLAN-INTERCOWAN
 ip address 55.X.240.1 255.255.255.248
#
interface Vlan-interface30
 description INT-VLAN-VOIX
 ip address 58.X.8.1 255.255.252.0
 dhcp select relay
 dhcp relay server-select 1
#
interface Vlan-interface901
description INT-VLAN-ADMIN-RESEAU
 ip address 55.X. 0.1 255.255.255.240
#
interface Ethernet1/0/1
 port link-mode bridge
 description ROUTEUR-BTE
 port access vlan 5
 speed 100
 duplex full
 stp disable
#
interface Ethernet1/0/2
 port link-mode bridge
 description TEL+PMF
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 4 30
 port trunk pvid vlan 4
```

```
 undo voice vlan mode auto
 voice vlan 30 enable
 poe enable
 stp edged-port enable
 loopback-detection enable
 loopback-detection action shutdown
 loopback-detection enable
 loopback-detection per-vlan enable
 multicast-suppression 20
 broadcast-suppression 20
#
```

#...Etc.

```
#
interface Ethernet1/0/24
 port link-mode bridge
 description IP-Phone+PMF
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 4 30
 port trunk pvid vlan 4
 undo voice vlan mode auto
 voice vlan 30 enable
 poe enable
 stp edged-port enable
 loopback-detection enable
 loopback-detection action shutdown
 loopback-detection enable
 loopback-detection per-vlan enable
 multicast-suppression 20
 broadcast-suppression 20
#
interface Ethernet2/0/1
 port link-mode bridge
 description IP-Phone+PMF
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 4 30
 port trunk pvid vlan 4
 undo voice vlan mode auto
 voice vlan 30 enable
 poe enable
 stp edged-port enable
 loopback-detection enable
 loopback-detection action shutdown
 loopback-detection enable
 loopback-detection per-vlan enable
 multicast-suppression 20
 broadcast-suppression 20
#
```

#...Etc.

```
#
interface Ethernet2/0/24
 port link-mode bridge
 description IP-Phone+PMF
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 4 30
 port trunk pvid vlan 4
 undo voice vlan mode auto
 voice vlan 30 enable
 poe enable
 stp edged-port enable
 loopback-detection enable
 loopback-detection action shutdown
 loopback-detection enable
 loopback-detection per-vlan enable
 multicast-suppression 20
 broadcast-suppression 20
#
interface Ethernet3/0/1
 port link-mode bridge
 description ROUTEUR-NXO
 port access vlan 5
 speed 100
 duplex full
 stp disable
#

 interface Ethernet3/0/2
 port link-mode bridge
 description IP-Phone+PMF
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 4 30
 port trunk pvid vlan 4
 undo voice vlan mode auto
 voice vlan 30 enable
 poe enable
 stp edged-port enable
 loopback-detection enable
 loopback-detection action shutdown
 loopback-detection enable
 loopback-detection per-vlan enable
 multicast-suppression 20
 broadcast-suppression 20
```

#...Etc.

```
#
interface Ethernet3/0/24
 port link-mode bridge
 description IP-Phone+PMF
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 4 30
 port trunk pvid vlan 4
 undo voice vlan mode auto
 voice vlan 30 enable
 poe enable
 stp edged-port enable
 loopback-detection enable
 loopback-detection action shutdown
 loopback-detection enable
 loopback-detection per-vlan enable
 multicast-suppression 20
 broadcast-suppression 20
#
interface GigabitEthernet1/0/25
port link-mode bridge
description AGG-010-N2-3600-LIEN1
port link-type trunk
undo port trunk permit vlan 1
port trunk permit vlan 4 30
port link-aggregation group 1
dhcp-snooping trust
#
interface GigabitEthernet1/0/26
port link-mode bridge
description Serveur DHCP
port access vlan 4
stp edged-port enable
dhcp-snooping trust
loopback-detection enable
loopback-detection action shutdown
loopback-detection enable
loopback-detection per-vlan enable
multicast-suppression 20
broadcast-suppression 20
#
interface GigabitEthernet2/0/25
Description SHUTDOWN
```

```
port link-mode bridge
shutdown

#
interface GigabitEthernet2/0/26
Description SERVEUR DHCP
port link-mode bridge
port access vlan 4
stp enable
stp edge-port enable
dhcp snooping trust
#
interface GigabitEthernet3/0/25
 description AGG-010-N2-3600-LIEN2
port link-mode bridge
port link-type trunk
undo port trunk permit vlan 1
port trunk permit vlan 4 30
port link-aggregation group 1
dhcp-snooping trust
#
interface GigabitEthernet3/0/26
 port link-mode bridge
 shutdown
#
interface GigabitEthernet1/0/27
 description STACKAGE
#
interface GigabitEthernet1/0/28
 description STACKAGE
#
interface GigabitEthernet2/0/27
 description STACKAGE
#
interface GigabitEthernet2/0/28
 description STACKAGE
#
interface GigabitEthernet3/0/27
#
interface GigabitEthernet3/0/28
 description STACKAGE
#
##### Routage par DR#####
#
 dhcp-snooping
#
info-center loghost source Vlan-interface 901
info-center loghost slog-reseau-org.ramage
#
 snmp-agent
 snmp-agent local-engineid 800063A203B8AF67AC8A04
 snmp-agent community read TOKTBAT22! acl 2099
 snmp-agent community write xxxxxxxx acl 2099
 snmp-agent sys-info contact François Pignon
 snmp-agent sys-info location RG
 snmp-agent sys-info version v2c
 snmp-agent trap enable default-route
#
header shell %
**************************************
*             ! Attention !          *
*                                    *
*    Acces reserve aux personnels du *
*         service informatique       *
*                                    *
*  Toutes les activites sur ce systeme *
*          sont enregistrees         *
*                                    *
*    Toutes preuves d activites non  *
*   autorisees seront traitees par les *
*    autorites competentes           *
*                                    *
*     Toute intrusion sur un systeme *
*   informatique est interdite par les *
*     articles 323-2 du code penal   *
*                                    *
**************************************
%
#
 dhcp enable
#
 ntp-service unicast-server 55.223.10.8
#
 ssh server enable
undo ssh server compatible-ssh1x
ssh user admin service-type stelnet authentication-type
password
#
 load xml-configuration
#
 load tr069-configuration
#
user-interface aux 0 2
 authentication-mode scheme
user-interface vty 0 15
 authentication-mode scheme
 protocol inbound ssh
#


irf-port 1/1
 port group interface GigabitEthernet1/0/27
#
irf-port 1/2
 port group interface GigabitEthernet1/0/28
#
irf-port 2/1
 port group interface GigabitEthernet2/0/27
#
irf-port 2/2
 port group interface GigabitEthernet2/0/28
#
irf-port 3/1
 port group interface GigabitEthernet3/0/27
#
irf-port 3/2
 port group interface GigabitEthernet3/0/28
#
```

STACK 3600 N2 :

```
#
sysname xxx-et-xxxxx-002-N2-3600-SR1
#
voice vlan mac-address XXXX-XXXX-XXXXX mask ffff-ff00-0000
description Postes Constructeur
#
clock timezone PARIS add 01:00:00
 clock summer-time PARIS repeating 02:00:00 03/27/2011
03:00:00 10/30/2011  01:00:00
#
irf mac-address persistent timer
 irf auto-update enable
 undo irf link-delay
 irf domain 2
irf member 1 priority 32
 irf member 2 priority 30
#
domain default enable system
dns resolve
dns server 55.223.10.1
dns domain cnamts.fr
#
loopback-detection enable
loopback-detection multi-port-mode enable
#
undo ip https enable
undo ip http enable
#
ip ttl-expires enable
ip unreachables enable
#
vlan 1
#
vlan 4
 name VLAN-DATA
#
vlan 30
 name VLAN-VOIX
#
vlan 901
 name VLAN-ADMIN-RESEAU
#
radius scheme system
 server-type extended
 primary authentication 127.0.0.1 1645
 primary accounting 127.0.0.1 1646
 user-name-format without-domain
#
domain system
 access-limit disable
 state active
 idle-cut disable
 self-service-url disable
#
user-group system
 group-attribute allow-guest
#
local-user admin
 password cipher MotDePasse
 authorization-attribute level 3
 service-type ssh terminal
 service-type web
#
 stp mode rstp
 stp enable
 loopback-detection enable
 loopback-detection multi-port-mode enable
 stp pathcost-standard dot1t
 stp bpdu-protection
#


#
Interface Bridge-Aggregation1
Description AGG-010-N2-HP 3600
port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 4 30
 link-aggregation mode dynamic
 dhcp-snooping trust
 mad nable
 stp loop-protection
#
interface NULL0
#
interface Vlan-interface901
Description INT-VLAN-ADMIN-RESEAU
 ip address 55.X.0.2 255.255.255.240
#
interface Ethernet1/0/1
 port link-mode bridge
 description IP-Phone+PMF
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 4 30
 port trunk pvid vlan 4
 undo voice vlan mode auto
 voice vlan 30 enable
 poe enable
 stp edged-port enable
 loopback-detection enable
 loopback-detection action shutdown
 loopback-detection enable
 loopback-detection per-vlan enable
 multicast-suppression 20
 broadcast-suppression 20
#
#...Etc.
#
interface Ethernet1/0/24
 port link-mode bridge
 description IP-Phone+PMF
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 4 30
 port trunk pvid vlan 4
 undo voice vlan mode auto
 voice vlan 30 enable
 poe enable
 stp edged-port enable
 loopback-detection enable
 loopback-detection action shutdown
 loopback-detection enable
 loopback-detection per-vlan enable
 multicast-suppression 20
 broadcast-suppression 20
#
interface Ethernet2/0/1
 port link-mode bridge
 description IP-Phone+PMF
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 4 30
 port trunk pvid vlan 4
 undo voice vlan mode auto
 voice vlan 30 enable
```

```
 poe enable
 stp edged-port enable
 loopback-detection enable
 loopback-detection action shutdown
 loopback-detection enable
 loopback-detection per-vlan enable
 multicast-suppression 20
 broadcast-suppression 20
#
```

#...Etc.

```
#
interface Ethernet2/0/24
 port link-mode bridge
 description IP-Phone+PMF
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 4 30
 port trunk pvid vlan 4
 undo voice vlan mode auto
 voice vlan 30 enable
 poe enable
 stp edged-port enable
 loopback-detection enable
 loopback-detection action shutdown
 loopback-detection enable
 loopback-detection per-vlan enable
 multicast-suppression 20
 broadcast-suppression 20
#
interface GigabitEthernet1/0/25
 Description AGG-010-N3-HP 3600-LIEN1
 port link-mode bridge
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 4 30
 port link-aggregation group 1
 dhcp-snooping trust
#
interface GigabitEthernet1/0/26
 port link-mode bridge
 shutdown
#
interface GigabitEthernet2/0/25
 port link-mode bridge
 Description AGG-010-N3-HP 3600-LIEN2
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 4 30
 port link-aggregation group 1
 dhcp-snooping trust
#
interface GigabitEthernet2/0/26
 port link-mode bridge
 shutdown
#
interface GigabitEthernet1/0/27
 description STACKAGE
#
interface GigabitEthernet1/0/28
 description STACKAGE
#
interface GigabitEthernet2/0/27
 description STACKAGE
#
interface GigabitEthernet2/0/28
 description STACKAGE
#
 dhcp-snooping
#
 ip route-static 0.0.0.0 0.0.0.0 55.X.0.1
#
 Info-center source vlan-interface 901
 info-center loghost slog-reseau-org.ramage
#
 snmp-agent
 snmp-agent local-engineid 800063A203D07E28A646A7
 snmp-agent community read TOKTBAT22! acl 2099
 snmp-agent community write xxxxxxxx acl 2099
 snmp-agent sys-info contact François Pignon
 snmp-agent sys-info location RG
 snmp-agent sys-info version v2c
 snmp-agent trap enable default-route
#
header shell %
**************************************
*             ! Attention !          *
*                                    *
*    Acces reserve aux personnels du *
*         service informatique       *
*                                    *
*  Toutes les activites sur ce systeme *
*          sont enregistrees         *
*                                    *
*    Toutes preuves d activites non  *
*   autorisees seront traitees par les *
*    autorites competentes           *
*                                    *
*     Toute intrusion sur un systeme *
*   informatique est interdite par les *
*     articles 323-2 du code penal   *
*                                    *
**************************************
%
#
 ntp-service unicast-server 55.223.10.8
#
 ssh server enable
undo ssh server compatible-ssh1x
 ssh user admin service-type stelnet authentication-type
password
#
 load xml-configuration
#
 load tr069-configuration
#
user-interface aux 0 1
 authentication-mode scheme
user-interface vty 0 15
 authentication-mode scheme
 protocol inbound ssh
#
irf-port 1/1
 port group interface GigabitEthernet1/0/27
#
irf-port 1/2
 port group interface GigabitEthernet1/0/28
#
irf-port 2/1
 port group interface GigabitEthernet2/0/27
#
irf-port 2/2
 port group interface GigabitEthernet2/0/28
#
```

4 GUIDE DE CONFIGURATION DES ARUBA 2930FLE MODELE ARUBA 2930F

C'est un switch N2/N3 avec :

- 8 ports 10/100/1000 Mb/s POE pour la connexion de téléphones IP et de PMF
- 2 ports modulaires fibre optique SFP/SFP+ à 1 ou 10 Gb/s pour l'éventuelle interconnexion gibabit avec un autre swicth.

Il est « fanless » (sans ventilateur). Il peut donc être utilisé :

- au niveau 2 et à l'extrémité dans tout site ayant un autre modèle de switch N3 (siège de CPAM, MEDICAL…) :
  - placé dans une baie dans un répartiteur
  - placé dans un bureau mal desservi en prises RJ45
- Même si c'est un switch niveau 3, **il ne devra pas être installé en tête de réseau car il est non compatible Ramage v6**.

Photo :



Ce switch est stackable mais cela n'a que peu d'intérêt : en cas de besoin de plus de ports, autant plutôt mettre en place un HP-3600 par exemple.

4.2 PRISE EN MAIN

La connexion aux switches se fait via le câble bleu fourni dans le carton d'emballage du switch que l'on connecte sur le port série d'un PC. Ensuite, la prise en main se fait via « Putty » ou « Hyperterminal » par exemple.

Pour passer les commandes, il faut être en mode « configuration ». Pour cela, il faut taper « conf t » au prompt de base (#). Le prompt change pour un **(config)#** .

```
Aruba-2930F-8G-PoEP-2SFPP# conf t
Aruba-2930F-8G-PoEP-2SFPP(config)#
```

Le Ctrl+Z permet de revenir au prompt initial hors mode configuration.
Le « ? » permet de visualiser les commandes disponibles à l'endroit où on se trouve.
La touche tabulation permet de compléter automatiquement une commande commencée.
Les commandes ressemblent beaucoup à celles de Cisco : « write memory » pour sauvegarder…

4.3 COMMANDES DE BASE

show run : voir la configuration courante

show interface brief ou status / : voir le status des interfaces

show interface … : informations importantes sur les interfaces (erreurs, CRC…)

show lldp […] : voir les informations et voisins lldp

sh ntp status : voir le serveur ntp

show flash : voir les fichiers de la flash

reload at … : rebooter le switch à une heure donnée

show vlans…: voir les vlans

show logging : affiche les logs

show version : affichage d'information de version

write memory : sauvegarder la configuration

power-over-ethernet : activer PoE sur une interface (activé par défaut)

sh power-over-ethernet brief : status du PoE

Pour configurer un switch Aruba 2930F, il faut passer en mode « conf t » (configure terminal) comme en Cisco. Pour cela, il faut être connecté en « admin ».

Des commandes de base sont disponibles pour tout usager n'ayant pas le login « admin » :

```
2930-89-CNGR>
 chassislocate       Control the chassis locate LED.
 display             Display current system information.
 enable              Enter the Manager command context.
 exit                Return to the previous context or terminate current
                     console/telnet session if you are in the Operator
                     context level.
 link-test           Test the connection to a MAC address on the LAN.
 logout              Terminate this console or telnet session.
 menu                Enter the menu-based console user interface.
 page                Toggle paging mode.
 ping                Send ping requests to a device on the network.
 ping6               Send IPv6 ping requests to a device on the network.
 quit                Exit the current command view
 show                Display switch operation information.
 traceroute          Trace the IPv4 route to a device on the network.
 traceroute6         Trace the IPv6 route to a device on the network.
 verify              Verify the signature of a switch firmware image.
```

4.4 CONFIGURATION POUR UNE INSTALLATION AU N2 A L'EXTREMITE

Dans les sièges d'Organisme, le switch Aruba 2930Fsera installé au niveau 2 dans le VLAN 901 à l'extrémité du réseau fédéré par un switch N3. Il pourra être connecté directement au fédérateur ou cascadé derrière un HP 3600 par exemple.
Dans les agences, le switch Aruba 2930F sera installé au niveau 2 dans le VLAN 4 à l'extrémité du réseau fédéré par un switch N3.
Le cas de l'installation en agence au niveau 3 en tête de réseau via le VLAN 5 d'IntercoWan, sera traité si besoin dans un autre chapitre.
Le port normalisé d'interconnexion avec le switch parent est le port 8.
Si un agrégat est souhaité, cet agrégat sera construit avec les ports 7 et 8.

4.4.1 Accès console, SSH et HTTPS

Règle de construction du mot de passe :

- **Taille :** le mot de passe doit avoir au moins 12 caractères
- **Complexité :** Le mot de passe doit contenir au moins 4 types de caractères différents, et au moins 2 caractères pour chaque type

Exemple de mot de passe :
. Exemple : « 12ABcd$!12AB »
2 x Caractères spéciaux : $!
2x Majuscules : AB
2x Minuscules : cd
2x Nombres : 12

Ces commandes permettront de paramétrer un accès au switch ou au stack en console, ssh et http via le login « admin » et un mot de passe (à personnaliser) :

```
password manager user-name admin plaintext motdepasse          | remplacer «motdepasse» par le vôtre
```

➔ Un message indique que l'auto-config en DHCP va être inhibé ➔ ignorez et retapez la commande.

```
no telnet-server                                               | enlever telnet
ip ssh                                                         | valider ssh
crypto pki enroll-self-signed certificate-name CNAM subject
        Enter Common Name(CN) : cnam
        Enter Org Unit(OU) : cnam
        Enter Org Name(O) : cnam
        Enter Locality(L) : cnam
        Enter State(ST) : cnam
        Enter Country(C) : fr
#
aaa authentication ssh enable local
No web-management plaintext                                    | pas de HTTP
No web-management ssl                                          | pas de HTTPS
#
no front-panel-security password-clear                         | pas de reset password en face avant
                        **** CAUTION ****
        Disabling the Clear button prevents switch passwords from being easily reset or
        recovered.  Ensure that you are familiar with the front panel security options
        before proceeding.

        Continue disabling the Clear button (y/n)? y           | Répondre oui
#
front-panel-security display-in-config
```

4.4.2 Sauvegarde de la configuration (running)

write memory

4.4.3 Résolution DNS

Pour permettre l'utilisation de nom DNS au lieu d'adresses IP quand cela est possible, il est nécessaire d'entrer ces commandes :

ip dns domain-name assurance-maladie.fr
ip dns server-address priority 1 55.223.10.1

4.4.4 Configuration du Spanning-Tree et protection des boucles

En global :

spanning-tree enable
spanning-tree mode rapid-pvst
Changing STP modes may take several seconds, possibly allowing loops on redundant links. Continue (y/n)? y | Répondre « y »
#
loop-protect mode port
Any Loop Protect enabled VLAN will be deleted.
Do you want to continue?[Y/N] y | Répondre « y »
#
loop-protect trap loop-detected
loop-protect disable-timer 60
#

Sur les interfaces pour PMF et/ou téléphone (exemple de 1 à 7) :

Loop-protect 1-7

4.4.5 SNMP / SYSLOG

4.4.5.1 SNMP

#
Snmp-server enable
snmp-server contact *NOM*
snmp-server community *COM_SNMP* manager unrestricted | « COM_SNMP » = votre nom de communauté
snmp-server community TOKTBAT22! manager restricted | UNIQUE pour serveurs de polling
no snmp-server community public

Remplacer *« COM_SNMP »* par votre communauté « write » habituelle.

Autoriser les sous-réseaux sources (idem ACL) :

ip authorized-managers 55.244.0.0 255.255.0.0 access manager | CSH-SUD
ip authorized-managers 55.245.0.0 255.255.0.0 access manager | CSH-GE
ip authorized-managers 55.18.0.0 255.255.0.0 access manager | DR

4.4.5.2 SYSLOG

SYSLOG : Il s'agit d'un serveur national qui recueille les logs des switches dans le cadre des outils IRMA. Cette commande est à entrer dans tous les switches car elle conditionne le bon fonctionnement de HP-NA :

logging 55.243.104.12 | adresse unique valable pour tous
logging origin-id hostname

Pensez à consulter les tutoriels sur le site du DR.

4.4.6 Nommer le switch

Le nommage des switches est normalisé : voir le § « Nommage des switches » plus haut dans ce document.

La commande à utiliser est « sysname ».

Exemple :

[] sysname 351-sw-et-redon-011-n2-2930F-RG

4.4.7 Configuration du VLAN d'Amin-réseau

Installés uniquement à l'extrémité au niveau 2, ces switches n'auront qu'une seule adresse IP : celle de l'interface VLAN 901.

4.4.7.1 En siège

VLAN 1 inhibé
Adresse IP sur VLAN 901 (exemple 55.X.221.17) :

Interco fédérateur via INT 8 sans agrégat	Interco fédérateur via INT 7 et 8 avec agrégat trk1
vlan 1 name "DEFAULT_VLAN" no untagged 1-7 untagged 8-10 no ip address forbid 1-7 exit # vlan 901 name "ADMIN-RESEAU" tagged 8 ip address 55.X.221.Z 255.255.255.0 exit #	vlan 1 name "DEFAULT_VLAN" no untagged 1-6 untagged 9-10,Trk1 no ip address forbid 1-6 exit # vlan 901 name "ADMIN-RESEAU" tagged Trk1 ip address 55.X.221.Z 255.255.255.0 exit #

4.4.7.2 En agence

VLAN 1 inhibé
Adresse IP sur VLAN 901 (exemple 55.80.0.3) :

Interco fédérateur via INT 8 sans agrégat	Interco fédérateur via INT 7 et 8 avec agrégat trk1
vlan 1 name "DEFAULT_VLAN" no untagged 1-7 untagged 8-10 no ip address forbid 1-7 exit # **vlan 901** **name "ADMIN-RESEAU"** **tagged 8** **ip address 55.X.24[0-1].Z 255.255.255.240** **exit** #	vlan 1 name "DEFAULT_VLAN" no untagged 1-6 untagged 9-10,Trk**1** no ip address forbid 1-6 exit # **vlan 901** **name "ADMIN-RESEAU"** **tagged Trk1** **ip address 55.X.24[0-1].Z 255.255.252.240** **exit** #

Remarque : les tableaux du plan d'adressage IP normalisé pour le VLAN 901 sont dans les référentiels LAN.

4.4.8 Configuration des interfaces du 2930F

4.4.8.1 Permettre l'utilisation de SFP ou SFP+ non Aruba

Par défaut, les modules SFP ou SFP+ d'autres constructeurs que Aruba ne sont pas acceptés. Pour que cela fonctionne, il faut taper une commande « cachée » mais attention : A TAPER EN ENTIER SANS TABULER et en mode configuration :

Tout d'abord, insérez le SFP ou SFP+.

Switch# config
Switch(config)# allow-unsupported-transceiver

Pour vérifier : Switch# show interface transceiver detail

Eventuellement, un reboot du switch peut être nécessaire.

4.4.8.2 Interfaces non utilisées



Pour des raisons de sécurité, au moins dans les lieux sensibles comme les accueils… (possibilité pour un inconnu de se connecter au réseau sur une prise dans les lieux ouverts au public, possibilité de connecter un PC « non PLC » ou un hub ou un switch ou un sniffer sur une prise libre dans son bureau….) :

- ⇨ **il est demandé de mettre à « shutdown » toutes les interfaces Ethernet non utilisées.**

4.4.8.3 Speed / Duplex

RAPPEL :

1/ Configurer l'interface sans s'occuper des « speed et duplex » : laisser en auto par défaut

2/ Entre des « hosts » (PMF, téléphone, serveurs) et des switches, lorsque :
- **le débit négocié est inférieur à celui escompté**
- **un quelconque problème apparaît (lenteurs, accès à des ressources…)**
- **des erreurs sont constatées sur les interfaces**

⇨ **il faut forcer les speed et duplex côté switch et côté « host » (si possible).**

Par défaut, les interfaces sont en mode auto et 1000 Full-Duplex.
Il est possible de laisser en mode auto, forcer le mode auto ou forcer speed et / ou duplex :

En conf t :

```
int 1
(eth-1)# speed-duplex ?
 10-half                10 Mbps only, half duplex.
 100-half               100 Mbps only, half duplex.
 10-full                10 Mbps only, full duplex.
 100-full               100 Mbps only, full duplex.
 1000-full              1000 Mbps only, full duplex.
 auto                   Auto-negotiate link parameters.
 auto-10                10 Mbps only, auto-negotiate link parameters.
 auto-100               100 Mbps only, auto-negotiate link parameters.
 auto-2500              2500 Mbps only, auto-negotiate link parameters.
 auto-5000              5000 Mbps only, auto-negotiate link parameters.
 auto-2500-5000         2500 or 5000 Mbps only, auto-negotiate link parameters.
 auto-1000              1000 Mbps only, auto-negotiate link parameters.
 auto-10-100            10 or 100 Mbps only, auto-negotiate link parameters.
 auto-1000-2500         1000 or 2500 Mbps only, auto-negotiate link parameters.
 auto-1000-2500-5000    1000, 2500, or 5000 Mbps only, auto-negotiate link
                        parameters.
auto-10g          10 Gbps only, auto-negotiate link parameters.
```

Si vous devez forcer, choisissez les bonnes valeurs !

4.4.8.4 Téléphone + PMF

PRECONISATION DR : comme pour tout host (sauf les routeurs RAMAGE), il est demandé de configurer les interfaces LAN des téléphones IP en mode auto-négociation et de laisser les interfaces de swiches en mode auto (par défaut). Ensuite, il faut vérifier :
- **que la négociation s'est correctement déroulée et que les interfaces sont à 100 FULL**
- **qu'il n'y a aucune erreur sur les interfaces**

Pour vérifier, utiliser la commande « sh interface status ».

Interface 1 à 7 « TEL + PMF » ➔ VLAN 4 (PMF) et 30 (TEL)
et interface 8 en interconnexion vers fédérateur :

```
#
vlan 4
  name VLAN-DATA
  untagged 1-7
  tagged 8
```

```
  no ip address
  exit
#
vlan 30
  name VLAN-VOIX
  tagged 1-8
  no ip address
  voice
  exit
#
```

Configuration des interfaces de 1 à 7 (ou 1 à 6 si agrégat) de manière identique :

```
Int 1
(eth-1)#
 name "TEL+PMF"
 power-over-ethernet                    | En show run, « high » apparaît
 poe-lldp-detect enabled
 rate-limit bcast in percent 20
 rate-limit mcast in percent 20
 rate-limit unknown-unicast in percent 20
#
Int 2
(eth-2)#
 name "TEL+PMF"
 power-over-ethernet
 poe-lldp-detect enabled
 rate-limit bcast in percent 20
 rate-limit mcast in percent 20
 rate-limit unknown-unicast in percent 20
#
Int 3
(eth-3)#
 name "TEL+PMF"
 power-over-ethernet
 poe-lldp-detect enabled
 rate-limit bcast in percent 20
 rate-limit mcast in percent 20
 rate-limit unknown-unicast in percent 20
#
Int 4
(eth-4)#
 name "TEL+PMF"
 power-over-ethernet
 poe-lldp-detect enabled
 rate-limit bcast in percent 20
 rate-limit mcast in percent 20
 rate-limit unknown-unicast in percent 20
#
Int 5
(eth-5)#
 name "TEL+PMF"
 power-over-ethernet
 poe-lldp-detect enabled
 rate-limit bcast in percent 20
 rate-limit mcast in percent 20
 rate-limit unknown-unicast in percent 20
#
Int 6
(eth-6)#
 name "TEL+PMF"
 power-over-ethernet
 poe-lldp-detect enabled
```

```
 rate-limit bcast in percent 20
 rate-limit mcast in percent 20
 rate-limit unknown-unicast in percent 20
#
Int 7
(eth-7)#
 name "TEL+PMF"
 power-over-ethernet
 poe-lldp-detect enabled
 rate-limit bcast in percent 20
 rate-limit mcast in percent 20
 rate-limit unknown-unicast in percent 20
#
spanning-tree 1 admin-edge-port
spanning-tree 1 loop-guard bpdu-protection
spanning-tree 2 admin-edge-port
spanning-tree 2 loop-guard bpdu-protection
spanning-tree 3 admin-edge-port
spanning-tree 3 loop-guard bpdu-protection
spanning-tree 4 admin-edge-port
spanning-tree 4 loop-guard bpdu-protection
spanning-tree 5 admin-edge-port
spanning-tree 5 loop-guard bpdu-protection
spanning-tree 6 admin-edge-port
spanning-tree 6 loop-guard bpdu-protection#
spanning-tree 7 admin-edge-port
spanning-tree 7 loop-guard bpdu-protection#
loop-protect 1-7
#
```

4.4.8.5 PMF seul

Configuration de l'interface 1 pour un « PMF » ➔ VLAN 4 (PMF) :

```
vlan 4
 name VLAN-DATA
 untagged 1
#
int 1
(eth-1)#
 name "PMF"
 no power-over-ethernet
 rate-limit bcast in percent 20
 rate-limit mcast in percent 20
 rate-limit unknown-unicast in percent 20
#
spanning-tree 1 admin-edge-port
spanning-tree 1 loop-guard bpdu-protection
loop-protect 1
```

4.4.8.6 Equipement e-GFA

Configuration de l'interface 1 pour un équipement E-GFA ➔ VLAN 224 :

```
spanning-tree 1 admin-edge-port
#
vlan 224
 name VLAN-ACCES-PART
 untagged 1
#
int 1
(eth-1)#
 name "E-GFA"
 speed-duplex 100-full
 no power-over-ethernet
 rate-limit bcast in percent 20
 rate-limit mcast in percent 20
 rate-limit unknown-unicast in percent 20
#
spanning-tree 1 admin-edge-port
spanning-tree 1 loop-guard bpdu-protection
loop-protect 1
```

4.4.8.7 Borne wifi

Configuration de l'interface 1 pour une borne wifi :

```
spanning-tree 1 admin-edge-port
#
vlan 50                          | pour wifi interne
 name VLAN-WIFI-AGENTS
 tagged 1
#
vlan 54                          | si wifi invité
 name VLAN-WIFI-INVITE
 tagged 1
#
vlan 4 ou 901                            | Admin réseau
 name VLAN-ADMIN-RESEAU
 #
vlan 902                         | Admin wifi
 name VLAN-ADMIN-WIFI
 tagged 1
#
int 1
(eth-1)#
 name "Borne Wifi"
 power-over-ethernet
 power-over-ethernet                     | En show run, « high » apparaît
 poe-lldp-detect enabled
```

4.4.9 Interconnexion des switches

Dans les sièges, les Aruba 2930F sont placés à l'extrémité du réseau et connectés au cœur : les fédérateurs HP 5500. Il va donc falloir configurer des trunks d'interconnexion sur des interfaces en veillant à n'autoriser que les VLAN nécessaires à transiter (« permit vlan x y … »). En effet, sur les interfaces des 2930F, on ne trouve que des téléphones ou des PMF : seuls les vlan 4 et 30 sont utiles sur ces trunks d'interco – sans oublier le VLAN 901 pour permettre l'administration.

Dans les architectures normalisées des sièges d'Organismes (cf Référentiels), les interconnexions des fédérateurs et des 2930F sont à faire si possible via des liens agrégés. Vous trouverez ci-dessous la configuration des trunks d'interconnexion AVEC ou SANS agrégation (si besoin).

Pour l'interconnexion des Aruba 2930F avec d'autres switches, on utilisera :
- **l'interface 8 pour une interconnexion sans agrégat**
- **les interfaces 7 et 8 pour une interconnexion avec agrégat**

4.4.10 Interconnexion de switches SANS AGREGATION

Interconnexion avec autorisation des vlan 4, 30 et 901 (par exemple) sur l'interface 8 :

```
Vlan 4
 tagged 8
#
Vlan 30
 tagged 8
#
Vlan 901
 tagged 8
#
interface 8
 (eth-8) device-type network-device
#
```

4.4.11 Interconnexion de switches AVEC AGREGATION

Si cela est vraiment nécessaire, vous pouvez configurer un agrégat entre le 2930F et le fédérateur. Dans ce cas, utilisez les interfaces 7 et 8.

Configuration d'un agrégat avec les interfaces 7 et 8) :

Agrégat :

```
Trunk 7-8 trk1 lacp                    | N° de l'agrégat = 1 ici
```

VLAN autorisés – exemple 4, 30 et 901 :

```
Vlan 4
 tagged trk1
#
Vlan 30
 tagged trk1
#
Vlan 901
 tagged trk1
```

Au final, pour un site avec 6 « TEL + PMF » et un agrégat :

Siège	Agence

vlan 1
  name "DEFAULT_VLAN"
  no untagged 1-6
  untagged 9-10,Trk1
  no ip address
  forbid 1-6
  exit
vlan 4
  name "VLAN-DATA"
  untagged 1-6
  tagged Trk1
  no ip address
  exit
vlan 30
  name "VLAN-VOIX"
  tagged 1-6,Trk1
  no ip address
  voice
  exit
vlan 901
  name "VLAN-ADMIN-RESEAU"
  tagged Trk1
  ip address *@IP* 255.255.255.0
  exit
#
	vlan 1
	** name "DEFAULT_VLAN"**
	** no untagged 1-6**
	** untagged 9-10,Trk1**
	** no ip address**
	** forbid 1-6**
	** exit**
	vlan 4
	** name "VLAN-DATA"**
	** untagged 1-6**
	** tagged Trk1**
	** no ip address**
	** exit**
	vlan 30
	** name "VLAN-VOIX"**
	** tagged 1-6,Trk1**
	** no ip address**
	** voice**
	** exit**
	vlan 901
	** name "VLAN-ADMIN-RESEAU"**
	** tagged Trk1**
	** ip address *@IP* 255.255.255.240**
	** exit**
	#

Vérification :

2930-89-CNGR# **sh trunks**

Load Balancing Method: L3-based (default)

Port	Name	Type	Group	Type
7	Vers-5130	100/1000T	Trk1	LACP
8	Vers-5130	100/1000T	Trk1	LACP

2930-89-CNGR# **sh lacp**

LACP

Port	LACP Enabled	Trunk Group	Port Status	LACP Partner	Admin Status	Oper Key	Key
7	Active	Trk1	Up	Yes	Success	0	532
8	Active	Trk1	Up	Yes	Success	0	532

4.5 CONFIGURATION DU DHCP

4.5.1 DHCP relais

Un switch Aruba 2930F placé à l'extrémité du réseau n'a acune fonction de relais DHCP. Ce rôle n'est assuré que par le fédérateur niveau 3.

4.5.2 DHCP Snooping



A quoi ça sert ?

DHCP-Snooping est utilisé pour éviter la mise en œuvre d'un serveur DHCP pirate en sécurisant la fonction DHCP sur un réseau. Veuillez consulter la procédure 072NA001_Préconisations_DHCP sur l'intranet du DR pour plus d'explications.

Les commandes ci-dessous sont donc à configurer sur les switches Aruba niveau 2 à l'extrémité du LAN en siège : sur tous les switches du réseau utilisant un serveur DHCP.

```
#
dhcp-snooping
dhcp-snooping option 82
```

Trust sur le(s) port(s) d'interconnexion vers le fédérateur :

```
#
dhcp-snooping trust 8
```

ou

```
dhcp-snooping trust trkx                | dans le cas d'un agrégat
```

ou

```
interface Trkx                          | dans le cas d'un agrégat
  dhcp-snooping trust
```

Vérification : show dhcp-snooping

```
2930-89-CNGR# sh dhcp-snooping

 DHCP Snooping Information

  DHCP Snooping           : Yes
  Enabled VLANs           :
  Verify MAC address      : Yes
  Option 82 untrusted policy : drop
  Option 82 insertion     : Yes
  Option 82 remote-id     : mac
  Store lease database    : Not configured

                Max     Current Bindings
  Port  Trust  Bindings  Static   Dynamic
 -----  -----  --------  ----------------
   Trk1  Yes     -       -        -

 Ports 1-6,9-10 are untrusted
```

4.6 ROUTAGE

Ces switches ne peuvent pas être fédérateurs sur Ramage V6. Le routage est toujours le même :

no ip routing
ip default-gateway @IP-Interface-vlan-901-du-stack-fédérateur

4.7 AUTRES CONFIGURATIONS

4.7.1 LLDP : découverte

L'activation de LLDP permettra de visualiser de nombreuses informations sur les PMF, les téléphones, les serveurs… connectés sur les interfaces du 3600 et, via CDP de prendre en compte les Cisco :

<>system-view
#
lldp run

Exemple de commandes de visualisation : show lldp information …

4.7.2 NTP : tous à la même heure

Une seule adresse IP de référence : 55.223.10.8. Voir la nouvelle version des procédures 027NA001 et 027NT002 sur l'intranet du DR.

ATTENTION : il se peut que l'implémentation de la version 3 minimum de NTP soit nécessaire sur certains serveurs Linux :

➔ **mettre :** *server @ip-serveur-NTP version 3* **dans** */etc/ntp.conf*
➔ **relancer le process NTP :** */usr/sbin/ntpd –c /usr/ntp.conf*

Configuration sur tous les switches avec changement automatique heure d'été / heure d'hiver :

#
time daylight-time-rule user-defined begin-date 03/27 end-date 10/30
time timezone 60
ntp enable
ntp unicast
ntp server 55.223.10.8 | adresse unique pour tous
timesync ntp

Vérification du bon fonctionnement :

Show ntp status :

2930-89-CNGR# sh ntp status
NTP Status Information

NTP Status : Enabled NTP Mode : Unicast
Synchronization Status : Synchronized Peer Dispersion : 0.00000 sec
Stratum Number : 3 Leap Direction : 0
Reference Assoc ID : 0 Clock Offset : 927447361.777...
Reference ID : 55.223.10.8 Root Delay : 0.03899 sec
Precision : 2**-18 Root Dispersion : 927447362.146...
NTP Up Time : 0d 1h 15m Time Resolution : 820 nsec

Drift : 0.00000 sec/sec

System Time : Thu May 23 15:07:23 2019
Reference Time : Thu May 23 14:28:54 2019

Show time :

2930-89-CNGR# sh time
Thu May 23 15:08:17 2019

4.8 EXEMPLES COMPLETS DE CONFIGURATION

4.8.1 Avec Agrégat en INT 7 et 8 en SIEGE d'organisme

```
; JL258A Configuration Editor; Created on release #WC.16.08.0003
; Ver #14:27.6f.f8.1d.9b.3f.bf.bb.ef.7c.59.fc.6b.fb.9f.fc.ff.ff.37.ef:04
#
hostname "SIEGE-2930-89-RG"
module 1 type jl258a
dhcp-snooping
trunk 7-8 trk1 lacp
banner exec %
****************************************
*             ! Attention !            *
*                                      *
*    Acces reserve aux personnels du   *
*         service informatique         *
*                                      *
*  Toutes les activites sur ce systeme *
*          sont enregistrees           *
*                                      *
*    Toutes preuves d activites non    *
*   autorisees seront traitees par les *
*    autorites competentes             *
*                                      *
*     Toute intrusion sur un systeme   *
*   informatique est interdite par les *
*     articles 323-2 du code penal     *
*                                      *
****************************************
%
logging 55.243.104.12
logging origin-id hostname
timesync ntp
ntp unicast
ntp server 55.223.10.8
ntp enable
no telnet-server
time daylight-time-rule user-defined begin-date 03/27 end-date 10/30
time timezone 60
no web-management
no web-management ssl
ip authorized-managers 55.244.0.0 255.255.0.0 access manager
ip authorized-managers 55.18.0.0 255.255.0.0 access manager
ip authorized-managers 55.18.0.0 255.255.0.0 access manager
ip default-gateway 55.X.221.1
ip dns domain-name "ramage"
ip dns server-address priority 1 55.223.10.1
interface 1
  name "TEL+PMF"
  power-over-ethernet high
  poe-lldp-detect enabled
  rate-limit bcast in percent 20
  rate-limit mcast in percent 20
  rate-limit unknown-unicast in percent 20
  exit
interface 2
  name "TEL+PMF"
  power-over-ethernet high
  poe-lldp-detect enabled
  rate-limit bcast in percent 20
  rate-limit mcast in percent 20
  rate-limit unknown-unicast in percent 20
  exit
interface 3
  name "TEL+PMF"
  name "TEL+PMF"
  power-over-ethernet high
  poe-lldp-detect enabled
  rate-limit bcast in percent 20
```

```
   rate-limit mcast in percent 20
   rate-limit unknown-unicast in percent 20
   exit
interface 4
   name "TEL+PMF"
   power-over-ethernet high
   poe-lldp-detect enabled
   rate-limit bcast in percent 20
   rate-limit mcast in percent 20
   rate-limit unknown-unicast in percent 20
   exit
interface 5
   name "TEL+PMF"
   power-over-ethernet high
   poe-lldp-detect enabled
   rate-limit bcast in percent 20
   rate-limit mcast in percent 20
   rate-limit unknown-unicast in percent 20
   exit
interface 6
   name "TEL+PMF"
   power-over-ethernet high
   poe-lldp-detect enabled
   rate-limit bcast in percent 20
   rate-limit mcast in percent 20
   rate-limit unknown-unicast in percent 20
   exit
interface 7
   name "Vers-FEDERATEUR"
   exit
interface 8
   name "Vers- FEDERATEUR"
   exit
interface Trk1
   dhcp-snooping trust
   exit
snmp-server community "cngr" manager unrestricted
snmp-server community "TOKTBAT22!" operator
snmp-server contact "F-PIGNON"
vlan 1
   name "DEFAULT_VLAN"
   no untagged 1-6
   untagged 9-10,Trk1
   no ip address
   forbid 1-6
   exit
vlan 4
   name "VLAN-DATA"
   untagged 1-6
   tagged Trk1
   no ip address
   exit
vlan 30
   name "VLAN-VOIX"
   tagged 1-6,Trk1
   no ip address
   voice
   exit
vlan 901
   name "ADMIN-RESEAU"
   tagged Trk1
   ip address 55.X.221.11 255.255.255.0
   exit
spanning-tree
spanning-tree 1 admin-edge-port
spanning-tree 1 loop-guard bpdu-protection
spanning-tree 2 admin-edge-port
spanning-tree 2 loop-guard bpdu-protection
spanning-tree 3 admin-edge-port
spanning-tree 3 loop-guard bpdu-protection
spanning-tree 4 admin-edge-port
```

```
spanning-tree 4 loop-guard bpdu-protection
spanning-tree 5 admin-edge-port
spanning-tree 5 loop-guard bpdu-protection
spanning-tree 6 admin-edge-port
spanning-tree 6 loop-guard bpdu-protection
spanning-tree Trk1 priority 4
spanning-tree mode rapid-pvst
front-panel-security display-in-config
no front-panel-security password-clear
no tftp server
loop-protect 1-6
loop-protect trap loop-detected
loop-protect disable-timer 60
no autorun
no dhcp config-file-update
no dhcp image-file-update
no dhcp tr69-acs-url
password manager
```

4.8.2 Sans agrégat mais interconnexion INT 8 en Agence

Dans l'exemple, le VLAN 4 est 55.X.8.0 /22 et le fédérateur est en 55.X.8.1.

```
#
hostname "SIEGE-2930-89-RG"
module 1 type jl258a
dhcp-snooping
banner exec %
****************************************
*             ! Attention !            *
*                                      *
*    Acces reserve aux personnels du   *
*         service informatique         *
*                                      *
*  Toutes les activites sur ce systeme *
*          sont enregistrees           *
*                                      *
*    Toutes preuves d activites non    *
*   autorisees seront traitees par les *
*    autorites competentes             *
*                                      *
*     Toute intrusion sur un systeme   *
*   informatique est interdite par les *
*     articles 323-2 du code penal     *
*                                      *
****************************************
%
logging 55.244.111.45
timesync ntp
ntp unicast
ntp server 55.223.10.8
ntp enable
no telnet-server
time daylight-time-rule user-defined begin-date 03/27 end-date 10/30
time timezone 60
no web-management
web-management ssl
ip authorized-managers 55.244.0.0 255.255.0.0 access manager
ip authorized-managers 55.18.0.0 255.255.0.0 access manager
ip authorized-managers 55.18.0.0 255.255.0.0 access manager
ip default-gateway 55.X.8.1
ip dns domain-name "ramage"
ip dns server-address priority 1 55.223.10.1
interface 1
  name "TEL+PMF"
  power-over-ethernet high
  poe-lldp-detect enabled
  rate-limit bcast in percent 20
  rate-limit mcast in percent 20
  rate-limit unknown-unicast in percent 20
  exit
```

```
interface 2
   name "TEL+PMF"
   power-over-ethernet high
   poe-lldp-detect enabled
   rate-limit bcast in percent 20
   rate-limit mcast in percent 20
   rate-limit unknown-unicast in percent 20
   exit
interface 3
   name "TEL+PMF"
   name "TEL+PMF"
   power-over-ethernet high
   poe-lldp-detect enabled
   rate-limit bcast in percent 20
   rate-limit mcast in percent 20
   rate-limit unknown-unicast in percent 20
   exit
interface 4
   name "TEL+PMF"
   power-over-ethernet high
   poe-lldp-detect enabled
   rate-limit bcast in percent 20
   rate-limit mcast in percent 20
   rate-limit unknown-unicast in percent 20
   exit
interface 5
   name "TEL+PMF"
   power-over-ethernet high
   poe-lldp-detect enabled
   rate-limit bcast in percent 20
   rate-limit mcast in percent 20
   rate-limit unknown-unicast in percent 20
   exit
interface 6
   name "TEL+PMF"
   power-over-ethernet high
   poe-lldp-detect enabled
   rate-limit bcast in percent 20
   rate-limit mcast in percent 20
   rate-limit unknown-unicast in percent 20
   exit
interface 7
   name "TEL+PMF"
   power-over-ethernet high
   poe-lldp-detect enabled
   rate-limit bcast in percent 20
   rate-limit mcast in percent 20
   rate-limit unknown-unicast in percent 20
   exit
interface 8
   name "Vers- FEDERATEUR"
   dhcp-snooping trust
   exit
snmp-server community "cngr" manager unrestricted
snmp-server community "TOKTBAT22!" operator
snmp-server contact "F-PIGNON"
vlan 1
   name "DEFAULT_VLAN"
   no untagged 1-6
   untagged 9-10,Trk1
   no ip address
   forbid 1-6
   exit
vlan 4
   name "VLAN-DATA"
   untagged 1-6
   tagged 1-7
   no ip address
   exit
vlan 30
   name "VLAN-VOIX"
```

```
  tagged 1-6
  no ip address
  voice
  exit
vlan 901
  name "ADMIN-RESEAU"
  tagged 8
  ip address 55.X.0.3 255.255.255.240
  exit
spanning-tree
spanning-tree 1 admin-edge-port
spanning-tree 1 loop-guard bpdu-protection
spanning-tree 2 admin-edge-port
spanning-tree 2 loop-guard bpdu-protection
spanning-tree 3 admin-edge-port
spanning-tree 3 loop-guard bpdu-protection
spanning-tree 4 admin-edge-port
spanning-tree 4 loop-guard bpdu-protection
spanning-tree 5 admin-edge-port
spanning-tree 5 loop-guard bpdu-protection
spanning-tree 6 admin-edge-port
spanning-tree 6 loop-guard bpdu-protection
spanning-tree 7 admin-edge-port
spanning-tree 7 loop-guard bpdu-protection
spanning-tree mode rapid-pvst
front-panel-security display-in-config
no front-panel-security password-clear
no tftp server
loop-protect 1-7
loop-protect trap loop-detected
loop-protect disable-timer 60
no autorun
no dhcp config-file-update
no dhcp image-file-update
no dhcp tr69-acs-url
password manager
```

4.9 L'EXPLOITATION

4.9.1 Mirroring d'interface

Port écouté : 1
Port miroir : 4

```
#
mirror 1 port 4
#
interface 1 monitor all both mirror 1
```

4.9.2 Sauvegardes

Tout switch ou stack installé sur RAMAGE doit être intégré au SI. Il est alors automatiquement sauvegardé dans NCM. La sauvegarde contient la configuration de l'ensemble du stack.

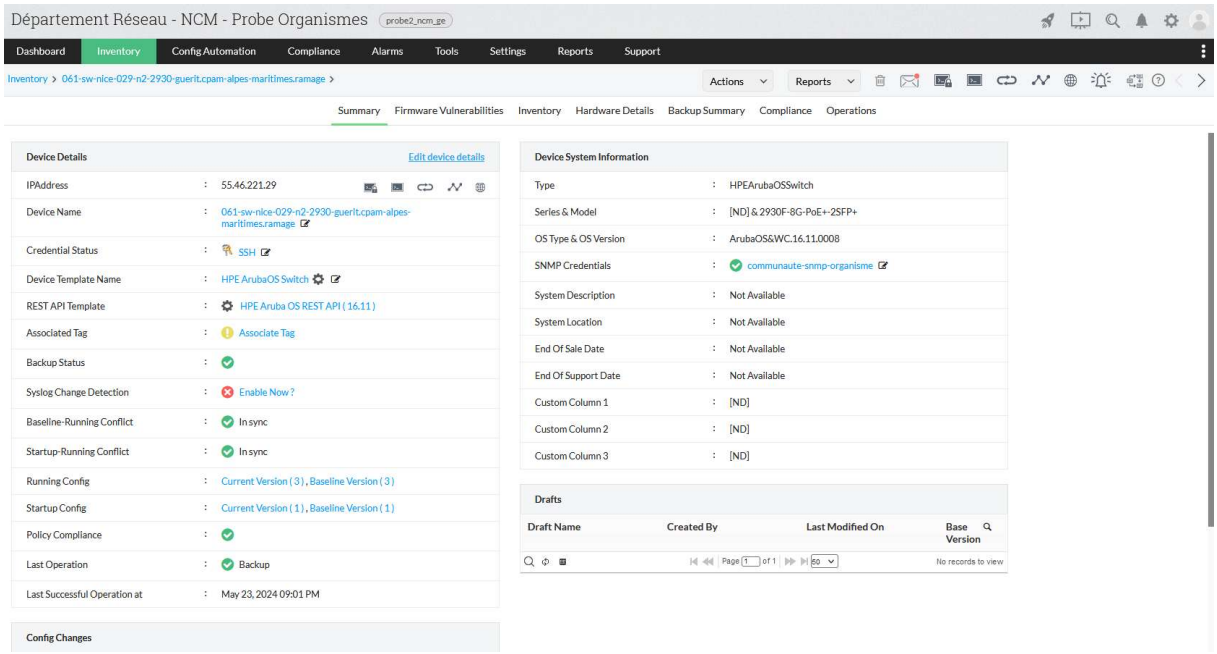
Sinon :

2930-89-CNGR(config)# tftp *@IP-SERVER* put startup-config *fichier*.txt

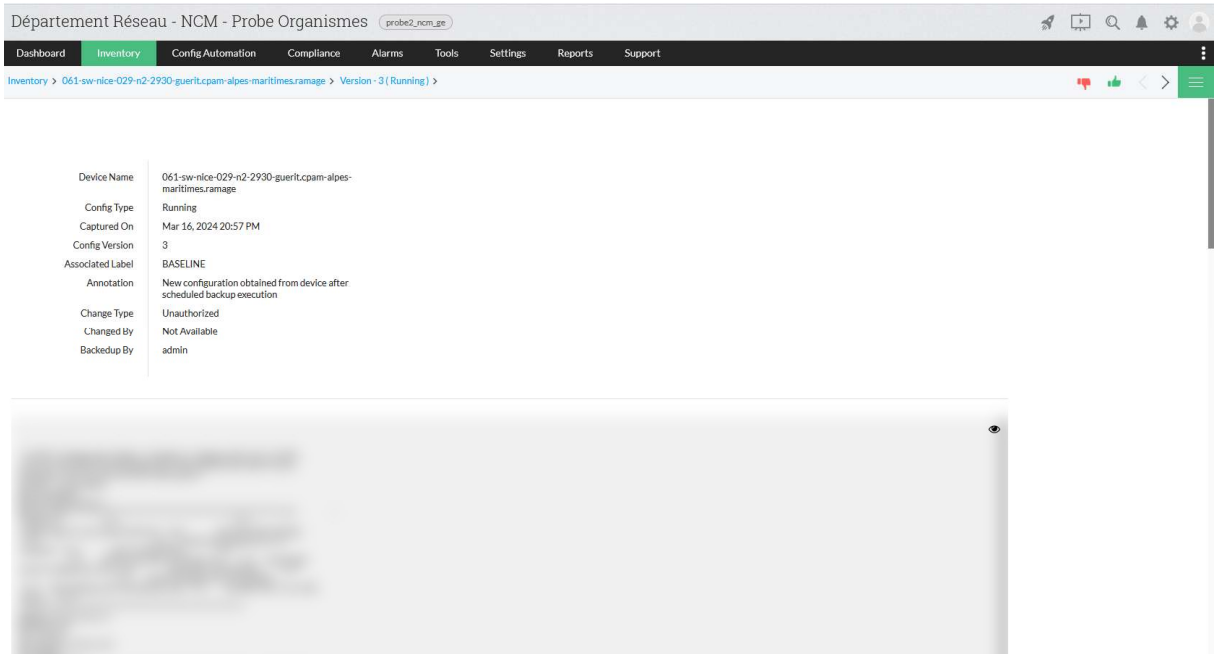
4.9.3 Restaurations

4.9.3.1 Depuis l'outil NCM (Méthode 1)

Se placer sur l'équipement souhaité dans l'inventaire du logiciel Network Configuration Manager :

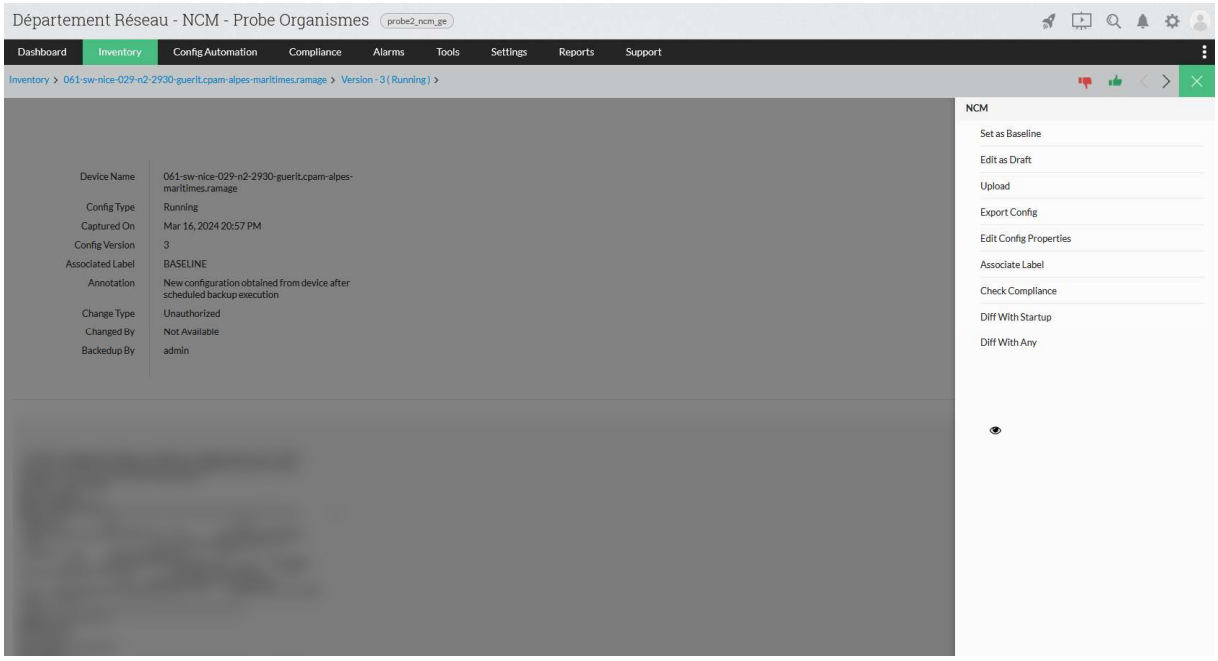


Cliquer sur la dernière version de la configuration « Current Version de la « Running Config » :

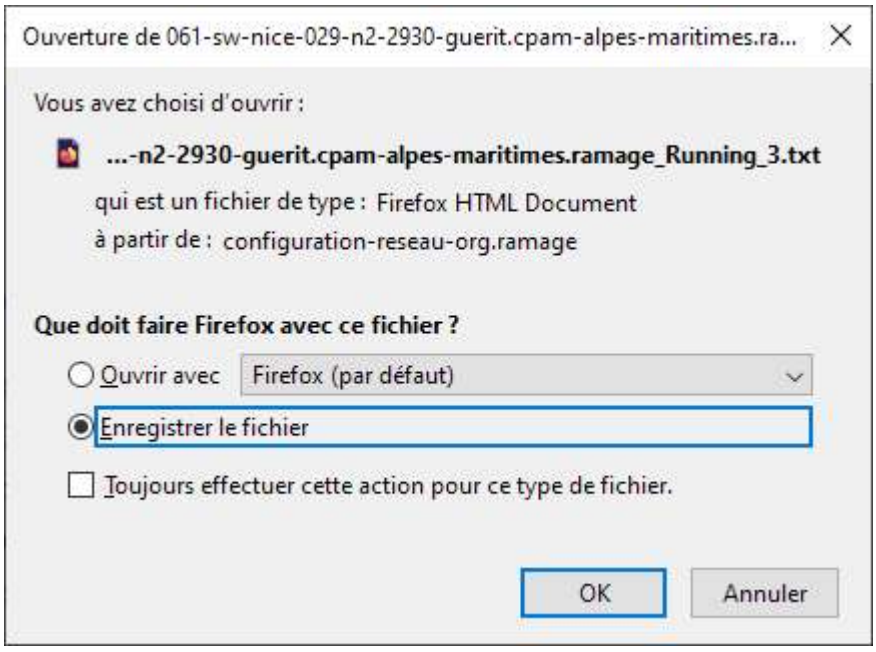


Cliquer sur le bouton en haut à droite 

Cliquer sur « Exporter la configuration » :



Enregistrer le fichier dans le dossier de votre choix :



Vous devez renommer le fichier de .txt à .cfg

Mettre votre fichier à la racine du dossier de votre serveur TFTP et vous pouvez faire la restauration de configuration et passer la commande suivante :

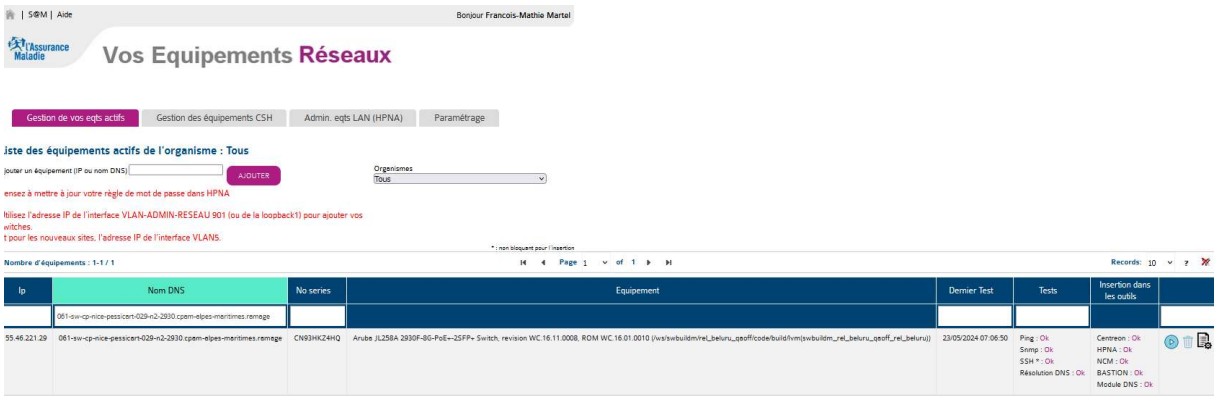
copy tftp startup-config *@IP-SERVER fichier*

4.9.3.2 Depuis le portail du SI (Méthode 2)

Se connecter à la page suivante sur le portail du DR :

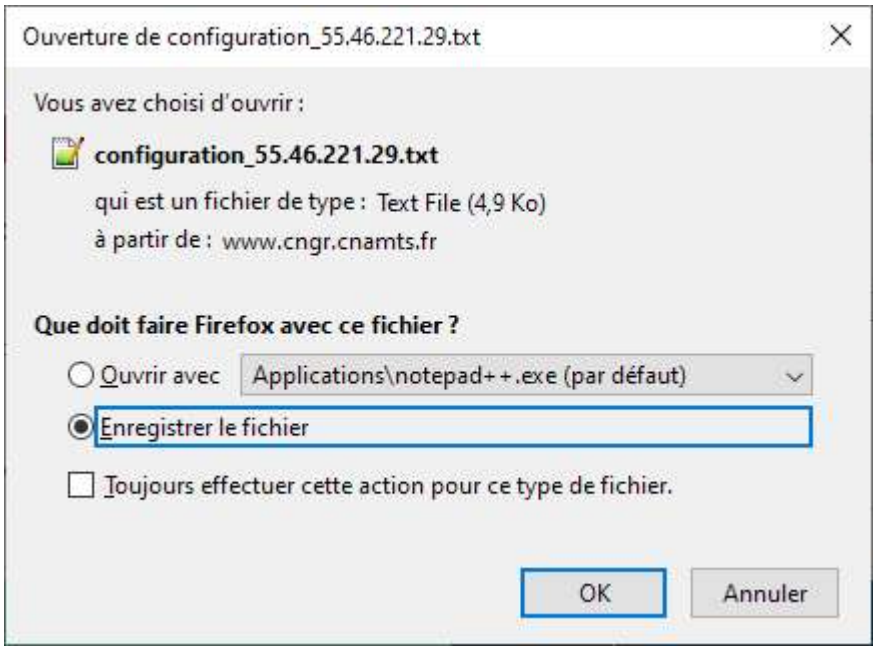
https://www.cngr.cnamts.fr/supervision/equipementActif/

Rechercher votre équipement via son adresse IP ou son nom dns :



Cliquer sur le bouton  pour télécharger la configuration de votre équipement.

Une fenêtre de téléchargement va apparaitre :



Vous devez renommer le fichier de .txt à .cfg

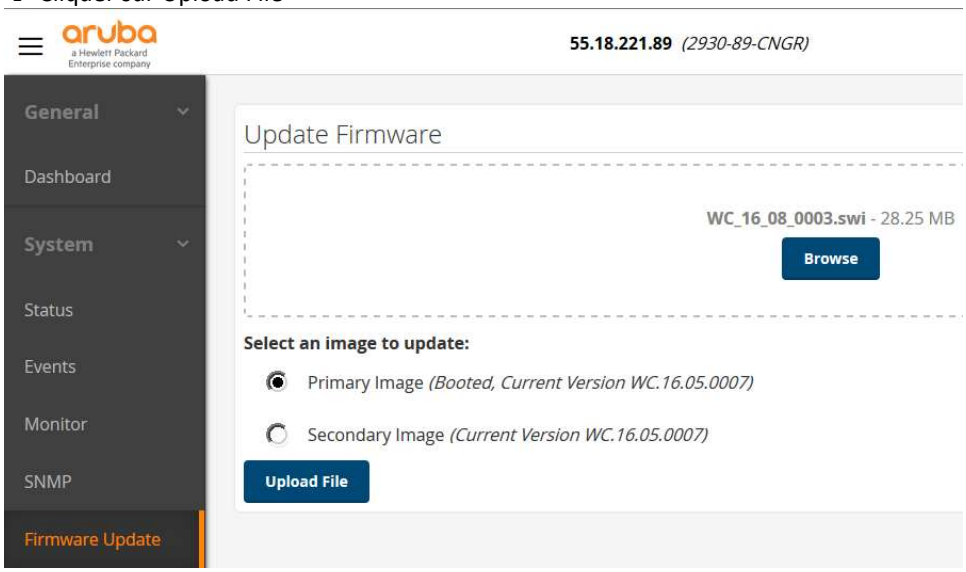
Mettre votre fichier à la racine du dossier de votre serveur TFTP et vous pouvez faire la restauration de configuration :

copy tftp startup-config *@IP-SERVER fichier*

4.9.4 Mise à jour de la version

Récupérer la dernière version mise à disposition sur le portail du DR.

Il est nécessaire de préconfigurer le switch en console pour définir les accès (ssh et https) ainsi qu'une adresse IP sur un VLAN dans le même sous-réseau que le PMF stockant la version de mise à jour.
Stocker le fichier sur un PMF dans un dossier.
Se connecter au switch en https et se connecter en « admin ».
Dans la frame à gauche, cliquer sur System ➔ Firmware upgrade
➔ Laisser coché « PrimaryImage »
➔ Glisser-déposer le fichier .swi (ou indiquer où il se trouve)
➔ Cliquer sur Upload File



Démarrer la mise à jour en cliquant sur « yes » :

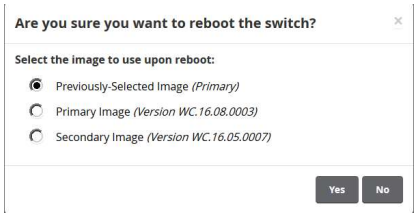
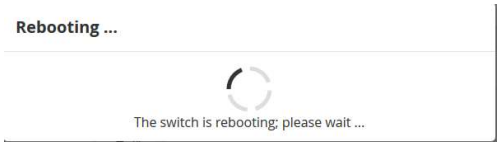
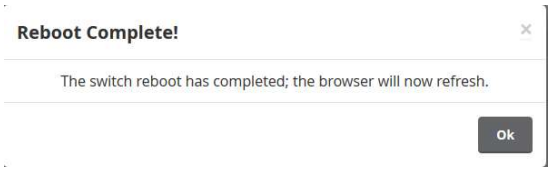
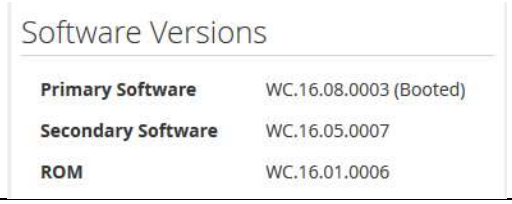


La mise à jour est rapide. Il est indiqué que pour la prise en compte, il est nécessaire de redémarrer le switch.
Cliquer sur OK.





Le switch embarque désormais 2 versions. Pour rebooter le switch :

- immédiatement : cliquer sur « reboot » en haut à droite	 Laisser cochéé la case proposée et valider avec « yes » :  Le switch redémarre :   Après le reboot, vérifier en https dans System ➔ Status que le switch a bien booté dans la bonne version : 
- en différé : se connecter en console et taper la commande :	Reload at HH :MM Après le reboot, vérifier la version.

4.9.5 Remettre un switch en configuration usine

4.9.5.1 Vous connaissez le login / password

```
#
Erase starup-config                | config supprimée – accès et mot de passe conservé
#
#
Erase all                          | Tout est supprimé
#
```

4.9.5.2 Vous NE connaissez PAS le login / password

Il vous faut être à proximité du switch. Utilisez deux pointes fines (comme deux trombones par exemple) et les boutons (creux) « reset » et « clear » sur la face avant du switch (en bas à droite) :

1/ Appuyez sur Clear et Reset en même temps
2/ Tout en continuant d'appuyer sur Clear, lâchez Reset
3/ Quand la LED de status global commence à clignoter en orange (après 5 secondes environ), lâchez Clear
4/ Le switch redémarre en configuration usine.